CYBERPLAT TECHNOLOGIES:

FOUNDATION OF THE NEW ECONOMY'S GLOBAL INFRASTRUCTURE

The largest electronic payment system: more than 1 480 000 outlets

CONTENT

INTRODUCTION

ADDRESS BY THE MANAGER

GRIBOV ANDREY YURIEVICH

Director General of CYBERPLAT LLC

More than a decade and a half ago, Russia entered the XXI century - the century of knowledge economy, and the CyberPlat® system has emerged and has been developing in response to the increased business needs of the third millennium. New emerging functionalities and services of ultimate availability for the ever wider segments of the population call for the creation of new payment instruments.

A while back, banks were created to store large amounts of money. Thus, banks have fortified walls, armored doors and are serviced by highly qualified and, consequently, highly paid personnel, and also use the best technical achievements to ensure the safety of money. As a result, the prime cost of a cash acceptance and payment transaction is usually at least $ 1.

The knowledge economy has created many businesses (such as those providing telecommunication services) serving tens of millions of subscribers. These businesses collect a very large number of small payments. The average amount of a transaction in the CyberPlat® system in Russia is only about $ 8.5. Making such small payments is not profitable for banks.

At the same time, the procedure for accepting such amounts does not require high levels of security. It is quite safe to collect payments in the amount of several US dollars through the checkout counters of conventional retail chains (communications stores, supermarkets, pharmacies, gas stations), which is much cheaper. These days, private clients make regular small payments - for communications, Internet, cable TV services - mainly through retail networks. In addition, as the changes to the legislation are made, other operations are becoming retail, such as bank loans repayment and bank accounts replenishment, paying traffic fines and taxes, sending money transfers, paying for housing costs and utilities. At the end of 2018, over 8 thousand payment recipients - suppliers of goods and services - registered in the CyberPlat® electronic payment system.

CyberPlat® facilitates finding get new sources of income and increasing turnover for its partners, members of the electronic payment system in their core businesses.

For this we have created and are developing a powerful payment infrastructure. Even today, it surpasses the entire banking system of the country by the number of payment acceptance outlets.

GLOSSARY

OPERATOR — any organization providing services to the public and accepting payments through CyberPlat®. These are mobile and fixed-line services companies (MTS, Beeline, MegaFon, Tele2, Rostelecom, etc.), commercial TV providers (NTV +, Akado, etc.), Internet access and IP telephony providers (Qwerty, Dom.ru, etc.), housing and utilities infrastructure and energy enterprises, air ticket sales services, etc.

SUBSCRIBER — any individual or legal entity paying for operator services through CyberPlat® either in prepaid mode (personal account replenishment operation), or in the form of a subscription fee, or in the form of payment for the services that are already provided, for example, utilities.

PAYMENT ACCEPTANCE OUTLET — any workplace where the acceptance of subscribers' payments to operators through CyberPlat® is established - a cashier's office, a payment terminal, a workplace of a bank cashier or a communications store manager, a vending kiosk seller, etc.

CASHIER — a payment acceptance outlet specialist serving the subscriber directly.

DISTRIBUTION NETWORKS — the body of payment acceptance outlets united by a brand (for example, “Euroset” communications store chain, MTS retail network, “Eldorado” retail chain); a large supermarket with a dozen checkout counters, each of which is a payment acceptance outlet, is also considered a retail chain.

PAYMENT TERMINAL (SELF-SERVICE CASH-IN KIOSK) — a fully automated payment acceptance outlet operating without a cashier – an alternative to ATM. There are payment terminals of such networks as “Eleksnet”, “PlatezhKa”, “Plat-Forma”, etc.

PAYMENT AGENT (AGENT) — a legal entity (retail chain or a single payment acceptance outlet, for example, a shop, a kiosk or a pharmacy) or an individual entrepreneur accepting payments from subscribers through CyberPlat® to service providers.

BANK PAYMENT AGENT — a legal entity, with the exception of banks, or an individual entrepreneur engaged by a bank to provide payment services through the CyberPlat® system.

REGIONAL REPRESANTATIVE — a representative of the CyberPlat® company engaged in attracting new agents for the electronic payment system. The income of such representatives is formed based on a commission, the amount of which directly depends on the turnover of yjr4 agents attracted.

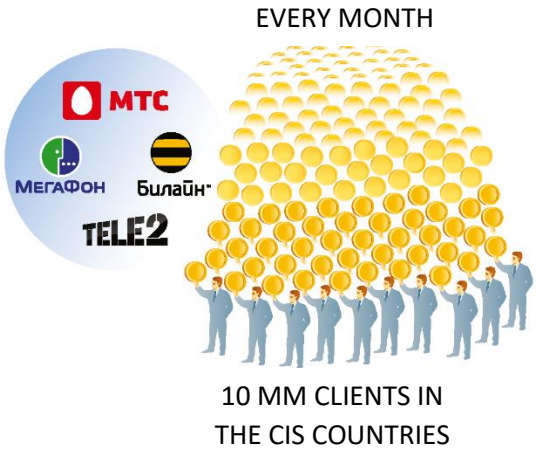
KEY ROLE OF THE ONLINE PAYMENT MARKET IN THE MODERN ECONOMY

WHAT IS THE BANKING SYSTEM NEEDED FOR?

The trade functions efficiently only in the conditions of a well-developed banking network. However, the infrastructure of the current banking system in operation is not smoothly running in the context of small transactions. Banks are traditionally used as a place for a safe storage and transfer of large amounts of money. Fortified walls, bulletproof windows, armed guards and highly professional personnel are integral attributes of a banking institution.

For these reasons, the prime cost of a retail bank transaction is very high. The payment procedure is also time consuming for both the client and the highly compensated bank personnel. In this connection, a retail payment in a bank cannot be a cheap transaction, and its cost is at least $ 1 for the credit institution.

REQUIREMENTS OF THE NEW ECONOMY

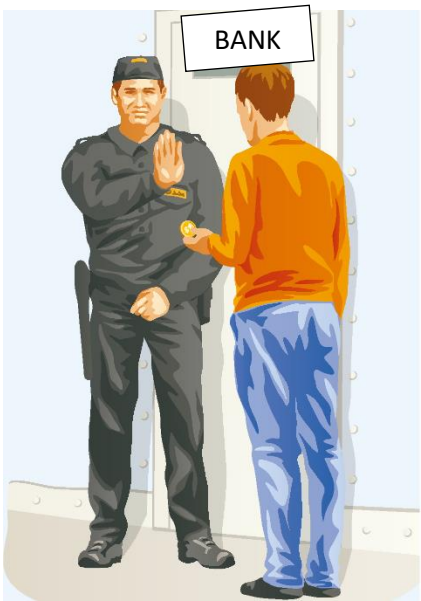


The new, modern sectors of the economy are characterized by the network nature of services provision. Mobile communications, Internet, cable TV serve a sagan of subscribers with relatively low amounts of regular payments. The point at issue is tens and hundreds of millions of customers, each of which often pays just $ 5-10 per month.

Thus, for example, the average income per user (ARPU) in mobile communications in Russia is more than $ 7. The average amount of a payment through the CyberPlat® system is $ 8.5. The average payment amount in Moscow is above $ 12, and $ 3 in the regions of Russia, $ 5.9 in Kazakhstan, and $ 2.1 in India.

MODERN BANKING SYSTEM AND THE REQUIREMENTS OF THE NEW ECONOMY

When a customer of a mobile operator replenishes their subscriber account for $ 5 at a branch of an ordinary bank (Russia has about 30.7 thousand banking divisions per more than 146 million inhabitants), the cost of such a transaction for the bank, as shown above, is approximately $ 1. Taking into account the bank margin (as the bank cannot work for free) about $ 1.5 will be withheld from the client,



approximately amounting to 30% of the payment sum. Obviously, for the client, such a commission is unacceptable.

In such a way, the need for the formation of a new, more efficient financial infrastructure for carrying out a large number of relatively small payments is determined. The natural base for this new infrastructure is retail business. Small payments can easily be accepted by a cashier in a store, whose salary is significantly lower than the average salary of a bank employee.

In addition, stores do not need armored walls, vault safes and ultra-reliable security systems (they are simply not needed for the payments amounting to $ 3-5). Consequently, the prime cost of accepting payments in retail is significantly lower than in banks.

Naturally, small payments cannot be made in vast numbers without creating a new financial infrastructure. This means that the development of the new economy is seriously hampered if there is none - businesses will not have channels to collect money for their services, and people will be limited in their use of the modern digital services. The lack of a new financial infrastructure is among the reasons for the class division of society on the basis of access to the modern functionalities and services, which is commonly called the “digital inequality” (or “digital divide”).

INABILITY TO MEET CERTAIN REQUIREMENTS WITH NO COST-EFFECTIVE FINANCIAL INFRASTRUCTURE

Services such as, for example, iTunes, offering users content and products at relatively low prices, often less than $ 1, are well represented on the market and are developing dynamically. Today, on the Internet, one has the opportunity to download and use the hits of famous artists legally at a price of $ 0.5, $ 0.25 or even less. It is clear that such a business cannot develop without an appropriate money acceptance system.

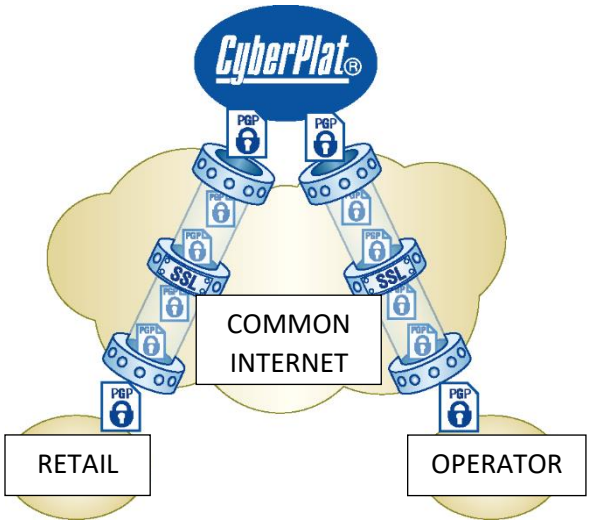
This also applies to other types of distribution services selling intellectual content, and not only in the field of entertainment, including Google Earth, paid directory services, etc. For example, LexisNexis provides its clients with access to millions of documents and records from over 45,000 legal, news and business sources. The service is available for a monthly fee (approximately $ 50 per month). Using the technologies offered by us, you can pay $ 1, find what you need, and disconnect from the Internet service.

Such micropayment technologies are certainly capable of creating a serious momentum to the development of a new economy.

A RELIABLE TECHNOLOGY

It is essential that the inexpensive payment methods offered by CyberPlat® were of the highest reliability.

Each provider and all agents of the electronic payment system are connected to the CyberPlat® processing via the Internet – either using a dedicated line, dial-up communication or a regular GPRS batch data communications system.



With each such transaction, an SSL connection (secure connection protocol) is established, which is used to transfer, encode and certify files of 1 kilobyte with an electronic digital signature.

Since the size of such file is very small, it allows using any type of Internet connection - even if it is very weak.

The reliability of such transactions is high (for encryption, a 2048-bit key is used) and is more than enough for payments of $ 5. For more than 20 years since the CyberPlat® system was put into operation, not a single case of system hacking has occurred. Experience has shown that such a system cannot be hacked neither theoretically nor practically.

THE REASON IT IS POPULAR

MOBILE SERVICE COVERAGE

Why has CyberPlat® business developed at such a rapid pace, for example, in Russia? The reason for this is that it provided more than 100% actual coverage of the population with mobile services. Today, even a child from a poor Russian family uses a mobile phone. Data from authoritative international studies indicate that the number of the SIM-cards in use has increased to 250 million per more than 146 million inhabitants in Russia. To make this calculation, experts take into account people who use several mobile phones, as well as a certain number of “silent” SIM-cards. As a matter of fact, the rate of mobile services use in Russia is about 90%, proving the fact that even every child in Russia uses mobile services.

This is only possible because children are able to transfer their pocket money, even though they may be very modest, to their own mobile phone account.

Since the system's launch, several million low-income young subscribers started using CyberPlat® services, as they can quite well afford to spend 150-200 RUB per month for mobile communications. In their tariff plans, certain regional mobile operators offer the opportunity to send up to 100 SMS messages free of charge - this is actively used by children who use voice communication less often, but actively communicate in SMS format.

INCREASED TRAFFIC FROM PARENTS

Children generate incoming traffic from their parents. It is for this very reason that they are an important customer category for mobile operators. Indeed, regular calls from parents to children ("Where are you?", "When did you come home from school?", "Have you eaten?", "Have you done your homework?", etc.) cause a serious increase in voice traffic from the parents, thus increasing the income received by mobile operators.

Average Monthly Revenue per Subscription (ARPU)

ABOUT US

GENERAL INFORMATION

An integrated universal multibank payment system named CyberPlat® was created in 1997 on the basis of the Platina Bank's e-commerce department. It was developed with the aim of providing information and technological support for e-commerce non-cash payments for the entire range of financial services - from micropayments to interbank payments. CyberPlat® spun off as a separate entity in 2000.

CyberPlat® is the pioneer Russian electronic payment system - the first transaction was made to the Garant-Park company on March 18, 1998, and the first online payment via the Internet was made to the “Beeline” mobile operator on August 12, 1998.

During more than 20 years of operation in the market, the company has accumulated vast experience in organizing payment acceptance in retain and service chains. By the end of 2018, payments to more than 8,000 service providers, including mobile and fixed-line telephony companies, cable TV, wire and mobile Internet providers, security alarm systems, housing and utilities services enterprises and energy sales companies throughout almost all regions of the Russian Federation were accepted through the system. Using the CyberPlat® system, you can pay for aviation and train tickets, repay bank loans and make money transfers, as well as make state payments: pay taxes and charges, traffic police fines, work permit fees, etc.

Ongoing modernization of the technological platform allows the CyberPlat® electronic payment system to conduct more than 1400 financial transactions per second - this record for Russia provides a 15-fold margin with respect to the maximum peak system loads.

This performance is complemented with absolute security of financial transactions. Up to 16 operations (postings) are performed in the system, certified by an electronic signature and carried out using secure methods of data transmission via the Internet within the framework of a single transaction. This technology ensures absolute security of financial transactions and minimizes the number of payments made in error. There has not been a single case of information system hacking or illegal transaction occurred in the CyberPlat® system.

By the criteria of reliability and uninterrupted operation, the CyberPlat® electronic payment system is also unparalleled in the Russian market - the system fault tolerance indicator exceeds that of its closest competitors by several times.

All major players in the telecommunications market, the largest Russian banks, including Sberbank of Russia, VTB, Post Bank, Alfa-Bank, Rosselkhozbank, Rosbank, Unicredit, Russia, Russian Standard Bank, etc., federal retail chains “Eldorado”, “Euroset”, etc., JSC “Kazpost”, government agencies, energy sales and transport companies, housing and utilities enterprises and many others are partners in organizing payment acceptance that have appreciated the benefits of using the CyberPlat® system.

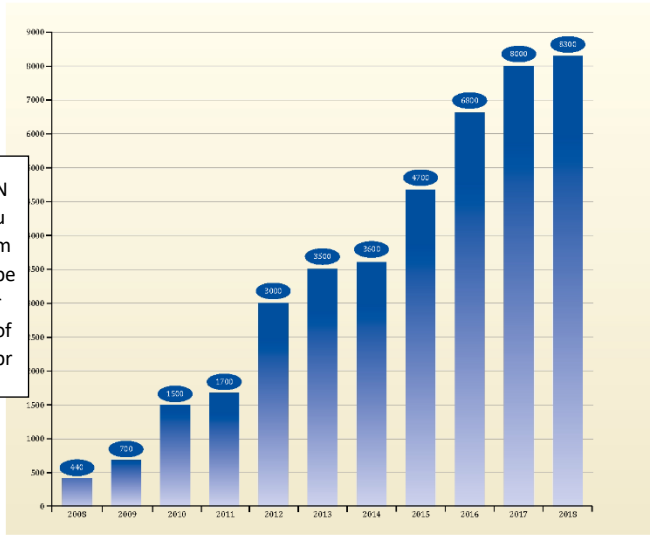
The CyberPlat® system performs the function most important for the state, which is ensuring a large volume of payments from the population to various suppliers of goods and services, contributing to the active development of new economy sectors based on the provision of modern services in the areas of telecommunications, banking and insurance, retail sales. The share of payments for housing and utilities and payments to government agencies (taxes, duties, fees, fines) has significantly increased in recent years. The CyberPlat® electronic payment system was chosen as a partner of the Federal Treasury and the Federal Tax Service and took part in pilot projects to develop new mechanisms for financial interaction between citizens and government agencies.

KEY FIGURES

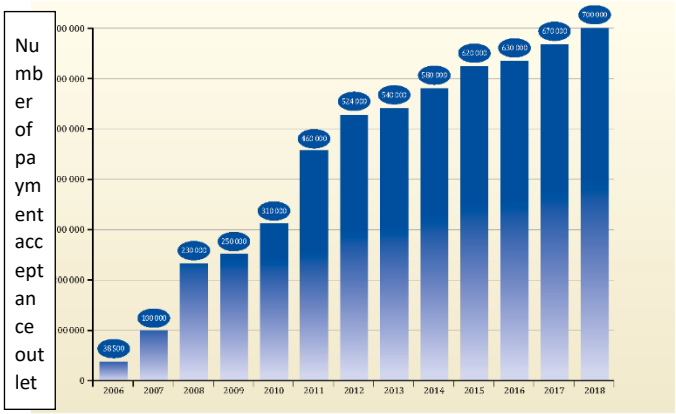
In 2018, as in previous years, CyberPlat® showed stable business dynamics. The total number of payment acceptance outlets exceeded 1,480,000, of which more than 700,000 are located in Russia and the CIS countries, and the others - in the largest cities of many countries around the world.

The total number of CyberPlat® payment acceptance outlets in Russia and the CIS countries is currently 20-fold larger than the size of the entire Russian banking system (as of January 1, 2019, the number of banking institutions with all branches, divisions and even mobile cash desks in the Russian Federation was about 31,000).

As of the end of 2018, more than 250 banks are members of the system.



Dynamics of the number of providers



Dynamics of the number of payment acceptance outlets in Russia, the CIS countries

PARTNERS' COMMENTS ON THE CYBERPLAT® SYSTEM

Samokhvalov Aleksander Vladimirovich,

Chairman of the Board of JSC "Russian Standard Bank":

Our bank is a member of the CyberPlat® electronic payment system, and I must say that for the entire period of our cooperation, we have never regretted it. CyberPlat® specialists have developed a whole range of excellent products for banks, many of which are actively used by us - we accept payments through the CyberPlat® system and have integrated this feature into our Internet banking system for our clients. The use of CyberPlat® technologies allows us to improve our business and make it more efficient.

Guskova Oksana Aleksandrovna,

CEO of United Company Svyaznoy | Euroset:

CyberPlat® was a pioneer in the payment acceptance market and for many years it worked so that the Russian consumer could pay for a variety of services in the way that is most convenient. CyberPlat® is our long-standing and reliable partner.

Galushko Evgeny Pavlovich,

Director General of the "MTS" retail chain:

The CyberPlat® system has made a significant contribution to the development of services for accepting payments in Russia, which played a role in mobile communication, among other things, becoming a massive and affordable service in the country. The company is constantly looking for new ways of development, improving the already launched services, and we value productive cooperation with CyberPlat® - this is one of the account replenishment channels of our users. CyberPlat® has repeatedly become the winner of MTS tenders in various regions, and we have also cooperated with CyberPlat® on a long-term basis in accepting payments through the cash desks of MTS retail outlets.

Pokolodny Daniil Sergeevich,

Director for Telecommunications and Financial Services, Svyaznoy Group of Companies:

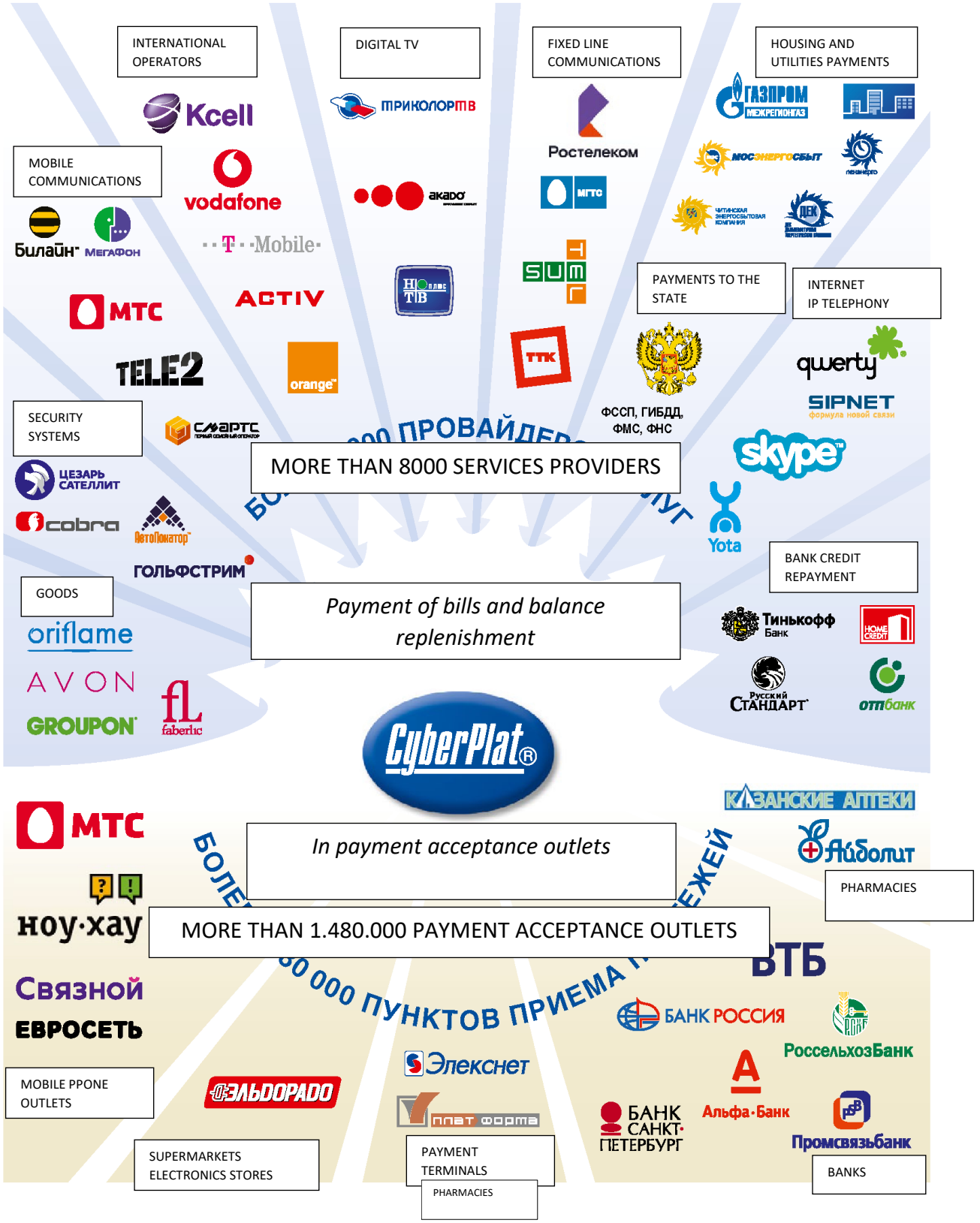
A wide range of client services provided in the Svyaznoy chain has become one of the key drivers of our company's business growth.

Taking the popularity of financial services among clients and our desire to provide services of the highest level into account, we cooperate with the most reliable and effective partners only, which undoubtedly includes the CyberPlat® electronic payment system. Together with CyberPlat®, we have already implemented such services as payment of utility bills, traffic police fines, payments to energy sales companies, the feature for card replenishment. I am

sure that the list of our joint projects will expand in the future and we will be able to offer our clients a wider range of additional opportunities.

HOW CYBERPLAT® WORKS

CYBERPLAT® BUSINESS ORGANIZATION CHART



COMPANY'S PARTNERS

For service providers, the issue of cost optimization in collecting revenue for the services rendered becomes pressing as their customer base grows. The CyberPlat® system allows to make the revenue collection process more efficient, therefore the number of organizations using CyberPlat® is growing dynamically during the entire period of the company's operation in the market.

Today, the CyberPlat® electronic payment system integrates payment gateways to the largest service providers, including leading mobile and fixed-line operators, satellite and cable television operators, housing and utilities service organizations, energy and gas retail companies and many others.

The largest operators in their respective sectors, to which direct payment gateways have been developed, are given below. In addition, the CyberPlat® system includes all significant service providers from all regions of the Russian Federation (including regional housing and utilities, gas and energy retail companies), payments to which are made through the Banking Provider gateway.

SOME OF THE LARGEST OPERATORS AND SERVICE PROVIDERS

Mobile communication

MTS

All-Russian operator

MegaFon

All-Russian operator

Beeline

All-Russian operator

Tele2

All-Russian operator

Motiv

Yekaterinburg and Sverdlovsk regions

Fixed line communication

Rostelecom

All-Russian operator

MGTS

Moscow

Transtelecom

All-Russian operator

Sum Telecom

in St. Petersburg, Nizhny Novgorod, Tula, Tver, Orel, Lipetsk, Voronezh, Rostov-on-Don, Krasnodar and Makhachkala, Derbent, Kaspiysk, Kiziljurt

Television and Internet

NTV-Plus

All-Russian operator

Tricolor-TV

All-Russian operator

AKADO

Moscow

Yota

Moscow

Dom.ru

Orion Express

Utilities payments

Gazprom Mezhregiongaz

Mosoblgaz

TNS Energo

Mosenergosbyt

Moscow

MOSOBLEIRTS JSC “EIRTS LO”

Dalenergosbyt

Sverdlovsk Energy and Gas Company

Yakutskenergo

Tyumen Power Sales Company

Yekaterinburg Electric Grid Company

Security systems

Cesar Satellite

Satellite security system

Autolocator

Satellite anti-theft system

Cobra Connex

Satellite security search system

Golfstream

Satellite security system

Air tickets

Ozon-Travel

Flight booking

Tour operator “Intourist”

UFS

Air and train tickets booking

Bilet-On-Line

Sale of air and train tickets

Tour operator "Delfin"

Goods (direct sales)

Avon

Oriflame

Faberlic

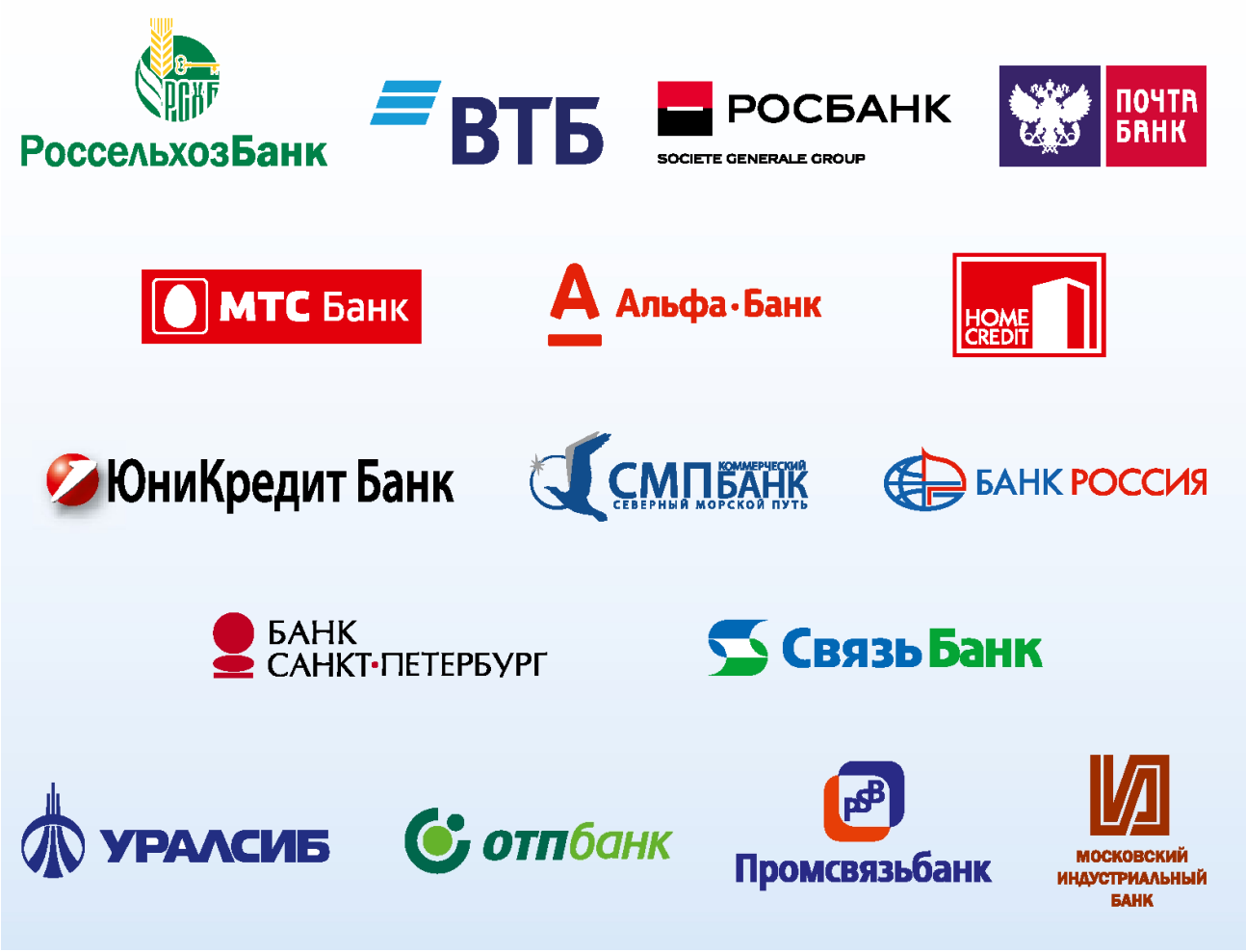
Zepter

For a complete list of service providers, please visit the Company's website: http://www.cyberplatru/about/providers

BANKS - PARTNERS OF THE CYBERPLAT® SYSTEM

By the end of 2018, the CyberPlat® electronic payment system had contractual relations with more than 250 banks. Many banks cooperate with the system as agents, organizing payment acceptance through the CyberPlat® system in their offices, ATMs or in the networks of self-service banking terminals. At the same time, many of them serve as operators, recipients of payments as well, using CyberPlat® as an effective channel for repaying loans issued to individuals and replenishing bank accounts, including cards.

In their activities, many banks use a unique product developed by CyberPlat® specialists - the Money Transfer System Integrator (MTSI), which greatly increases the efficiency in the field of money transfer business. Some of the largest partner banks are listed below.



PAYMENT ACCEPTANCE NETWORK (LARGEST RETAILERS)

The most well-known agents of CYBERPLAT LLC currently are:

- federal networks of communications stores “Svyaznoy”, “Euroset”, “Know-How”, mono-brand networks of communications stores of MTS, MegaFon, Tele2;
- JSC "Kazpost";
- Mosobleirts, Lenobleirts branches;
- Eldorado electronics stores;
- networks of payment terminals “Eleksnet”, “PlatezhKa”;
- Rosselkhozbank, Alfa-Bank, Russian Standard Bank, Russia Bank, SDM-Bank, Promsvyazbank, Bank Saint Petersburg, SMP Bank and many others.

CYBERPLAT® BUSINESS GEOGRAPHY

Regional representative offices of CyberPlat® operate successfully in various federal districts of the Russian Federation and are located in Samara, Kursk, Yekaterinburg, Stavropol.

CyberPlat® is successfully developing its business in the CIS countries - a subsidiary of the electronic payment system operates in Kazakhstan.

CyberPlat® is the pioneer electronic payment system in Kazakhstan. Its subsidiary company in Kazakhstan - CyberPlat-Kazakhstan LLP - was registered on September 15, 2005. The first payments through the system were made in April 2006. By the end of 2018, Kazakhstan had over 20 thousand payment acceptance outlets connected to the CyberPlat® system, and the company's regional representative offices operate in all major cities of Kazakhstan: Alma-Ata, Astana, Aktobe, Shymkent, Oskemen, Qaraghandy, Pavlodar, Kostanay and Oral.

Today, the partners of the CyberPlat® subsidiary in Kazakhstan are the largest banks, mobile operators, service providers, terminal networks and retail enterprises of the Republic of Kazakhstan.

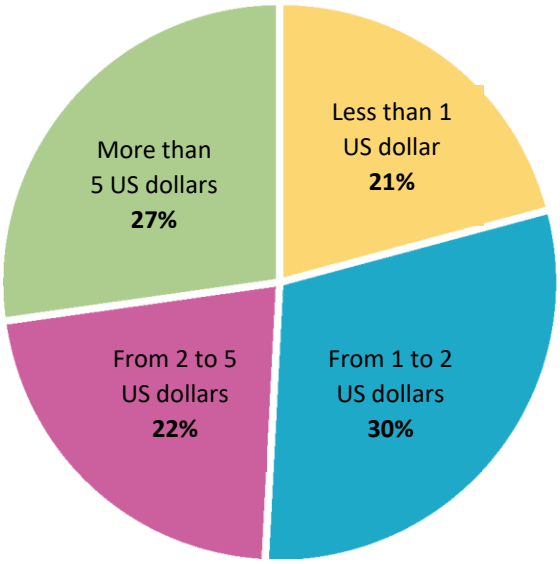
One of the largest international projects of CyberPlat® was launched in 2009 in India. CyberPlat India, based in the city of Mumbai, has developed at a rapid pace and has demonstrated an annual 100% growth for several years in a row, confidently outranking its competitors.

CyberPlat India is currently among the leaders in the national financial technology industry.

The company is included in the TOP-5 payment systems operating in one of the largest Asian markets, and ranks 1st in the number of payment outlets in the country: as of January 1, 2019, their number exceeded 760 thousand. More than 240 million transactions to more than 350 service providers in India and abroad, available in 600 partner networks, are performed each year in the system.

CyberPlat India is one of the few payment aggregators in India that cooperates directly with more than two dozen largest providers rendering services in the field of telecommunications, satellite TV and housing and utility services.

CyberPlat® network of representative offices in the CIS countries



SOCIAL MISSION OF THE CYBERPLAT® ELECTRONIC PAYMENT SYSTEM

As evidenced by the statistical data, at the end of 2018, only about 28% of payments made through the CyberPlat® payment system exceeded $ 5. At the same time, payments of up to $ 1 take a share of 21%, from $ 1 to $ 2 - 30%, from $ 2 to $ 5 - 22%. More than 50% of all CyberPlat® transactions are payments of up to $ 2, or of approximately 117 RUB.

The data given indicate that CyberPlat® provides the opportunity to use modern achievements of high technologies to the population with middle and low incomes. First of all, this is mobile communications and Internet access services. Since even the minimum balance allows the subscriber to stay in touch, send messages and make urgent calls.

The conditions created by the CyberPlat® system for the use of modern communication technologies by the widest swath of the population play a critical role in overcoming the issue of the so-called digital inequality in Russia. The statistical data on the prevalence of small payments and the total number of transactions passing through the system bring the fact that the operation of the CyberPlat® system contributes to an increase in the level of mobile communication coverage in Russia into sharp focus.

For example, if the account of a client has run out of funds and they have not enough money to buy a scratch card at a cost of 100 RUB (minimum denomination), they can top up their balance at any payment acceptance outlet.

Any subscriber can top up their account for an amount of just 10-20 RUB and use SMS services, as well as receive incoming calls.

It is also convenient that payment acceptance outlets are the most frequently visited places - shops, pharmacies, post offices, communications stores, payment terminals, gas stations. At the same time, transaction in real-time ensures that the payment amount is transferred to the subscriber's balance instantly.

Thus, the ability to top up the account with small amounts provides access to mobile communications for people with low-incomes, in particular children, students and old-age pensioners, fulfilling an important social mission of reducing digital inequality.

BENEFITS OF CYBERPLAT® TECHNOLOGIES

SAFETY AND SECURITY

CyberPlat® is an electronic payment system of a closed type. Its fundamental distinctive feature making it stand out from open-type systems is that all settlement participants - payers (agents accepting payments from subscribers) and recipients - are strictly defined. Funds from a retail outlet's account may only be transferred to the operator's account and credited to the subscriber's personal account. Withdrawal of funds from the system at the request of the employee of the payment acceptance outlet is not allowed.

CyberPlat® is a real-time system. Any transaction in the system takes no more than two seconds. This unprecedented level of performance is complemented with absolute security of financial transactions.

Up to 16 operations (postings) are performed in the system, certified by an electronic signature, within the framework of a single transaction. Secured methods of data transmission via the Internet, including checking the availability of phone numbers or personal accounts of customers in the billing systems of service providers, identification and authorization of payment acceptance outlets and other operations, are used. This technology ensures absolute security of financial transactions and minimizes the number of payments made in error.

There has not been a single case of information system hacking or illegal transaction occurred in the CyberPlat® system over the 20 years of its operation.

CROSS-PLATFORM HARDWARE

Ability to choose a payment method and use various devices for making a payment, depending on the capabilities of agents, are significant achievements of the CyberPlat® electronic payment system.

Payment can be made through a cashier using:

- a computer or smartphone connected to the Internet (for example, in a dealer company) making payments through the CyberPlat® system website;
- an automated cash register (for example, in a retail store) - in this case, interaction with the CyberPlat® system is carried out through the server of the commercial enterprise;
- other hardware;

These operations support the "1C: Enterprise" technology:

Without human participation:

- payment terminals;

Via Internet-Bank-Client:

- a bank computer connected to the Internet using the Internet-Bank-Client banking system
- POS terminals;
- smartphones and phones supporting Java, iOS and Android systems;

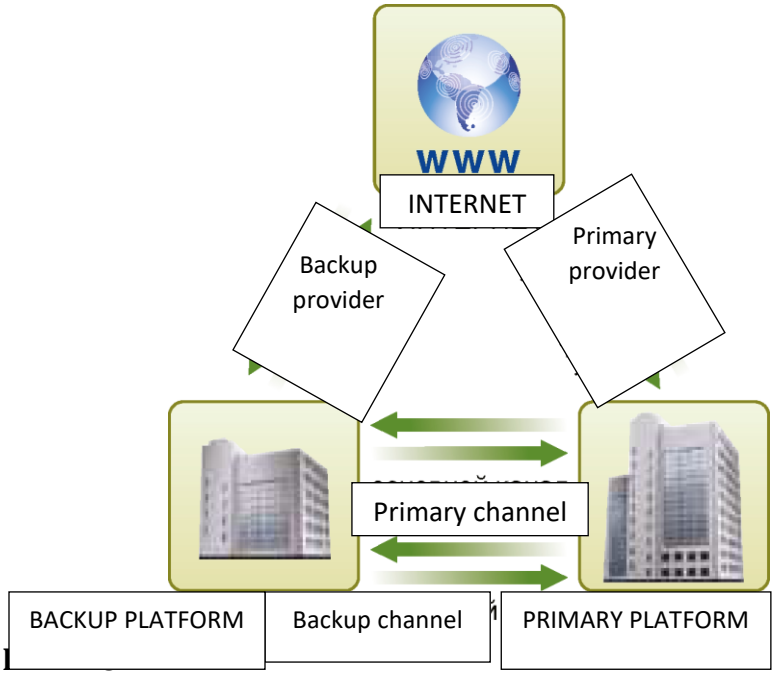
- ATMs;
- mobile display units.

For example:

- POS terminals are used for retail chains;
- a special technology using the company's internal network is used for the Eldorado chain;
- large retail chains (“Svyaznoy”, “Euroset”, MTS, Tele2, etc.) use a solution based on 1C or own proprietary solutions;
- electronics store chains (“Eldorado”, “Tekhnodom”, etc.).

Система «The CyberPlat® system maintains detailed records of all transactions that use any of the above mechanisms, and full payment statistics is available online to the agent's administrator on the company's website: http://www.cyberplatru.

STABILITY AND SCALABILITY OF THE TECHNICAL



The high performance indicators of the system are based on the following factors. The CyberPlat® system is premised on two duplicating processing centers located in Russia. The primary processing center is located in Moscow. Communication between the centers and channels over the Internet are duplicated through the networks of independent communication providers. Such a redundancy system combined with a modern cluster architecture ensures high fault tolerance of CyberPlat® and its independence from most force majeure circumstances.

CyberPlat® imposes the highest demands on software operation, which guarantees high quality and level of performance of each individual module and the entire system as a whole.

In addition, CyberPlat® has been successfully operating for more than 20 years, and the system has been debugged and optimized, its most important modules have been refined and polished over this period of time.

CYBERPLAT® PRODUCTS AND SOLUTIONS

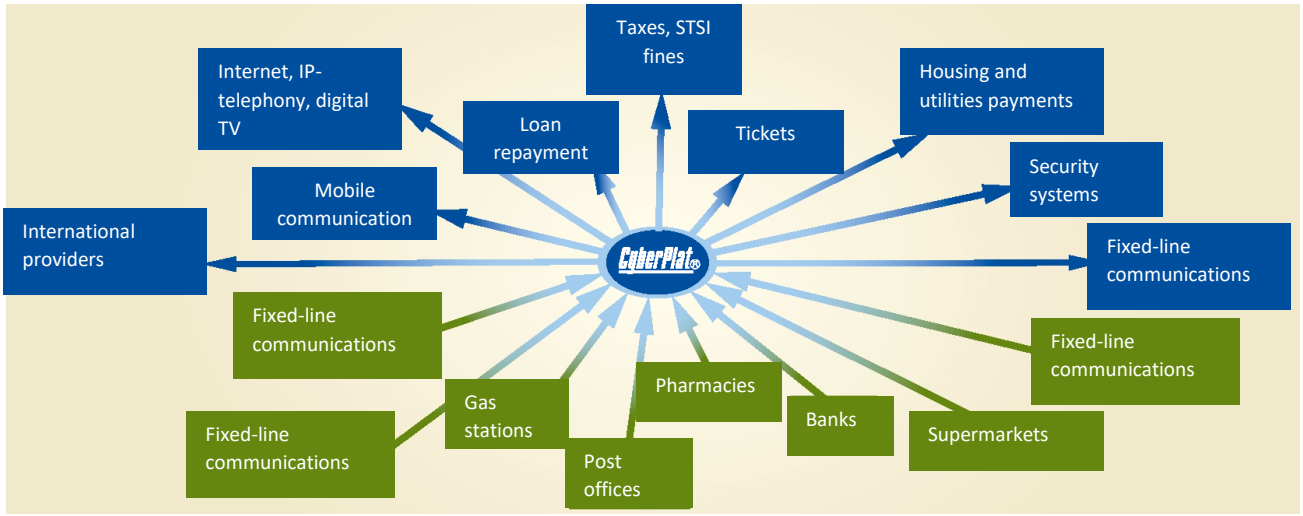
PRODUCTS AND SOLUTIONS FOR RETAIL BUSINESS

ORGANIZATION OF PAYMENT ACCEPTANCE (DOMESTIC TOP-UP)

The basis of the business model of the CyberPlat® electronic payment system is the system for organizing payments from individuals through a partner network (the "lower segment" of the business chart) to a wide range of different suppliers of services and goods (the "upper segment" of the business chart) developed and implemented on a global scale. The "lower segment", the payment acceptance network, is comprised of retail enterprises, bank offices and ATM networks, and self-service terminal networks.

At the end of 2018, the number of payment acceptance outlets in the "lower segment" was almost 1.5 million. In addition, a fairly large number of users of the Internet-Bank-Client systems owned by banks - partners of the CyberPlat® electronic payment system - exists, integrating the capabilities of making payments to service providers. Such users are also part of the "lower segment" of the CyberPlat® payment acceptance system.

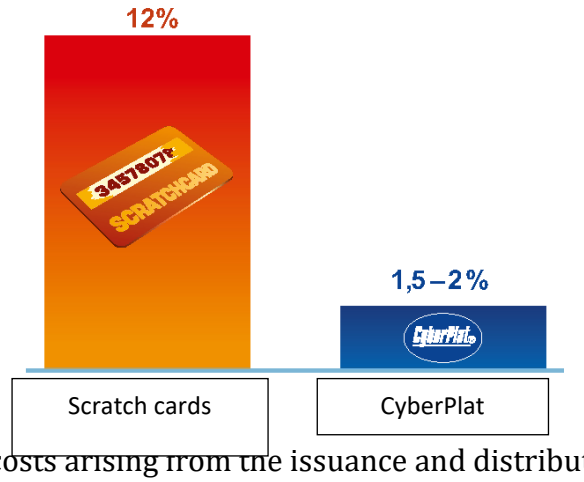
OPERATORS AND SERVICE PROVIDERS



PAYMENT ACCEPTANCE OUTLETS

ORGANIZATION OF PAYMENT ACCEPTANCE AT RETAIL ENTERPRISES. THE REASON WHY IT IS COST-EFFECTIVE

LOW COST OF REVENUE COLLECTION



When using the capabilities of the CyberPlat® system, the actual cost of revenue collection is significantly reduced, which is extremely important for operators. The cost of collecting revenue through the use of scratch cards is 12% of the rate. This is the full prime cost paid by the operator for collecting revenue using scratch cards.

It includes a discount for retailers (usually 5-6%), issuance (2-3%), logistics, protection against fraud and a number of other costs arising from the issuance and distribution of scratch cards.

When collecting payments through CyberPlat®, the average cost of collecting revenue in retail for mobile communications is reduced to 1.5-2%. This is a huge savings for service providers.

Saving 10% of the income of such a mobile operator as, for example, Beeline, the revenues of which amounted to $ 4.2 billion in 2018, leads to an additional profit of $ 400 million per year. This amount is tremendous.

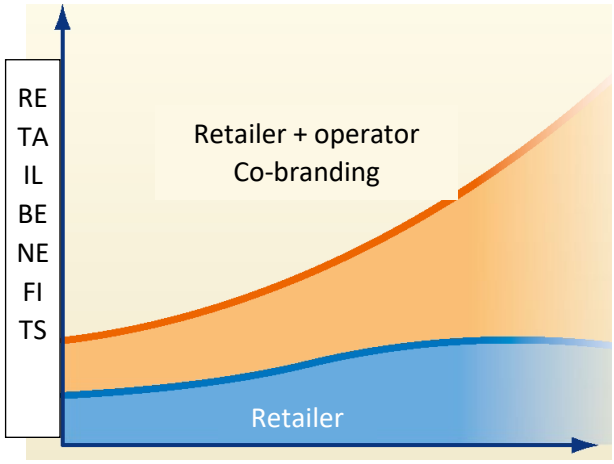
INCREASED CUSTOMER FLOW AND INCOME

Decades of experience in the operation of the electronic payment system shows that the throughput of service or retail outlets where payments are accepted via CyberPlat® is doubled. At the same time, the income from sales under the main profile of such commercial enterprise increases by 10-40% depending on the quality of advertising and on the “profile” of the goods. For example, if a retail outlet sells laundry detergent, the volume of laundry detergent sales will increase by about 10%. If the retail outlet sells mobile phones, the increase in sales can reach 40%.

Retail only

Retail + payment acceptance

RECEIVING PROFIT FROM CO-BRANDING



If we compare the CyberPlat® technology with the use of prepaid cards (scratch cards), the CyberPlat® technology reduces sales costs and provides the retailer with the possibility of co-branding with those operators who serve as the recepient of the payment acceptance transaction organized (and these are often global brands).

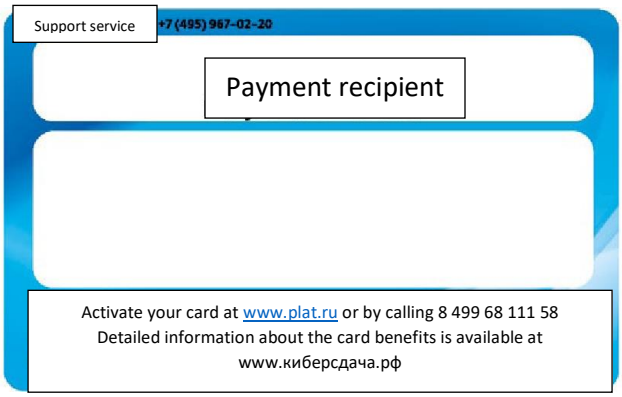
The chains that start accepting payments can get free advertising from the operator. For example, if a well-known Russian retailer starts accepting payments for mobile communications in its stores, the largest Russian mobile operator advertises this retail network free of charge. It is clear that joint advertising is always beneficial for the retailer, as the brand awareness of the mobile operator involved is always higher, and therefore it acts as a locomotive for promoting the retailer's brand.

"CYBERCHANGE" - A UNIQUE FINANCIAL SERVICE

"CyberChange" is a modern financial technology associated with the use of change left after payment for goods and services in retail chains, shops and small outlets (www.киберсдача.рф).

The amount of change can be transferred in real time to almost any service provider with no cashier's time wasted using a special CyberChange card.

The CyberChange plastic card is the same size as standard bank cards. It bears a 19-digit card number and a barcode.



The consumer can transfer the amount of change remaining after payment for goods or services to:

- A mobile phone account;
- A bank card;
- The current bank account linked to the Internet-Bank-Client (for example, to “PLAT.RU Payment Book”).

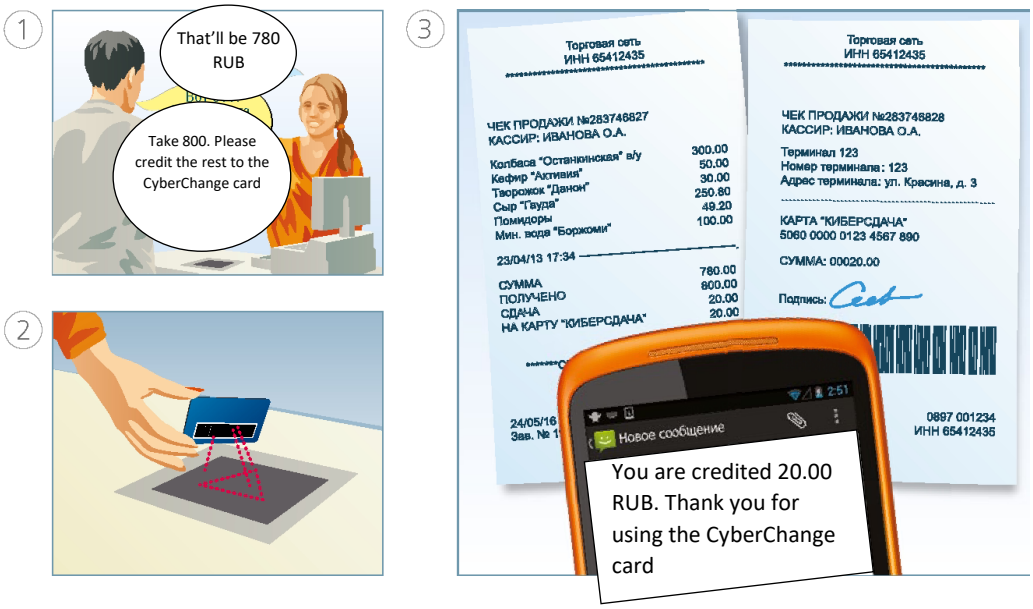
Any person can become a user of the service. In order to credit change or carry out a targeted transfer of funds to a bank or personal account with a service provider, you must first activate the CyberChange card. In the process of activation, the card number will be assigned a template containing payment details, for example, a service provider code and a mobile phone number, or a bank code and a bank or personal account number and a mobile phone number. The set of data is transferred to the CyberPlat® system and further serves as an electronic template for making transfers automatically, without entering any details.

To carry out transactions below the minimum payment threshold, a “Payment Book” (www.plat.ru) is automatically created by the provider for the client, and the change amount is credited there.

GENERAL PLAN OF CHANGE CREDITING

Let us consider a common situation: at the most unexpected moment, your mobile phone is blocked because you have run out of money. You immediately take off looking for the nearest payment acceptance outlet in order to replenish your account in a quick and convenient manner.

You walk into the nearest store of a well-known retail chain and ask the cashier to replenish the account. In response, the cashier offers to make a purchase, and transfer the amount of change to your mobile operator's account. You agree, because you understand that it is “killing two birds with one stone” at the same time: you replenish your account, “revitalizing” your phone, and purchase the desired product as well. As a result, store turnover increases and customer loyalty to the retail network grows.



INCREASED TURNOVER OF HIGH-MARGIN GOODS

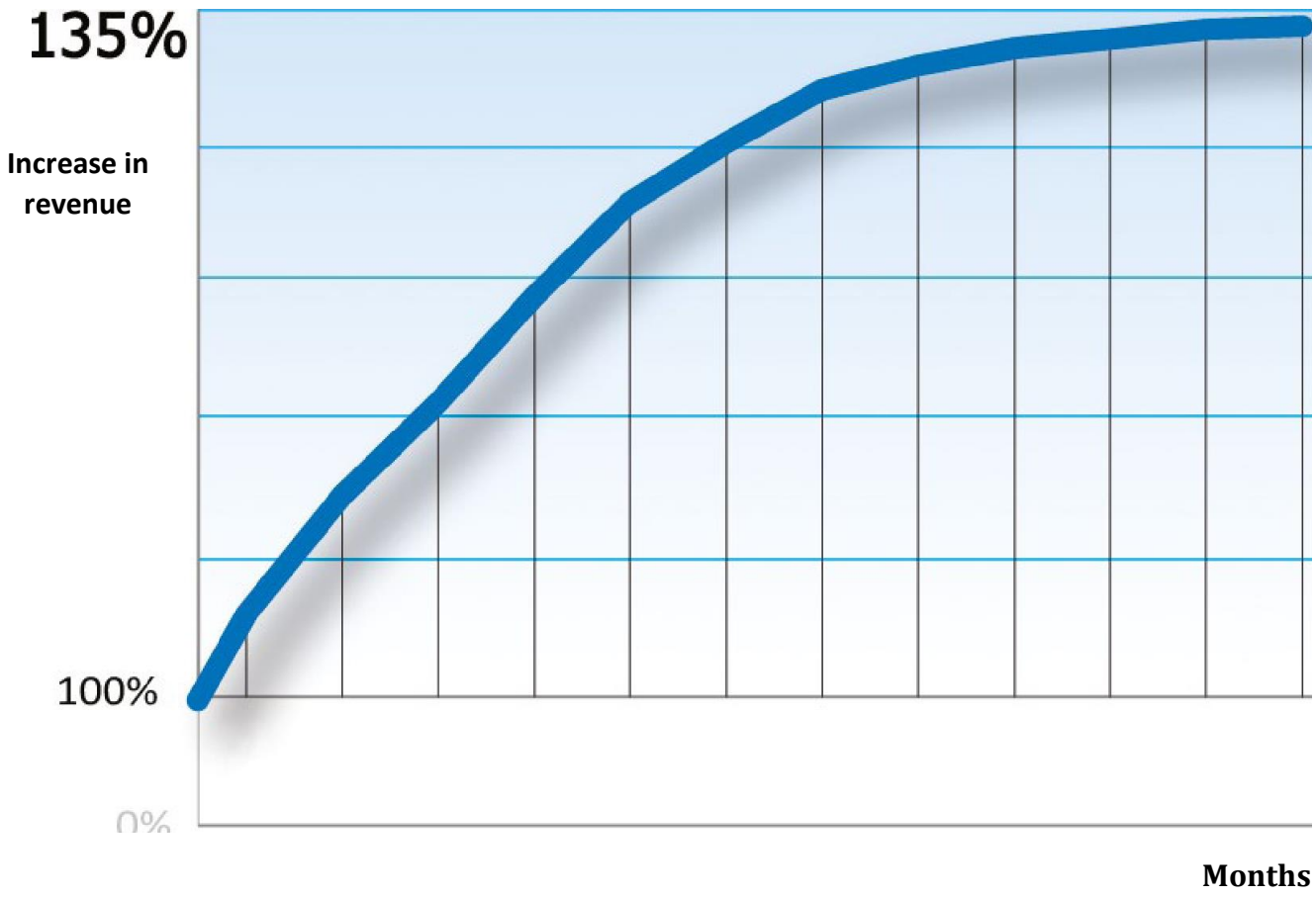
With the growth of foot traffic moving higher as a result of the implementation of the CyberChange project, the turnover of high-margin goods in the outlet increases. The client comes to pay for services using their CyberChange card and makes purchases of point-of-purchase goods with higher profitability, which are located in checkout areas.

E-retail experiences an increase in sales of accessories: covers for mobile phones, key fobs, memory cards, batteries, etc.

Sales of beer, cigarettes, alcohol, mineral water, chocolate, confectionery products, chewing gum are growing in grocery retail, as well as sales of non-food high-margin products.

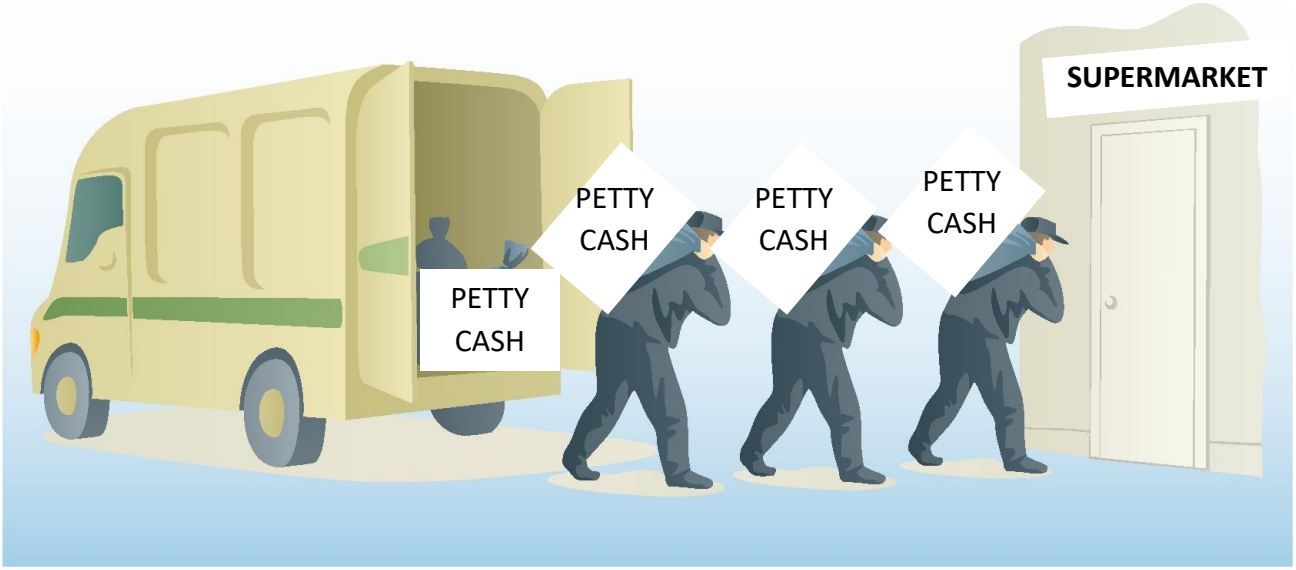
The CyberChange technology is similar to the Japanese Change to Card service. In Japan, the Felica system is operating successfully, where the change from retail purchases is credited to a noncontact card. Then this card can be used to pay, for example, transport services.

The turnover of this system in Japan reaches tens of billions of dollars - showing that the widespread introduction of Change to Phone can significantly increase operators' income. It will not reach millions or tens of millions, but rather hundreds of millions of dollars.


135%
Increase in revenue
100%
0%
Months

REDUCTION IN CASH TURNOVER

The service for transferring change to mobile phone accounts is very advantageous in terms of retail sales. The costs of receiving coins from banks are eliminated, which is of critical importance, since delivery of small change and its issuance to cashiers always poses a massive issue for any retailer.



SOLUTIONS FOR BANKS

AUTO PAYMENTS - A TURNKEY SOLUTION FOR BANKS

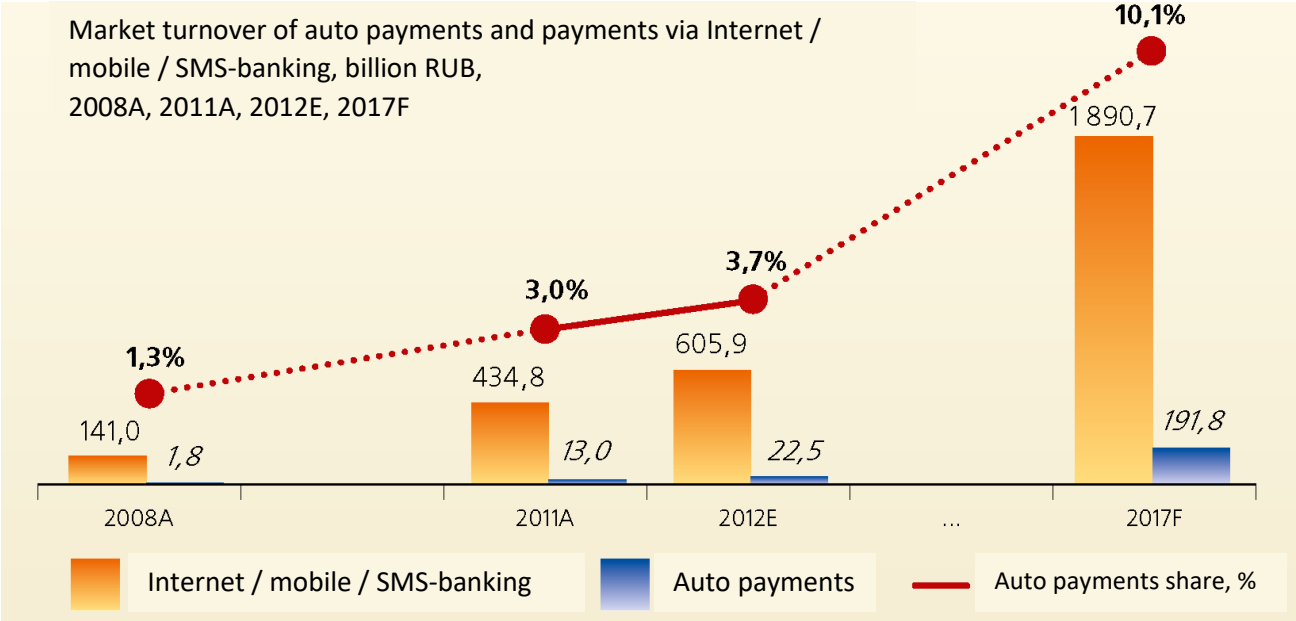
Auto payment is a service for automatic replenishment of mobile phone accounts or automatic payment for housing and utilities and services of energy sales companies, as well as traffic fines using a client's bank account.

Payment for mobile communication is carried out if the account balance drops to the minimum amount set by the subscriber, and other payments are made in accordance with the dates and amounts of payments set by the client themselves.

CyberPlat® provides a service as part of a package of remote financial services, including:

- Internet banking;
- Mobile banking;
- SMS banking.

According to the research company J'son & Partners Consulting estimates, auto payments in Russia make up about 10% of the turnover of payments of all remote financial services.



HOW THE SERVICE WORKS

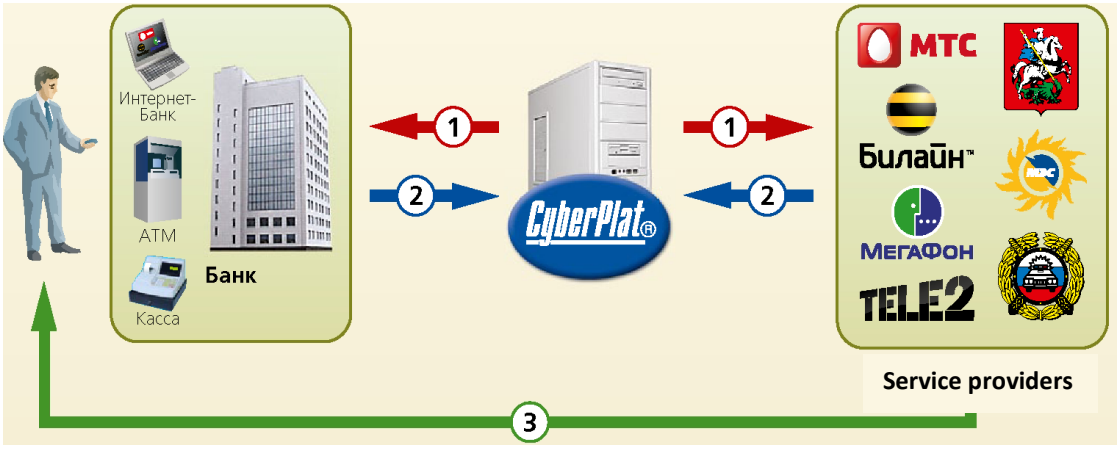
I. Registration

1. The Client sends an application for the activation of “Auto payment” to the Bank in order to pay for the services of the required provider. The Bank sends the application to the Provider through CyberPlat®. The Client can connect to the service through the Internet-Bank-Client system, at the Bank's office directly, as well as in the network of ATMs and bank terminals.

2. The Provider confirms the acceptance of the application through CyberPlat®.

3. The Provider sends the Subscriber an SMS with information on the service connection.

Further settings of auto payment characteristics - account balance, top-up amount, phone number, payment date - can be adjusted at the bank's office, at ATMs or bank terminals, via the Internet-Bank-Client, as well as using the Platru online service - CyberPlat® Payment Book hosted on the website www.plat.ru - at any time.

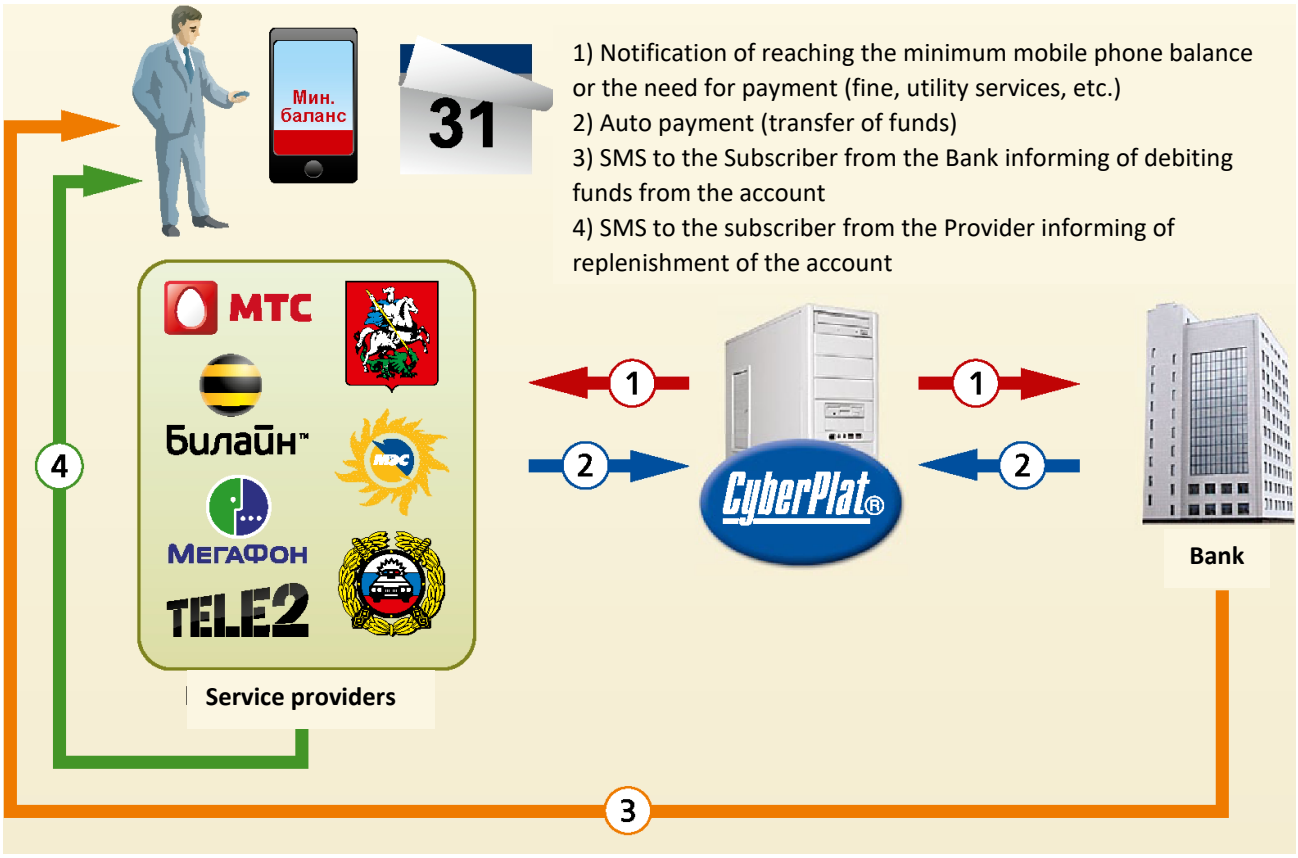


II. Auto payment

As soon as a need to make a payment arises, the Bank receives a request from the Service Provider to process the payment through the CyberPlat® system.

Funds are debited from the Client's bank card account automatically in the amount of the payment amount specified and are credited to the account of the beneficiary of payment.

The Bank's Client receives an SMS confirmation of the payment made.



ADVANTAGES FOR BANKS

- Increased commission rate.
- Service advertising support from MTS, Beeline, MegaFon, Tele2.
- Increased efficiency of using accounts due to an increase in the volume of customer payments in “own” bank.
- Customer loyalty is growing as the interest in maintaining a larger balance to top up the balance increases.
- Reduced volume of cash withdrawals for payments outside the bank.
- New clients are attracted through the provision of additional services.
- No development costs: CyberPlat® provides a ready-made innovative solution.

ADVANTAGES FOR CLIENTS

- No need to waste time replenishing your account.
- Payments are credited in real time.

- Ability to pay for several numbers from one account.
- Ability to carry out auto payments while abroad.
- Ability to control payments made at any time using card reports.
- Each crediting of funds is confirmed by an SMS notification.
- Ability to change the parameters of the service: the account balance, the top-up amount, the addition of new phone numbers.
- Variability of settings. For example, auto payment schedule: every day, every week, etc. or setting a monthly payment limit.
- Bonus programs from the bank.

PRODUCTS AND SOLUTIONS FOR TERMINAL NETWORKS

SOFTWARE PACKAGE "TERMINAL CLIENT 3.0.X.X"

The software package developed and offered for use by the partners of the electronic payment system consists of two main components:

- terminal part of the software - TerminalClient 3.x.x;
- “Terminal Monitoring” technical service.
- TerminalClient 3.x.x is installed directly on the payment terminal.

Technical monitoring can be installed at the client's office or at CyberPlat®.

ADVANTAGES OF THE SOFTWARE OFFERED

- High reliability, fault tolerance, protection against cyber threats.
- Versatility of the solution, allowing to accept payments through the majority of payment terminals on the market.
- A large and constantly expanding list of supported hardware.
- Support for fiscal registrars officially approved for use in terminals.
- Flexible software settings.

- Ability to monitor the status of terminals remotely.
- Several GUI design options.
- Ability for users to change the design of the graphic interface independently.
- independently to switch modes online and offline.
- Acceptance of payments to operators not represented in the CyberPlat® system.
- Support for several types of watchdog timers.
- Open source software.

An exclusive feature of the software is the ability to accept payments to service providers that are not CyberPlat® system operators, for example, local utilities companies, Internet providers, etc.

OPEN SOURCE CODES AND TECHNOLOGIES

A distinctive feature of the CyberPlat® software, which attracts large customers, is availability of open codes of the programs developed.

Since 2009, the open-source software development project for CyberPlat® payment terminals has switched to the classic Open Source technology. This software development mode is in line with the software development technology in projects such as Linux, MySQL and other global software products.

Shifting away from the concept of software development within the framework of the company that has created the product and moving to the classic open source code mode are dictated by the growing popularity and the extent of use of software for terminals developed by CyberPlat® specialists. An important advantage of the product offered is its rapid development compared to closed projects due to the constant collaboration of different development groups between themselves and the community of users of Open Source products.

While previously only the specialists of the CyberPlat® electronic payment system made all the necessary changes to the terminal software package by themselves, within the framework of the new concept, CyberPlat® provides an opportunity for all market participants and independent developers to participate in software development. At the same time, CyberPlat® acts as a moderator and integrator of the efforts of all developers, as well as the owner of the website where discussion and exchange of the results of their activities take place.

From a technological point of view, the project has the following features:

- The source code of the version is made for Windows;
- certain components of the program are presented as binary libraries;
- the code is provided to the participants in the “read-only” mode, and if the project participant wishes to make their code available, the code is sent to the moderators for control and publication.

The use of the Open Source technology by the CyberPlat® electronic payment system in the development of terminal software ensures easy scalability of the project without increasing its operating costs.

In order to participate in the project, anyone can register in the system at https://help.cyberplat.com/, download the project, get access to changes records and record changes in the process of development.

SOLUTIONS FOR MICROFINANCE ORGANIZATIONS

RECEIVING PAYMENTS FOR LOAN REPAYMENT

CyberPlat® technological solutions have been successfully used by the participants of the microcredit market over the course of several years. Within the framework of Federal Law No. 151 “On Microfinance Activities and Microfinance Organizations”, effective from 2010, the Company has developed a package of electronic financial services specifically for microfinance organizations (MFOs).

PARTNERS

CyberPlat® works with many MFOs included in the state register of microfinance organizations, some of which are listed below.

Innovative CyberPlat® technologies made it possible for the microfinance organizations to actively develop regional activities without attracting investments to expand the payment infrastructure.

SCHEME FOR ACCEPTING PAYMENTS TO MICROFINANCE ORGANIZATIONS

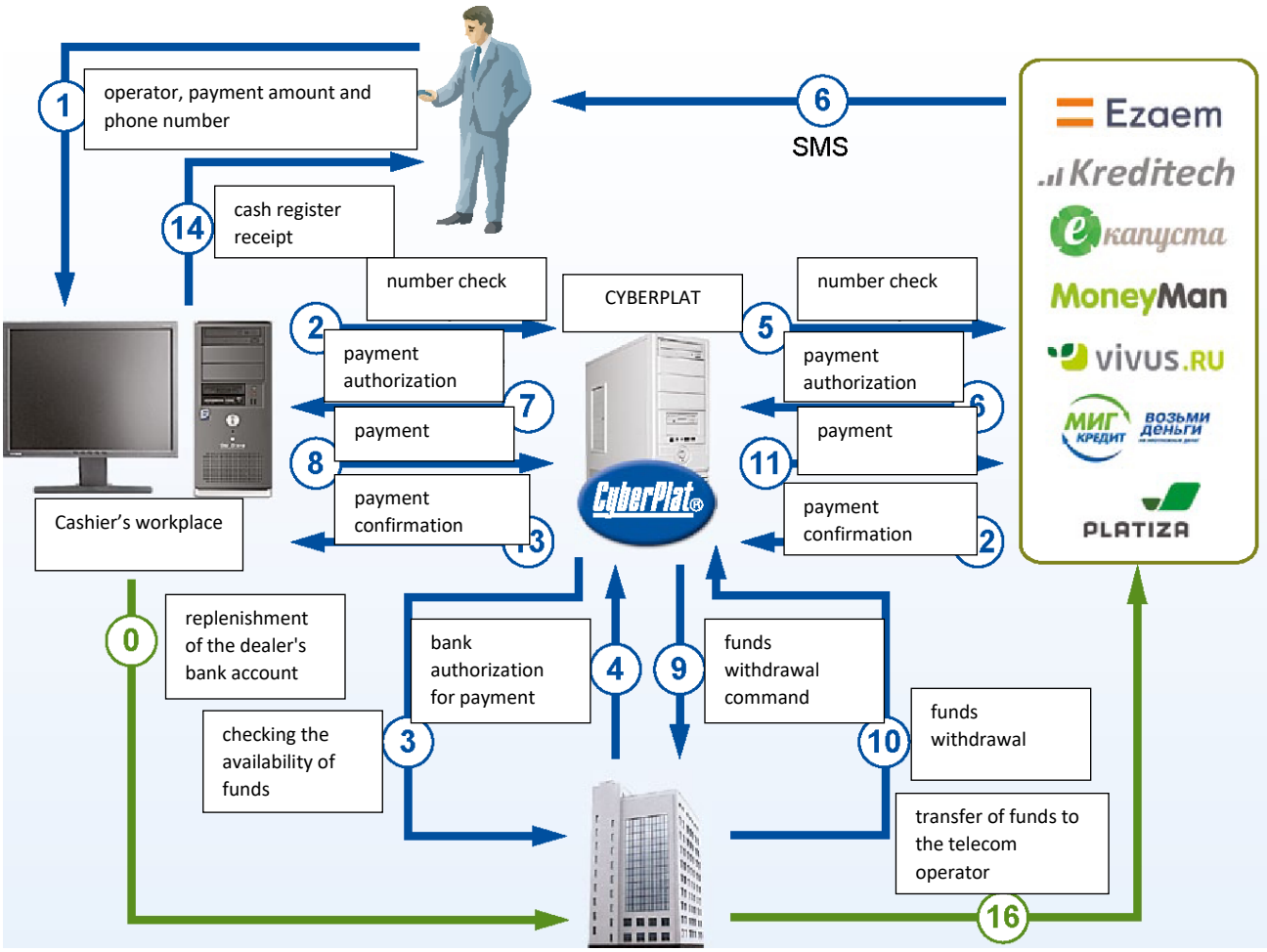
Transaction security

CyberPlat® is a closed-type system in which all settlement participants are strictly defined and cannot withdraw funds from the system at the request of the operator of a microfinance organization.

Each operation in the system is certified with an electronic signature, which eliminates the risk of fraud and guarantees the security of each payment. CyberCheck technology uses an asymmetric 2048-bit key encryption algorithm and monitors every step of the online payment process.

RECEIVING PAYMENTS FOR LOAN REPAYMENT

CyberPlat® owns a large-scale payment infrastructure throughout Russia. If a creditor organization does not have its own office and agent network in the area where the borrowers are located, the MFO can use the extensive network of CyberPlat® partners on attractive terms.



ISSUING LOANS TO BANK CARDS

CyberPlat® was among the first companies on the market to offer its own high-tech solution for issuing loans to cards of international payment systems such as Visa and MasterCard, as well as payment system MIR. A convenient and safe service is available for cardholders of any issuing bank in Russia.

Service benefits:

- Free connection.
- Minimum time and organizational costs.
- Lowest commission on the market.
- Affiliate support 24x7, minimum time for solving problems.

SERVICE FOR SIMPLIFIED IDENTIFICATION OF INDIVIDUALS

CyberPlat® was among the first companies in Russia to provide microfinance organizations with the service for simplified identification of individuals using documents issued by government agencies.

Identification of a client in an electronic payment system requires 2 documents:

1. passport of the citizen of the Russian Federation;

2. TIN or personal insurance policy number of the individual.

An MFO is able to obtain complete information about a potential borrower in just 2 steps, which will require a minimum of time and organizational effort. To do this, the microcredit organization has to:

1. Conclude a contract of instruction on simplified identification with LLC CB PLATINA.

2. Connect to the CyberPlat® system.

RATING INFORMATION SERVICE

Rating information service (a component of scoring) is designed to provide data stored in the CyberPlat® electronic payment system, to analyze the borrower's creditworthiness at the time of issuing a microcredit. The system database contains over 12 billion records.

CyberPlat® provides statistical information on payment transactions with identification by phone numbers, as well as financial information on loan repayment and bank account replenishment. The information contains nine characteristics that objectively identify the status of a potential borrower.

* The information is not of a personal nature in relation to a specific individual.

Information by phone number		
Phone number		926-***-*ф-84
Operator		Megafon Stolitsa
Report type		external (summary)
Analysis period		full history
Dominant region		Moscow
Criterion	Scoring	Description
Number existence	1	0 - does not exist in the CyberPlat database and in the Operator's billing 1 - exists in the CyberPlat database 2 - does not exist in the CyberPlat database, but exists in the Operator's billing
Date of the latest top up	5	0 – was not topped up within a long time (more than a year) 1 - was not topped up more than 6 months 2 - was not topped up more than 3 months 3 - paid in the last 3 months 4 - paid in the last month 5 - paid in the last 2 weeks
Number lifetime	4	0 - less than a month 1 - more than 3 months 2 - more than a year 3 - over 3 years 4 - more than 5 years
Total topped up amount	6	1 – low <500 RUB 2 – modest 500 1,000 RUB 3 - normal 1,000-5,000 RUB 4 – fair 5,000-20,000 RUB 5 – large 20,000-50,000 RUB 6 – tremendous > 50,000 RUB

Service benefits:

- Instant processing of large amounts of data.
- Answering to requests online.
- Ready API protocol.
- Free connection.

Upon a partner's request, CyberPlat® provides a two-month data volume free of charge for testing the service.

ACQUIRING - PAYMENT OF LOANS ON THE MFO WEB RESOURCES

The high-tech solution CyberPlat® allows to repay loans online using cards of the international payment systems such as Visa, MasterCard and NSPK Mir, issued by any bank in Russia.

Service benefits:

- Free connection.
- The lowest commission on the market and an impeccable quality of service.
- Partner support 24x7, priority in resolving all issues as soon as possible.

BANKING PRODUCTS

CYBERPLAT® INDUSTRY PRODUCTS

“PARKINGS” (PARKING AUTOMATION SOLUTION)

Many large cities of Russia, primarily Moscow, face serious issues concerning optimization of the traffic system, where modern infrastructure of car parking spaces has become an important component. The creation of such an infrastructure of paid parking spaces, first in the busiest central parts of the capital, and then an expansion of the service coverage to all areas of the city, demonstrated the effectiveness of this solution in the fight against traffic jams.

The CyberPlat® electronic payment system has developed a solution with the ability to pay for parking from any store, restaurant or cafe connected to CyberPlat®, regardless of the location where the car is parked.

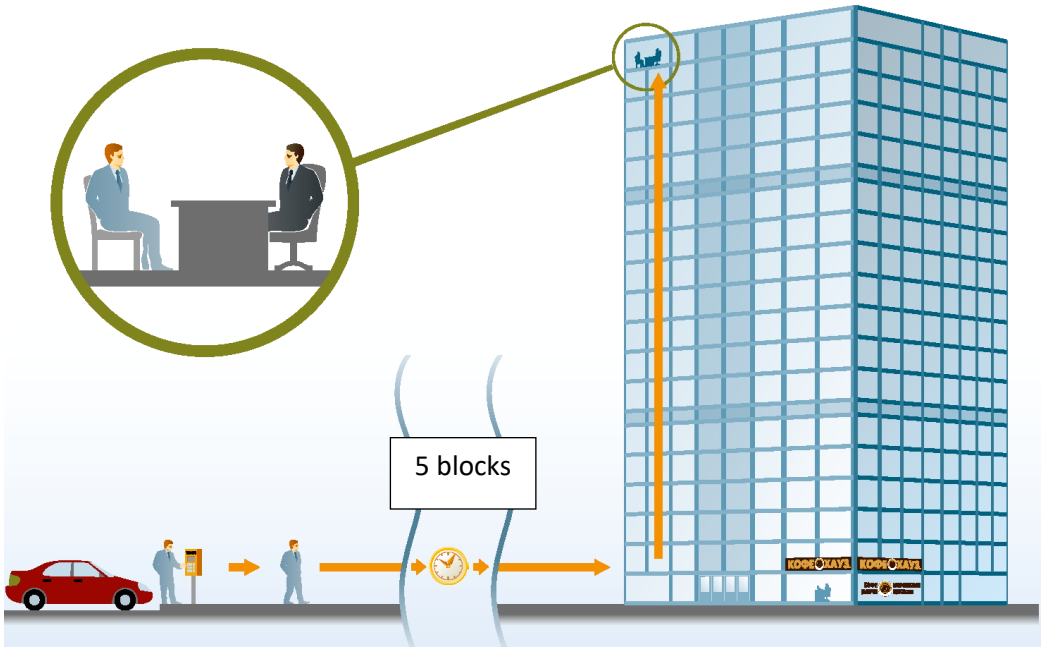
CyberPlat® solution is to create a centralized point for accepting and processing parking payments and connecting a large number of agents to this system. In this case, the procedure for paying for parking is as follows.

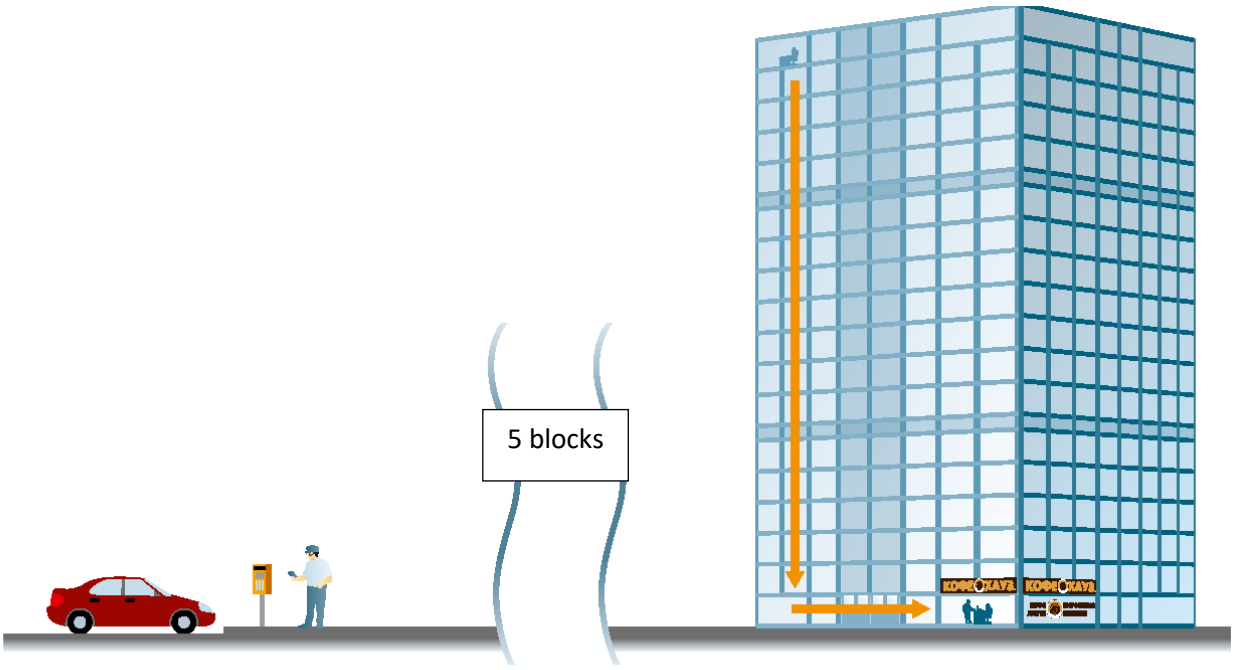
1. A driver parks their car in a permitted space. Each space is assigned a unique number within the region (for example, the city). The number is six-digit (up to 999,999 parking spaces can be numbered).
2. The driver can pay for parking on the spot as per the traditional procedure, occupying a parking space equipped with parking machines (parking meters).
3. However, for greater convenience, the car owner goes to the nearest payment acceptance outlet (it can be a cafe or a store), tells the cashier their phone number, full name and passport information and lodges money. The cashier makes the payment and gives the client a check with payment details. It is worth noting that payment (or additional payment) can be made from any payment acceptance outlet. For example, a person has parked their car a few blocks from a meeting place or work. They go on their way and, if a need for an additional payment for parking arises, they make it at the nearest payment acceptance outlet, having no need to return to their car.

Why it is advantageous

The proposed solution is very convenient for customers, and is also distinguished by reliability, maturity and low transaction costs. It is enough to compare alternative payment methods for parking.

1. The technology of payment through parking meters costs the city about 40% of the amount of payments: 20% - for the operation of the equipment, 20% - the cost of collection. It is also necessary to take into account the cost of equipping the parking spaces.
2. Payment via SMS costs 30-40% of the amount of payments - these are the tariffs of telecom operators.
3. Payment by cards (acquiring) for amounts of $ 2-3 costs 15%.

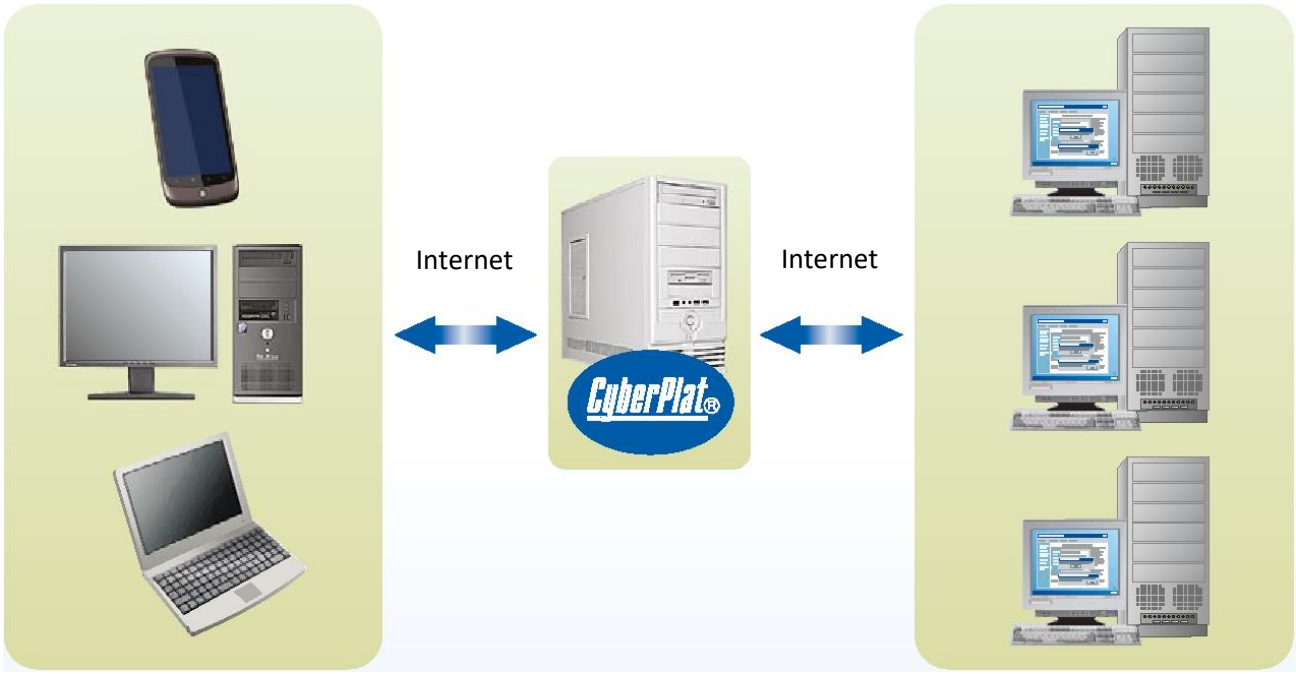

5 blocks


5 blocks


COUNTER
I want to pay for a parking space 123456... and one cup of coffee please

The cost of collecting money using the technology offered by CyberPlat® will initially amount to 10% with a subsequent decrease (approximately within two years) to 5%. The decrease in cost will be made possible due to the growing popularity of the service and, as a result, a decrease in the cost of a single transaction. Retail enterprises, cafes, restaurants, shops, that is, points within walking distance, will take a serious interest in this technology. The attractiveness of the service for them lies in the increase in the number of customers: a person comes in to pay for a parking space (the retailer receives a commission from the payment), and at the same time buys something or uses the relevant services.

General system architecture



Retailers
Starbucks, Coffee House, Euroset, Pyaterochka

Settlement systems for municipal and private parking

How it works

A person has parked their car in a parking space. If the space is equipped with a parking meter, payment for parking can be done on the spot.

If necessary, parking time can be extended at the nearest commercial or service outlet connected to the CyberPlat® electronic payment system.

For example, you can do this at a nearby coffee shop. In order to do this, all it takes is informing the cashier of the parking space number and the parking time, as well as to lodge money.

Implementation technology

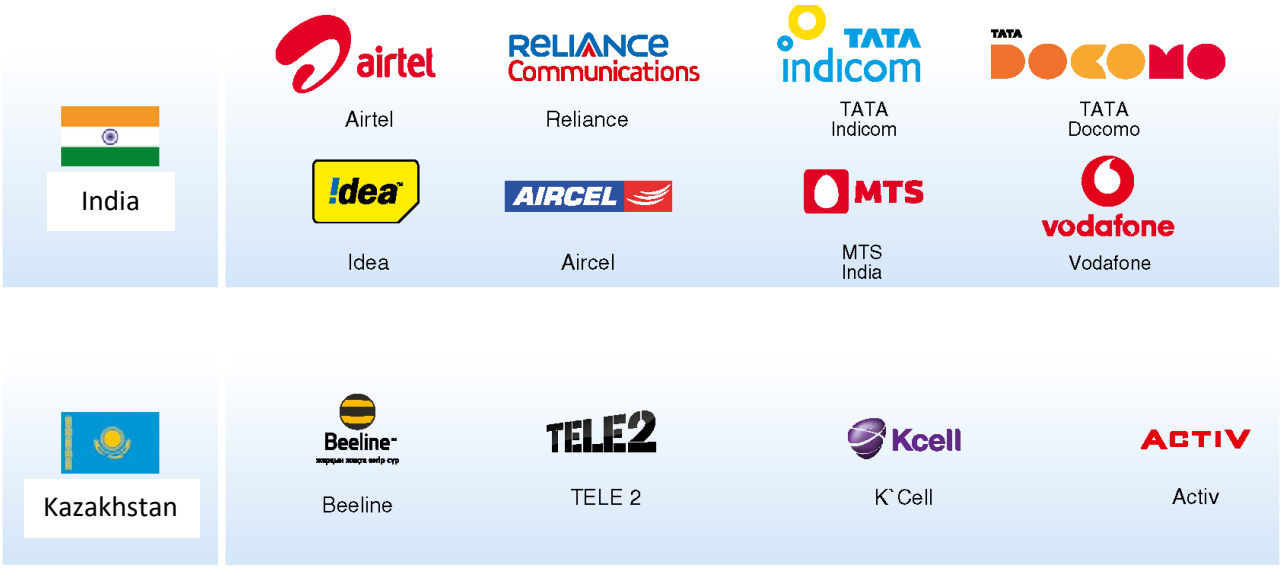
Implementing the solution for parking automation requires connection of the settlement systems of municipalities and large private parking spaces to the CyberPlat® processing center. At the same time, there is no need to modify the software and hardware of the municipalities. The infrastructure of the dealer network of the electronic payment system is quite sufficient for the immediate launch of the system – just pointing out that only Moscow and the Moscow region have 30 thousand payment points connected to CyberPlat® is quite telling.

INTERNATIONAL TOP-UP: INTERNATIONAL OPERATORS AND CROSS-BORDER PAYMENTS

Subscribers abroad can pay for mobile communications using the CyberPlat® international electronic payment system.

Many foreign countries have a well-developed network of payment acceptance outlets located at commercial and service enterprises and connected to the CyberPlat® system. Some of these countries are united by a unique system of cross-border payments. Residents of Kazakhstan, India and Russia, being part of the system, can replenish their accounts with various providers on the territory of any of these countries in a convenient and quick manner by making a payment in local national currency.

The infrastructure of cross-border payments developed by CyberPlat® creates comfortable conditions for the population of different countries. This service is especially in demand by subscribers of mobile operators living in adjacent territories or often traveling.



SOLUTIONS IN THE FIELD OF MOBILE COMMERCE

CYBERDEN TECHNOLOGY - A UNIQUE MOBILE COMMERCE TOOL

CyberDeN is an electronic payment system of a new generation that surpasses VISA. The optimized technology of mobile payments was developed by a group of leading specialists from CyberPlat®, MTS, Beeline, MegaFon, Sberbank of Russia, Russian Standard Bank.

The nature of mobile payments

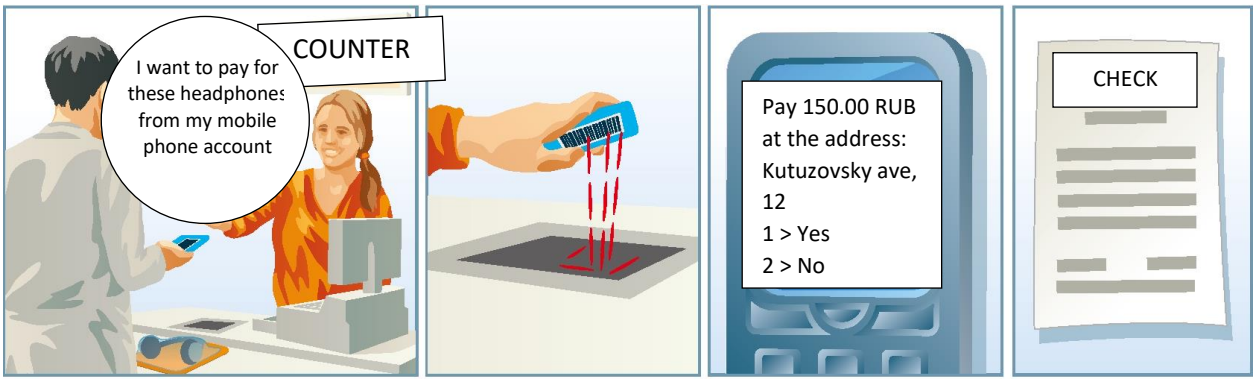
This is a new method of payments at retail outlets that allows you to debit money for making a purchase either from your personal account of the mobile operator or from the payer's bank account. The subscriber's personal account identifier is a bar code unique for each mobile phone number. The ability to pay from the subscriber's personal account allows you to make purchases in a situation where you have neither money nor a bank card on your person.

Its importance for mobile operators and banks

Participation in the project for the implementation of mobile commerce technology of CyberDeN allows mobile operators and banks to increase and consolidate balances on individual accounts intended for making purchases. At the end of 2018, the total volume of funds in the form of bank deposits was 28.5 trillion RUB (approximately $ 409 billion). Due to the expected rapid growth of the mobile commerce sector, its participants will be able to obtain a 30% share in the market of current deposits of individuals, that is, up to $ 123 billion. It is clear that this is very attractive for both mobile operators and banks.

How it looks from the client's point of view

At the time of payment, the seller scans the barcode attached to the mobile phone or a special card, and a USSD request is sent to the client's mobile phone for confirmation of the purchase indicating the amount and address of the location of purchase. The client accepts the payment, following which the seller receives a confirmation from the electronic payment system on the online transfer of funds, prints a receipt and gives the goods.



HOW IT WORKS

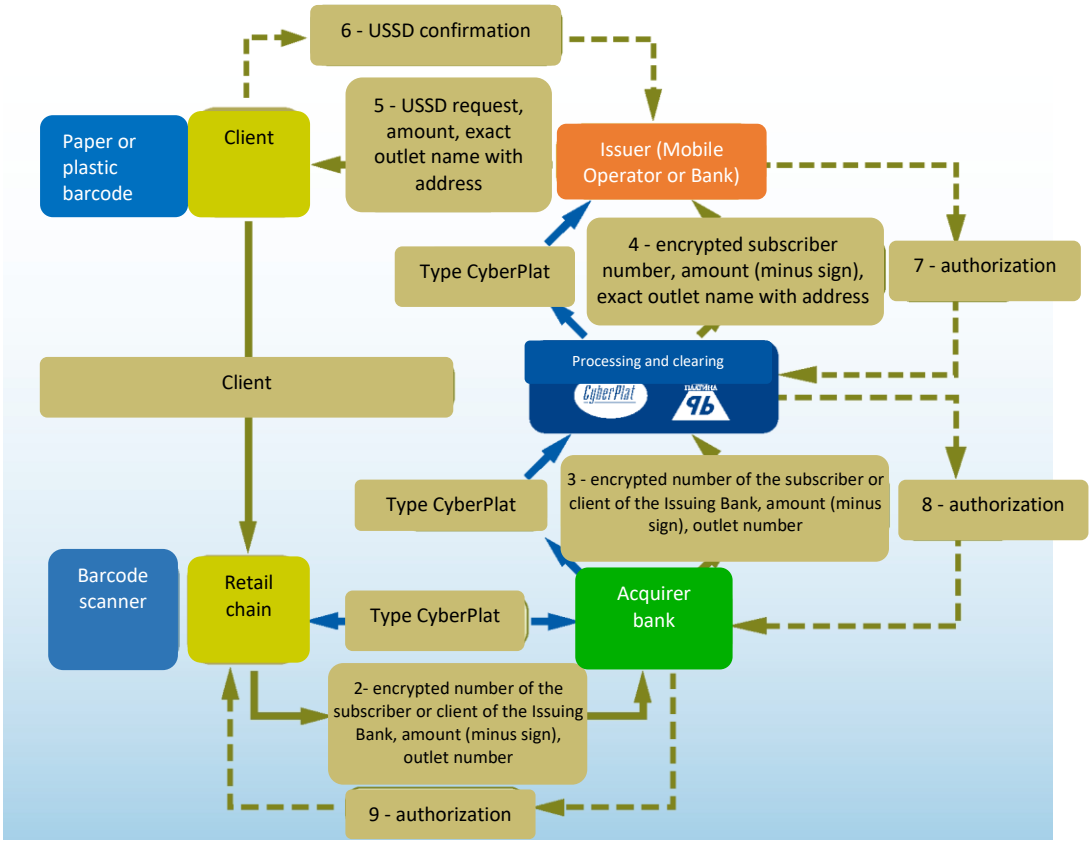
1. At the time of payment, the seller scans the barcode attached to the subscriber's phone or a special card.

2. Using CyberPlat® technology, the cash register software generates and transmits a request containing an encrypted number of the subscriber or the bank client, the amount and the outlet number to confirm the payment to the acquirer bank.
3. The acquirer bank transmits the request to the CyberPlat® electronic payment system using the CyberPlat® technology.
4. The CyberPlat® system determines the outlet's address by its code.
5. The CyberPlat® electronic payment system transmits the request to the issuing bank or mobile operator (barcode label issuer). The request contains the encrypted number of the subscriber or bank client, the amount, the address and the number of the outlet.
6. The mobile operator, if the subscriber's funds on the personal account are sufficient, sends the subscriber an encrypted or unencrypted USSD request containing the amount and the exact address of the outlet.
7. The subscriber accepts the USSD request or refuses to pay.
8. The mobile operator (if it is the barcode label issuer) transfers the payment authorization to the CyberPlat® electronic payment system.

or

1. The issuing bank (if it is the barcode label issuer):

- if the client's funds in their current account are sufficient, sends a preliminary acceptance to the CyberPlat® electronic payment system (confirms that the payment is possible in principle), the client's phone number and the code of the serving mobile operator;
- CyberPlat® transmits to the client an encrypted or unencrypted USSD request containing the amount and the exact address of the outlet through its own USSD concentrator;
- the subscriber accepts the USSD request or refuses to pay;



- CyberPlat® transfers the payment authorization to the issuing bank;
- the issuing bank transfers the payment authorization to CyberPlat®.

2. CyberPlat® transfers the payment authorization to the acquirer bank.
3. The acquirer bank sends the payment authorization to the commercial outlet.
4. The commercial outlet receives payment authorization from the acquirer bank, prints a receipt and issues the goods.

The CyberPlat® technology assumes interaction via the regular Internet connection with the transmission of files with ES encrypted with a 2048-bit key over the SSL protocol (Secure Sockets Layer).

At the request of the operator or the subscriber, when using an encrypted USSD message, the subscriber must have an applet for encrypting / decrypting USSD and / or creating / decrypting the operator's electronic signature on the operator's side of the SIM card.

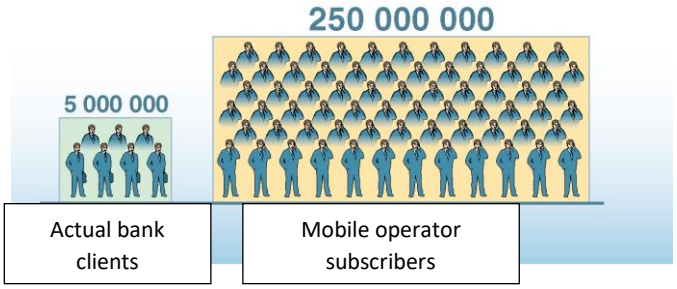
KEY ADVANTAGE - BARCODE USE

A barcode is read and identified from a special label attached to a card or the back of a mobile phone. The barcode can be printed via an information kiosk - barcode printer.

It takes only 3 seconds to complete a request, and 3 seconds to receive a response!

DIFFERENCES BETWEEN CYBERDEN TECHNOLOGY AND CLASSIC VISA TECHNOLOGY

1. There is no physical plastic card. It is replaced by an indelible barcode sticker containing information on the client's account number and its issuer (bank or mobile operator).
2. Unlike cards, you can have as many identical stickers as you like (for example, one on your phone, another on your savings book, the third on your wallet, etc.).
3. There is no paper document flow, because instead of signing the slip, the USSD request confirmation occurs. The analysis of conflict situations is greatly simplified, the costs of complaint management are reduced.
4. The amounts of payments are small, the bulk of transactions is up to $ 30 (maximum $ 50). However, this covers all retail (49% of total household turnover), which is approximately $ 330 billion per year.
5. Debiting of funds (cash-out transaction) is possible not only from bank accounts, but also from personal accounts of subscribers with mobile operators (and even wider, from client accounts of any organization that has received a power of attorney from a bank to collect payment orders from clients in accordance with Federal Law No. 121).
6. Debiting from the client's account / crediting to the trade outlet is 2 times cheaper for a retailer than using VISA or MasterCard systems, and it takes place online.



- The Interchange fee for participants in the electronic payment system is fixed at $ 0.01.
- The cost of crediting in the operator's billing is 2 cents against 10 in the bank's accounting system.

7. It is possible to transfer money both to the specified bank accounts (cash-in transaction), and to the personal accounts of subscribers with telecom operators (top up). First of all, this opportunity is expected to be used for cash payments such as “change to phone or to a bank account”.

BENEFITS FROM USING THE "MOBILE PAYMENTS" SERVICE

For clients

- New contemporary payment instrument.
- Trust in telecom operators is higher than in banks.
- In the absence of cash, you can always pay for goods and services directly from your personal account using your mobile phone.
- Purchase speed is higher than when buying with a plastic card.
- Paperless document flow.
- Security — funds are not debited from the personal account without confirmation of the operation by the subscriber.
- Vast network for replenishing a personal account (incomparable with the number of offices and ATMs of a separate bank).

For retail enterprises

- Low cost of accepting payments (from 0.7 to 1%).
- Instant crediting of funds to a bank account.
- No need to replace operated equipment.
- Speed:
    - the complete procedure takes no more than 6 seconds (3 seconds from the outlet to the buyer and 3 seconds back);
    - higher speed of payment using a plastic card and lower costs for accepting payments;
    - allows you to start accepting payments in discounters and supermarkets.
- Increase in the volume of sales due to sales to persons who have run out of cash and who have “forgotten to take” their card (an increase in the number of payment instruments for the buyer).
- Sales of mostly inexpensive and high-margin products.
- Reducing the number of possible conflict situations.

- Reducing the risks of working with cash.

For mobile operators

- Growth of balances on personal accounts of subscribers will significantly increase the company's liabilities, according to estimates, by more than $ 1 billion in the future (for companies of the “big three” level),
- No investments.
- High speed of implementation.
- Staying ahead of the competition in implementing real mobile commerce.
- Creation of the image of a super-tech company at minimal cost.

- Stimulation of retail outlets to accept payments for mobile communication and implementation of the “change to phone or bank account” program.
- When using a procedure involving barcode reading:
- errors are minimized and, as a result, the cost of canceling and adjusting payments is reduced;
- procedure time is accelerated, which will allow retail chains to:
- reduce the cost of accepting payments,
- speed up the time for accepting one payment,
- start accepting payments in discounters and supermarkets.

For acquirer banks

- Closer “connection” of retail customers to the bank.
- Increased security of loans issued to retailers.
- Receiving additional acquiring income and competitive advantages.
- Opportunity to start working with commercial outlets that traditionally do not accept cards for payment due to high fees.
- Launching a product to the market that can compete with international payment systems.
- Stimulation of retail outlets to accept payments for mobile communication and implementation of the “change to phone or bank account” program.
- Leading competitors in the implementation of real "mobile commerce".
- Creation of the image of a super-tech bank.

-

ADDITIONAL SERVICES FOR CYBERPLAT® PARTNERS

ONLINE TRANSACTION MONITORING

For convenience of our clients who make payments through the CyberPlat® system, as well as for the agents of the electronic payment system, a special web service for checking the status of the payment made (info.cyberplat.ru) has been developed.

A client (or an agent) enters the mobile phone number (or the contract number – if the payment is made not to the mobile operator), the date of the payment and the verification code protecting against network robots into special fields.

After that, the user receives information on the payment status: “passed”, “not found”, “sent for processing to the provider”, “canceled” in the CyberPlat® system.

Depending on the status of the payment, the client is advised on further actions - for example, contact the provider, or the agent through whom the payment was accepted, or the CyberPlat® customer support service. This service provides extra services for clients and agents and greatly facilitates complaint management with payers.

B2C PRODUCTS

PLAT.RU — "CYBERPLAT PAYMENT BOOK"

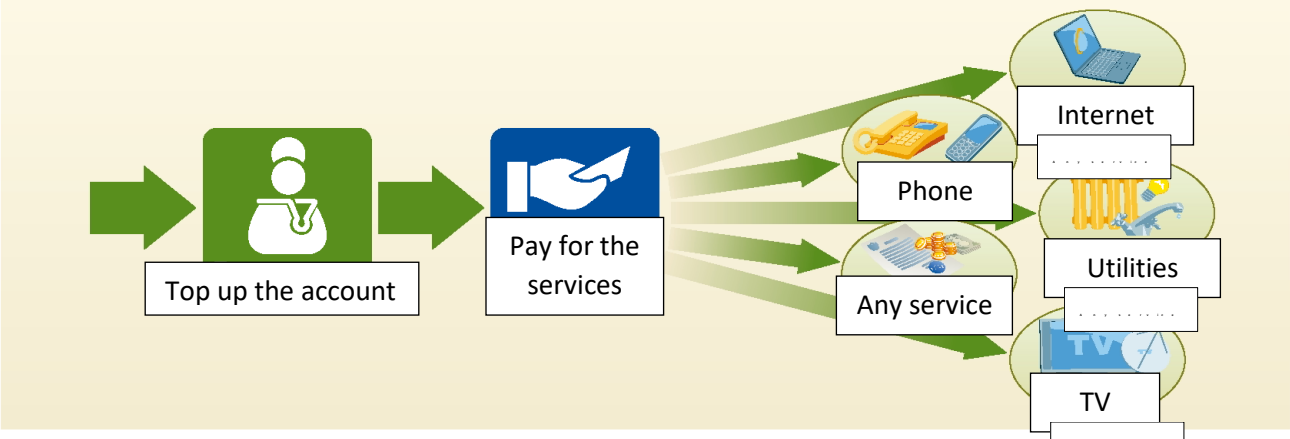
The Platru service – "CyberPlat® Payment Book", developed by CyberPlat® and Platina Bank specialists, has been successfully operated over the course of several years.

Opportunities for clients

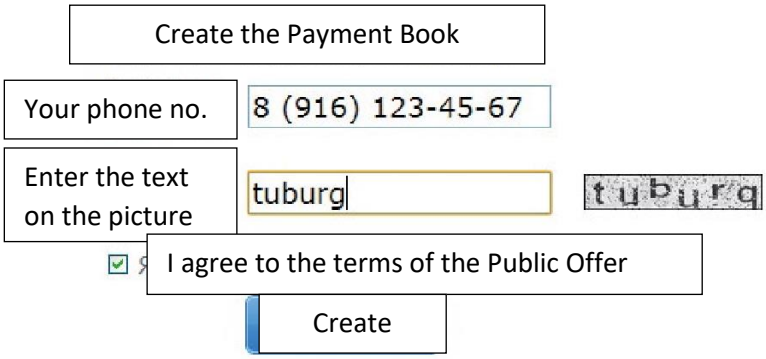
Any person who has registered their personal "Payment Book" on the platru website or through the terminals and cashiers of the CyberPlat® electronic payment system's partners can become a client of this convenient service. By replenishing the balance of their "Payment Book", the user is able to make payments to a wide range of service operators (more than 8 thousand) – mobile and wire communications, cable and satellite TV, Internet providers, utility providers, pay for government services, etc. using the web interface.

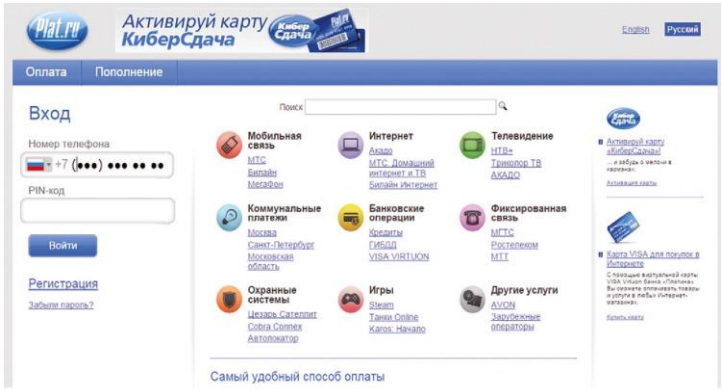
The balance of the "Payment Book" can be replenished through the terminals and checkout counters of the outlets of those CyberPlat® partners who are connected to the service. Replenishment of the "Payment Book" is subject to a commission paid by the client to the agent through whom the operation is carried out. Without additional commission, replenishment of the "Payment Book" balance can be carried out through the terminals of the "Platina" Bank (their addresses are listed on the website www.platina.ru).

The "Payment book" saves the details of regular payments, which allows you to carry out transactions to replenish personal accounts or repay the accumulated debt in a matter of seconds. Saving of the history of the carried out transactions will allow the users not only to control current expenses, but also plan their personal budgets.



An important advantage of the new service is that new recipients of payments have the ability to register in the system - for example, local mobile operators, cable TV or housing and utilities enterprises. Thus, the user of the "Payment Book" receives a unique "one contact" payment service at any time of the day, seven days a week, including in the event of an emergency need - for example, to top up the balance of their mobile phone.





“Payment Book” interface

The Platru service - CyberPlat® Payment Book allows to:

- make payments using the balance on the website to service providers;
- save the details of regular payments;
- register new service providers to process payments;
- track payment history.

Opportunities for partners

The business blueprint of the project provides for the distribution of the commission of service providers, to whom the payments will be made, between the CyberPlat® company and those agents who performed the initial registration of users.

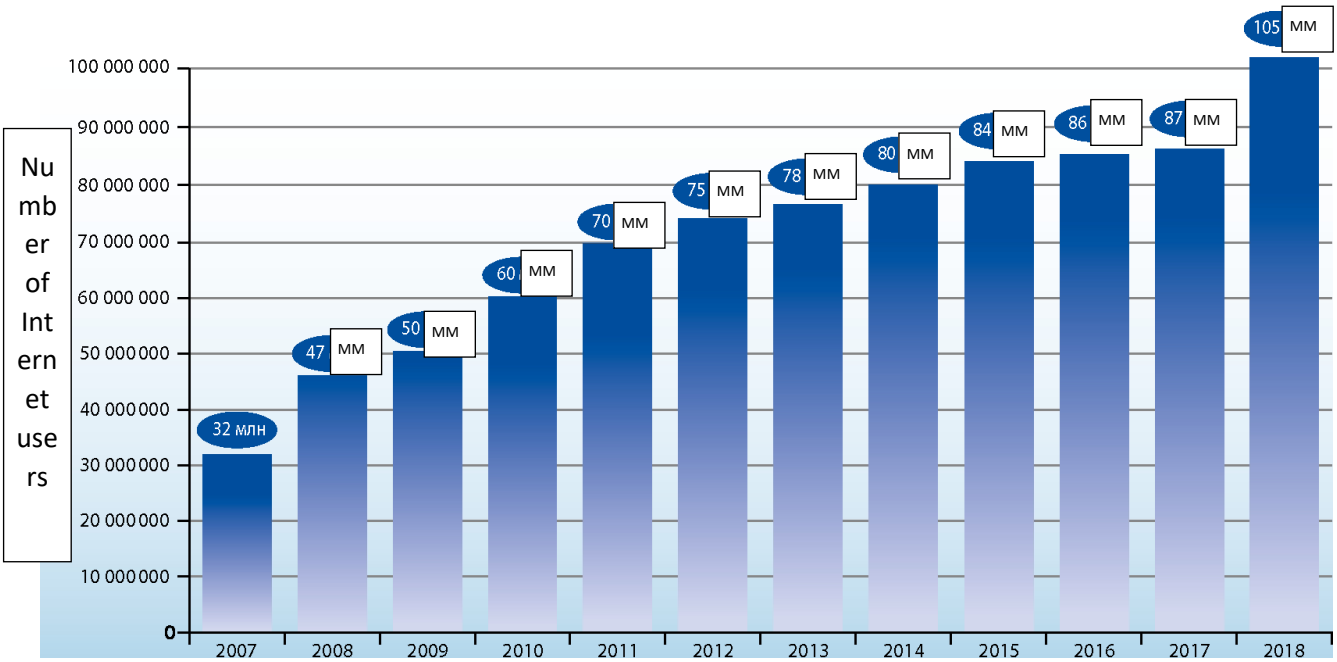
Thus, partners of the CyberPlat® electronic payment system are provided with an opportunity to receive additional income both at the expense of the commission from customers replenishing their “Payment Book” balance, and by participating in the income from the commission of service providers, to whom the payments from the balance of the new service are made.

Opportunities for banks

Platru - CyberPlat® Payment Book can be used as an ultra-lightweight version of the Internet-Bank-Client. Why is this important and possibly extremely beneficial for banks?

- The number of Internet users in Russia is 105 million and their number is growing.
- According to expert estimates, in 2018, the turnover of internet banking in Russia reached 2.4 trillion RUB.
- In 2018, the number of active users of Internet banking in the Russian Federation is estimated at 37 million people.

The Russian electronic sales market for 2018 is estimated at 1.66 trillion RUB.



Why is this happening?

The reasons are as follows.

- Modern information security systems are cumbersome to use. They require advanced user skills.
- IS systems are overloaded with redundant functionalities.
- “One-button” solutions are practically non-existent - any terminal is easier to use.
- That is why CyberPlat® offers banks its “Payment Book” - a convenient, simple and affordable tool for making payments that does not require special user qualifications.

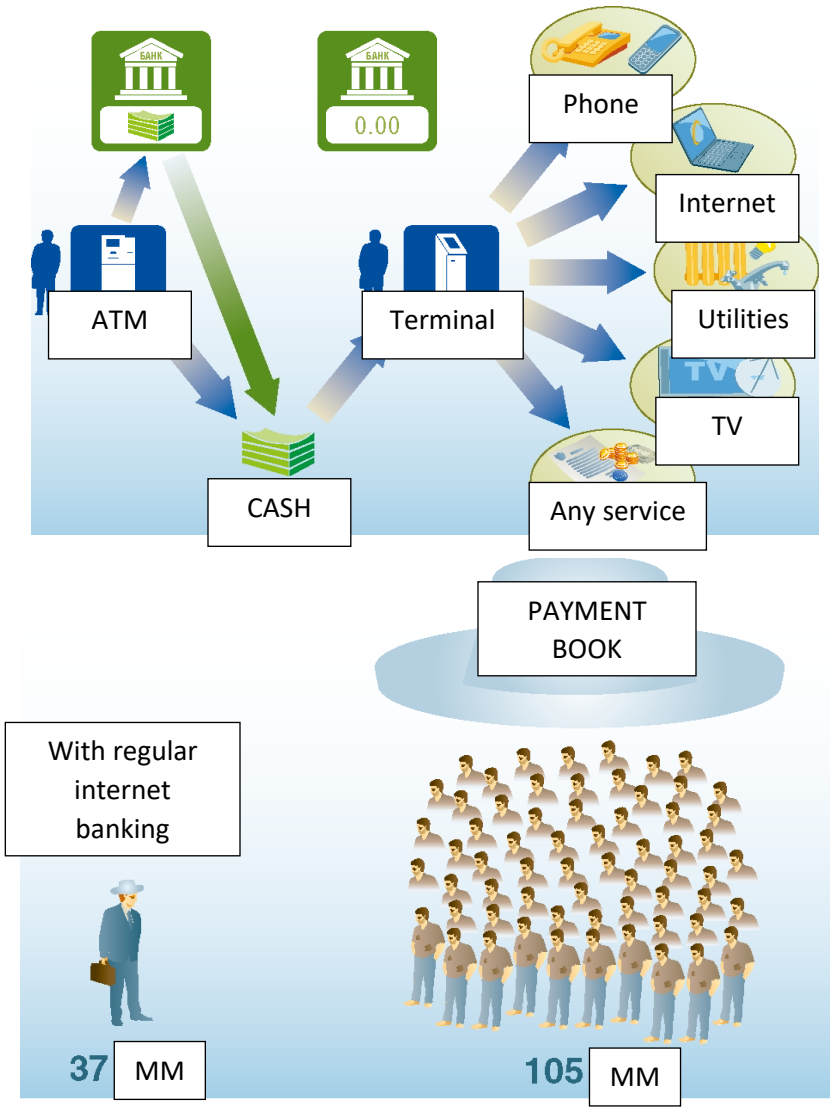
Key advantages of the “Payment Book”

- A simple and intuitive interface.
- Can be used not only through the website, but also at cash-in terminals.
- Easy and fast cash replenishment.
- There is no need for full identification when opening a personal account, since payments are limited to 15 thousand RUB, and such payments are the vast majority in the system.
- The clients are afraid to keep their money in banks, and they deposit cash into the terminal, the cash is immediately converted into replenishing the “Payment Book” balance, and the clients immediately pay using the previously created template.
- The balance from “non-round” payments does not disappear, but remains on the book balance.

Using the “Payment Book’ as a lighter version of the Internet-Client-Bank system gives banks the opportunity to increase the number of their clients dramatically and reach a maximum of 105 million Internet users.

The absence of any significant costs for the implementation of the “Payment Book” is a big advantage.

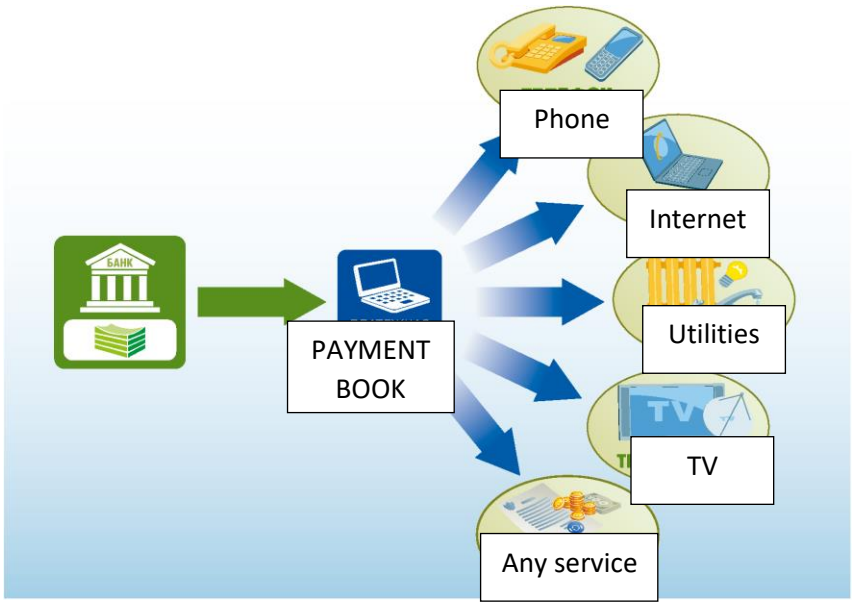
Unlike similar products and developments, “Payment Book” is distributed as per the White Label / API principle, and partner banks can use this flexible and easy-to-use product under their own brand.



Using the “Payment Book” as your own product ensures that income from payments is distributed between CyberPlat® and the partner bank.

The partner bank receives the following benefits:

- A sharp increase in the number of customers.
- Capture of the low-income clients sector.
- Increase in the share of fee and commission income in the income structure.
- Savings of money on the development and implementation of their own Internet-Bank-Client systems.
- Increase in account balances.
- Promotion of the bank's brand as a “socially useful” entity.


Phone
Internet
Utilities
TV
Any service
PAYMENT
BOOK

Opportunities for service providers

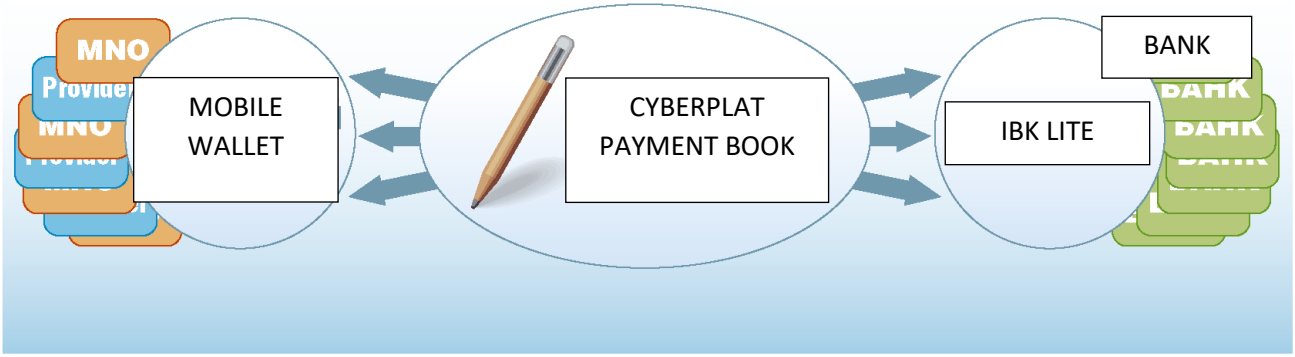
"Payment Book", this simple technological solution, makes it possible to implement a new profitable service "Payments from a personal account" for the clients of telecom operators, Internet and commercial TV providers, and other providers of mass services. The introduction of such a service increases subscriber loyalty and has a positive effect on the growth of business capitalization.

Currently, a clear trend towards the creation and development of such services by all leading mobile and fixed-line operators, Internet and commercial television operators is observed. The benefits from the development of this service are obvious.

- First of all, customers are offered a convenient payment tool, which:
  - expands the range of services;
  - improves the quality of service.
- Secondly, companies receive additional profits by receiving commission income from regular payments made by subscribers from their personal accounts.
- Thirdly, the balances on the personal accounts of clients are increased and consolidated and the problems caused by recurring debts and the need to disconnect clients from using paid services are eliminated.

Replenishment of the account of a service provider (for example, a mobile operator or an Internet provider) is possible at almost any retail outlet or payment terminal. But the situation is reversed with the service "Payments from a personal account" from CyberPlat®. With the help of a personal account in the operator's billing system, customers will be able to pay for the same utilities, Internet access, replenish bank accounts, make money transfers and much more. The implementation of this solution requires practically no costs and no significant work effort.

Experience suggests that the implementation of the service offered is possible within two weeks. At the same time, additional income will begin to be generated immediately after the service is launched. The White Label Affiliate Program allows operators to launch the Personal Account Payments service under their own brand. This requires only a change in the appearance of the screen interfaces and their design in the operator's corporate style.



REPLENISHMENT OF VISA, MASTERCARD, MIR CARDS IN THE CYBERPLAT® NETWORK

With the participation of the international payment systems Visa, Mastercard and the Russian NSPK Mir, the CyberPlat® electronic payment system provides a service for replenishment of any cards issued in the Russian Federation.

In terms of technology, this process is carried out through special gateways, which makes it possible to transfer data on the transactions of replenishing a specific card to the issuing bank almost in an instant. The duration of crediting funds directly to the card account depends on the bank - the card issuer - and can either be instantaneous, or take from two to four days.

Replenishment of cards can be done in the networks of payment terminals and ATMs operating through the CyberPlat® system, in which this service is available. In order to replenish a card, enter the card number through the interface of the payment terminal or ATM and deposit the required amount of funds.

This service provided by CyberPlat® is in high demand for the purposes of regular payments on the loans received. Recipients of loans, holders of VISA, MasterCard and Mir cards, are relieved of the necessity of visiting bank branches and can replenish the card balance at CyberPlat® payment outlets located within walking distance - in shops, pharmacies, gas stations, etc.

Convenient replenishment of cards through the CyberPlat® payment acceptance network increases the attractiveness of plastic cards among the population and makes their use practical.

MasterCard MoneySend

mastercard.

Transfer to VISA cards

МИР

VISA

HOW TO BECOME A CYBERPLAT® PARTNER

BECOME AN AGENT OF THE CYBERPLAT® SYSTEM IN 5 MINUTES! AUTOMATIC REGISTRATION OF AGENTS

The simplified procedure for ultra-fast automatic registration uses the provisions envisaged in Art. 428 of the Civil Code of the Russian Federation, under which the agent joins the Agreement on Accepting Payments (the Accession Agreement, which can be found on the website http://www.cyberplatru/agent/dogovor.pdf), just by submitting the corresponding Application.

The procedure for generating electronic signatures and working with the agent network has been significantly simplified by unifying all the necessary actions within the framework of a single software module “Key Manager”. Following registration, the user downloads this program and, observing instructions of the “wizard”, creates a set of keys and registers their public key in the system. The administrator can register a sales outlet or cashier in the Agent's Cabinet, receive key cards for them, generate a set of keys using the Key Manager and register public keys in the Agent's Cabinet independently. The simplified registration procedure in the CyberPlat® electronic payment system enables you to connect to the system quickly without opening a current account or your personal presence at the CyberPlat® office.

You must complete the following steps to carry out automatic registration.

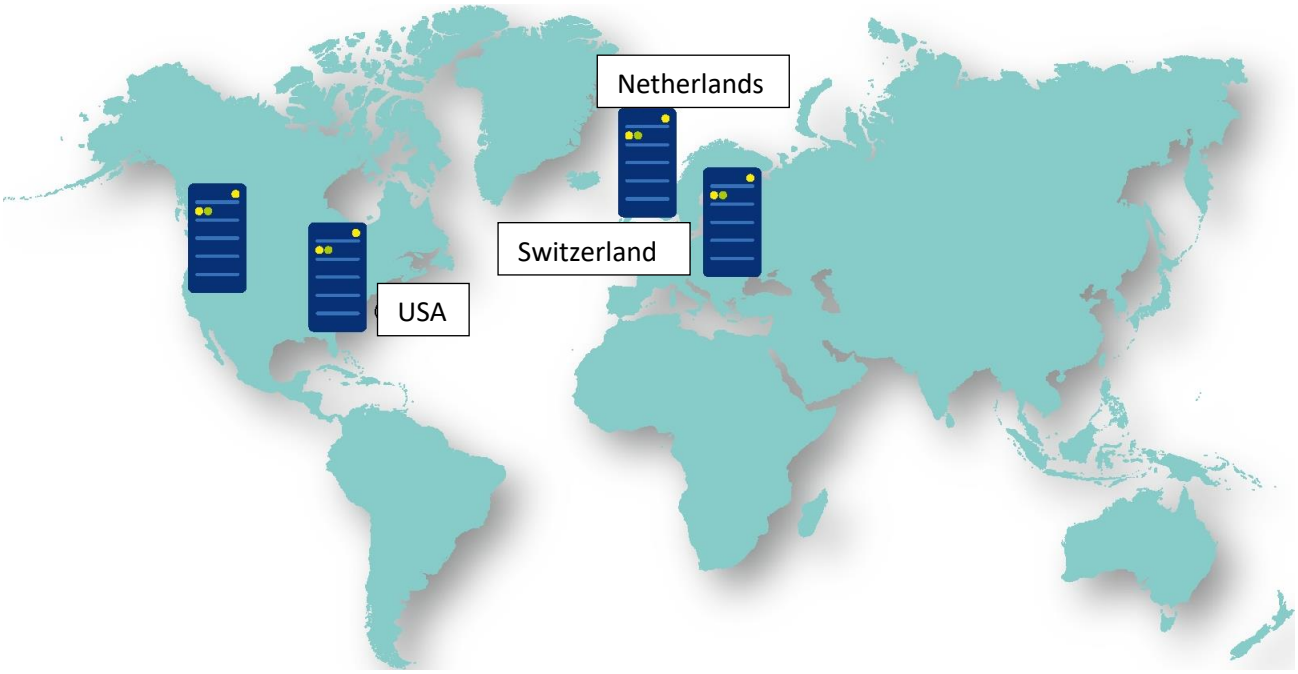
- Go to the website section “Registration of a new dealer”, fill in the registration form and register Login and Password.
- After initial registration, gain access to the “Agent's Cabinet” section. Using your Login and Password, you need to edit your company's data, register an administrator, generate a set of electronic digital signature keys and receive a package of necessary documents (application and certificate of receipt and transfer of electronic keys) in PDF format.
- After signing the application and the certificate as a part of the full package of documents, you must send them by registered mail to the CyberPlat® office.
- The company's specialists will check the correctness of the documents, activate a new agent and, having signed the application and the certificate from their end, will send a copy to the addressee.
- The agent can independently register their payment acceptance outlets and cashiers in the system through the “Agent's Cabinet” and start accepting payments either through the web interface or using the program “Payment Acceptance”, which must be downloaded from the website www.cyberplatru and configured.

All automatic registration procedures are performed using the ergonomic interface optimized to the fullest extent and take less than five minutes in total. If you have encountered even the slightest problem at any stage of registration, you can consult by phone with the CyberPlat® support service specialists listed on the website http://www.cyberplat.ru/jom/dealer/about_reg/.

CYBERFT - A CONVENIENT AND SECURE FINANCIAL MESSAGING SYSTEM

CYBERFT PLATFORM

CyberFT platform is a high-tech Russian development, which is an IT platform supporting the most modern data exchange formats, including SWIFT InterAct, SWIFT FileAct and SWIFT Fin (all documents of the MT category), as well as packages of documents in Bank of Russia formats required to provide remote banking services, with the ability to create new banking services.



SWIFT: EXISTING LIMITATIONS

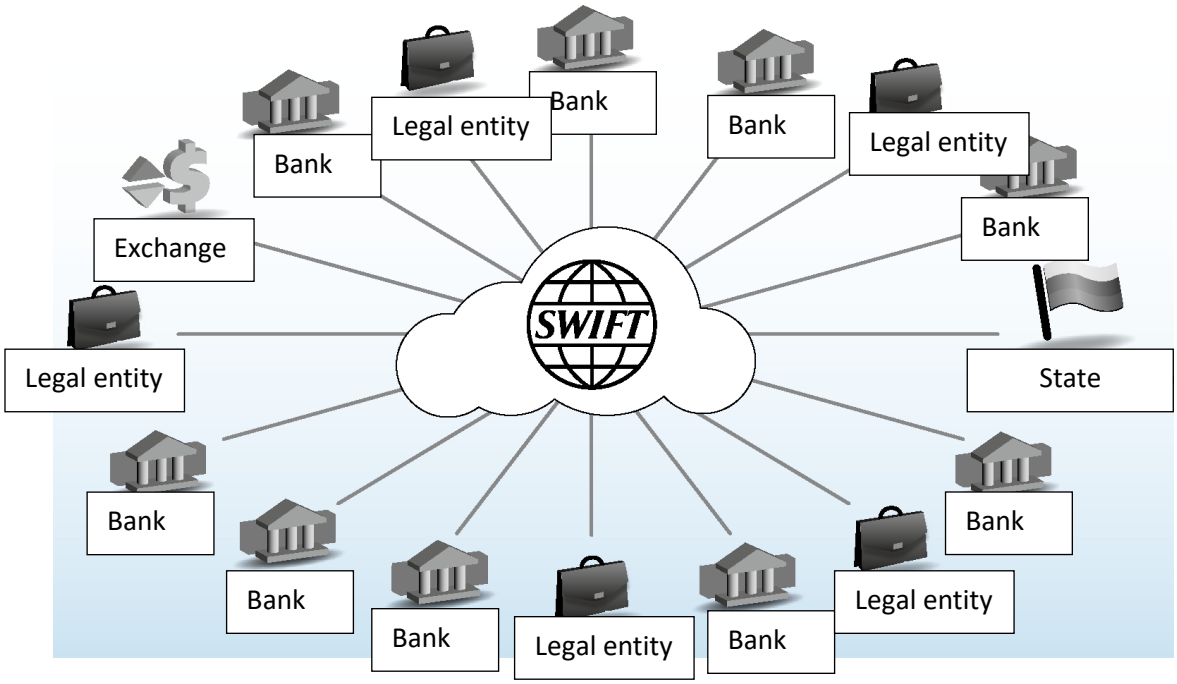
Prior to Edward Snowden's speech on mass surveillance, the banking community gave little thought to the risks and limiting factors existing and related to using the SWIFT international banking messaging system.

- Monopoly of the SWIFT system occupying about 90% of the market.
- High political dependence (examples: disconnection of Iran in 2012, regular threats against Russia, especially during the period of sanctions).
- An outdated SWIFT network topology, the so-called star, which reliability is threatened in the event of a targeted attack.
- In total, there are 4 data centers, located in three countries (USA, the Netherlands and Switzerland).
- Legislative restrictions: information on domestic payments must not leave the country in accordance with Federal Law of the Russian Federation 161-FZ “On the National Payment System”.
- Changing the encryption method at the choice of the system participant is impossible.
- Availability of the transmitted data to the network operator, which creates risks of large-scale leakage of commercial information.

- Difficulties in recognizing the transmitted messages as legally significant.
- Limited period of data storage on the SWIFT side before they are transferred to the archive is up to 121 days.
- Non-flexible message formats and complicated adaptation to the specifics of the formats of a particular country.
- High cost of connection and maintenance.

For many years, security specialists have drawn attention to the vulnerability of such an arrangement and the legal prohibition of local (in-country) banking information leaving the territory of their country in all developed countries of the world. For example, in the countries of the European Union, personal information (financial transactions often contain personal data) cannot be processed in a country located outside the European Union, if the latter does not provide an adequate level of personal data protection. In early 2011, the People's Bank of China (PBOC) issued a Notice to Banking Financial Institutions demanding the protection of financial information. The document, among other things, prohibits banks from storing, processing or analyzing any personal financial information that was collected in China outside of the country.

Thus, domestic interbank communication networks must be independent, otherwise the sovereignty of the country is threatened and may depend on unfriendly actions taken by the United States or other forces.

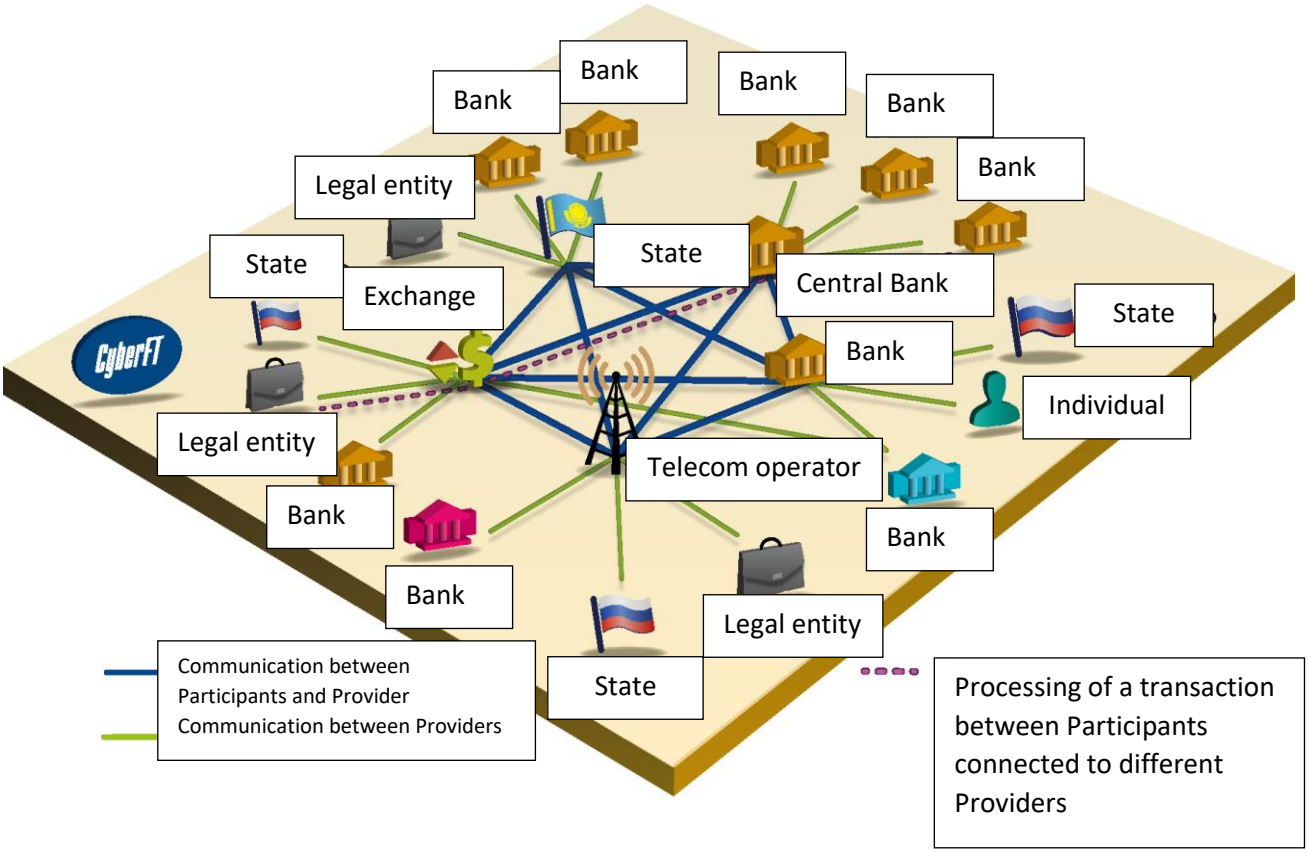


A NEW APPROACH TO FINANCIAL MESSAGING

CyberFT is a universal system for secure electronic exchange of financial data and legally significant documents between financial institutions, government authorities, legal entities and individuals (www.cyberft.ru).

Unlike many other systems operating on the world market, this software was developed by Russian specialists and has license and patent independence.

The terms of cooperation are premised on the fact that all servers of the CyberFT platform will be located on the local territory of a country which buys the platform, therefore, the probability of a leak of commercially important data in electronic document circulation is reduced dramatically.



KEY DEFINITIONS

• A software and hardware solution implementing a secure data highway for the transmission of any types of electronic messages.	• A legal entity, a privileged CyberFT member that manages the Processing.	• A hardware and software solution implementing legally significant electronic document flow in the CyberFT Network.
CyberFT Platform	CyberFT Provider	CyberFT Processing
• A legal entity or an individual using the connection with the CyberFT Provider to exchange information.	• Software installed on the CyberFT Client side to interact with the CyberFT Network.	• The totality of Providers and Clients who have connected to CyberFT.
CyberFT Client	Client Software	CyberFT Network

CYBERFT, SWIFT AND SPFS

The first release of the CyberFT system was issued in 2014 and from the start combined the near-complete functionality of SWIFT Fin with a number of additional options developed using the most modern technologies not available in SWIFT. Towards the end of 2014, the Bank of Russia, in response to the sanctions and threats to disconnect Russia from SWIFT coming from the West, developed a service for transferring financial messages SPFS, presented to the banking community as a full-fledged replacement for SWIFT on the territory of the Russian Federation.

Thus, CyberFT competes with two systems at the same time. On the one hand, the platform successfully proves its advantages over a system with a long history and an extensive customer base, which is also extremely inflexible, outdated and complex in terms of applied technologies, as well as expensive and politically dependent. On the other hand, CyberFT competes with a young and under-functional system with strong administrative resources.

	SWIFT	SPFS	CyberFT
Clients	Around 10 thousand banks and a limited number of legal entities	Credit institutions and their branches - clients of the Bank of Russia (only those possessing SWIFT BIC)	Potential coverage of all banks and legal entities with no limitations
Geography of services	Worldwide	Russian Federation	Worldwide
Compliance with the legislation of the Russian Federation	Does not comply with Part 11 of Art. 16 ФЗ № 112-ФЗ dated May 5, 2014 “On Amendments to the Federal Law “On the National Payment System”	Fully complies with all regulatory legal acts of the Russian Federation	Fully complies with the legislation of the Russian Federation
Working hours	24x7	Closed from 21:00 to 7:00 Moscow time, as well as on weekends and holidays	24x7
Encryption	CIPF encryption from SWIFT	CIPFs used in the transmission of electronic messages in the payment system of the Bank of Russia (SKAD “Signatura”)	Any interchangeable CIPFs, including CryptoPro, OpenSSL, Message-PRO, Agave, etc.
Message security	The transmitted data is available to the network operator	The transmitted data is available to the network operator	The transmitted data is not available to the network operator
Location of	USA, Switzerland and	Russian Federation	Russia, as well as

servers	the Netherlands		additionally anywhere in the world at the discretion of the platform owner
Reliability	Special procedure for receiving and transmitting messages due to the hot-standby operation of each element of the network. 4 data centers in total	Transmission of messages through the Bank of Russia Message Processing Center (MPC) using the Bank of Russia Customer Interaction Environment (ICS). All information systems of the Bank of Russia have backups. However, given the fact that a number of technical messages were developed to check the operation of the service together with the ED503, it can be concluded that the system's reliability is poor.	Effective modern software, hardware and organizational and administrative measures to ensure the reliability of the system. The number of providers is not limited
Network topology	Star (there is a single center to which all participants are connected)	Star (there is a single center to which all participants are connected)	Fully connected (an infinite number of centers can exist in the system, to which various participants are connected, while the centers themselves are also interconnected)
Connection price	No less than $ 53 thousand, taking into account the obligatory cable installation from a specific communication service operator; up to $ 200 thousand for each new client	Free of charge	Free of charge
Transaction price	FIN service: local transaction of 0.02-0.05 euros, international transaction of 0.03-0.18 euros	Fee for the transfer of financial messages within the country in the SWIFT format is 1.50-2.50 RUB (0.026-0.043 euros)	No more than 50% of the price of a similar SWIFT transaction

Service price	No less than 10 thousand euros per year	Free of charge	Free of charge
Connection time	No less than 8 weeks with a collective connection. No less than 16 weeks with own connection	No less than 4-6 weeks, since a paid revision is required on the ABS side to transfer data to the terminal	Connection to CyberFT processing takes from 1 to 3 weeks, including integration with ABS. When installing your own platform - no more than 2 weeks
Block rate	Several seconds	Several seconds	No more than 1.5 seconds
Supported formats	Envelope for messages in the SWIFT Fin format (MTXXX messages). At the same time, the correctness of the information entered is not checked as per the SWIFT rules, that is, in fact, any message can be placed in the envelope.	Envelope for messages in the SWIFT Fin format (at the same time, the correctness of the information entered is not checked as per the SWIFT rules, that is, in fact, any message can be placed in the envelop)	SWIFT Fin service (MTXXX messages), InterAct service (MX messages in ISO 20022 standard, adapted for Russia), FileAct (unstructured messages with attachments), as well as EDF documents (certificates, invoices, contracts), acceptance of payments and much more
Maximum size of one message	No more than 10 MB	The default maximum size is 20KB. The maximum possible size for a separate authorization is 5 MB	The basic setting for the maximum size of a single message is 100 MB. If necessary, this limit can be increased to any size
Data storage	The period is not limited on the client's side, the data is stored for 124 days on the SWIFT processing side, and then archived. Partial data can be obtained from the archive on a paid basis, but not at all times	Electronic messages are stored in the operational archive for 3 days, in the long-term archive – for 5 years	Perpetual storage of data on all stages of the transaction from the sender to the recipient
Interaction type	Processing only	Processing only	Processing and clearing
User interface	Several options for custom SWIFT Alliance applications	The mode of financial message transfer in SWIFT format through AWS KBR	Convenient web interface for full-fledged work with the system

	for full functionality	(KBR-S) using the file system directories or the UM MQ queue manager, messages are received in transport envelopes on the servers of the Bank of Russia ICS. For real commercial operation, the improvement of visual interfaces for the user and operator is required	
Additional services for legal entities	Preferential working conditions for corporate clients in comparison with banks, SWIFT Alliance Lite software, etc.	None	Preferential working conditions for corporate clients, specialized 1C module, service of electronic document management of legally significant documents
Development and revision speed	Very slow, custom modifications and integration modules are not offered	Mediocre, custom adjustments and integration modules are only offered for large members	Prompt, standard integration modules, individual modifications and integration solutions are provided. Individual developments are possible on a typical CyberFT platform

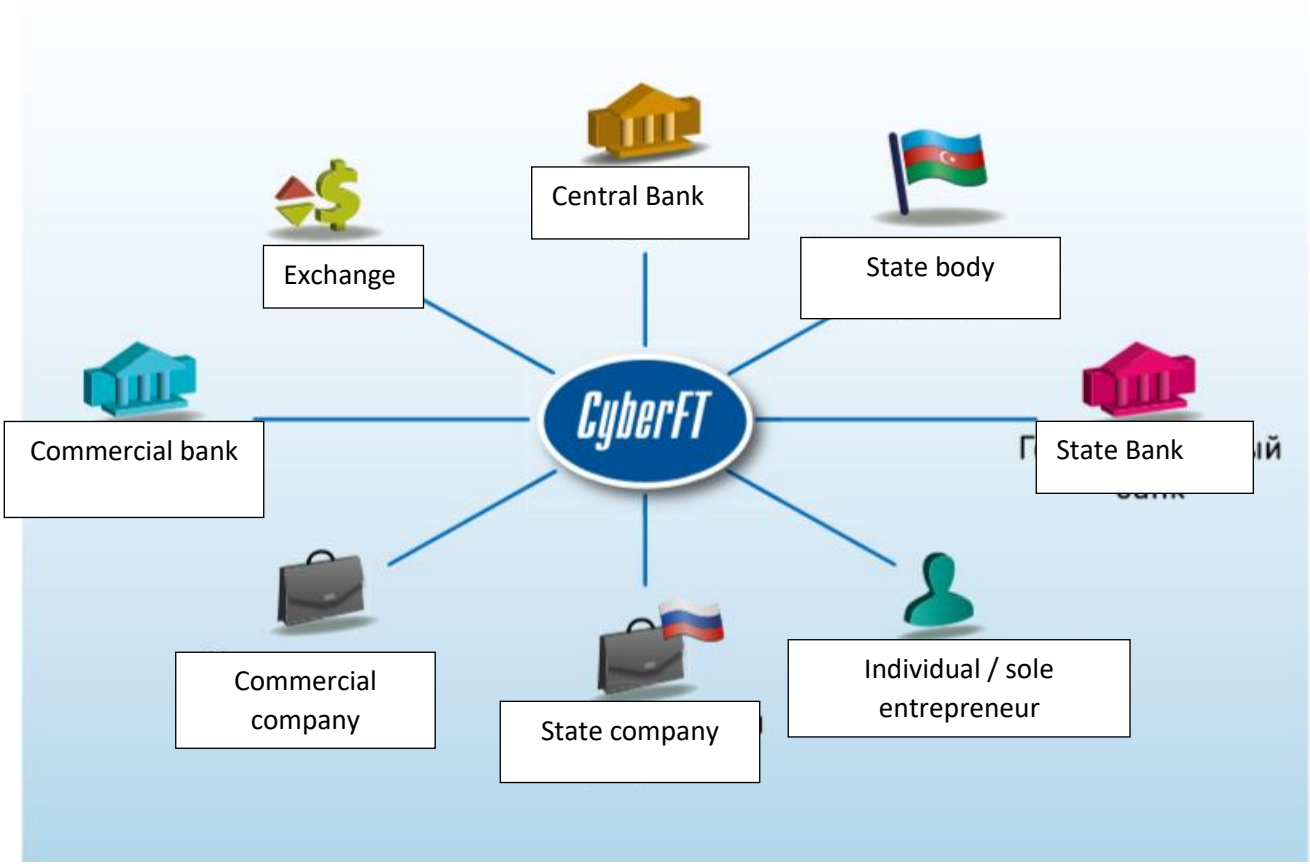
MULTIPLE PROVIDER SYSTEM

The CyberFT network consists of an unlimited number of clients (participants) using the CyberFT platform for electronic document flow management.

The CyberFT platform is deployed at the buyer's platform and is independent of CyberPlat®. The CyberFT provider can serve banks and legal entities anywhere in the world or work within a separately selected banking or corporate group.

Both banks and corporate clients, exchanges, brokers, government bodies and other organizations can act as CyberFT providers and participants. Each participant is assigned a unique identifier according to the SWIFT rules (if the participant is not registered in SWIFT), otherwise the existing identifier of this participant in the SWIFT network is used.

The directory of network participants is available to each participant and is updated automatically on a centralized basis. The identifier is unique not only within one provider, but throughout the whole CyberFT network.



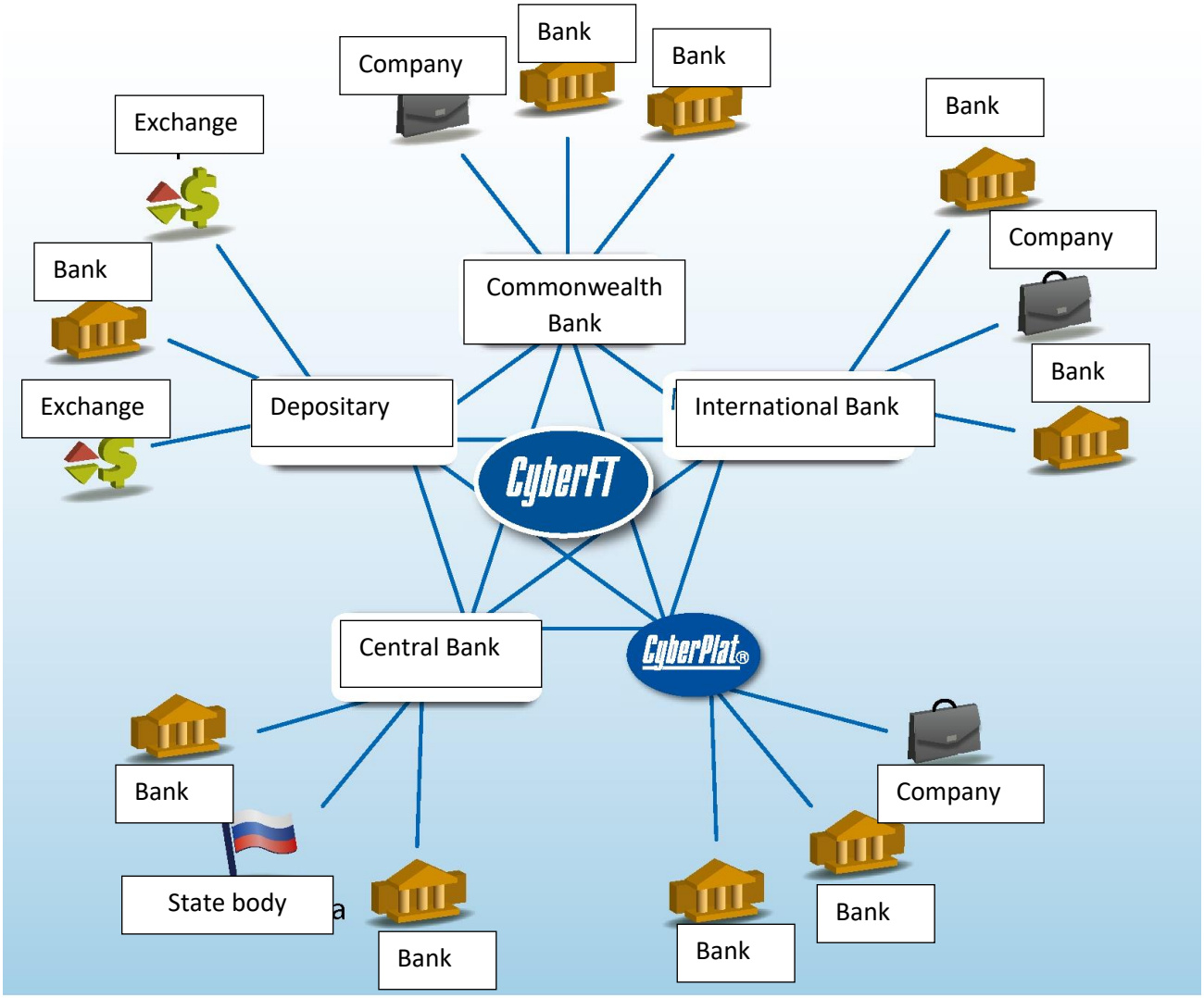
Thus, a participant with a specific identifier can only be connected to one provider, which ensures the integrity of the network.

CyberFT providers can connect to each other in various ways, some of which are presented below.

1. Everyone to everyone*

Information on the processing of each message is logged on the side of each provider participating in its transmission. In addition, the messages themselves, are stored together with the sender's electronic signatures on the side of the sender, recipient and provider for an unlimited period of time (on the provider's side, all messages are stored in an encrypted form, and their content is not available to the provider). Thus, each participant in the information exchange process has full legally significant electronic documents.

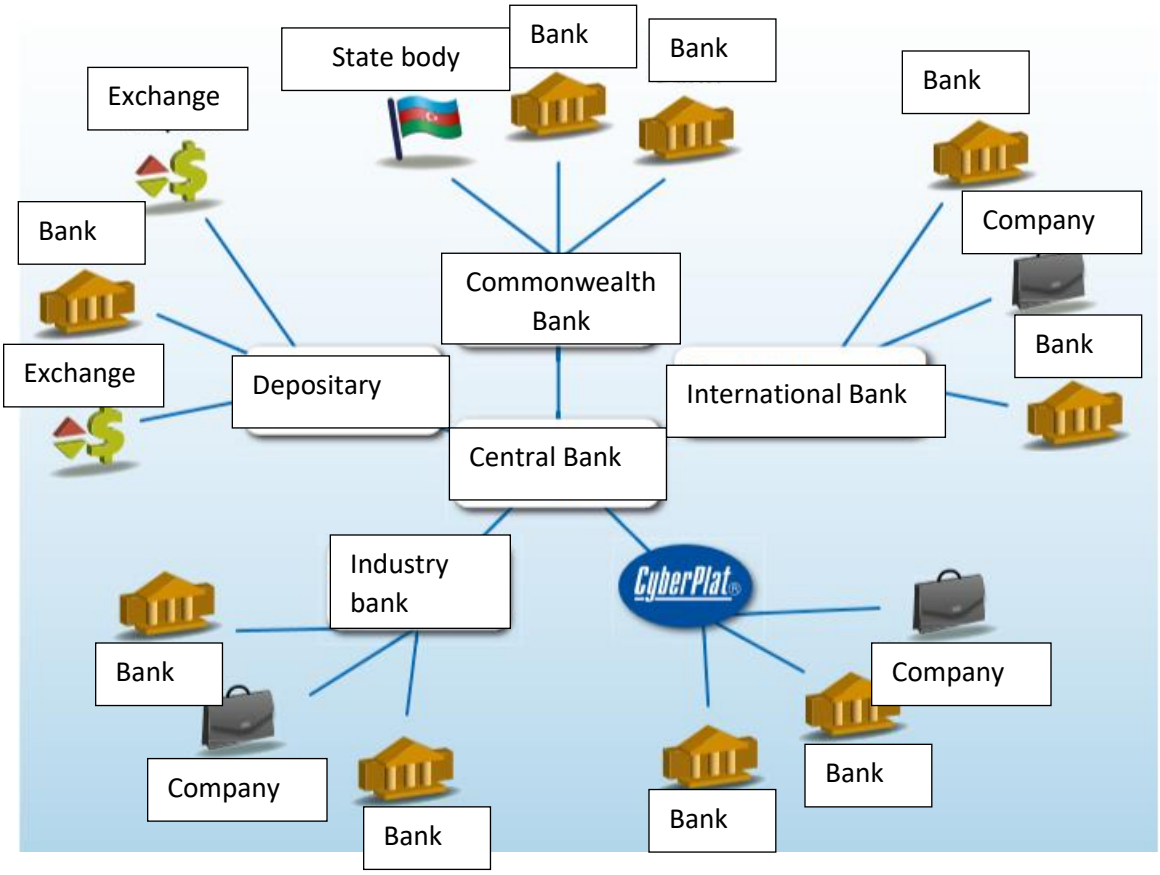
* Here and elsewhere: the names of organizations are given as an example



2. Through a centralized CyberFT provider selected jointly

For example, any large banking group or commercial organization can become a CyberFT provider and connect subsidiaries, correspondent banks and customers. At the same time, in order to exchange data between participants connected to different providers, these providers enter into an agreement with a single provider (for example, the Interstate Bank), which is responsible for routing messages between them.

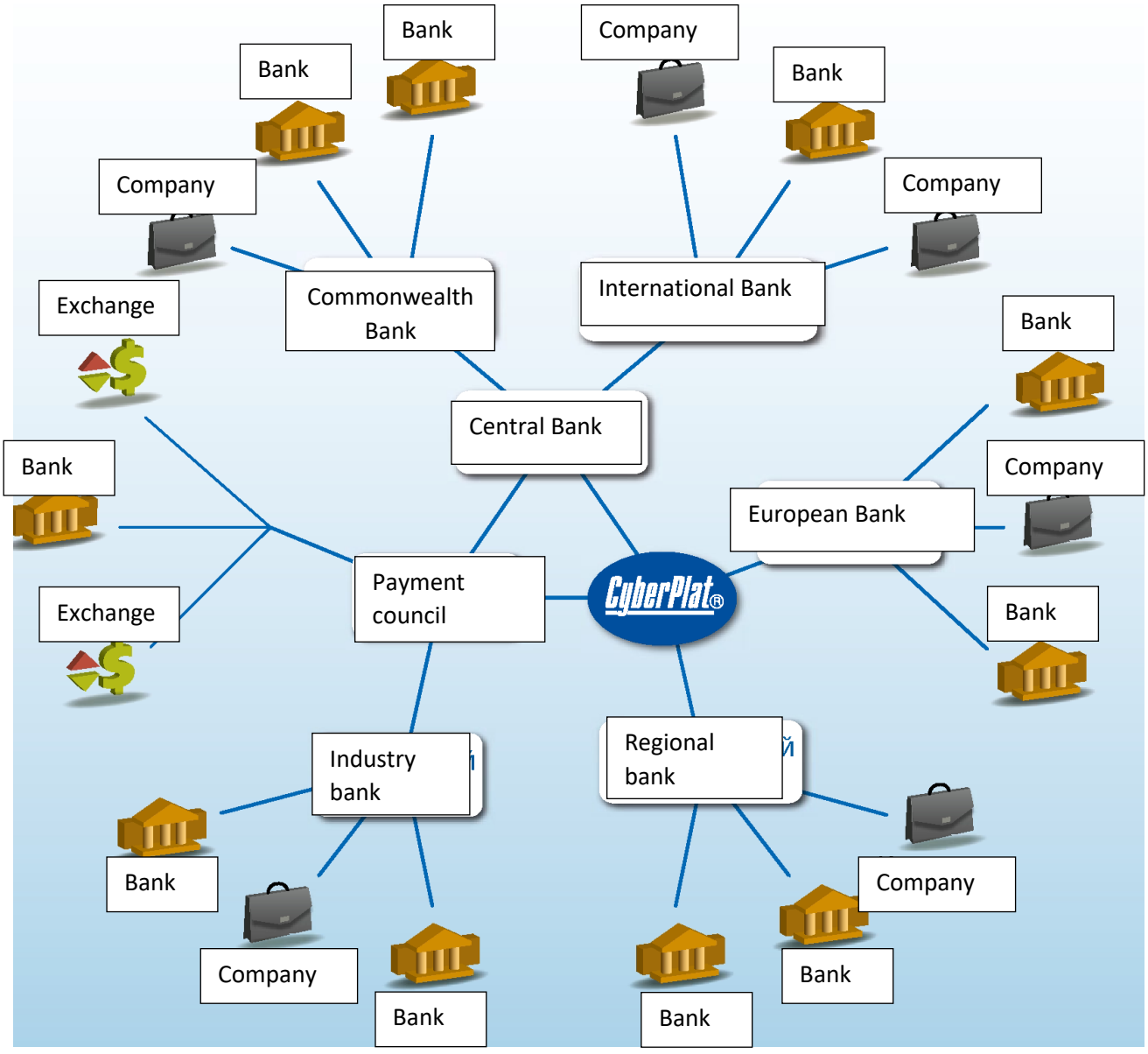
On the one hand, such a network topology greatly simplifies the organizational aspects associated with establishing relations between providers, and makes it possible to work through a single organization (central provider), trusted by all participants. On the other hand, in the event of a failure on the side of the central provider, communication between network participants becomes impossible.

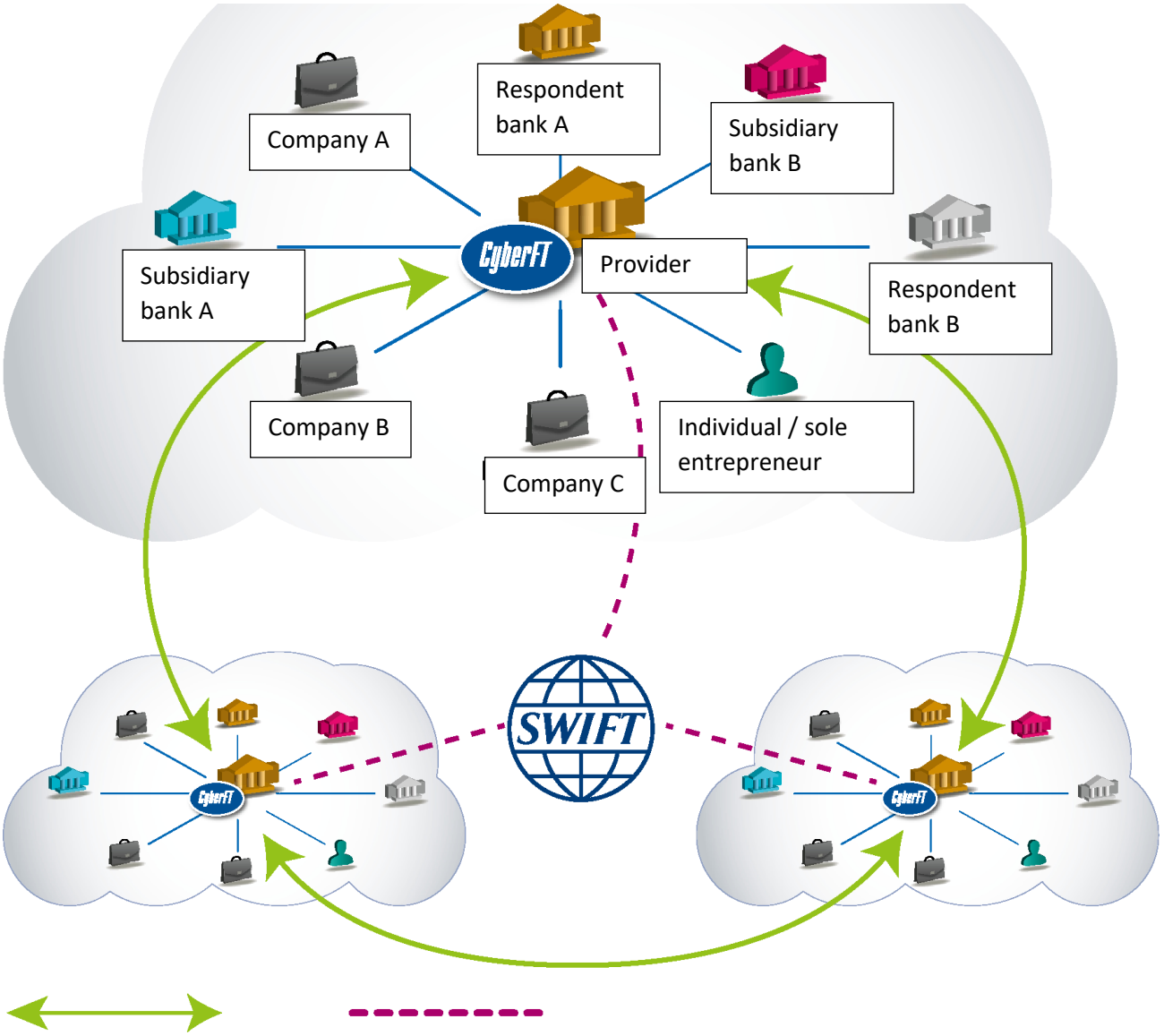


3. Through a group of interconnected CyberFT providers

This version of the network topology, in disregard of the organizational processes of establishing relations between providers being more complex, has increased fault tolerance. In case of technical issues arising on the side of one of the central providers, communication between all CyberFT network participants will not be disrupted.

CyberFT network participants can also interact with other counterparties connected to the SWIFT system. One of the examples of such interaction is shown in the figure.





Communication between CyberFT providers

Communication between CyberFT and SWIFT providers

Thus, the CyberFT network allows its participants to interact through the SWIFT system, if one of the parties is not yet connected to CyberFT (see the section on integration and interaction with SWIFT).

FLEXIBILITY

The CyberFT network is needed not only by the banks, which receive a safer, more reliable, functional, flexible and cost-effective solution, but also by the clients of financial institutions.

Large and medium-sized companies that work simultaneously with several banks are currently forced to support many different Client-Bank systems, as well as use various data exchange formats and data cryptographic protection facilities. CyberFT allows them to organize the “Universal Client-Bank” system for such companies.

In practice, it means that drawing up a financial document (or message) and selecting the required settlement bank, following which the document will be sent via a single channel to this bank, is sufficient. Through the same channel, the client will receive centralized feedback from their settlement banks (statuses on the sent documents, statements, etc.). Thus, companies will be able to interact with banks directly through their accounting systems, as well as apply uniform technologies in the exchange of data.

CyberPlat® has also developed a payment module for the 1C system, which allows customers to manage accounts in their settlement banks remotely and directly from 1C. At the same time, the transfer of information between 1C and the bank is carried out through the CyberFT network.

Within the framework of a unified transport solution the CyberFT network offers a possibility of managing legally significant electronic document flow. CyberFT allows optimizing business processes involving the exchange of documents with government authorities: tax reporting, customs declarations, interaction with the IEIS state system, etc., as well as intercorporate communications, including the signing of contracts, provision of reporting documentation, filing exchange bids etc.

It is also possible to construct such CyberFT-based solutions required by corporate clients as interbank physical Cash Pooling.

SAFETY

CyberFT is the warrantor of the safety of important commercial information. One of the key tasks of the CyberFT network is to ensure the security of information containing banking and commercial secrets. According to the forecast of Zecurion, by the end of 2018, the total losses of companies and banks from leaks of confidential information may exceed $ 50 billion.

Important commercial information processed by payment systems and passing through communication channels is exposed to a number of threats.

1. Security threat to the interbank communications, since the vast majority of SWIFT transactions pass through servers located in the United States, the Netherlands and Switzerland.

Hosting servers in these countries puts SWIFT clients in other countries in an extremely vulnerable position, since the servers can be turned off at any time (for example, when the political situation changes), which will not only make data exchange with foreign counterparty banks, but also internal exchange financial information via SWIFT system cease.

2. Threat of theft directly from the system processing and conducting payments.

Information can be either “taken”" at the request of the special services of a foreign state, or intercepted by malevolent intruders or other attackers on any part of communication lines, the length of which can be up to 20 thousand kilometers. This information, usually related to the information covered by bank secrecy, can be used by both the thieves themselves and the persons who intercepted it from the thieves (which is the case in high-profile international scandals of recent times).

3. Threat of “leaking” of previously stolen information.

High-profile scandals of recent times (for example, the Snowden case or the emergence of WikiLeaks) indicate that commercial information available to special services often becomes publicly available.

4. Threat of information transfer to competitors.

An example of such a leak is the scandal that broke out in the 1990s in the United States, where Airbus lost a $ 6 billion contract with the national airline of Saudi Arabia as a result of negotiations being intercepted by the National Security Agency. The contract went to McDonnell Douglas, a division of Boeing, Airbus's main competitor.

5. Threat of selling stolen information.

Information is a valuable commodity and the more value it has, the more it is worth. Therefore, information containing commercial and banking secrets is a “tasty morsel” for international cybercrime participants. Protection against these threats is regulated by the laws of a number of countries, prohibiting the transfer of local financial information to the territory of a foreign state or providing access to it from the territory of a foreign state.

Using the CyberFT platform significantly reduces all risks of theft, loss and sale of important information owned by banks and their clients. Since the hardware will be located in the computer center of the platform buyer, the threat of theft of commercial information from the servers of the communication center is significantly reduced, and since the communication channels become much shorter, the risk of theft of commercial information from communication lines is also significantly reduced.

The text of the message sent by the client through the CyberFT network and not addressed to the CyberFT provider is available only to the recipient of the message - another CyberFT client.

SUPPORTED FORMATS, FLEXIBILITY AND VARIABILITY OF DEVELOPMENT

At the moment, the CyberFT network has fully implemented the SWIFT Fin service, which includes the following message groups:

- 1st (customer payments and checks);
- 2nd (transfers of financial institutions);
- 3rd (financial resources markets - forex, money markets and derivatives);
- 4th (collection of payments and cash letters);
- 5th (securities markets);
- 6th (transactions with precious metals and syndicated loans);
- 7th (documentary acceptance credits and guarantees);
- 8th (traveler's checks);
- 9th (cash management and client status);
- acceptance of CyberPlat® payments.

The system supports the SWIFT InterAct service, that is, the exchange of messages in SWIFT MX formats (ISO 20022 standard), and the SWIFT FileAct service (the exchange of unstructured messages containing attachments with sizes of up to 100 MB).

The CyberFT system contains whatever is required to ensure information interaction between payment agents and banks when receiving payments.

The system supports a package of documents required for the provision of remote banking services (RBS) in Bank of Russia formats.

Among the areas of development of the system, there is provision of secure complex information interaction in specialized areas of business. In CyberFT, you can exchange structured and unstructured contracts, certificates, invoices and other types of documents. As a result of integration with internal automated workflow and records management systems, organizations can implement end-to-end electronic document flow management. The CyberFT system allows concluding and completing transactions in an electronic form in accordance with the applicable law.

However, the CyberFT platform is not limited to SWIFT capabilities. Movement of interbank information can reserve as many “information bands” (categories of messages) as customers need, taking into account the specifics of their activities. The ability to adapt to customer needs is the cornerstone of building any reliable and streamlined system such as CyberFT.

At the request of a customer, developers can implement the Direct Debit system available worldwide. Moreover, this system can be created either as a separate category, or as an addition to the SWIFT invoicing category, or in the format of the auto payment service.

At the request of holding companies, a solution within the CyberFT platform that allows to optimize the internal electronic document flow management, interbank Cash Pooling and other solutions demanded by the market can be developed.

CyberPlat® is analyzing the offers of market participants online and is developing CyberFT functionality taking into account the information received.

INTERACTION WITH SWIFT, EASY INTEGRATION FOR BANKS

When clients are connected to CyberFT platform, CyberFT client software can operate in parallel with SWIFT. A diagram of interaction between CyberFT and SWIFT systems on the client side is given below.

A special “Message Router” module in CyberFT software distributes outgoing messages between CyberFT and SWIFT automatically.

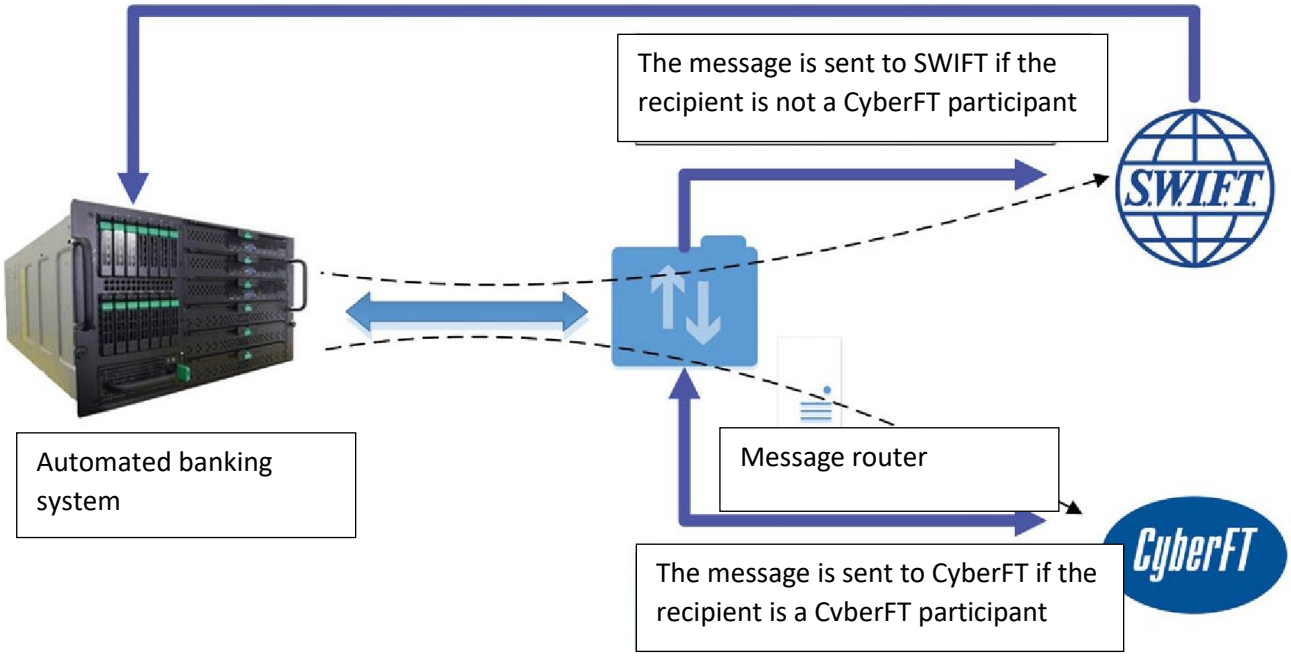
If the recipient of the message is not connected to the CyberFT network, the transaction is carried out through the SWIFT system.

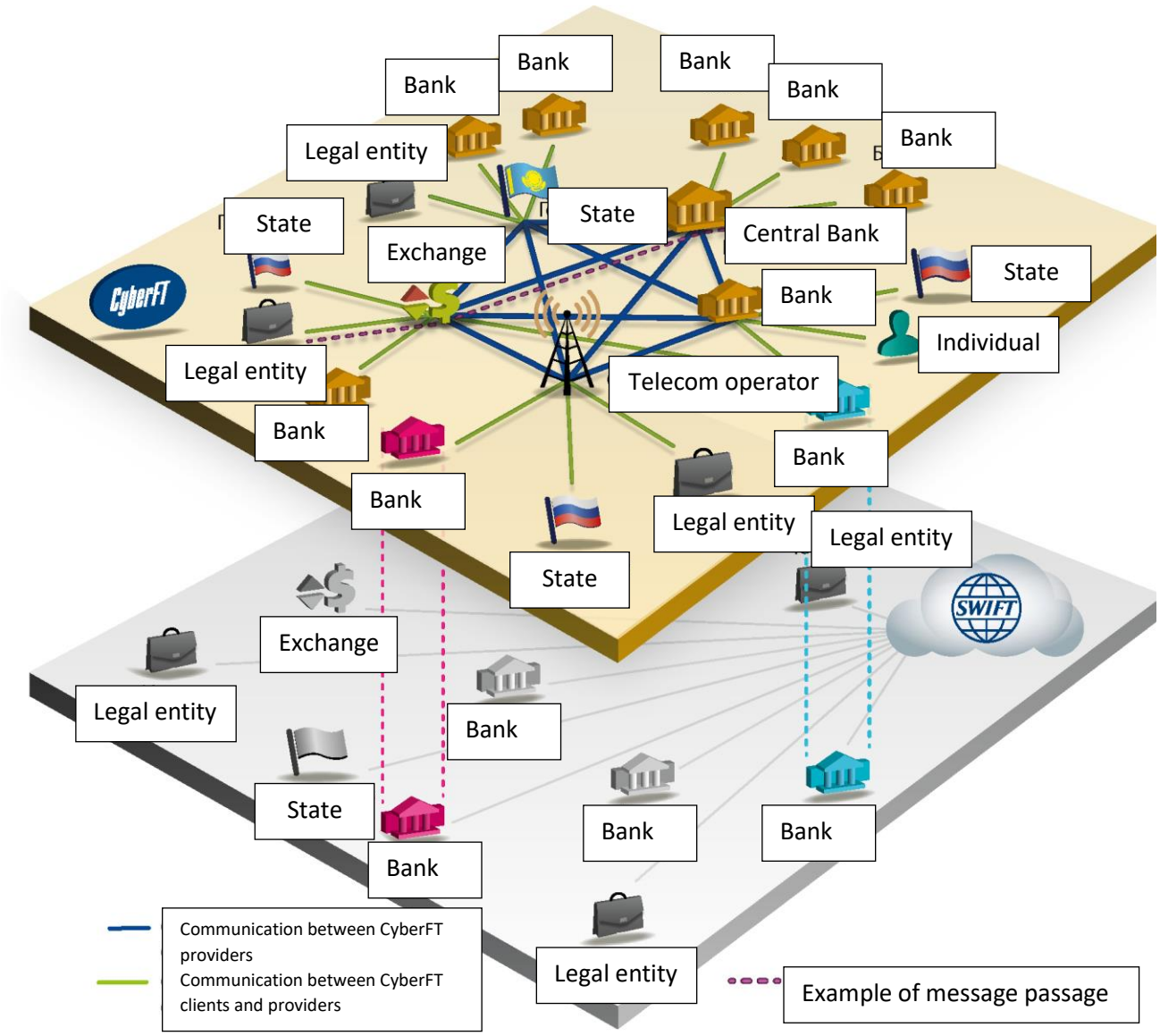
At the same time, the client can set flexible parameters that will allow sending outgoing messages strictly to SWIFT, even if the recipient of the message is a CyberFT participant: for example, to certain recipients, of a certain type or category, exceeding a threshold amount, etc.

Before using CyberFT

Automated banking system

Using CyberFT



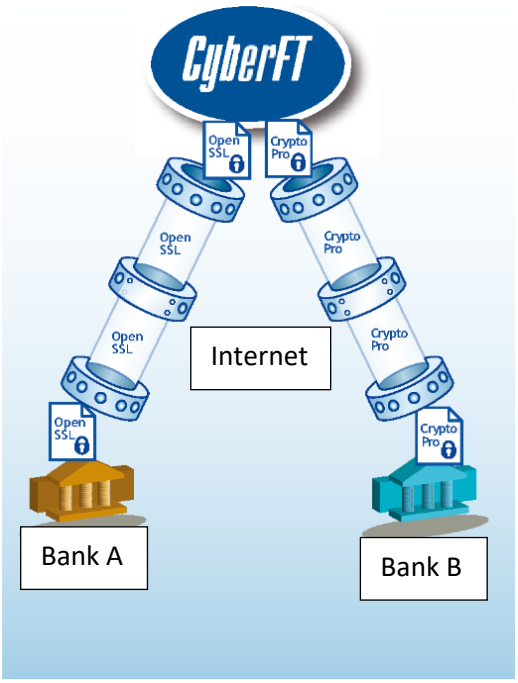


When a new participant is connected to CyberFT, the centralized directory of participants will be updated remotely in automatic mode. CyberFT software is provided to customers free of charge.

CyberFT easily integrates with all types of client-side accounting systems and can work together with SWIFT.

ACCESSIBILITY

The fundamental difference between the CyberFT platform and SWIFT is the departure from hardware encryption and the use of software encryption methods only.



Connection to the CyberFT network is carried out through a dedicated channel, VPN or public Internet connection, which allows the client to choose a network service provider freely and not be tied to a specific telecommunications operator.

Thanks to the approaches taken, if the connection is lost, its restoration will occur through a new channel within one minute automatically.

Interaction occurs in a protected form only through open Internet channels using the proprietary practices in the field of financial messages processing.

CyberPlat® uses HTTPS data transmission as the main network transport mechanism in its solutions. All transmitted messages are signed with electronic signatures.

This mechanism provides CyberFT customers and providers with the ability to connect without performing complex actions associated with setting up network equipment. In particular, this connection method allows you to connect to the CyberFT network through any proxy server.

On the counterparty's side, no additional network devices or, in most cases, no changes to the network security policy are required. The absence of additional approvals and engineering works ensures a high connection speed and makes it available for everyone.

Over the course of 20 years of operation of the CyberPlat® system, more than 12 billion messages have been transmitted through open channels using software encryption methods without a single case of hacking; this is why the interaction between the client and the processing in CyberFT is carried out via any Internet channels without any special equipment. The use of software encryption only and of any communication channels reduce the cost of connection to the CyberFT network dramatically. CyberPlat Company, CyberFT's provider, does not charge a connection fee, and the software is provided free of charge as well.

If necessary, dedicated communication channels can be used for making connection. For example, they can be used for payments of significant amounts between especially large customers. CyberFT platform developer recommends the following evaluation parameters.

- If the volume of payments is up to $ 1 million per day, there is no need for a dedicated channel.
- If the volume of payments ranges from $ 1 to $ 20 million per day, the need for a dedicated channel is determined at the discretion of the counterparty.
- If payments exceed $ 20 million per day or the transactions are time-critical (Forex, stock market transactions, etc.), a dedicated channel is recommended. In this case, the connection via the public Internet will be used as a backup communication channel.

The CyberFT system uses interchangeable (connectable) cryptographic information protection systems (CIPF), including OpenSSL and GOST algorithms (based on CryptoPro, Signal-COM, etc.). In addition, CyberPlat® is willing to connect any other means of crypto protection in the shortest possible time - within a few days.

COMPETITIVENESS

For the client, working in the CyberFT network is more efficient and cost-effective than using a foreign counterpart - the SWIFT system.

The transmission of messages in the CyberFT network with the CyberPlat® provider is two times cheaper than the transmission of such messages in the international SWIFT system. At the same time, no fees are charged for connecting to the CyberFT network or service.

Moreover, unlike SWIFT, CyberFT does not charge commissions for additional services such as providing data from the archive or, for example, assigning an identifier to a participant and including it in a centralized directory.

An unlimited number of users can work with the CyberFT client end, and there is no fee for connecting additional workstations. The module for integration with accounting banking systems is also supplied within the CyberFT client software free of charge.

The hardware requirements for working in CyberFT are significantly lower than those established by SWIFT, therefore, using the platform will reduce the cost of maintaining server and telecommunications equipment, as well as the cost of employing personnel servicing said equipment.

CURRENT SITUATION WITH SETTLEMENTS IN THE RUSSIAN FEDERATION

The settlement system currently existing in Russia does not fully meet the needs of the economy for timely payments. Comparing the existing parameters of payments passing through the Interregional Information Processing Center (IIPC) of the Bank of Russia with the experience of other countries in order to illustrate this statement is sufficient.

Market size (capacity)

According to unofficial information, the Bank of Russia processes 600 million payments from commercial banks for a total of 900 trillion RUB per year. Up to 80% of the total number of payments (400 million) are settlements for amounts not exceeding 100 thousand RUB. In total, these payments make up less than one percent of the total turnover (only 6 trillion RUB).

Cost of making payments in the Center for Interbank Settlements of the National Bank of the Republic of Kazakhstan, given in KZT and RUB

Payment processing time	Cost, KZT	Cost, RUB
from 4:00 pm to 9:00 am	9	2,8
from 9:00 am to 1:00 pm	11	3,4
From 1:00 pm to 4:00 pm	22	6,8

Cost of payments for banks

The minimum payment cost for banks is 7 RUB, and the average payment cost is 12 RUB. The total costs of banks for the services provided by the Bank of Russia IIPC for small payments amount to 4.8 billion RUB, and according to the lowest estimates - 2.8 billion RUB. A decrease in this figure will have a favorable effect on the structure of banks' expenses, i.e. increasing the stability of the banking system as a whole.

At the moment, the cost of payment through the Bank of Russia IIPC is:

- from 7 to 24 RUB for per-transaction processing, the duration of payment is from one to several hours;
- 25 or 30 RUB in case of online BESP (does not operate at night and on weekends).

Undoubtedly, the current tariffs are too high and can potentially be reduced by several times - as proved by the cost of similar services in neighboring countries.

Let us consider, for example, the tariff classification of similar services in the Center for Interbank Settlements of the National Bank of the Republic of Kazakhstan. At the same time, all settlements between banks in Kazakhstan are carried out in real time and take no more than a few minutes.

Thus, the cost of an urgent payment in Russia is 3.6 (!) times higher than the most expensive payment in Kazakhstan. Processing of all payments in the Center for Interbank Settlements takes a few minutes, and up to 9 hours in Russia.

This is obviously the case because Russia does not currently have a full-fledged system of online interbank settlements.

It should be noted that the creation of a continuously operating system for processing small non-cash payments has become not only necessary, but also practically feasible. The technological development leads to the fact that the cost of payment processing can be significantly reduced and brought to a level at which it will become available to each and every market participant with no exception (according to our calculations, no more than 1 RUB per payment).

Economy cut for banks will amount to an average of 4.4 billion RUB or at least 2.4 billion according to the most pessimistic forecasts. It should be borne in mind that processing relatively small payments entails much lower risks and, therefore, requires less effort in terms of organizing physical security and payment control. This circumstance makes it possible to isolate this type of settlements within the framework of a separate system, which should be reliable on the one hand, and cost-effective and economically profitable for the participants on the other.

SOFTWARE REQUIREMENTS [*]

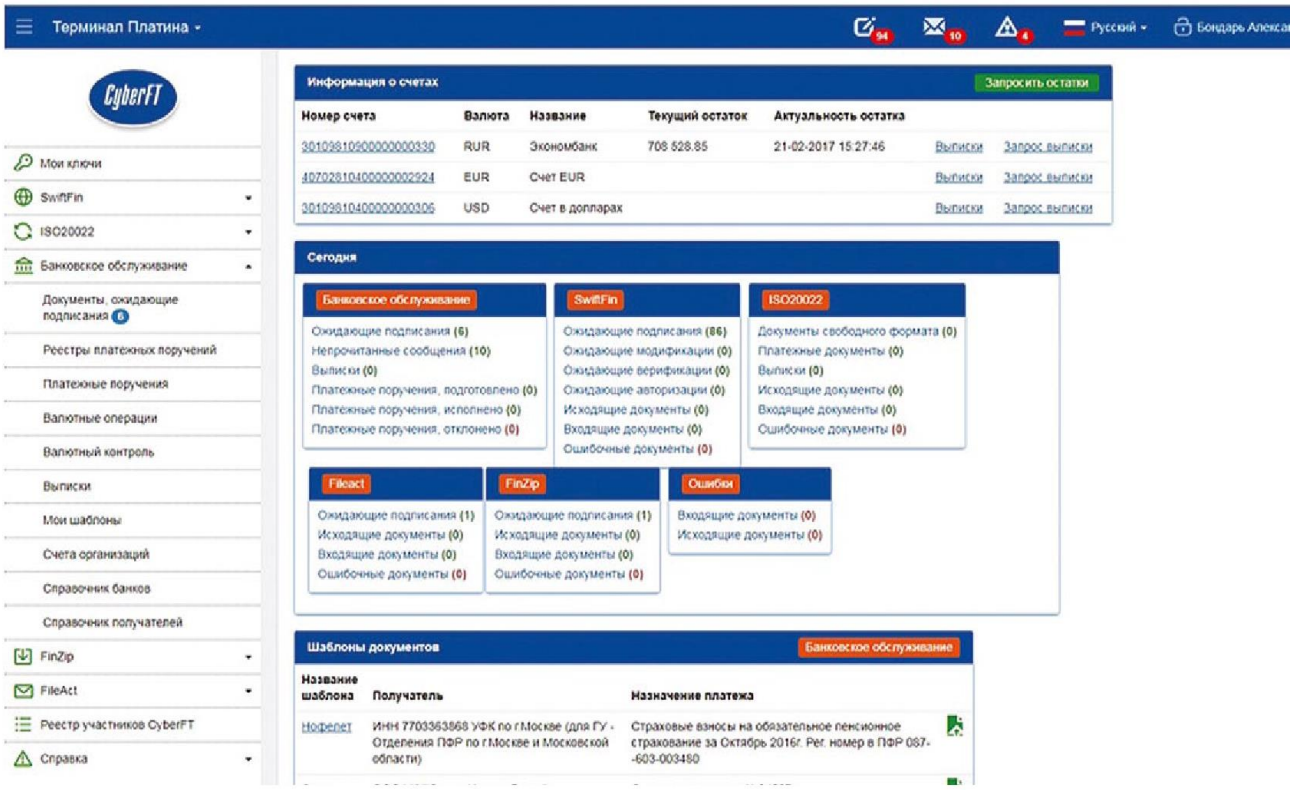
The CyberFT platform is designed for mass use by market participants, therefore, minimum system characteristics are required: a simple workstation and a web browser are sufficient for the system to be operated by users.

CyberFT terminal software requirements:

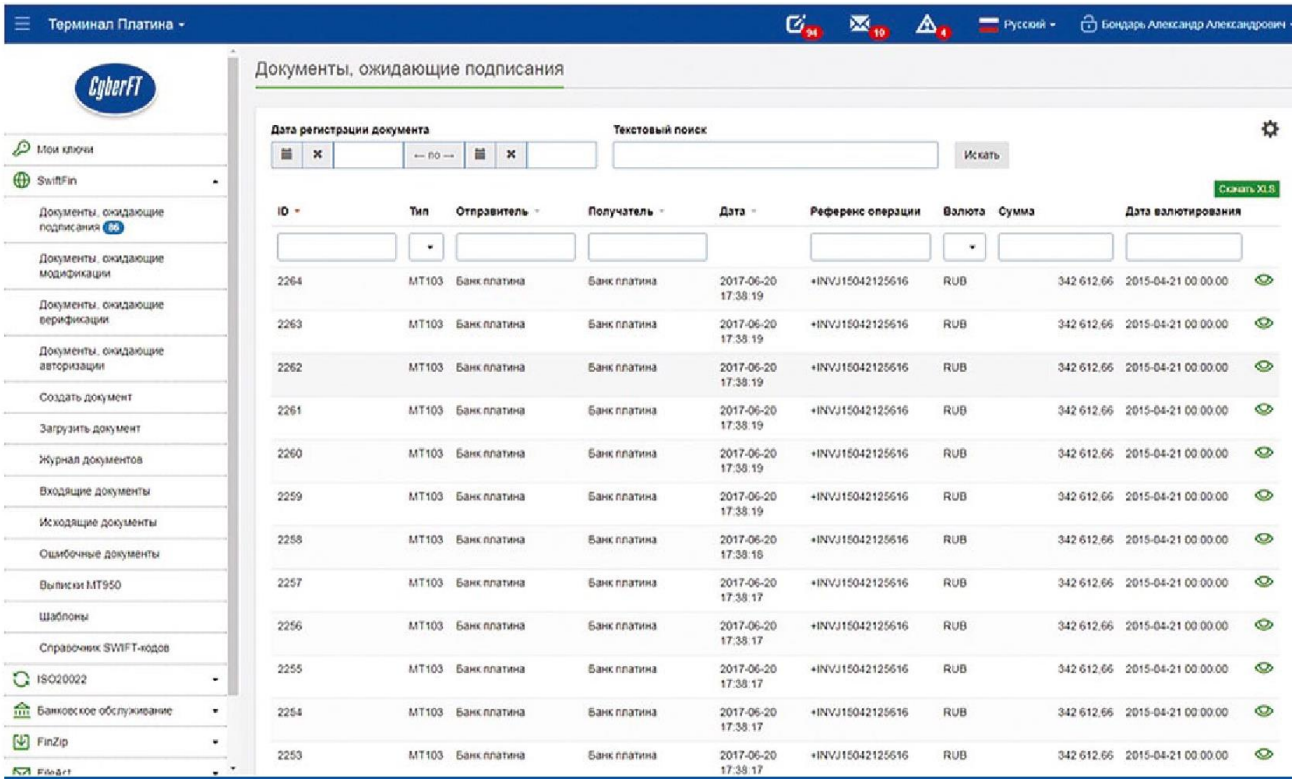
- Debian GNU / Linux 7.6 (wheezy) Release: 7.6;
- ext3 or ext4 file system;
- installation of software on a virtual machine is possible!

CyberFT terminal hardware requirements:

- x86-64 processor architecture;
- At least 4Gb of RAM;
- Multi-core CPU at the level of Intel Core 2 Duo 3.0 Ghz or higher;
- Not less than 40Gb of hard disk capacity.

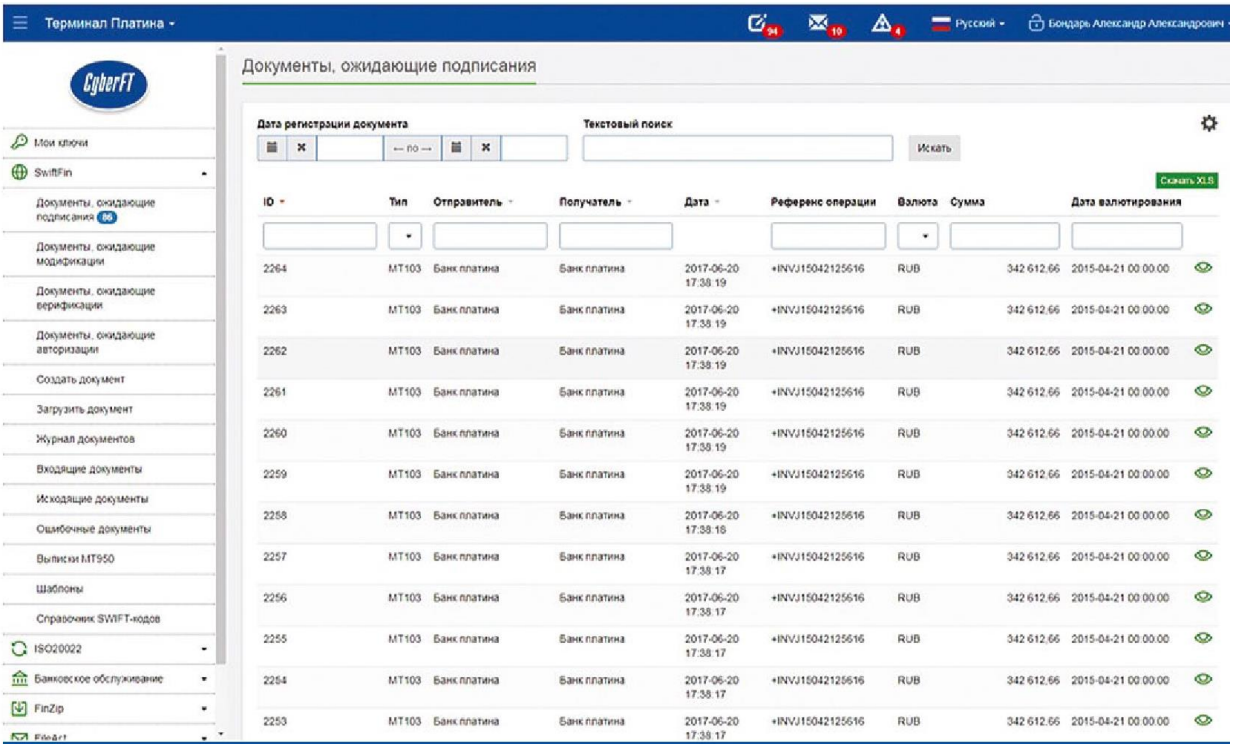


MAIN MENU

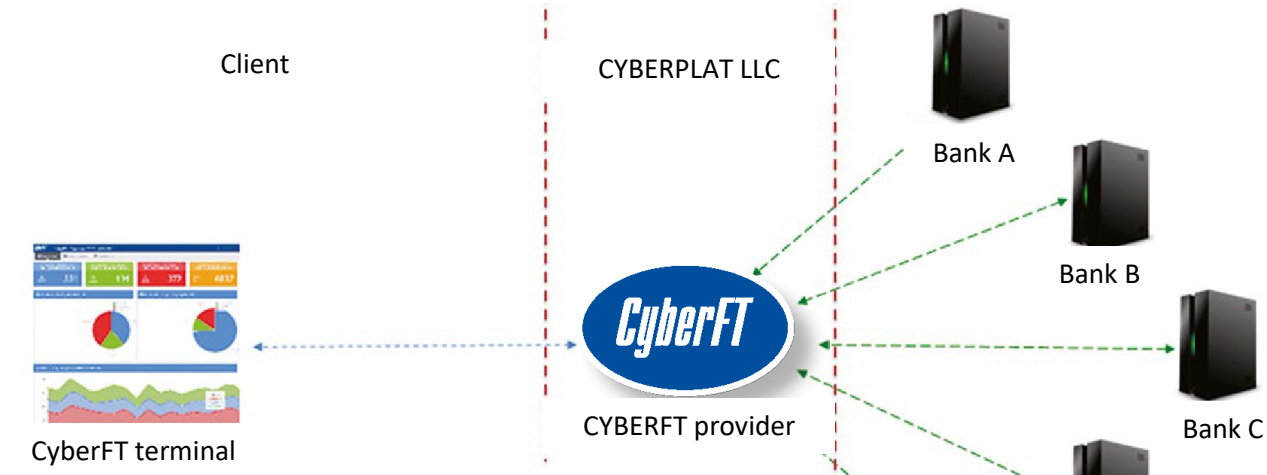


DOCUMENT LOG

CYBERFT TERMINAL



WORKING WITH DOCUMENTS

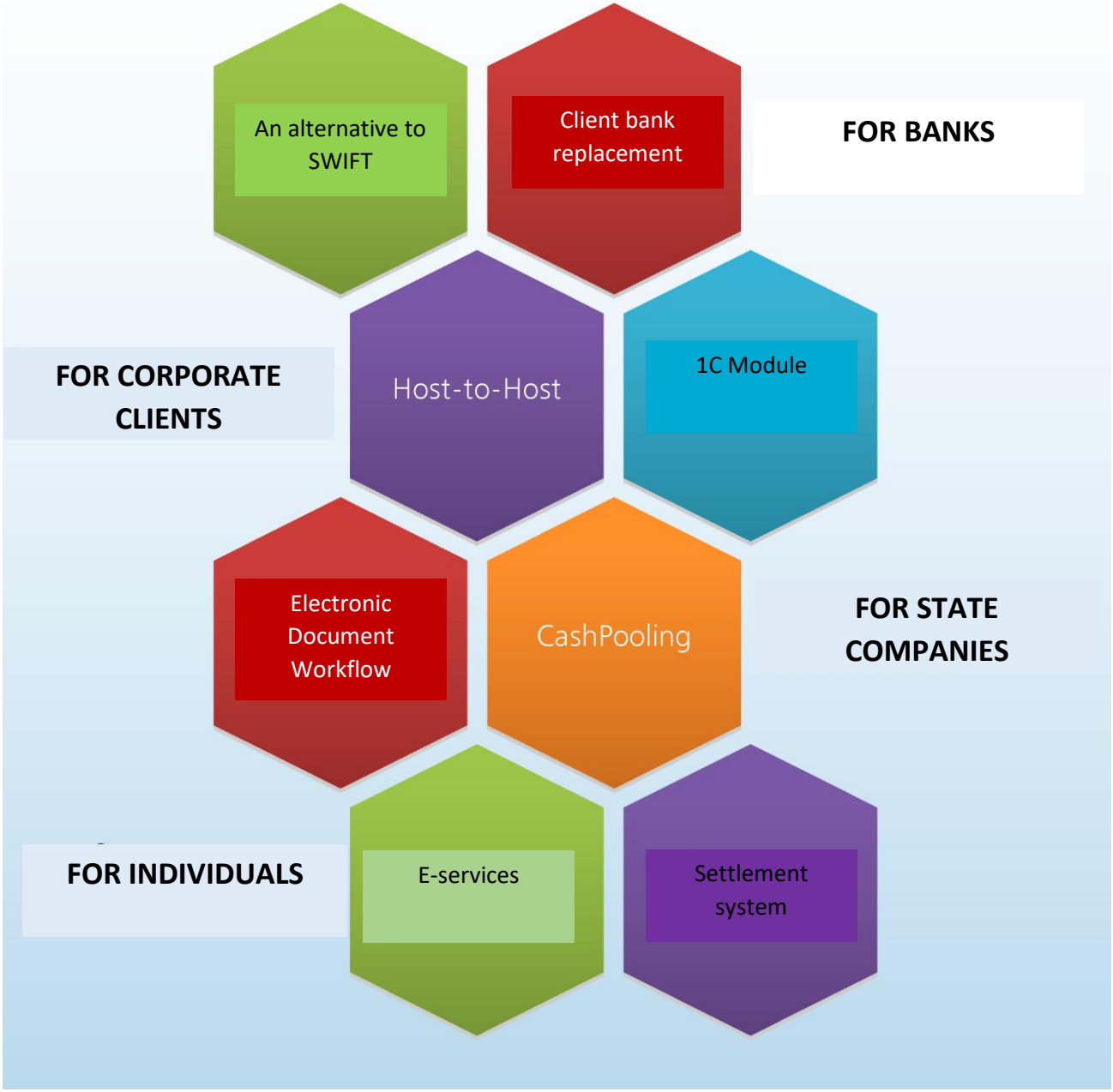


1. Creating documents in CyberFT Terminal
2. Signing and sending documents through the CyberFT Terminal
3. Routing of documents through CyberFT processing to the client's settlement banks

* CyberFT terminal can be installed as an application on the client end, or available as a “lean” client

TERMINAL WORK DIAGRAM

CYBERFT: ONE SYSTEM FOR SOLVING A HOST OF TASKS



A UNIVERSAL SOLUTION FOR INTERACTION OF CORPORATE CLIENTS WITH BANKS

Holding companies use classical remote service systems to manage their accounts in various banks, and large holdings' settlement banks can be measured in tens. This leads to the result that a holding is forced to service many Client-Bank systems at the same time, which gives rise to a number of difficulties. Additional costs for personnel to manage and support the Client-Bank systems from different banks, as well as hardware and software, are required. Moreover, the functionality of many Client-Bank systems often does not allow organizing a full-fledged remote operation with the bank.

The use of systems of the "Corporation Settlement Center" or "Financial Control Center" level does not help much due to the lack of a universal mechanism for working with different banks.

Even direct integration of the client's accounting system with the bank (Host-to-Host) does not completely solve the problem, since each bank offers the client its own data exchange channel, specific formats and specific means of cryptographic information protection.

Limitations of the classic approach to remote account management

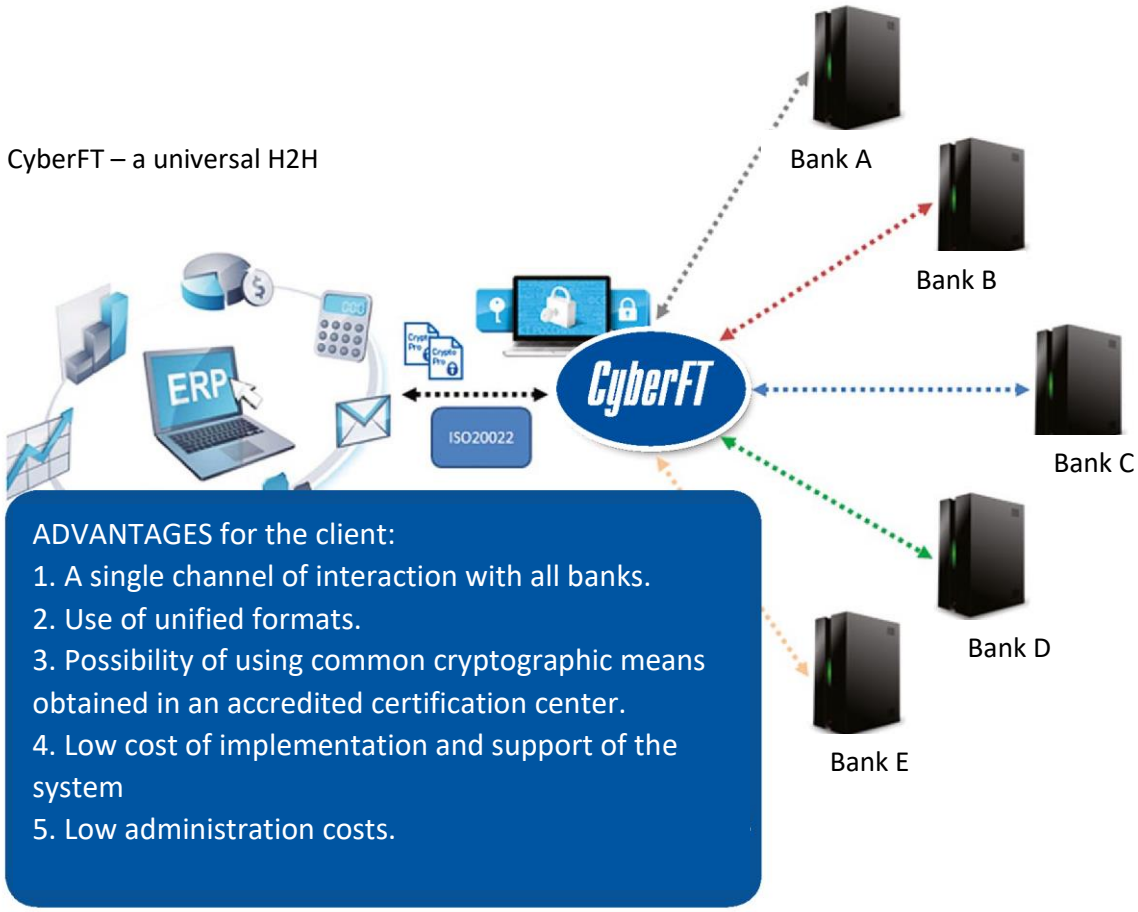
Payment processing time	RBS	CSC	Classic H2H
Number of RBS systems installations	High	Average	Not required
Complexity of management	High	High	Average
Flexibility	Low	Low	Average
Security	Low	Low	Average
Variability of cryptography used	High	Average	Average
Variability of data exchange formats	High	Average	Average
Standardization	Low	Low	Average
Connection and maintenance fee	High	Very high	Average

UNIVERSAL HOST-TO-HOST

The CyberFT platform allows solving the problems listed above, reduce the financial and time costs for remote banking services by completely abandoning the Client-Bank systems and using a single CyberFT terminal, which provides the following opportunities of:

- organizing a single secure channel for interaction with all settlement banks;
- using common formats for data exchange with different banks;
- easy integrating with client-side accounting systems in various ways;
- using unified means of cryptographic information protection when working with various banks;
- using additional options for remote banking services that are not available when working through the standard Client-Bank systems;
- using the signature keys (enhanced qualified signature) obtained in an accredited certification center.

Currently, the service is widely used to interact with servicing banks by legal entities - bank clients, as well as companies that are part of one of the largest holdings - EVRAZ.

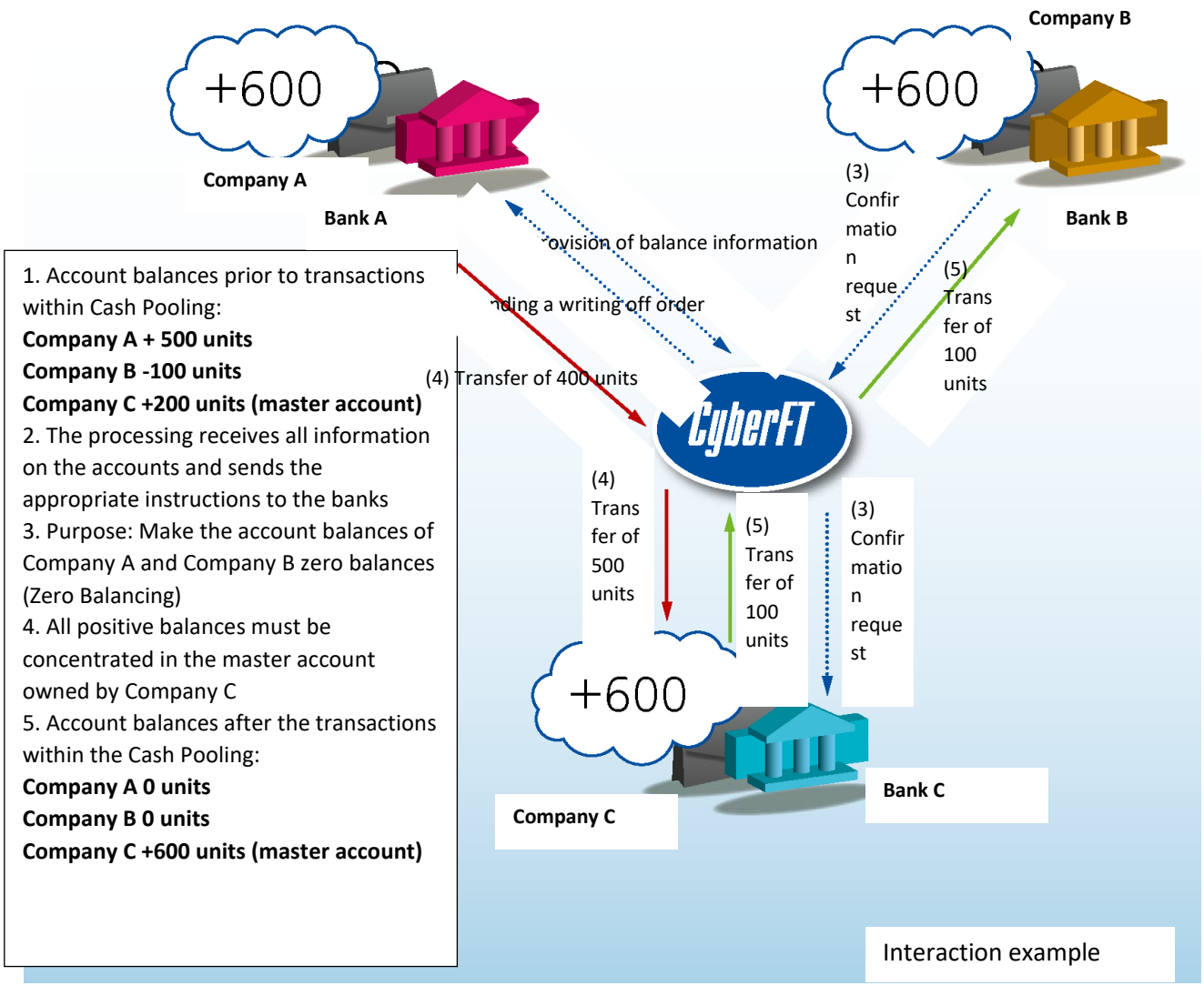


INTERBANK CASH POOLING

The CyberFT system allows organizing interbank Cash Pooling, free of the most important drawback - linking of accounts to a specific bank.

The role of the settlement center, which is usually played by an automated banking system within one bank, is performed by CyberFT processing. Thus, corporate clients receive great capabilities for organizing automatic interbank transfers within a holding or a group of companies.

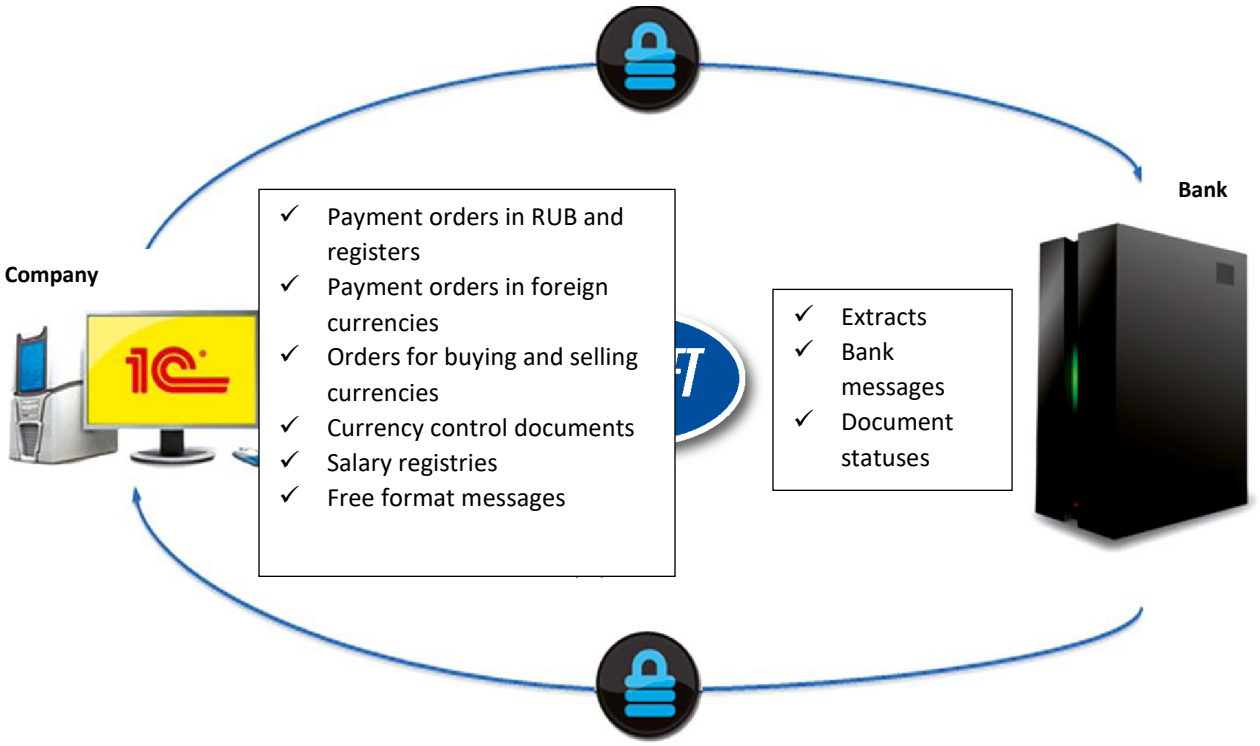
In turn, banks that currently do not provide Cash Pooling or wish to expand its functionality without making significant improvements will be able to use CyberFT capabilities for these purposes.



CYBERFT 1C PAYMENT MODULE

The CyberFT 1C payment module allows customers to create, sign and send to the bank various payment documents, including ruble and currency transfers, orders for the purchase and sale of currency, currency control documents, etc., as well as to receive statements from the banks, messages, other information on the status of the documents sent, all from the 1C system interface.

CyberFT 1C provides direct interaction with banks, without using such “intermediate links” as the “Client-Bank” system. This significantly reduces the time for preparing and sending documents to the banks, reduces transaction costs and risks associated with errors in the preparation and verification of outgoing documents.



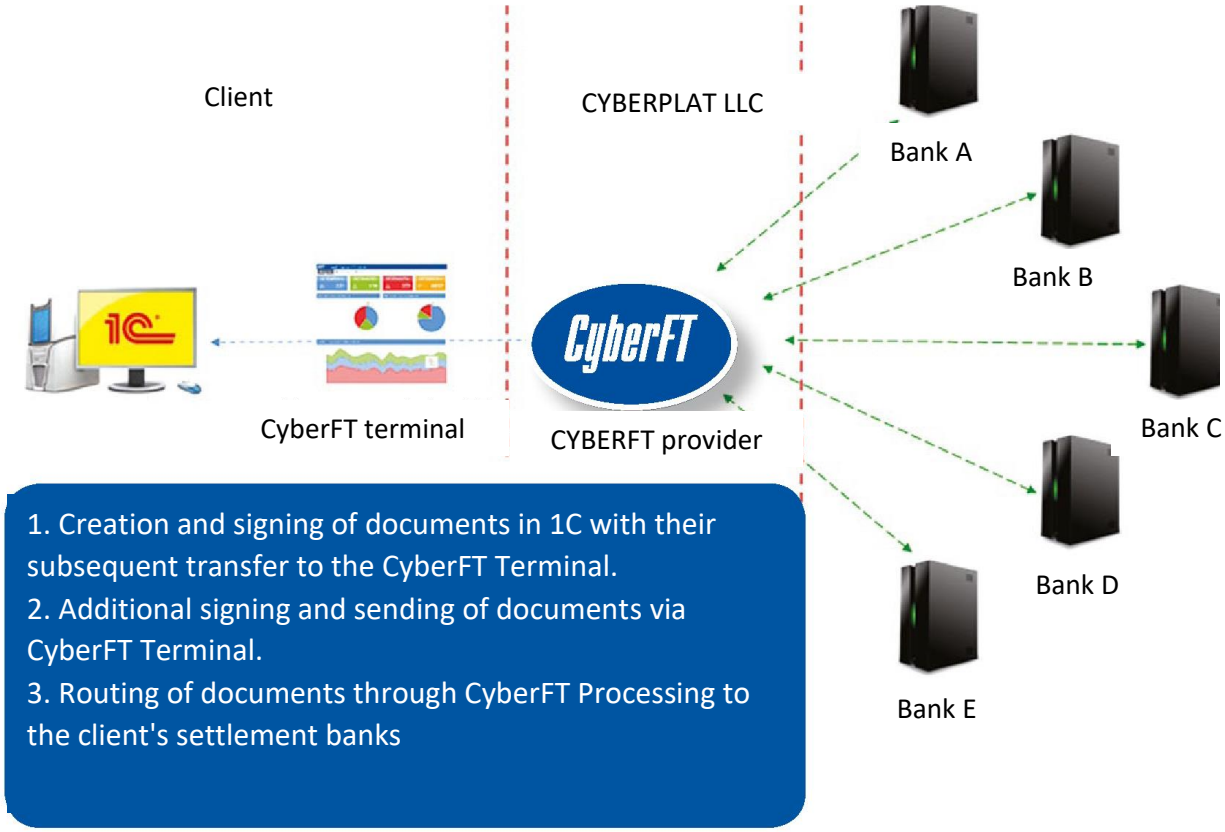
Key advantages of the CyberFT 1C payment module

- Compatibility with 1C: Enterprise Accounting 3.0 and the 1C: Enterprise 8.3 platform.
- “Thick” and “lean” versions.
- Universal and full-fledged replacement of all Client-Bank systems.
- High level of security.
- Support for the basic types of documents required to work with banks.
- CryptoPro and e-Token support.
- The ability to work with different banks.
- Various options for integration with banks.
- Working with the list of trusted recipients.
- User rights management.

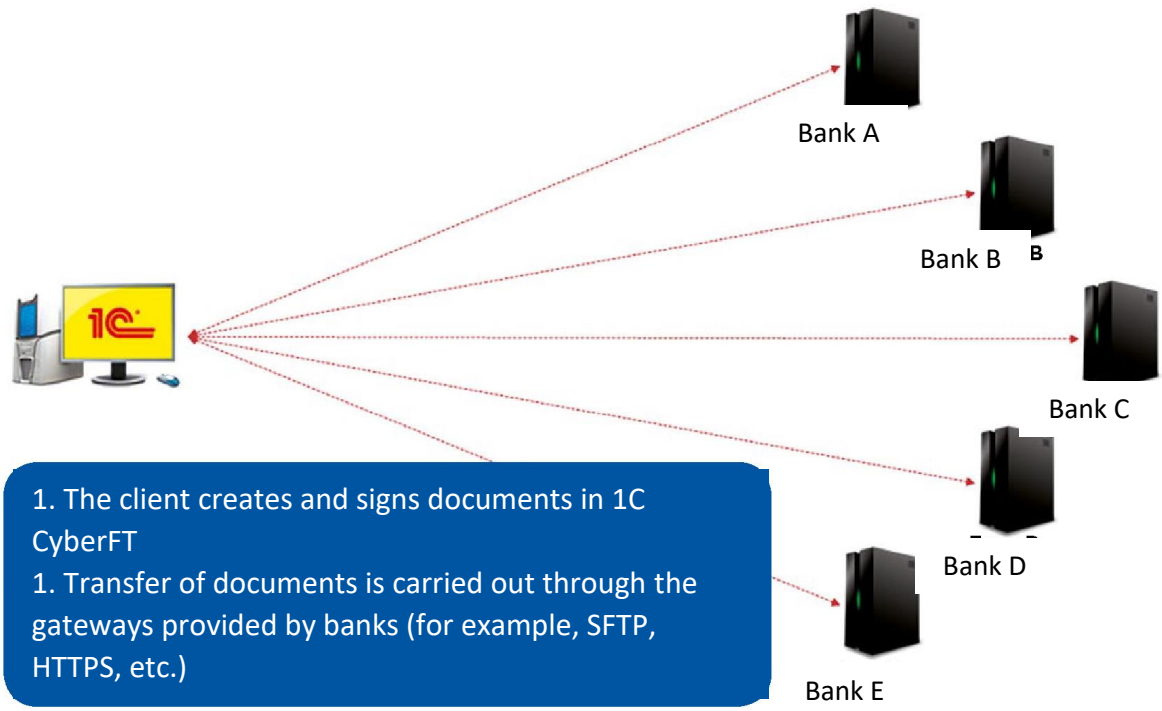
- Signing documents directly in 1C.

WORK DIAGRAM

Option 1

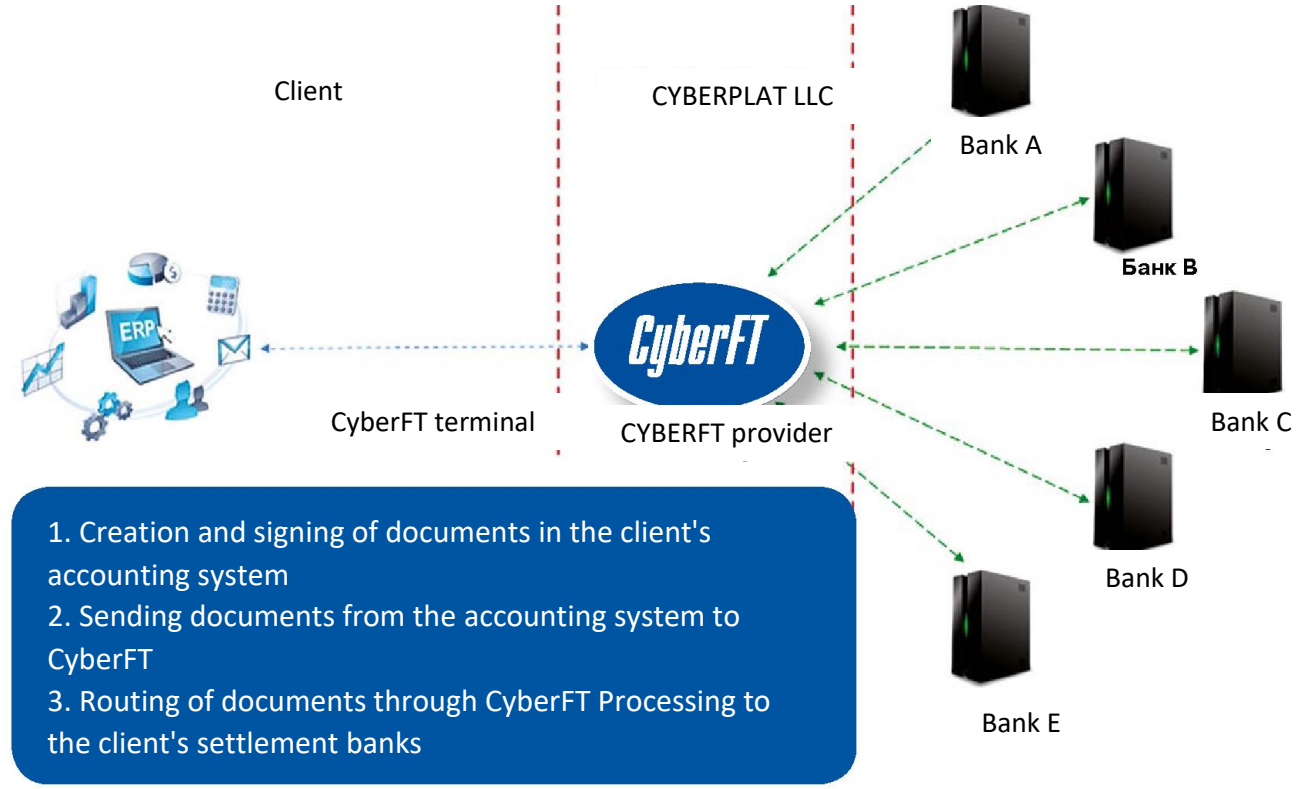


Option 2

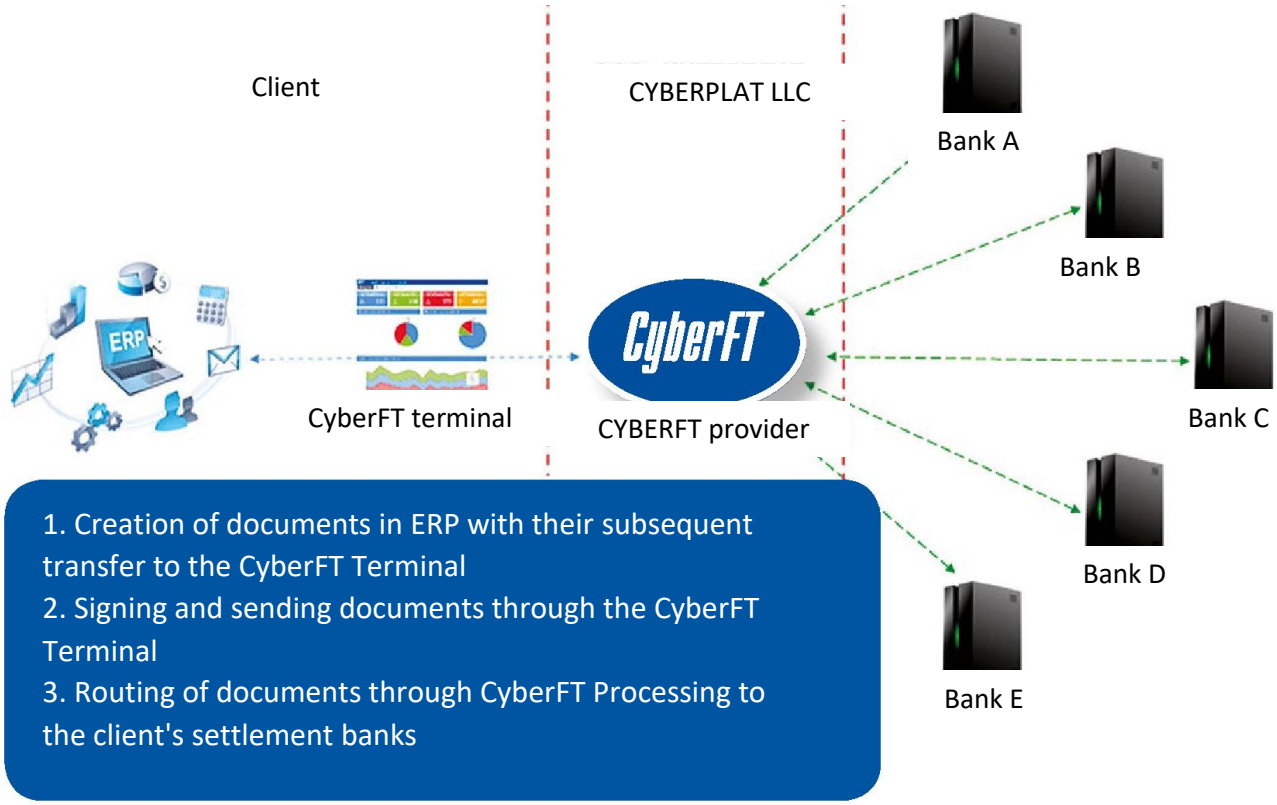


ERP WORKING DIAGRAM

Option 1



Option 2

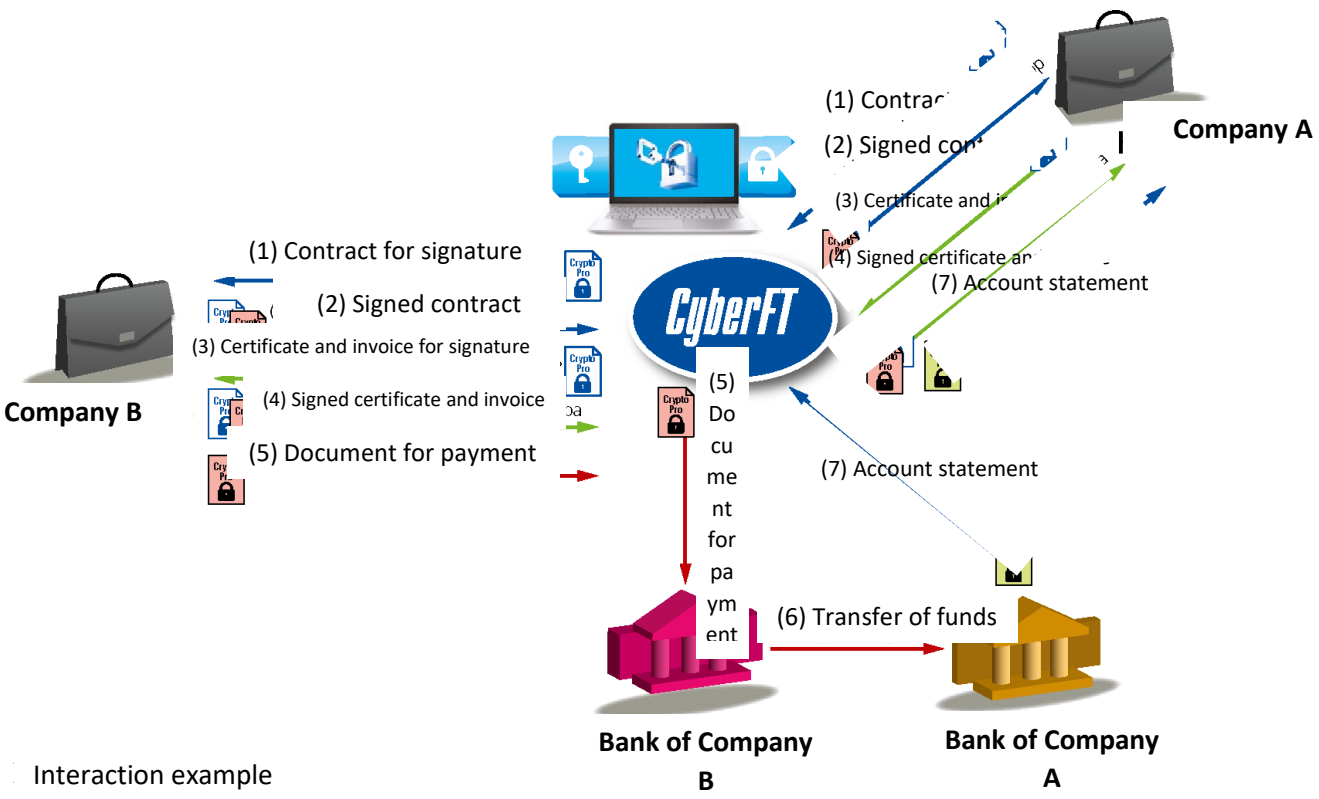


LEGALLY SIGNIFICANT INTERCORPORATE ELECTRONIC DOCUMENT WORKFLOW

Companies can interact through CyberFT not only with banks, but also with each other, organizing an electronic workflow of legally significant document. For example, two participants, having established a trusting relationship with each other, can exchange contracts, invoices and other information necessary for business operations in electronic form.

Also, with the participation of banks, it is possible to build a system of electronic invoicing and payment (e-Invoicing) and interbank direct debit (Direct Debit) on the basis of CyberFT, in which funds will be debited from service recipients to the service provider automatically based on an acceptance given previously.

Notwithstanding the variety of electronic document management systems existing on the market, CyberFT allows covering all corporate clients and all banks not only in Russia, but also abroad. At the same time, the CyberFT Terminal can be integrated with the local electronic document management system operating on the side of the company.



Interaction example

KEY CYBERFT BENEFITS

- Optimization of costs associated with financial transactions and the exchange of documents with counterparties.
- High security standards and guaranteed safety of transmitted information, including data containing commercial secrets.
- Full compliance with the law when conducting financial transactions.
- Fast and low-cost implementation and deployment.
- Various connection options, taking into account the features of the organization and the requirements for the level of security.
- Availability 24x7.
- Absolute independence from the foreign policy situation.
- High fault tolerance of the system.
- Online transactions.
- Support for modern data exchange formats, including SWIFT InterAct, SWIFT FileAct and SWIFT Fin (all documents of the MT category).
- Flexibility and scalability of the system both in the field of data exchange formats and integration with cryptographic libraries and support for data transmission channels.
- System use multivariance: from a closed group of banks to interaction at the international level.
- Ability to create a whole range of new services for bank customers.
- Instant financial transactions.
- Ability to conduct financial transactions outside the business day.
- Electronic document flow of legally significant documents for bank clients
- Integration with ERP, accounting or book-keeping systems of the client and building a universal Host-to-Host solution.
- Opportunity to switch to a single channel for interaction with banks (Host-to-Host) and to abandon traditional Client-Bank systems for corporate clients.
- Possibility of organizing interbank physical Cash Pooling and much more.

EFFECT FROM CYBERFT IMPLEMENTATION

The expected effects from the system implementation will primarily be seen in the retail banking market and small and medium-sized business segment coverage. In addition, CyberFT allows creating a platform that will help increase the amount of payments and reach a fundamentally new level.

For the retail banking market

Development of the retail banking services market has reached a level where banks need to provide their clients with the services of the highest possible level in order to compete effectively. For example, loan holders expect that cash lodgements made in any way convenient for them will instantly remove their claims from the bank. Depositors prefer to work with banks in which the funds deposited appear in the account instantly.

Thus, a system meeting modern requirements for prompt money crediting with reasonable transaction costs will immediately become sought-after.

When the problem of issuing change to the end user in making payments between banks is solved, the Bank of Russia will support the development of this payment system segment.

For the small and medium business market

A key problem of small business development is the absence of any limits imposed on the counterparty. At the same time, the level of trust of counterparties to each other when buying and selling goods or consumer services is extremely low, especially outside Moscow and St. Petersburg. The risk of losing assets and profits for a small business is extremely high, because the unfair behavior from the counterparty can jeopardize the very existence of its business.

For example, a vehicle loaded with grain is waiting at the silo until the silo receives money for the shipped goods. And even if the payment is sent before the vehicle arrives, route processing can take several hours, which are several hours of the driver's work. Moreover, a delay in the delivery of grain, even within a few hours, can affect the operation of the entire flour mill or bakery.

Impossibility of making non-cash payments during all the working hours of outlets, that is, around the clock, seven days a week, is one of the problems of retail and small-scale wholesale businesses. Sales revenue that accumulates over the weekend cannot be used to pay for new small-scale wholesale supplies of goods necessary to maintain the product range.

In the absence of sufficient trust between wholesalers and retailers, the former expect payment prior to shipment, and the latter are often not willing to make advance payments of large amounts of money prior to delivery. This problem is especially exacerbated during the holidays, when the trade turnover objectively grows, and the number of bank vacation days increases. To maintain their turnover, retail outlets are forced to apply for loans from banks in advance in order to build up their stocks. However, securing a loan is not always possible and

is quite expensive, and the accumulation of stock balances is unacceptable when selling perishable products.

The problem of trust has long been resolved in the settlements of retail stores with individual customers. Payments are made in cash or by bank transfer using credit cards. In practice, settlements between retail outlets (especially small ones) and suppliers also have a tendency to gravitate towards cash. In this case, cash is entrusted to non-specialized persons (drivers, freight forwarders). This situation objectively hinders the development of cashless payments, giving rise to criminal risks and creating grounds for abuse of cash that is unaccounted for.

In addition to solving many other urgent tasks, CyberFT platform allows to solve the described problem of retail chains in a highly efficient manner, accelerate the turnover of funds and lead to an increase in retail turnover by 5-7%.

CYBERFT PLATFORM FOR AUTHORITIES, DEPARTMENTS, PUBLIC AND PRIVATE COMPANIES

CURRENT SITUATION WITH INTRA- AND INTERDEPARTMENTAL DOCUMENT FLOW IN RUSSIA

Currently, the issue of interdepartmental electronic interaction within the Russian Federation does not have a centralized solution, since IEDM (Interdepartmental Electronic Document Management (Resolution of the Government of the Russian Federation on the approval of the regulation on IEDM No. 754 dated 22.09.2009) to be operated by the FSO, is still at the stage of its creation (only the message standard - PDF / A has been agreed) - and a test operation with the participation of the Ministry of Industry and Trade, the Ministry of Economic Development and two or three other structures is underway. At the same time, IEDM is in fact only a secure interdepartmental e-mail service. The issue of integration with heterogeneous EDM systems used in various organizations (at least at the level of maintaining an agreed format) is still being discussed. In addition to difficulties of integration at the stage of test operation, significant technological limitations were identified, in particular, the impossibility of transferring large amounts of information in a single message (over 0.5MB).

The absence of an efficient IEDM does not allow departments and organizations ensuring the fulfillment of the requirements of said Resolution when organizing exchange of official information having high commercial value or security classification. Publicly available postal services, which are used in such cases, multiply the risks of losing official information and are prohibited from use by the competent authorities when transferring data containing state secrets.

Quite often, government bodies and other agencies are forced to resort to use the courier services for sending secret information. This method of transferring particularly important data slows down the process of making responsible decisions dramatically, and also significantly increases the cost of such information exchange.

The current systems for the transmission of secret data permitted for use, first of all, are not sufficiently widespread, and secondly, do not allow the transmission of a large amount of information, for example, maps or telemetry.

In addition, they are based on hardware data protection, which meets the current risks no longer and carries significant threats of decryption of the intercepted messages by malevolent intruders.

Local solutions for government agencies interaction are based on portal solutions and do not stand up to criticism from the viewpoint of the security level. Such portal solutions are quite often protected only by the user's password and, unfortunately, do not support electronic signatures and, consequently, cannot serve for the exchange of legally significant documents. Moreover, the use of portal technologies does not allow the use of these solutions for automated interagency interactions. With the current volume of interdepartmental communications, one can find it difficult to imagine that each message for communication

between departments is entered in the portal web interface, therefore, the need for an integrated solution for the interaction of existing information systems of departments is obvious.

The Interdepartmental electronic interaction system (IEIS) has been operating since 2013, contains 83 regional nodes and a central hub, more than 600 participants, 7 data centers, operated by Rostelecom. IEIS (according to Federal Law of July 27, 2010 No. 210-ФЗ "Concerning the Organization of the Provision of State and Municipal Services") is, in fact, a data bus to which the accounting systems and EDM systems of participants are connected. Due to the fact that the SOA architecture of the system is implemented based on 84 Oracle ESB buses, the security issue of this solution also raises serious concerns.

CYBERFT PLATFORM - AN ELEMENT OF NATIONAL SECURITY AND A GUARANTOR OF THE IMPORTANT STATE INFORMATION SECURITY

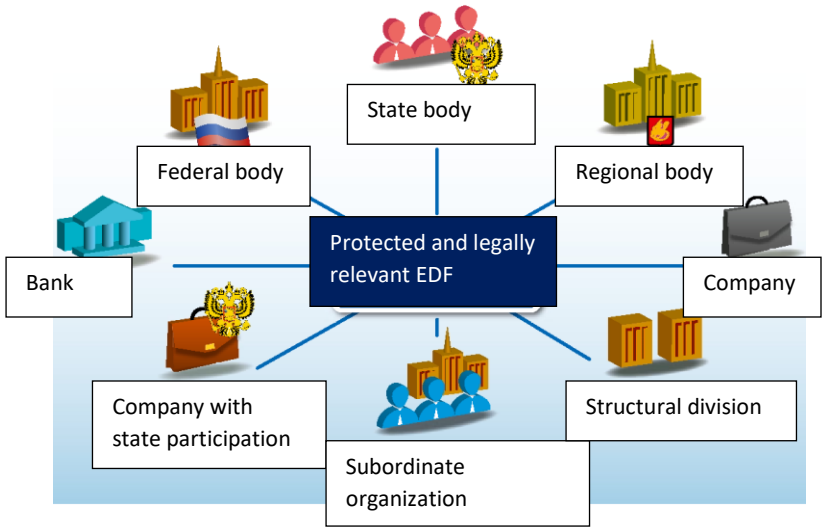
In this situation, the dire need of the state and commercial structures of the country in a modern online information exchange system that can become the basis for a secure document flow of any degree of secrecy is obvious.

This system must be:

- relatively simple;
- inexpensive;
- performance-critical;
- easily scalable;
- with a high bandwidth;
- based not on hardware, but on software methods of data protection with the ability to quickly change crypto libraries.

CyberFT platform fully meets these criteria, allowing government agencies and other participants in the workflow:

- carrying out information exchange in full compliance with local legislation;
- fully protecting the information transmitted from foreign policy threats;
- guaranteeing the safety of information containing state and commercial secrets;
- organizing electronic document flow of legally significant documents between government bodies and other participants;
- optimizing costs and increasing the speed of information transfer.



In simple terms, the CyberFT platform can be seen as an alternative to the Internet. However, the fundamental differences between CyberFT and the World Wide Web are the guaranteed identification of participants and the exchange of structured information in an encrypted form.

Prior to the speeches of Edward Snowden and Julian Assange on mass surveillance and information leakage, not all government agencies were well aware of the level of electronic and computer intelligence of developed countries and private intelligence companies, they did not contemplate enough the danger of hostile influence on the exchange of data containing confidential information.

The use of the CyberFT platform is an effective way to implement a protected and legally significant interaction between the authorities, ministries and departments of the country, both with each other and with commercial, public and other organizations.

CyberFT allows to form a network of an unlimited number of agencies that are organizers of information exchange (CyberFT providers). The CyberFT platform is deployed at the provider's site and is independent of its developer - CyberPlat®.

The CyberFT provider can serve all of its structures and their counterparties within its footprint in the regions, or work within separately selected organizations controlled by the department or their groups.

Departments can communicate with each other through a cross-platform communication service controlled by a responsible department official who gives users from one department the right to correspond with another department.

Unlike other systems operating on the world market, all software is developed by Russian specialists (which is licensed and patent independent). All servers of the CyberFT platform will be located in the secured provider perimeter, therefore, the probability of leakage of government and important commercial data in electronic document flow is sharply reduced.

LOCAL LAW ENFORCEMENT INSTRUMENT

For government agencies, CyberFT is a software platform implementing a secure data highway for the transmission of all generally accepted types of messages for intradepartmental, financial and commercial electronic document flow management, functioning in accordance with the order of the Ministry of Telecom and Mass Communications and the Federal Security Service (FSO) dated September 22, 2015 "On Approval of Requirements to the Organizational and Technical Interaction between Government Agencies and Government Organizations through the Exchange of Documents in Electronic Form" and meeting a number of requirements:

- For the electronic document file formats, as well as electronic document image files that support the transfer of electronic documents in the form of files of any format, including the PDF / A-1 format defined by the international standard ISO 19005-1: 2005, as well as ISO 20015 and ISO 20022
- for the enhanced qualified electronic signature using a specialized PKCS # 7 format;
- for the transport containers and the possibility of converting containers from one type of presentation to another in the process of creating, processing and storing documents.

SECURE INFORMATION EXCHANGE TOOL

The CyberFT solution assumes that both dedicated communication channels and open Internet channels can be used for documents of the "for internal use only" and "secret" level of sensitivity. At the same time, the technology ensures the creation of an encrypted channel between messaging points. These channels transmit encrypted messages signed with an electronic signature.

The bulk of the transmitted information can pass through open Internet channels and / or dedicated channels of the department in a protected form using the know-hows in the field of processing secure messages.

In its solutions, CyberPlat® uses a data transmission method as the main network transport mechanism, where all transmitted messages are signed with legally significant electronic signatures and transmitted over the network in cryptocontainers with a key length of 2048 inside an SSL tunnel.

Рекомендации по использованию интернета, VPN и выделенных каналов связи

	For internal use only	S
Internet	Yes	In case of an accident with a more secure type of connection and a strong need to urgently send a message
VPN	Possible, but not necessary	Yes
Dedicated channel or	Possible, but not necessary	Possible, but not necessary

specially protected line		

BASIC STRATEGIC PRINCIPLES AND CAPABILITIES OF THE CYBERFT NETWORK

CyberFT platform is a convenient and absolutely secure solution based on the following principles:

- self-reliance;
- continuity;
- safety;
- identification of each user;
- structuredness of the transmitted data;
- compatibility;
- versatility;
- availability;
- expandability.

CyberFT platform provides:

1. Construction of a secure and reliable system of electronic interaction and workflow.

2. Online messaging - the equivalent of a closed legally significant e-mail service with confirmation of receipt.

3. Transfer of data in full compliance with federal, local and departmental regulations using certified cryptographic information protection tools:

- encryption of messages and signing with electronic signatures (ESs);
- support for interchangeable CIPFs, certified by the appropriate government agencies, including OpenSSL, CiyptoPro, SignalCOM, Agava, etc., as well as support for enhanced qualified electronic signatures in accordance with the requirements of Federal Law No. 63-ФЗ “On Electronic Signatures”;
- using HTTPS protocols (TLS tunnel) when transferring data;
- VPN and dedicated communication channels support;
- ability to transfer software-encrypted messages through open Internet channels using encrypted tunnels that do not allow decryption, in case of emergency unavailability of dedicated channels.

4. Use of modern standards, regulatory requirements and the ability to customize your own message formats, as well as the order of exchange and processing.

CYBERFT NETWORK FEATURES

Multiple provider system

CyberFT platform for authorities, departments, public and private companies is deployed at the provider's site and is independent of CyberPlat®. CyberFT provider can serve or work within a separately selected state structure.

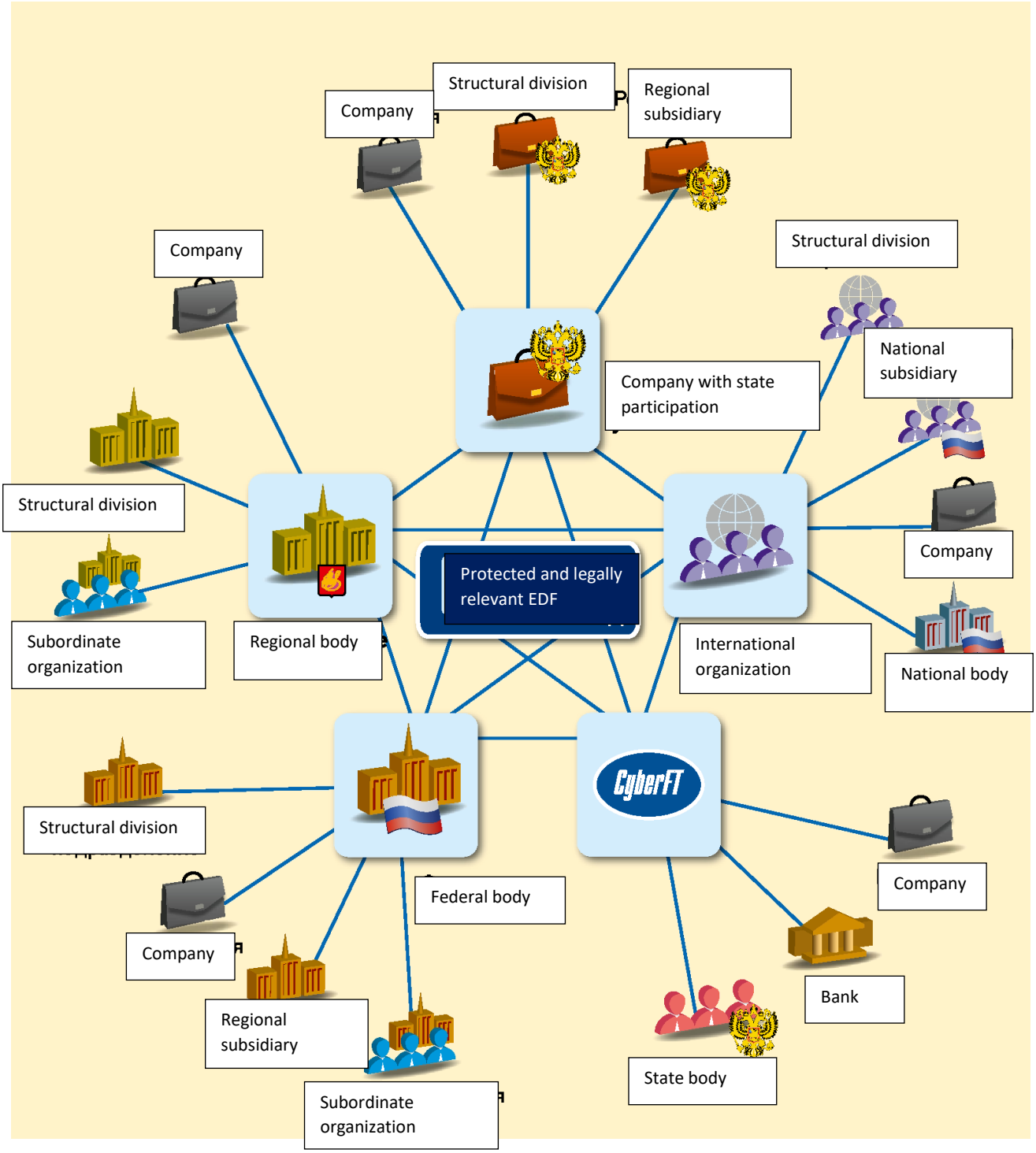
Both state bodies and other organizations can act as CyberFT providers and participants. Each participant is assigned a unique CyberFT identifier.

The directory of network participants is available to each participant and is updated automatically on a centralized basis. The identifier is unique not only within one provider, but throughout the whole CyberFT network. Thus, a member with a specific identifier can only be connected to one provider, which ensures the integrity of the network.

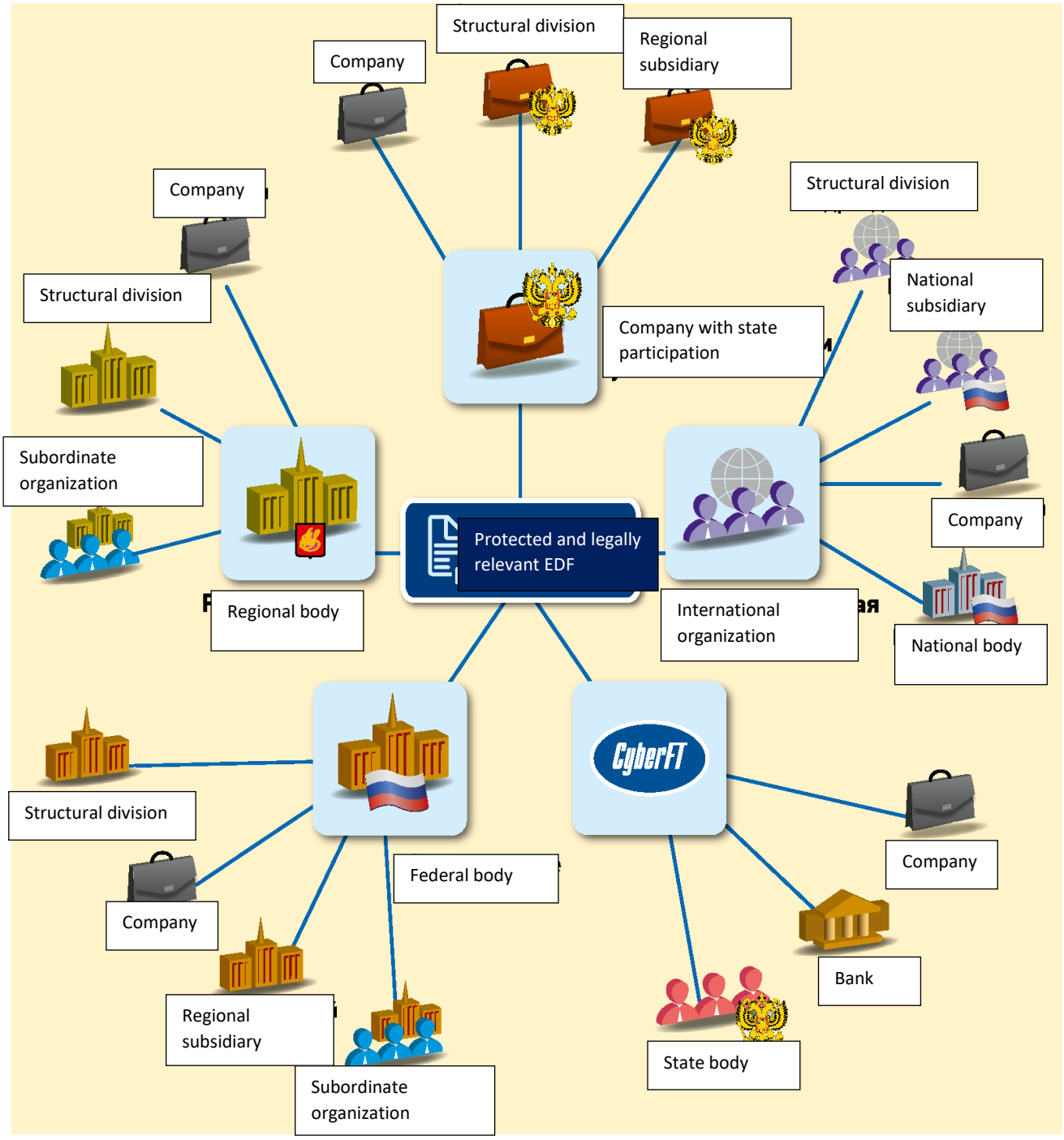
Information on the processing of each message is logged on the side of each provider participating in its transmission. In addition, the messages themselves, are stored together with the sender's electronic signatures on the side of the sender, recipient and provider for an unlimited period of time (on the provider's side, all messages are stored in an encrypted form, and their content is not available to the provider). Thus, each participant in the information exchange process has full legally significant electronic documents.

CyberFT providers can connect with each other in various ways, based on the complexity of the organizational processes of establishing relationships between providers. Some diagrams are presented below.

1. Everyone to Everyone



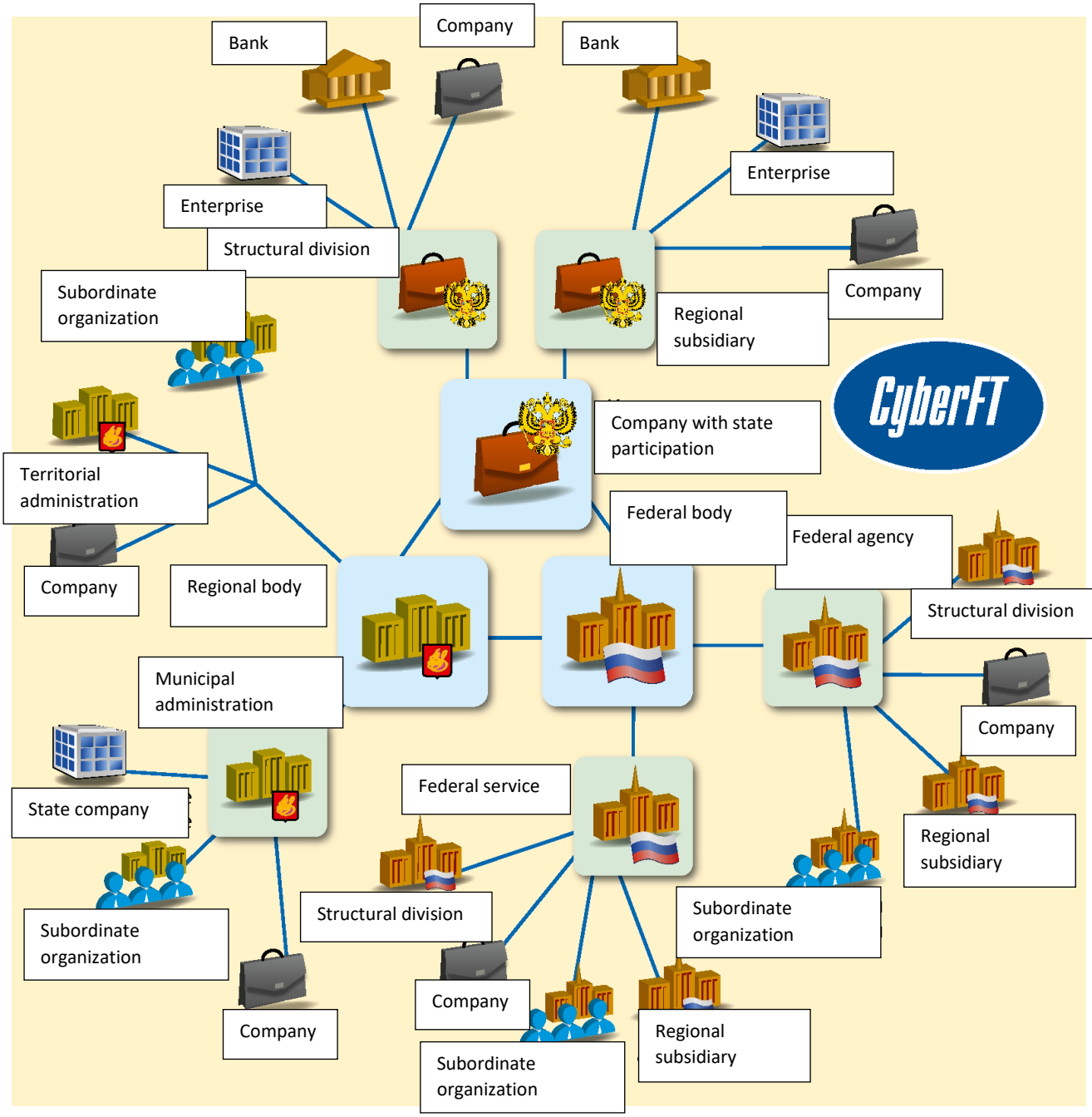
2. Through a centralized CyberFT provider selected jointly



For example, any large body or state organization can become a CyberFT provider and connect geographically remote subdivisions, subsidiaries and other participants in their workflow. At the same time, in order to exchange data between participants connected to different providers, these providers enter into an agreement with a single provider (for example, a ministry), which is responsible for routing messages between them.

On the one hand, such a network topology greatly simplifies the organizational aspects associated with establishing relations between providers, and makes it possible to work through a single organization (central provider), trusted by all participants. On the other hand, in the event of a failure on the side of the central provider, communication between network participants becomes impossible.

3. Through a group of interconnected CyberFT providers



This version of the network topology, in disregard of the organizational processes of establishing relations between providers being more complex, has increased fault tolerance.

In case of technical issues arising on the side of one of the central providers, communication between all CyberFT network participants will not be disrupted.

Compatibility

CyberFT network members can also interact with other contractors connected to other IEDM networks. An example of such interaction is shown in the diagram below.

CyberFT software allows quick integration with most electronic document management systems used in various departments, supporting the main document formats, which simplifies the process of uploading and loading documents into the internal information systems of participants.

When a new participant connects to CyberFT, the centralized directory of participants will be updated remotely in automatic mode.

CyberFT software is provided to customers free of charge.

Accessibility

Connection to the CyberFT network is carried out through a dedicated channel, VPN or public Internet connection, which allows the client to choose a network service provider freely and not be tied to a specific telecommunications operator. Thanks to the approaches taken, if the connection is lost, its restoration will occur through a new channel within one minute automatically.

Interaction occurs in a protected form only through open Internet channels using the proprietary practices in the field of financial messages processing. CyberPlat® uses HTTPS data transmission (TLS-tunnel) as the main network transport mechanism in its solutions. All transmitted messages are signed with electronic signatures. For example, messages of S level can pass through them.

The system uses interchangeable (connectable) cryptographic information protection systems (CIPF), including OpenSSL and GOST algorithms (based on CryptoPro, Signal-COM, etc.). In addition, CyberPlat at the requests of partners and clients is willing to connect any other means of crypto protection in the shortest possible time - within a few days.

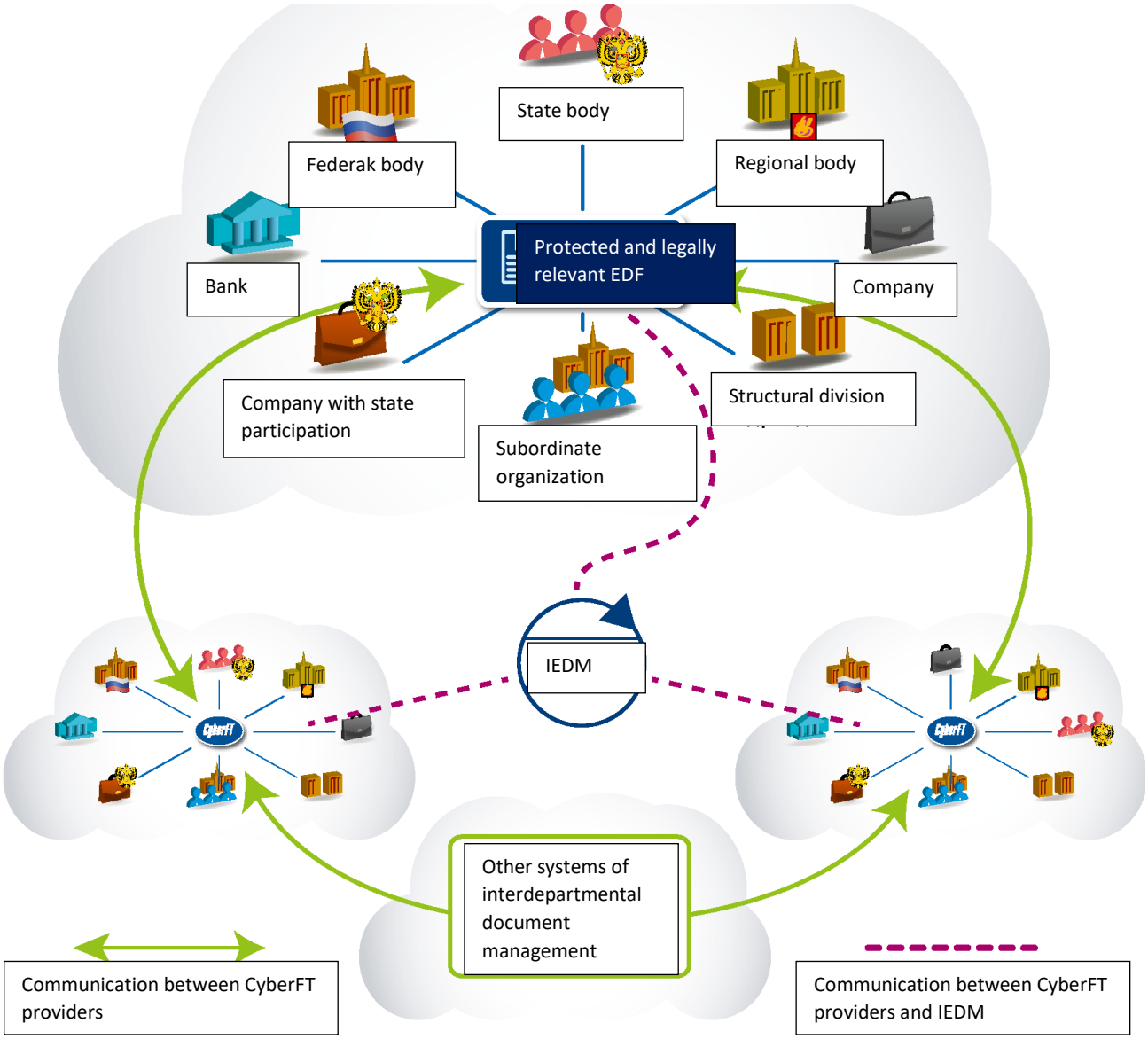
Competitiveness

The fundamental difference between the CyberFT network and other solutions that can be used as a medium for interdepartmental electronic document management is its operational readiness at the moment, low cost and efficiency of use, as well as the highest level of security and protection.

It should also be noted that the hardware requirements for working in CyberFT are significantly lower than those established by other IEDM developers, therefore, the operation of CyberFT allows to reduce the costs of maintaining server and telecommunications equipment, as well as the cost of employing personnel servicing said equipment.

Flexibility

As part of a universal transport solution, the CyberFT network has the capability of integration with most electronic document management systems used in departments. The application of this approach allows to optimize business processes involving the exchange of documents with government authorities (including interaction with the state IEIS system), as well as interdepartmental communications.



Scalability

CyberFT has implemented a service that allows exchanging any structured and unstructured messages, as well as messages containing attachments. As part of the solution offered, it is possible to implement new formats in the CyberFT network within the existing types of electronic messages.

CyberFT platform can be quickly modified taking into account the needs of customers. In particular, it is possible to promptly create new types of electronic documents using the format designer, which makes the CyberFT platform much more flexible compared to its competitors.

EFFECT OF IMPLEMENTATION

- Efficient work in full compliance with the requirements of the legislation of the Russian Federation and accepted standards.
- Maximum operational reliability and security of the information transmitted.
- Coverage of a large number of participants in the interagency document flow.
- Complete independence from the developer company.
- Sending and receiving encrypted messages online.
- Budget savings on infrastructure and network maintenance.

“CYBERCHANGE” - A UNIQUE FINANCIAL SERVICE FOR RETAIL BUSINESSES, BANKS, SERVICE PROVIDERS

ESSENCE OF THE PRODUCT

“CyberChange” is a modern financial technology associated with the use of change left after payment for goods and services in retail chains, shops and small outlets (www.киберсдача.рф).

The amount of change can be transferred in real time to almost any service provider with no cashier’s time wasted using a special CyberChange card.

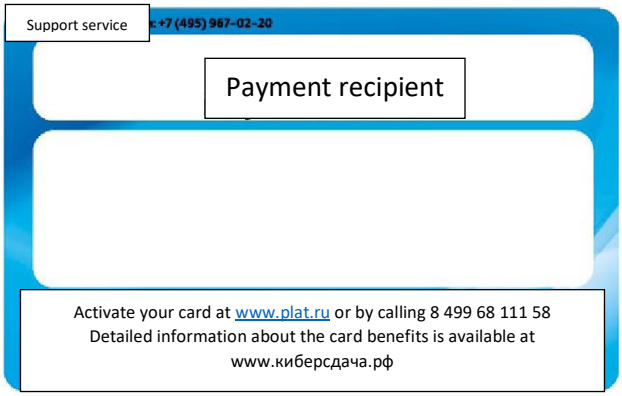
According to expert estimates, there is the most active demand for transferring the change amount to a mobile phone account, bank card, as well as a bank account linked to an Internet Bank-Client, such as Alfa Click, Bank in Pocket, Platru - Payment Book CyberPlat®.

Any person can become a user of the service. In order to implement the service (crediting change or carrying out a targeted transfer of funds to a bank or personal account with a service provider), you must first obtain an inactive CyberChange card and activate it. In the process of activation, the card number will be assigned a template containing payment details, for example, a service provider code and a mobile phone number, or a bank code and a bank or personal account number and a mobile phone number. The set of data is transferred to the CyberPlat® system and further serves as an electronic template for making transfers automatically, without entering any details.

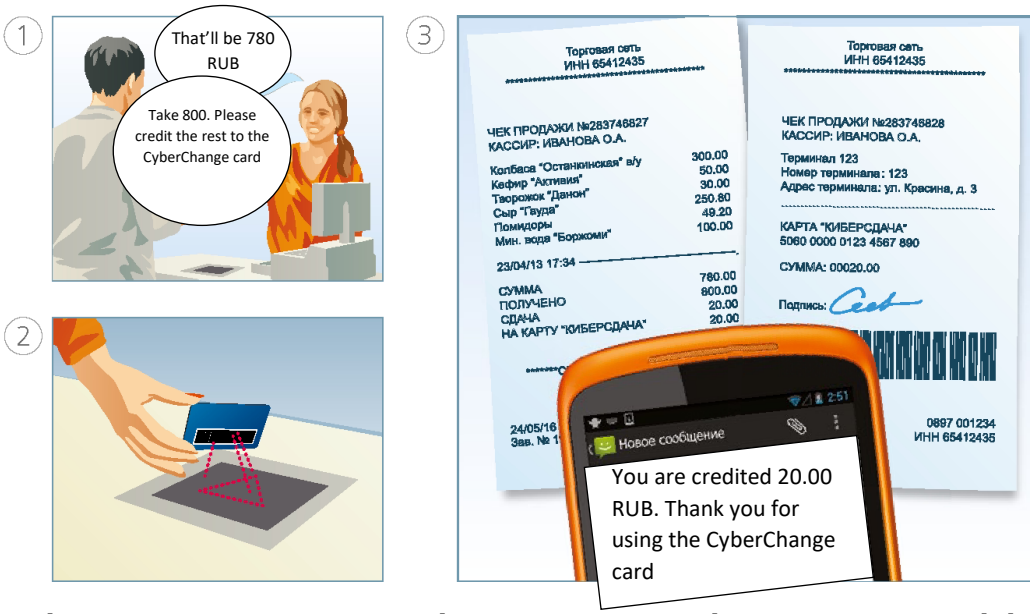
To carry out transactions below the minimum payment threshold, a “Payment Book” of Platru is automatically created, and the change amount is credited there.

CYBERCHANGE CARD

The CyberChange plastic card is the same size as standard bank cards. It bears a 19-digit card number and a barcode.



GENERAL PLAN OF CHANGE CREDITING



Let us consider a common situation: at the most unexpected moment, your mobile phone is blocked because you have run out of money. You immediately take off looking for the nearest payment acceptance outlet in order to replenish your account in a quick and convenient manner.

You walk into the nearest store of a well-known retail chain and ask the cashier to replenish the account. In response, the cashier offers to make a purchase, and transfer the amount of change to your mobile operator's account. You agree, because you understand that it is "killing two birds with one stone" at the same time: you replenish your account, "revitalizing" your phone, and purchase the desired product as well. As a result, store turnover increases and customer loyalty to the retail network grows.

The amount of impulse demand goods in mini-market chains can account for up to 50% of turnover, in super- and hypermarkets – for up to 20%.

ADVANTAGES OF ABANDONING SMALL MONEY (COINS AND BANKNOTES) WHEN RECEIVING AND GIVING CHANGE

For payers

- Saving time in queues at the checkout.
- Saving time on replenishing personal accounts with providers of various services, as it is a related operation.
- Exemption from the need to use coins that are inconvenient to store in large quantities in pockets or wallets.
- Allows spending money for oneself, and not turning it into “tips” to the cashier, leaving them a small amount of change.
- Reduces the risks associated with the use of unhygienic metal and paper money.

For cashiers in retail chains

- Saving working time spent on cashing and calculating small money.
- No need to constantly monitor the availability of small change at the cash desk and involve a senior manager to change large bills.
- No need to ask buyers to prepare small money or pay for purchases in exact amounts without using change.
- Increase in efficiency and comfort of work, increase in the speed of customer service, decrease in queues at the checkout.

For retailer chains

- Increase in turnover of up to 35% within a year from the date of service implementation.
- Reduced number of errors associated with incorrect entry of payment details.
- Acceleration of customer service at the checkout ("CyberChange - high speed of payment” video at: http: // youtube / 8PXcbqL5ZtO).
- No need to order coins and small bills.
- Reduced delays in the exchange of cash, including for other cashiers.
- Fewer refusal to buy s due to lack of change and less negative sentiment in queues
- Increase in revenue and savings on cashier wages.
- Creating psychological comfort in the work of cashiers and increasing their efficiency.
- Attracting impulse shoppers to the shopping space.
- Organizing marketing campaigns in the form of bonuses on CyberChange cards at the end of the year (quarter) in order to motivate customers and increase their loyalty.

ADVANTAGES OF THE UNIQUE "CYBERCHANGE" FINANCIAL SERVICE

For payers

- Fast money crediting.
- Elimination of errors in manual entry of phone numbers and other payment identifiers.
- Preserving the privacy of personal data, since there is no need to tell your phone number for all to hear.
- There is no need to give your bank card to the wrong hands. On the contrary, you can give out a card tied to your number to everyone: "let them put their change on my account".
- The ability to deposit not only change, but also large amounts (up to 15 thousand RUB) into the account.
- SMS confirmation of the change amount crediting.
- The ability to credit the change amount to a bank card, even multiple times, and then withdraw funds from an ATM.

For retail chains

- Elimination of errors in manual entry of phone numbers and other payment identifiers.
- Acceleration of customer service at the checkout (cashiers do not waste time issuing change).
- There is no need to order coins and small bills from the bank.
- Savings in collection costs, since collection of coins and small bills is charged at a higher rate by the banks.
- Simple connection: only one CyberChange gateway instead of a group of gateways (Visa Money Transfer, MasterCard Money Send, bank gateways, provider gateways).
- Using information on the buyer (number of the CyberChange card) received upon payment for advertising and marketing purposes: drawing up a "portrait" of the buyer, direct SMS mailing via CyberPlat® informing of discounts, expansion of the product range, and much more.
- Expanding the capabilities of own loyalty programs by accruing bonuses and holding motivating promotions.
- Growth in sales of impulsive goods due to the convenience of paying for mobile communications at the checkout.
- Convenient and quick acceptance of "heavy" payments (payment of STSI fines, replenishment of cards and bank accounts, repayment of loans, payment for utilities, etc.) with the CyberChange card attracts additional clientele with medium and high purchasing power to retail chains.

PERFORMANCE ASSESSMENT

Comparative analysis of grocery retail for small and medium-sized stores showed the following statistics

	Medium store	Small shop
Commercial area, sq. m	Up to 1,500	Up to 200
Average number of checkout counters	4	2
Average number of checks per day at the checkout counter, pcs.	460	460
Increase in supermarket traffic from the implementation of the CyberChange project,%	20	30
Average check amount, RUB	359	233
Average change amount, RUB	270	263

Operating efficiency indicators *

	Direct costs (prime cost of goods),%	Indirect costs (staff salaries, rent, etc.),%
Group X5	74	21
Group MAGNIT	71	21
Group DIXY	66	25

* http://www.dixygroup.ru/~/media/Files/D/Dixy/financial-results/archive2014/RUS/FY2014RUS.pdf

http://www.x5.ru/ru/investors/financial_reports

http://ir.magnit.com/flnancial-reports-rus

Small food retail shop example *

	Assessment prior to CyberChange implementation	Assessment following CyberChange implementation
Average number of checkout counters	2	3
Average number of checks per month for a store with 2 checkout counters	27 600	37 260
Average check amount, RUB	233	233
Shop turnover per year, MM RUB	77,2	104,2

Average direct costs (cost of goods),% of revenue	74	74
Average direct costs (cost of goods), MM RUB	57,1	77,1
Average indirect costs (salaries, rent, etc.),% of revenue	17	13
Average indirect costs (salaries, rent, etc.), MM RUB	13,1	13,8
Average profitability, MM RUB	6,9	13,3
Average profitability, %	9	13

* The data is assessed according to the financial statements of DIXY, Magnit, X5.

The increase in profitability is 6.4 million RUB per store per year.

- Revenue is increased by 35%.
- Wages rise by 5%, while rent payments remain on the same level. This increase in profitability can be achieved in 1-2 months after saturation of the base of regular customers with CyberChange cards.

Example of a medium-sized supermarket *

	Assessment prior to CyberChange implementation	Assessment following CyberChange implementation
Average number of checkout counters	4	3
Average number of checks per month for a store with 2 checkout counters	55 200	37 260
Average check amount, RUB	359	233
Store turnover per year, MM RUB	237,8	104,2
Average direct costs (cost of goods),% of revenue	74	74
Average direct costs (cost of goods), MM RUB	176,0	77,1
Average indirect costs (salaries, rent, etc.),% of revenue	19	13
Average indirect costs (salaries, rent, etc.), MM RUB	45,2	13,8
Average profitability, MM RUB	16,6	13,3
Average profitability, %	7	13

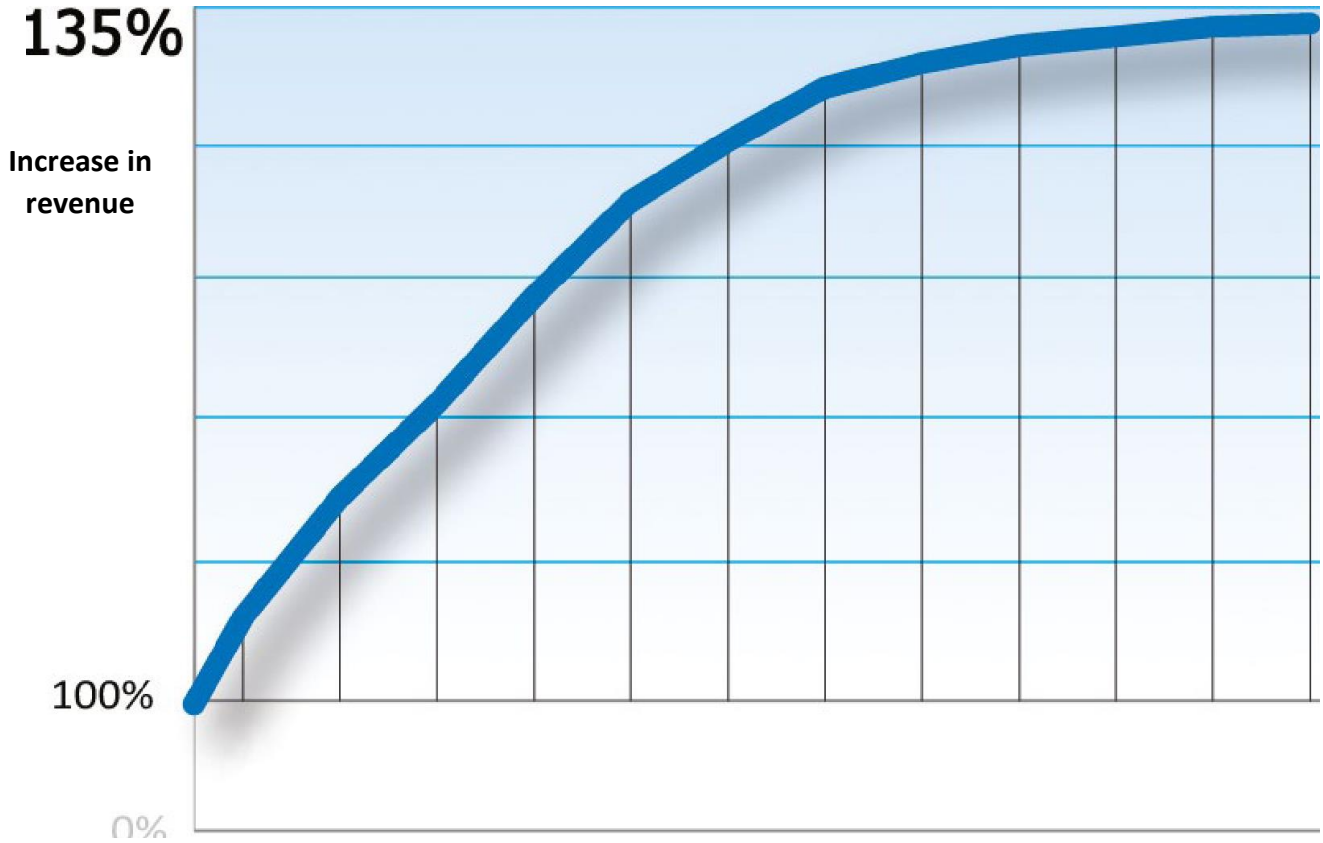
* The data is assessed according to the financial statements of DIXY, Magnit, X5.

The increase in profitability is 13.2 million RUB per store per year.

- Revenue is increased by 35%.
- Wages rise by 5%, while rent payments remain on the same level. This increase in profitability can be achieved in 2-3 months after saturation of the base of regular customers with CyberChange cards.

GRAPH OF THE EXPECTED GROWTH IN REVENUE DUE TO THE INCREASE IN FOOT TRAFFIC

Comparison of the effectiveness of the implementation of the CyberChange project in small and medium retail businesses



The CyberChange project has a beneficial effect on increasing the turnover of a commercial outlet in small and medium retail stores connected to the service. An increase in profitability can be achieved within 3-6 months.

Thus, the introduction of CyberChange is more attractive for small shops than for larger stores.

	Indicators of a small grocery network after the implementation of CyberChange	Indicators of a medium format supermarket after the introduction of CyberChange
How much the average profitability increases,%	Ha 4	Ha3
How much revenue per square meter increases,%	Ha 26	Ha 20

INCREASED TURNOVER OF HIGH-MARGIN GOODS

With the growth of foot traffic moving higher as a result of the implementation of the CyberChange project, the turnover of high-margin goods in the outlet increases. The client comes to pay for services using their CyberChange card and makes purchases of point-of-purchase goods with higher profitability, which are located in checkout areas.

E-retail experiences an increase in sales of accessories: covers for mobile phones, key fobs, memory cards, batteries, etc.

Sales of beer, cigarettes, alcohol, mineral water, chocolate, confectionery products, chewing gum are growing in grocery retail, as well as sales of non-food high-margin products.

HOW THE SERVICE IMPACTS TERMINALS INSTALLED IN RETAIL CHAINS

As a rule, retail chains have already payment terminals installed, which bring them additional income in the form of rent payments. The launch of the CyberChange project will have a positive impact on the profitability of the installed terminals for a number of reasons.

1. Most small payments in the amount of 10 to 100 RUB will be accepted at the checkout counters, not through the terminal. As a result:

- the load on the terminals will significantly decrease, since small payments account for up to 70% of transactions, but only 5% of the total amount;
- the number of customer claims will sharply decrease, since 90% of issues are related to small payments crediting. This will reduce the load on the terminal network customer support;
- the costs of collecting small bills from the terminals will decrease, since almost all of them will be accepted at the checkout counters.

2. Terminals are rarely equipped with a barcode scanner, thus, accepting payments to the STSI, utility service providers and tax authorities at the checkout will only increase the number of retail customers. Consequently, the client flow of large payments through terminals will increase. Even if the terminal is equipped with a barcode scanner, these gateways for terminal owners are usually an additional service, and a primary source of income.

3. The primary income of the terminal business - repayment of loans in the amount of 2,000 to 5,000 RUB - will remain, because:

- it is very difficult to imagine a person at the checkout counter making a small purchase (for example, beer or chips) and paying for it with a five thousandth bill;
- in almost all cases, these payments are made with an external additional commission from the payer;
- charging a commission for payments of change at the checkout will cause negative feedback from buyers, therefore, retail chains probably will not implement loan repayment at the checkout.

4. Terminals with a barcode scanner provide an opportunity to activate CyberChange cards, which will bring a stable good income to the terminal owner. The amount of commissions for activation is determined by the retailer.

5. Experience shows that the CyberChange card has proven to be a very convenient tool when paying at the terminal. Customers who activated the card at the checkout began to use terminals much more often.

CHANGE CREDITING

Crediting at smart checkout counters

- The cashier scans the card with a permanently installed or hand-held scanner or enters the card number on the keyboard.
- When using a smart cash register with a barcode reader, the barcode is scanned from the CyberChange card.

In addition, the change amount is already stored in the memory of the cash register in both cases.

Crediting in small outlets

An inexpensive Android smartphone can be used in the absence of a cash register with a wide range of functions at the outlet.

The Cyberplat Mobile application installed on the smartphone allows reading the barcode from the CyberChange card. In this case, the amount of change is entered by the seller manually or transmitted from a connected computer with the installed software “Dealer's Cabinet”.

Payment in self-service terminals

- If a barcode reader is installed in the terminal, the barcode is scanned from the CyberChange card.
- Software of the payment terminal immediately displays “CyberChange” and the card (template) number on the provider's screen.

The amount of payment is shown after the client deposits money into the bill acceptor and clicks the "Next" button.

ACTIVATING THE CARD

Activation on the websites of www.киберсдача.рф and www.plat.ru

1. The client goes to the card activation page at www.киберсдача.рф or www.platru, enters the number of the existing card, selects the payee, specifies the phone number and enters the displayed CAPTCHA code aimed at protection against fraud.
2. The website service accesses the CyberPlat® database and checks if the card is activated. If the card has not yet been activated, the client is asked to select a provider and enter the required data: provider's personal account number, mobile phone number and other information.
3. The client enters the requested data.

   Data entry examples:

   MTS, 985-222-33-22;

   VISA, 1234 5678 9012 3456;

   Replenishment of accounts in Alfa-Bank, settlement account 40817810123456789012,985-111-22-33.

4. Having received the data, the CyberPlat® system assigns the entered template to this card number and sends the client an SMS confirmation of card activation.

Activation with pre-recorded voice messages (IVR)

1. The client makes a call to the multichannel number + 7 (499) 68-111-58.
2. A pleasant voice says: “Hello, you have called the CyberChange card activation service. Please enter your card number”
3. The client enters the 19-digit number of their existing card.
4. The service checks if the card is activated. If the card has already been activated, it receives a refusal from the CyberPlat® DB.
5. The client hears: “Unfortunately, this card has already been activated. Enter the number of another card”, then goes to step 3.
6. If the card has not yet been activated, the system determines the phone number from which the call is made, and the client hears: “Your phone number is NNN NNN NN NN. Press to link this number to the CyberChange card. If you need to link another mobile number, enter the required 10-digit phone number, including the prefix, and confirm the correctness by pressing “*”.
7. The client enters the desired phone number, for example, “985 123 45 67”.
8. The client hears: “Operation has been completed successfully. The phone number 985 123 45 67 is linked to your card number 000 0000 0000 0000 1234. I repeat, the operation has been completed successfully. The phone number 985 123 45 67 is linked to your card number 000 0000 0000 0000 1234” (repeated 3 times).

9. In an error is made when entering the phone number, the client hears: “Attention: error! The specified phone number is incorrect Please enter the correct 10-digit phone number and press “*”.

Activation in self-service payment terminals

The client can activate their card in terminals equipped with a barcode scanner only.

1. After performing the usual operation of accepting payment, the client selects the function “Assign the “CyberChange” card number to the payment template” in the terminal software.
2. The client scans the non-activated card number in the barcode scanner.
3. The terminal software accesses the CyberPlat® DB via the CyberChange - Issue (template entry) gateway and checks if the card has been activated. If the card has not yet been activated, it transmits the provider's code, the provider's personal account number, mobile phone number and other information.
4. CyberPlat® assigns the entered template to the given card number and confirms in the terminal software.

The storage of personal data - the name of the provider, the personal account number with the provider, the mobile phone number and their connection to the template number - is prohibited by the rules of the CyberChange payment service.

Activation at cash registers

1. After performing the usual operation of accepting payment, the cashier selects the function “Assign the “CyberChange” card number to the template” in the cash register software (or in the “Dealer's Cabinet” software).
2. The client scans the number of the non-activated card with a permanently installed or hand-held scanner or enters the card number on the keyboard.
3. The cash register software accesses the CyberPlat® DB and, if the card has not yet been activated, transmits the provider's code, provider's personal account number, mobile phone number and other information.
4. CyberPlat® assigns the entered template to this card number and confirms the operation in the cash register software or the dealer's Cabinet software.
5. The cashier gives the card back to the client saying: “Next time come with this card, it will be faster. Take a couple of non-activated cards with you for your family members, activate them at home at websites www.киберсдача.рф and www.platru.

The storage of personal data - the name of the provider, the personal account number with the provider, the mobile phone number and their connection to the template number - is prohibited by the rules of the CyberChange payment service.

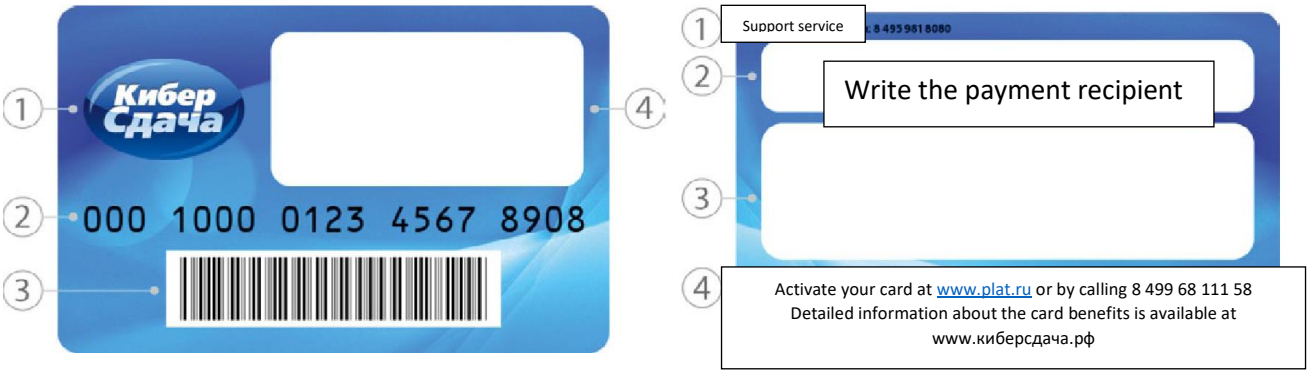
Advantages for "activators" of cards at checkout counters and terminals

Compared to other market participants, retail chains and terminal owners who use this modern service receive serious competitive advantages, which include:

- accelerated transactions for receiving payments;

- increased customer loyalty through the introduction of a new convenient service;
- additional income from the emission of activated cards with advertiser's advertising;
- income from commissions for payment at any other point. In the first year, it is a fixed amount, which is determined depending on the turnover on the activated card.

APPEARANCE OF THE CYBERCHANGE CARD



Exterior styling and design

CyberChange card has the size of a standard bank card. The front side of the card has the following distinctive features:

1. CyberChange logo.

2. Card number: 19 digits, the first three of which are always zero.

3. Barcode.

4. The field for advertising the issuer.

The reverse side of the card has the following distinctive features:

1. Phones of the issuer's support service.

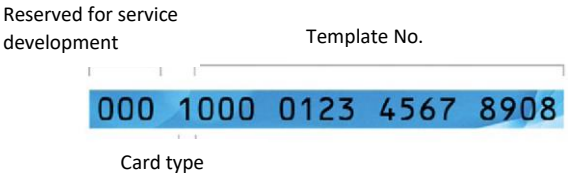
2. Paper strip for manual writing in of the payee.

3. Place for advertising.

4. Detailed instructions for activation.

Also, a sticker with a barcode can be attached to the back of the card, which, if necessary, can be re-attached to the back of the mobile phone.

Number format and template number



The first three digits in the card number are always 0. This feature of card numbering is set to reserve the base of card numbers for the development of the service.

Card type

1 - CyberChange

2 - CyberChange Heavy

3 - CyberPayment

The template number assigned in the CyberPlat® system for this card contains 16 digits, which reflect the card type and template corresponding to the data set in the CyberPlat® database:

1. Service provider. For example, MTS.

2. Personal (or bank account) in the provider's accounting system. For example, 79851112233.

3. Other information.

In the type of card, number 1 means that this is a CyberChange card, number 2 means a CyberChange heavy card, and number 3 means a CyberPayment card.

VIRTUAL CYBERCHANGE CARD

The CyberChange card can be issued in electronic, virtual form on the Internet, saved as a file and used when reading from the phone screen.

- The client goes to the website www.platru and indicates the details of the service provider, the mobile phone number, and enters the displayed CAPTCHA code aimed at protection against fraud in the section “Activate the CyberChange card”.
- The system generates a new card number, displays a barcode on the screen and sends an SMS to the specified mobile phone number with a link to download this code.

CYBERCHANGE CARD ISSUE

Mass issue of non-activated cards

Cards are printed in bulk by an issuer that has concluded an agreement on the implementation of the CyberChange service within the batch of card numbers allocated by the CyberPlat® system.

To maximize coverage of the target audience the following technologies are used in the distribution of cards, including:

- mass mailing;
- distribution at hyper- and supermarkets, shopping and entertainment centers and other places with high customer traffic at the checkout;
- placement in checkout areas, as well as close to payment terminals.

Mass issue of pre-activated cards by the issuing provider

The greatest interest in the mass issue of cards is shown by mobile operators, banks, especially by those with a developed retail network, as well as by providers whose services are used by almost every resident of the country, for example, energy sales companies.

1. The issuing provider sends an application to CyberPlat® and transmits a range of phone numbers or personal accounts.
2. CyberPlat® assigns card numbers that are not yet taken to the received numbers and reports them to the issuer.

3. The issuing provider prints cards in the printing house on their own in accordance with the data received from CyberPlat®.
4. The issuing provider distributes cards by mass mailing to the addresses of its subscribers, and also distributes them in its and partner service offices.

CYBERCHANGE CARD PRE-ACTIVATED BY THE ISSUING PROVIDER

Front side of the card:

1. "CyberChange" logo.

2. Card number.

3. Name of the card (present only on pre-activated cards).

4. Barcode.

5. Field for the issuer's advertising.

Reverse side of the card:

1. Phones of the issuer's support service.

2. Place for advertising.

3. Contact information of the issuer.

Example of a CyberPlat issuer

Support service	Contact Information
Support service: +7 (495) 981-80-80	Details on the advantages of the card are available on the website www.киберсдача.рф The card is the property of CYBERPLAT LLC. 123610, Moscow, Krasnopresnenskaya emb., 12, entrance 7, 12 floor.

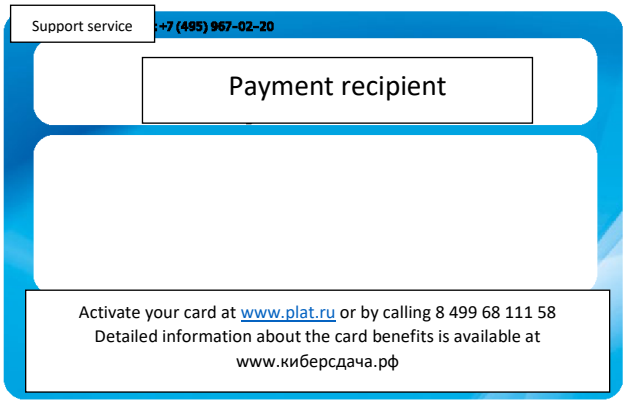
LINKING THE “CYBERCHANGE” CARD TO THE RETAIL CHAIN LOYALTY PROGRAM

The CyberChange card can be combined with a retail chain loyalty card or linked to it. At the same time, the retail chain itself determines the correspondence of the numbers of the CyberChange cards to the numbers of their loyalty cards and independently performs the actions to accrue points and issue trade bonuses.

Project interaction can take place as per the following scenarios.

1. CyberPlat® provides the retail chain with a range of card numbers (barcodes). The retail chain issues half-activated “CyberChange” cards with its own logo, with a loyalty card attached, but the payment details are not yet available. The retail chain distributes cards to customers, and customers independently bind their cards to the payment details required in each specific case: for example, a mobile phone number or a personal account in the management company serving their apartment.
2. The retail chain can link the already existing “CyberChange” card to the new retailer's loyalty card. In this case, the client no longer needs to carry a retail chain loyalty card with them, since they will use the “CyberChange” card as an identifier when receiving bonuses from the chain.

“CYBERCHANGE HEAVY” CARD



Features of the "CyberChange Heavy" card

Transfer of the change amount to the CyberChange card, starting from one kopeck and above, is guaranteed. This is very convenient when a small change remains after paying for the purchase, for example 1 RUB 20 kopecks, which can be transferred to a mobile phone account.

At the same time, not every client wishes to transfer a substantial amount of change to a mobile phone, for example, 800 RUB. If you need to repay a loan or replenish a bank card, the client will appreciate the opportunity to transfer a large amount of change there, but in some cases banks (and some providers) charge a commission for crediting money to the account.

To distinguish between the cards, which amounts can be credited without a commission, and the cards, which always take a commission, a special “CyberChange heavy” card is introduced.

With the help of the “CyberChange heavy” card, you can transfer funds to service providers, payments to which are accepted with an additional fee.

It is recommended to use the CyberChange Heavy Card for replenishing Mir, Visa, MasterCard cards, depositing funds to bank accounts, as well as for making other regular payments.

Exterior styling and design

The “CyberChange heavy” card is visually distinguished only by the “heavy” sign in the name.

From a functional point of view, this means that payments from it are accepted with the obligatory collection of an additional commission from the payer.

Front side of the card:

1. “CyberChange Heavy” logo.

2. Card number of 19 digits, first four digits: 000 2.

3. Barcode.

4. Field for the issuer’s advertising

The reverse side looks the same as that of a regular CyberChange card.

OFFERS FOR ADVERTISERS

An example of a fast "promotion" of a retail network accepting CyberChange cards for payments to a mobile operator

The partnership between a retail chain and a mobile operator in the implementation of the CyberChange service is mutually beneficial. A retailer who accepts CyberChange cards for payments to a mobile operator receives significant benefits for the dynamic growth of customer traffic and, consequently, an increase in the turnover of its retail outlets. The mobile operator obtains has the ability to target the audience for the development of the subscriber base with maximum accuracy without special costs: for example, choosing a specific settlement or even its specific district - in addition to the stable growth in the volume of payments.

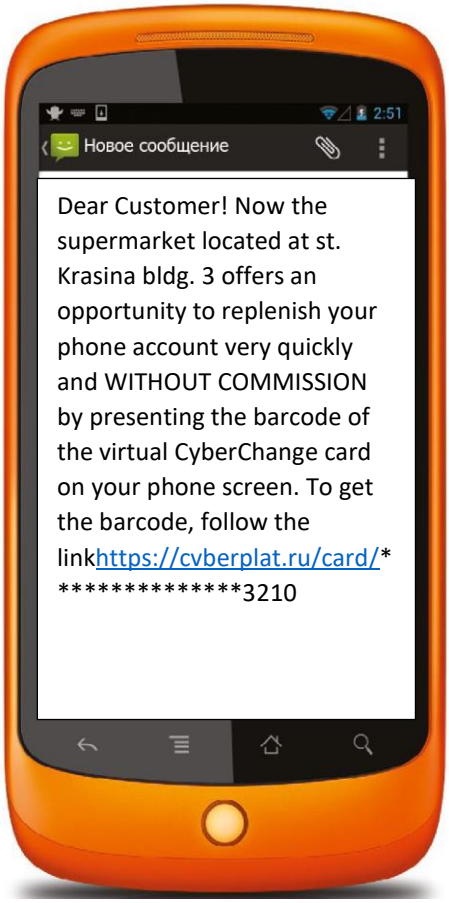
The interaction algorithm is as follows.

1. A preliminary agreement is concluded between a retail chain (super- or hypermarket) and a mobile operator.
2. A fairly large retail outlet is connected to the acceptance of CyberChange cards.
3. The mobile operator sends a message with an approximate content: “Dear customer! Now the supermarket located at the address (the address is indicated) offers an opportunity to replenish your phone account very quickly by showing the barcode of the CyberChange virtual card on your phone screen. To get a barcode, follow the link” to its customers living within the radius of only one cell.
4. An interested customer comes to the supermarket and checks out the service.
5. The cashier, who has previously completed the training, gives the buyer an unactivated card with an advertisement of the retail chain printed on it saying: “It doesn’t always read well from phone. Please activate your plastic card”. Immediately after this, they offer the payer to take several more non-activated cards for themselves or their relatives and friends, as well as a flyer with a detailed description of the benefits of the service.

An example of a fast "promotion" of a payment acceptance network accepting CyberChange cards

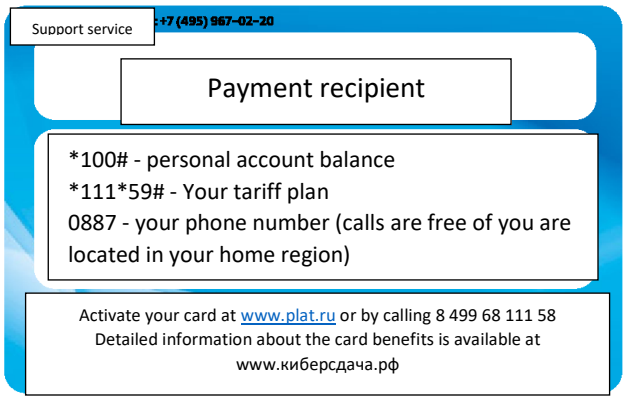
The network of payment acceptance outlets has great potential for profitability growth from the viewpoint of implementing the CyberChange service at checkout counters. For fast and effective promotion, one need to use the existing client base for targeted SMS-mailing * with an invitation to use a new modern and convenient service.

The client receives a message with a link to the virtual CyberChange card, already linked to their mobile phone number, downloads the barcode from the message and uses the phone screen when making the next payment at the checkout counter.



ADVANTAGES FOR ISSUING PROVIDERS* ISSUING CYBERCHANGE CARDS WITH THEIR OWN LOGO

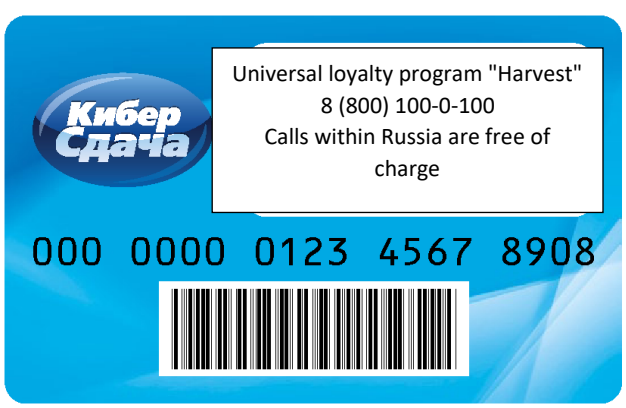
1. According to expert estimates, the growth potential of the amount of funds received to the personal accounts of subscribers as change is $ 72.5 billion throughout the country. It consists of $ 60 billion in food retail and $ 12.5 billion in non-food retail. This value is significantly higher than the entire revenue of mobile communications businesses in Russia.
2. Significant facilitation of the competitive fighting for customers at a minimum cost, since CyberPlat® presents the payment infrastructure and acts as a catalyst for the process.
3. Increased subscriber loyalty through a new modern and convenient service.
4. Increase in ARPU – a key indicator of business performance.
5. Reduced period of subscriber silence due to number blocking caused by insufficient funds on the account, as well as a significant decrease in the probability of such situation occurrence.
6. Increase in the volume of customer information for more accurate marketing activities.

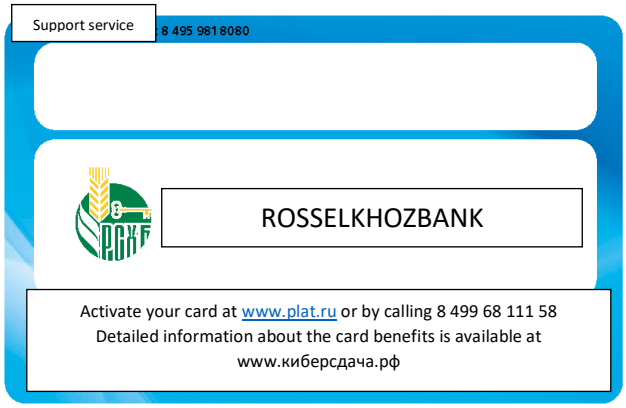


* The names of the organizations are given as examples.

ADVANTAGES FOR ISSUING BANKS* ISSUING CYBERCHANGE CARDS WITH THEIR OWN LOGO

1. Increase in receipts to settlement accounts of individuals who are bank customers by the amount of change.
2. Improved “repayment” of loans and increased payment discipline of clients in general.
3. Tracking of the dynamics of changes in customer loyalty to loan repayment.
4. Increased volume of customer information for providing more accurate marketing activities.
5. No competition fighting for the clients from the service developer’s side. On the contrary, CyberPlat® provides banks with a payment infrastructure and is a catalyst of the process. Increased customer loyalty of the bank thanks to a new modern and convenient service.
6. Elimination of the risk of skimming, since there is no need to use bank cards.
7. A very simple startup: the change amount is credited to bank accounts through the NSPK Mir payment gateways, Visa Money Transfer and MasterCard Money Send, which are already available in the CyberPlat® system. In the future, if necessary, you can develop a direct gateway between the issuing bank and CyberPlat® in order to further reduce the cost of replenishing bank accounts.





* The names of the organizations are given as examples.

ADVANTAGES FOR ISSUING ADVERTISERS* ISSUING CYBERCHANGE CARDS WITH THEIR OWN LOGO

By issuing CyberChange-Tinkoff branded cards, Tinkoff Bank will be able to cover the entire population of Moscow, spending no more than $ 10 million. At the same time, the number of card uses by one consumer will be from 10 to 40 times per month.

For the distribution of cards, Tinkoff Bank uses technologies to maximize coverage of the target audience:

- distribution of cards to cashiers in supermarkets, placement of cards in checkout areas, as well as in places of payments (communication stores, utilities payment acceptance outlets, etc.);
- direct online and offline mailing.

We estimate that marketing costs of around $ 1 per potential cardholder, while plastic production costs should not exceed $ 0.01 per card.

* The names of the organizations are given as examples.

MASS CARD ISSUE*

MASS ISSUE BY BANKS

An aggressive bank, such as Tinkoff Bank, issues cards with its logo and financial services advertisements in bulk and distributes them to customers for free.

The economic efficiency of the CyberChange-Tinkoff card service is determined by the loyalty of its potential clients. On average, cardholders use them from 10 to 40 times per month and keep them “at hand” in their wallets because they are in high demand. When making payments, the client usually informs others about its capabilities, convenience and functionality, many of whom see the card for the first time.

POSSIBLE PROTECTION OF COMPETITORS

A competitor bank offering a standard package of financial services, which does not include the CyberChange card, has to use the “mirroring” technology to ensure the fastest possible response in conditions of severe time pressure.

The Bank promptly issues cards and carries out mass mailing of pre-activated CyberChange cards with its logo and advertising services.

To reduce costs, the bank is forced to focus on controlled retail. For example, Alfa-Bank will first of all carry out mass distribution of non-activated cards in X5 Retail Group retail chains.

MASS ISSUE BY COMMUNICATION PROVIDERS

An aggressive communication provider, such as MTS, distributes cards with their logo and advertising of MTS services to customers in their showrooms for free.

The economic efficiency of the CyberChange-MTS card service is determined by the loyalty of its potential clients. Cardholders use them up to 40 times per month and keep them “at hand” in their wallets because they are in high demand. When making payments, the client usually informs others about its capabilities, convenience and functionality, many of whom see the card for the first time.

Actions of competitors, for example, Beeline

Protection: mass mailing of pre-activated "CyberChange-Beeline" cards with the Beeline logo to their customers.

Attack: mass distribution of non-activated cards in friendly retail chain, for example, in the “Sedmoy Kontinent” chain of stores.

MASS ISSUE OF NON-ACTIVATED CARDS BY ADVERTISERS

An aggressive advertiser, such as Coca-Cola, is distributing cards free of charge with a logo and drink advertisements.

The economic efficiency of the CyberChange-Coca-Cola card is determined by the loyalty of potential owners, which is characterized by the above parameters. Despite the wide popularity of the Coca-Cola brand, the unusual advertising medium attracts the attention of others, many of whom have never seen such a card before.

Protection of competitors such as Pepsi-Cola

To form an effective response, the traditional competitor of Coca-Cola is also forced to issue a card with its logo and massively distribute non-activated cards in friendly retail chains, for example, in the McDonald's fast food chain, in order to save time and resources.

* The names of the organizations are given as examples.

ADDITIONAL OPPORTUNITIES FOR BUSINESS DEVELOPMENT

Barcode payments

Versatility of the CyberChange solution allows the implementation of additional client services based on the tasks facing companies.

If a retailer is interested in an influx of customers with an average and high degree of purchasing power ("rich" buyers), a quick and convenient payment of STSI fines can be organized at the checkout counters of the retail network using the barcode located on the notification.

If a retail chain is interested in increasing the traffic of customers with different purchasing power, payment for utility bills and taxes can be arranged at the checkout counters.

Payment for goods / services from mobile phones

Demand for mobile commerce as one of the most affordable payment methods is growing every year. The CyberChange card allows paying for purchases in stores not only in cash or with a bank card, but also from your mobile phone account.

1. The buyer asks the cashier to pay for the goods / services from the CyberChange card linked to their mobile phone number.
2. The cashier reads the information from the card barcode with a scanner and enters the type of payment and amount. This information, as well as the address and number of the outlet, are encrypted through the CyberPlat® system and are sent to the mobile operator.
3. If the funds on the subscriber's account are sufficient and the payment amount is less than 1,000 RUB, the mobile operator sends a USSD request to confirm the withdrawal of funds. In response, the subscriber sends “1” (agree) or “0” (disagree) from their mobile phone.
4. For payment amounts over 1,000 RUB, a PIN is required by the USSD request.
5. If the subscriber agrees, funds in the specified payment amount are debited from the account in real time.
6. Information on this is transferred to the outlet, and the cashier, having received confirmation, transfers the goods to the buyer or makes a payment for the service and issues a check.

COMMISSION POLICY

For a dynamic mass service introduction, CyberPlat® uses a flexible commission policy and does not establish a single standard tariff plan for all of its partners.

The developer does not limit the amount of the external commission either: its value is set according to the agreement concluded between the card acquirer and the retail chain.

The commission of “activators” of “CyberChange” cards is fixed at 0.25% (including VAT) of the entire turnover of activated cards at outlets not owned by the “activator”, in the first year of service launch.

In the future, the commission amount can be reduced. The issuer's income from advertising at the initial stage of implementation will not be taken into account in the commission policy.

The SMS-message confirming the fact of the payment, indicates the amount credited to the service provider.

BENEFITS FOR THE PROJECT PARTICIPANTS

Benefits for retail chains

- Increase in sales due to buyers who have run out of cash and had no bank cards. Thus, "CyberChange" expands the list of payment instruments for the buyer.
- Growth in sales, primarily of low-cost and high-margin goods, which are usually located in the checkout area.
- No additional costs due to the use of a ready-made high-tech solution.
- The fastest payment speed, surpassing the payment time when using a bank card: the whole transaction takes no more than 6 seconds.
- The use of a barcode practically eliminates the possibility of entering erroneous data and, as a result, eliminates the cost of processing erroneous payments.
- Reduced risks of working with cash.

Benefits for mobile operators

- No investments.
- Staying ahead of the competition in implementing real mobile commerce.
- Creation of the image of a super-tech company.
- Minimizing errors and reducing the cost of canceling and adjusting payments as a result.
- Reducing the transaction time, which will allow to:
  - reduce the cost of accepting payments,
  - speed up the time of accepting one payment.
- growth of balances on subscribers' accounts, which leads to a significant increase in the company's liabilities.
- increase in revenue, increase in popularity, and, consequently, capitalization of the company.

Benefits of participation for clients

- The buyer receives a new convenient modern payment instrument.
- additional psychological comfort when paying, since the trust in telecom operators in our country is higher than in banks.
- Maximum security: no need to tell the phone number for all to hear, the withdrawal of funds is confirmed by the subscriber.
- the broadest possibilities for replenishing a personal account: the retail chain is significantly larger than the infrastructure for accepting cards of a particular bank.
- The payment speed is faster than with a bank card.

GLOBAL E-BUSINESS TECHNOLOGIES. INTERNATIONAL CYBERPLAT® PROJECTS

CYBERPLAT INDIA — A LEADER OF THE NATIONAL FINTECH MARKET

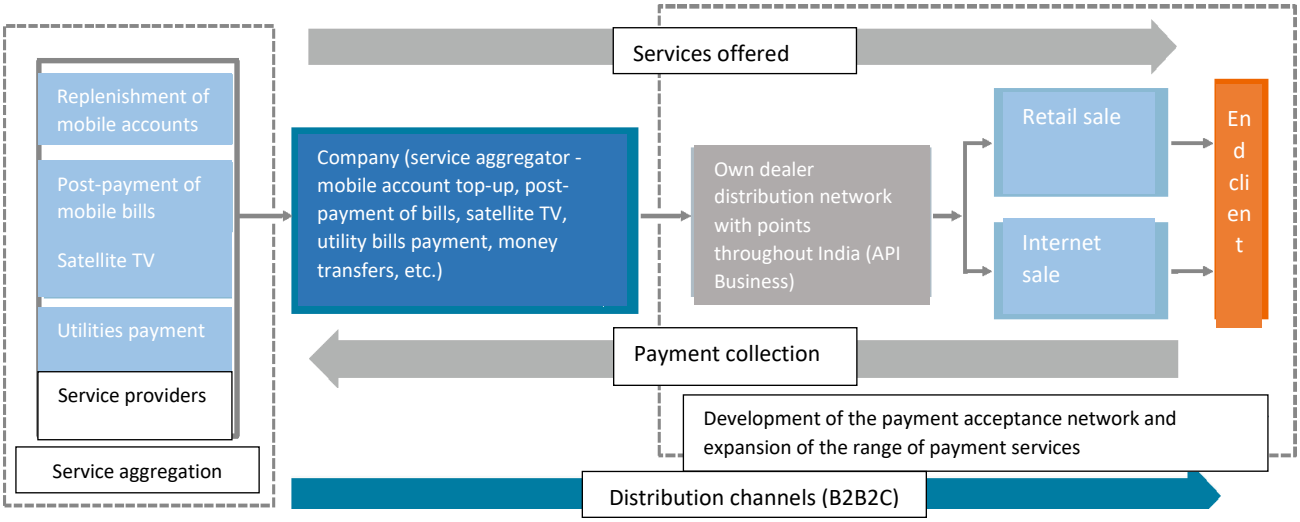
GENERAL INFORMATION

One of the largest international projects, CyberPlat®, was launched in India more than 10 years ago: CyberPlat India was founded in Mumbai in 2009 (www.cyberplat.in).

The company developed at a rapid pace and has demonstrated an annual 100% growth for several years in a row, confidently outranking its competitors.

CyberPlat India is currently among the leaders in the national financial technology industry. The company is included in the TOP-5 payment systems operating in one of the largest Asian markets, and ranks 1st in the number of payment outlets in the country: as of January 1, 2019, their number exceeded 760 thousand. More than 240 million transactions to more than 350 service providers in India and abroad, available in 600 partner networks, are performed each year in the system.

CyberPlat India is one of the few payment aggregators in India that cooperates directly with more than two dozen largest providers rendering services in the field of telecommunications, satellite TV and housing and utility services.



Business model

PRODUCTS AND SOLUTIONS

CyberPlat India offers its partners a wide range of modern financial services that are in demand among the country's residents.

Replenishment of mobile phone accounts

CyberPlat India is one of the few payment integrators in the country that has direct gateways with all telecom operators and offers a unique multifunctional service for replenishing personal accounts of mobile operators using various devices.

Cross-platform hardware allows choosing a payment method and making payments using a computer connected to the Internet, a web application, an Android phone, an ATM or a self-service payment terminal.

Payment for satellite TV services

CyberPlat owns the most extensive infrastructure for collecting payments for services of all commercial television (DTH) providers operating in the country. The unique CyberPlat® API and web platforms allow the supplier to choose the most efficient and marginal option from the view point of its business.

Post-payment for mobile and fixed line communication services

CyberPlat arranges collection of payments to all mobile and fixed-line operators providing services both in the country and abroad. CyberPlat partners gain an important competitive advantage by offering the whole range of the most popular telecommunication providers at a single payment acceptance outlet.

Payment for internet service providers

Internet users, the number of which exceeds 283 million in the country, can pay for the services of Internet providers with maximum convenience by choosing an appropriate payment method: online or offline. For example, they can make a payment on the CyberPlat partners website or in a nearby retail store, and the money will be instantly credited to their account.

Payment for insurance services

Payment of insurance premiums must be made within strictly defined terms, and CyberPlat has to offer a ready-made effective solution allowing to organize the collection of insurance premiums from different companies according to the one contact principle.

Money transfers

Money transfer service is one of the most demanded services in India. However, large segments of the population living in rural and semi-urban areas still lack access to basic banking services due to an extremely low density of banking coverage of these conglomerates.

CyberPlat technologies make it possible to solve this problem: they combine banking services and e-wallets on a unified API platform and provide an opportunity to make money transfers in partner retail chains.

Payment for gift cards

CyberPlat offers the widest range of products from the Top Indian 50 brands, brought together on a single IT platform, giving users the opportunity to choose whatever they really need as a gift.

Payment for utility services

Timely payment for utilities - electricity and gas - is extremely important for the residents of the country. CyberPlat provides an opportunity for convenient and quick payment for the services of more than 25 suppliers of these energy resources at payment outlets located close to the consumers.

Business to Business

CyberPlat offers its B2B partners various distribution models and methods of online and offline integration, which are primarily addressed to:

- distribution companies;
- e-commerce companies;
- startups;
- retail businesses;
- banks;
- public service centers;
- support services.

DISTRIBUTION MODELS AND METHODS OF INTEGRATION

- Retail distribution - access to more than 500 thousand payment outlets of CyberPlat partners
- Distribution in rural areas - access to the “last mile” through the CyberPlat payment infrastructure with a high degree of availability in rural areas.
- Modern retail business- implementation of payment services in the largest modern retail chains operating in the country.
- Banking infrastructure - access to ATM networks, banking web portals and mobile applications.
- E-commerce - cooperation with leading players in the e-commerce market.
- Mobile commerce - partnership with the leaders of mobile commerce: all key players of the national market are available in the CyberPlat system.
- Terminal networks - integration of services into India's largest self-service payment terminal network.
- Loyalty programs – wide level of choice, ease of integration, flexibility of customization, efficiency.

BENEFITS FOR CLIENTS AND PARTNERS

- Innovative payment solutions used in many countries around the world, including Russia, Germany, and Austria.
- Ability to make payments using various devices: computers connected to the Internet, web applications, smartphones based on Android OS, ATMs or payment terminals.
- Complete security of payment transactions: within the entire period of system's operation there was not a single hack of the system or an illegal transaction.
- Acceptance of payments to cross-border service providers.
- Increase in the volume of high-margin transactions.
- Priority development of the services most demanded by the population.
- Expansion of the payment infrastructure by several times in the shortest possible time and with minimal costs.
- Steady and stable growth of a quality customer base.
- Strengthening loyalty of existing customers.

CYBERPLAT KAZAKHSTAN - THE FOUNDER OF THE ELECTRONIC PAYMENTS MARKET IN THE REPUBLIC OF KAZAKHSTAN

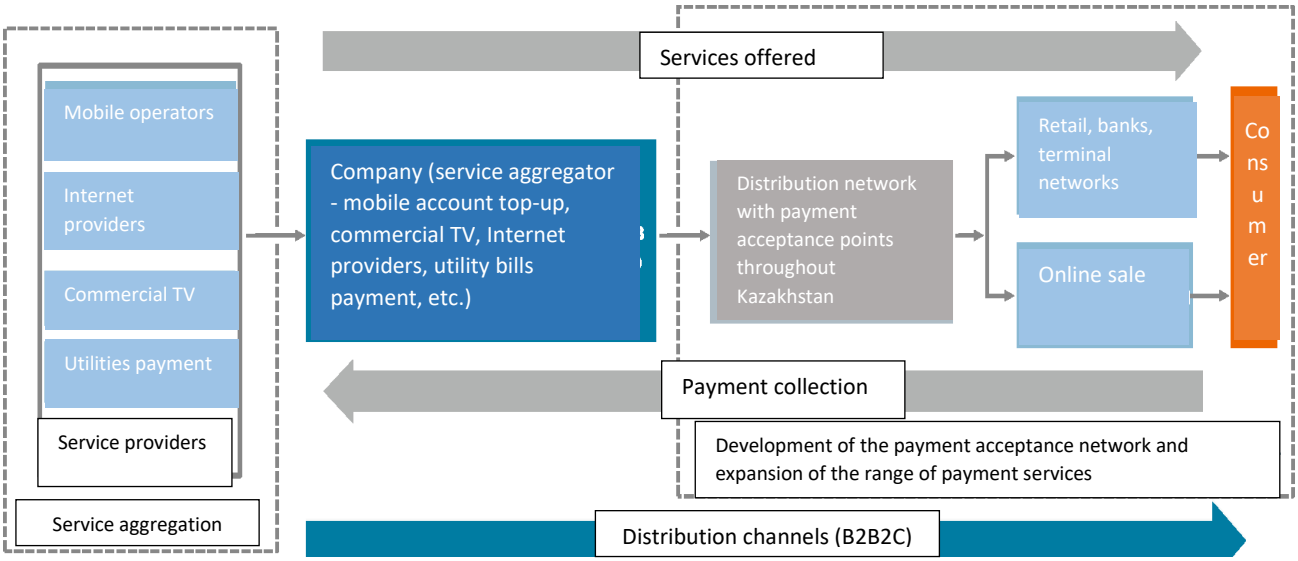
GENERAL INFORMATION

The Republic of Kazakhstan became the first foreign state within the framework of the CyberPlat® global e-business strategy, in which the company successfully implemented a project to create a large-scale payment infrastructure. CyberPlat Kazakhstan was founded on September 15, 2005, and the first electronic payment through the CyberPlat® system in this country was made in April 2006.

The development of the company took place at a rapid pace. In a short time, an extensive infrastructure for receiving retail payments was created in the country, allowing the population to pay for the most popular services in a quick and convenient way. At present, the CyberPlat® payment network in Kazakhstan has over 20 thousand outlets.

CyberPlat Kazakhstan offers its partners the opportunity to replenish accounts using various devices: computers connected to the Internet, web applications, smartphones based on Android OS, ATMs, self-service payment terminals.

The system operation is characterized by the highest reliability and fault tolerance. The system is based on two processing centers in the territory of Kazakhstan, the connection between which is duplicated through the networks of independent providers.



General business model

This redundancy arrangement in combination with a modern cluster architecture provides high fault tolerance and independence from force majeure circumstances.

Complete security of payment transactions is guaranteed: over the entire period of operation in the country there was not a single transaction hack.

The high quality of CyberPlat® service and its undeniable technological advantages contribute to the further intensive development of the electronic payments market in Kazakhstan.

CLIENT BASE

Service providers

Successful development of high-tech business segment in Kazakhstan immediately attracted the attention of the leading players of the national market, who shortly appreciated the effectiveness of cooperation with the electronic finance market leader.

CyberPlat Kazakhstan has payment gateways to all leading mobile operators, Internet providers, utility providers, energy sales companies, banks, microfinance organizations, MLM operators, bookmakers and other service providers.

The company also accepts payments to cross-border suppliers. The total number of providers exceeds 300 companies and organizations.

The partners of the electronic payment system are companies with a large-scale coverage: networks of mobile phone outlets, electronics and household appliances stores, the largest

terminal networks and other representatives of various business sectors of the Republic of Kazakhstan.

The joint project "CyberPlat Kazakhstan" implemented together with JSC "Kazpost" - the national postal operator with an extensive network of 3200 branches – was a key milestone in the development of the country's payment infrastructure.

Partner banks

Influential federal and industrial banks operating throughout Kazakhstan are among the company's partners. CyberPlat® is consistently developing cooperation, offering modern financial services for replenishing bank accounts, repaying consumer loans, replenishing cards of international payment systems and a large-scale republican payment network for making payment for various services by bank clients.

BENEFITS FOR CLIENTS AND PARTNERS

Partners of CyberPlat Kazakhstan hold the possibilities of cooperation with the leader of the country's payment industry in high regard, identifying the following positive factors in organizing a business as significant:

- innovative payment solutions used in different countries of the world;
- steady and stable growth of a high-quality customer base;
- strengthening the loyalty of existing customers;
- expansion of the payment infrastructure in the shortest possible time and with minimal costs;
- increase in the volume of high-margin transactions;
- wide and continuously updated list of services;
- priority development of payment services most demanded by the population;
- cross-platform payment solutions: the ability to make payments using various devices;
- highest fault tolerance and independence from force majeure circumstances via a modern reliable IT architecture with a multiple safety margin of resources;
- complete security of payment transactions: within the entire period of system's operation there was not a single hack of the system or an illegal transaction.

INNOVATIVE CYBERPLAT® SERVICES FOR FOREIGN TELECOM OPERATORS

OFFERS FOR FOREIGN TELECOM OPERATORS

As part of the global expansion to the world market of electronic financial services, a priority area of CyberPlat® is cooperation with the largest players in the telecommunication services segment.

CyberPlat® offers the following benefits to the foreign communication providers:

- 20 years of successful experience in efficient organization of payment acceptance;
- efficient transaction processing technology, exceeding similar products of competitors in performance by 10 times;
- proactive strategy of intensive development;
- availability of services in many countries;
- 4-fold reserve of processing technological capabilities;
- highly qualified team of IT developers and financial experts.

CROSS-PLATFORM HARDWARE

A key competitive advantage offered by the CyberPlat® system to foreign partners is the freedom to choose the convenient payment method and use various devices for making payments, depending on the partners' requirements.

Payment can be made using:

- computers or smartphones;
- cash registers;
- POS terminals;
- self-service payment terminals;
- ATMs;
- Internet Bank-Client;
- mobile display units.

SECURITY OF PAYMENTS

CyberPlat® technology ensures absolute security of financial transactions and minimizes the number of payments made in error.

Up to 16 operations are performed in the system, certified by an electronic signature, within the framework of a single transaction. Secured methods of data transmission via the Internet, including checking the availability of phone numbers or personal accounts of customers in the billing systems of service providers, identification and authorization of payment acceptance outlets and other operations, are used.

There has not been a single case of information system hacking or illegal transaction occurred in the CyberPlat® system over the entire period of its operation.

ADVANTAGES OF CYBERPLAT® OVER OTHER PAYMENT TECHNOLOGIES

Historically, the main competitor of CyberPlat® payment technologies in many countries is express payment cards, or scratch cards. This financial product is the equivalent of funds used to top up the personal accounts of mobile subscribers. Scratch cards are most in demand in the payment segment of $ 5 to $ 25, which turn out to be unprofitable when paying for communication services in the banking infrastructure.

Despite the certain demand for scratch cards, they have a number of obvious disadvantages:

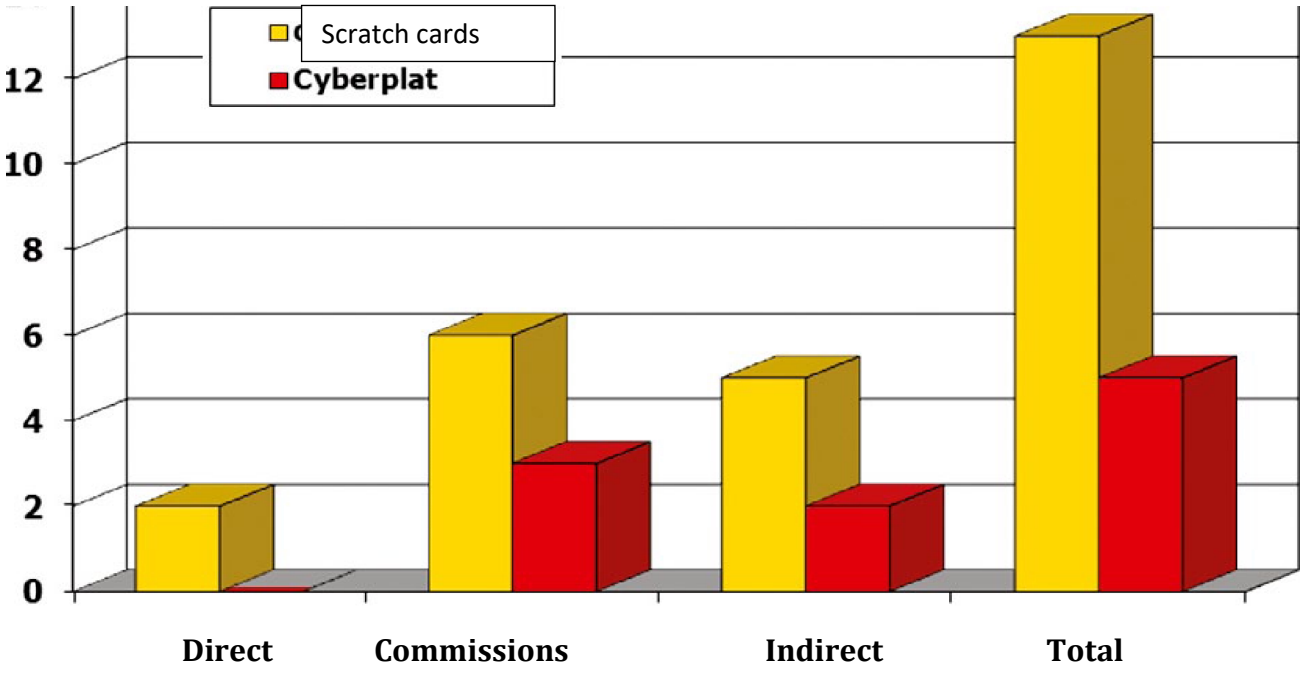
- high production cost;
- preset card denomination;
- a lengthy time interval between the production order and card activation;
- excess of registration access codes (closed and open, barcodes);
- short card "lifetime" for the user - in 99% of cases, it is 5-10 minutes;
- impossibility of activating the scratch card to another phone number.

Operator costs

Direct costs of mobile operators using scratch cards are quite high and reach 12%.

They consist of the following types of expenses:

- external costs (about 2%);
- card production - about $ 0.2 per card;
- costs of maintaining personnel of production and commercial units;
- costs of financial departments personnel;



Comparison of costs: CyberPlat® vs. scratch cards

- costs for safekeeping of cards;

- costs of monitoring the work of staff at the outlet (staff's fraud);
- anti-counterfeiting costs;
- collection costs;
- dealer commission (about 6%).

The operator's indirect costs depend on the trade margin of the retail chain selling the scratch cards, and usually amount to approximately 5%. In other words, in 95% of retail, a $ 10 card should be sold for $ 10.5, and, thus, a subscriber has to pay a 5% commission for receiving mobile services.

It is obvious that the subscriber anticipates the amount of money they are willing to pay and tries to avoid additional costs. That is why they will prefer to pay exactly the required amount through the CyberPlat® system instead of buying $ 10 with a $ 10.5 scratch card. The provider, in turn, will be able to receive the entire amount paid by the subscriber.

When paying in the CyberPlat® system, direct costs are made up of the provider's external costs for the personnel who developed the payment gateway (usually 5-7 persons in the IT department) and is engaged in its technical support. The total amount of costs does not exceed 0.01% of the turnover and can always be even closer to zero.

Another expense item is the commission paid to the CyberPlat® system. In the first year of operation, the commission is 3%, and decreases to 2% in subsequent years.

When using the CyberPlat® electronic payment system, mobile operators can reduce direct and indirect costs by an average of 5-13%.

	Scratch cards (prepaid service only)	CyberPlat® (any tariff plan)
Step 1	find an outlet selling cards of the required value	Find a CyberPlat® payment acceptance outlet
Step 2	Buy a card of the required denomination	Top up your account with any amount to any phone number
Step 3	Call the card activation system	No
Step 4	Enter PIN-code (12-16 digits) from the phone keypad	No
Step 5	Make sure that your phone balance is topped up	Make sure that your phone balance is topped up
Risks	Purchase of a counterfeit, expired card or its loss	No

Use of CyberPlat® technologies helps to improve the quality of the operator's subscriber base and strengthen the loyalty of service users, reduces the probability of customer outflow, and also reduces the cost of attracting new subscribers.

According to experts, these advantages of CyberPlat® alone cause the growth of the subscriber base of foreign telecom operators of 8-10%, and in the case of complex integration, it can reach 20%.

BENEFITS FROM IMPLEMENTING CYBERPLAT® PAYMENT SOLUTIONS

- Complete elimination of costs associated with the production and maintenance of scratch card technologies (cost savings - more than 10%).
- Reduced total cost of business support.
- An increase in the number of small payments ($ 5 or less), which make up the majority of payments, contributing to an increase in the company's turnover up to 10%.
- Customer base growth (up to 20%).
- Reduced duration of the "silence period" of subscribers.
- Increase in sales volume (up to 20%) due to an increase in the traffic of payers attracted by the convenience of payments in retail outlets with the CyberPlat® service.
- Additional income due to the crediting of change from purchases to the mobile phone account at the checkout counters of retail outlets.
- Profit growth and increase in the market value of the company.

CONTACTS

Cyberplat LLC

Central office:

123610, Moscow, World Trade Center, Krasnopresnenskaya emb., 12, entrance 7, floor 12

Tel.: +7 (495) 967-02-20, Fax: +7 (495) 967-02-08

e-mail: info@cyberplat.ru, sales@cyberplat.ru, market@cyberplat.ru

skype: CyberPlat

www.cyberplat.ru

Technical support service:

Tel.: +7 (495) 981-80-80,

+7 (495) 967-02-20

e-mail: help@cyberplat.ru,

support@cyberplat.ru

skype: support_cyberplat

Regional directorates:

Mid-Volga Region (Samara)

mobile +7 (960) 808-39-70

e-mail: samara@cyberplat.ru

Central Black Earth Region (Kursk)

mobile +7 (910) 210-81-84

e-mail: kursk@cyberplat.ru

Ural (Yekaterinburg)

Tel./ Fax +7 (343) 379-01-65

mobile +7 (922) 228-76-48

Yekaterinburg, Frontovykh Brigad st., 18a, room 308

e-mail: ekaterinburg@cyberplat.ru

South (Stavropol Territory)

mobile +7 (928) 815-52-08

e-mail: stavropol@cyberplat.ru

Subsidiary in Kazakhstan:

KYBERPLAT KAZAKHSTAN LLP

Republic of Kazakhstan,

050000, Alma-Ata,

Gogolya st., 84a, office 201

Tel.: +7 (727) 2-500-861,

+7 (727) 2-663-951,

+7 (727) 2-508-563,

+7 (777) 2-780-006

(Beeline numbers free of charge)

Fax: +7 (727) 2-508-564 (доб. 107)

e-mail: info@cyberplat.kz

www.cyberplat.kz

Subsidiary in India:

Stylus Serviced Offices, 801,

8th Floor, A-Wing, Reliable Tech Park, Behind Reliable Plaza, Off Thane Belapur Road, Airoli, Navi Mumbai — 400 708

Business Enquiries: +91-22-30114605, +91-22-30114604

Support Numbers: +91-9004-66-3334, +91-9004-66-3339

E-mail: help@cyberplat.in

Skype: helpdesk.cyberplatindia

http://www.cyberplat.in

APPENDIX

PAYMENT TECHNOLOGIES

CYBERCHECK USING BANK PLASTIC CARDS

Registration of a plastic card holder

1. The holder of the MIR, VISA, MasterCard plastic card (hereinafter referred to as the Buyer) is registered in the CyberPlat® electronic payment system.
2. When registering, the Buyer indicates:

- Their personal data (surname, first name, patronymic, passport data, e-mail address, postal address, telephone);
- parameters of their card (name of the payment system in which the card is registered; card number; expiration date; name of the cardholder in the transcription used on the card).

Information on the card is transmitted in a secure form only to the CyberCheck server of the CyberPlat® electronic payment system during the Buyer's registration and is not provided to the Store when the Buyer's transactions are carried out.

Online purchase and payment processing

The procedure for purchasing goods in Stores is carried out using the CyberPlat® technology.

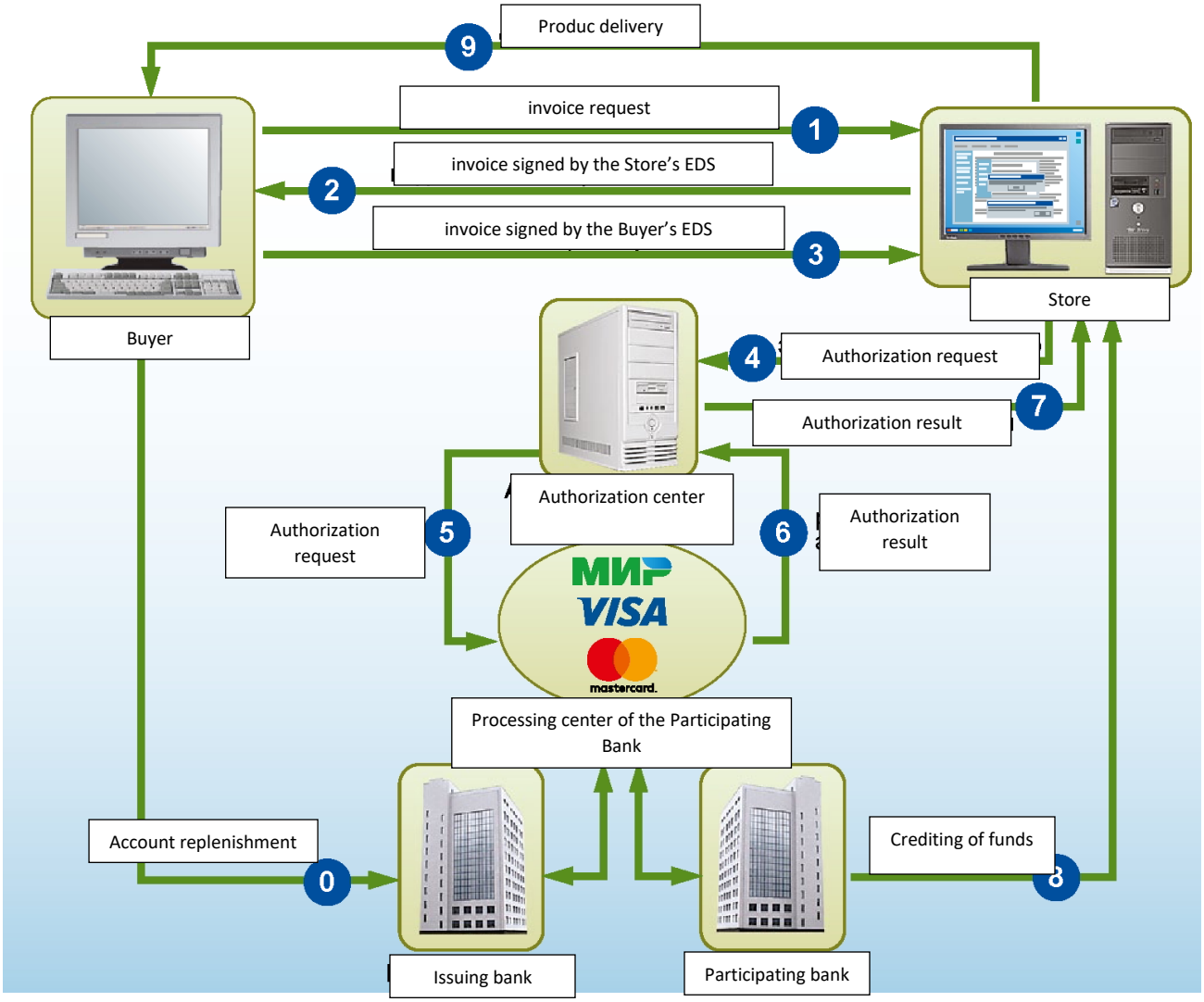
1. The Buyer connects to the Store's web server via the Internet, forms a basket of goods and sends a request to the Store to issue an invoice.
2. In response to the Buyer's request, Store sends them an invoice signed by its electronic signature, in which it indicates:

- name of the product (service);
- cost of goods (services);
- store code;
- time and date of the transaction.

From a civil law point of view, this invoice is an offer to conclude an agreement (formal offer).

3. The Buyer signs the invoice presented with their electronic signature and sends it back to the Store, thereby accepting the offer (agreement). The agreement is considered concluded from the moment the Buyer signs the invoice issued. In the system, the invoice signed by the Buyer becomes a check.
4. The receipt signed by two ESs (the Store and the Buyer) is sent by the Store to CyberCheck for authorization.
5. CyberCheck verifies the signed check:

- checks the Store and the Buyer in the system;
- checks the electronic signatures of the Buyer and the Store;
- saves a copy of the receipt in the CyberCheck database.



6. If the check result is negative:
- CyberCheck sends the refusal to process the payment to the Store;
- The Buyer receives the refusal with a description of the reason.
7. If the check result is positive:
- the check is forwarded to the CyberPOS server to generate an authorization request;
- CyberPOS transfers it to the processing center of the Participating Bank;
- the authorization request is transmitted through closed banking networks to the Bank - the Issuer of the Buyer's card or the processing center of the card payment system authorized by the Bank-Issuer.
8. With a positive result of authorization received from the card payment system:
- The processing center of the Participating Bank sends the positive authorization result to CyberPOS;
- CyberPOS sends the positive authorization result to CyberCheck;
- CyberCheck sends the positive authorization result to the Buyer;
- CyberCheck gives the Store permission to provide the service (release the goods);
- The Store provides the service (releases the goods);

- The Participating Bank credits funds to the Store’s account in accordance with the existing contractual relationship between the Participating Bank and the Store.

9. If authorization is refused:

- The processing center sends the refusal to process the payment to CyberPOS;
- CyberPOS sends the refusal with a description of the reason to CyberCheck;
- CyberCheck sends the refusal with a description of the reason to the Buyer;
- CyberCheck sends the refusal to process the payment to the Store.

The Buyer has complete control over the purchase process. As a documentary confirmation of the transaction, each party retains a signed electronic signature receipt, confirming the fact of the transaction and having legal force.

Statement of account

1. The Buyer requests a statement of their account by signing the request with their ES.
2. CyberCheck verifies the Buyer's code and electronic signature.
3. If the verification results are positive, CyberCheck sends the Bank a request for the statement, receives the statement and forwards it to the Buyer in the form of a cryptographically converted text with CyberCheck's digital signature.
4. The Buyer receives the message, verifies the CyberCheck signature and performs the reverse cryptographic transformation of the statement.
5. The Buyer saves the statement on their computer.

Request for processing Buyer's payments in the Store

1. The Buyer requests information on the payments made in the given Store, indicating their code in the CyberPlat® system.
2. Based on the received code, the Store provides information on the payments of this Buyer.

CRYPTOCURRENCY RISK MANAGEMENT

The question of blockchain arose before me for the first time after the speech of German Oskarovich Gref at the Davos Forum in 2014. I was asked then what Bitcoin was, and I had never dealt with it, and I had nothing to say. I even felt disappointed: how come that German Oskarovich Gref knows about it, but I don't? Moreover, he and I talked for a long time about technologies (he wanted to buy Cyberplat, but we did not agree on the terms) in 2010-2011, and I have a very good idea of the amount of his knowledge in digital technologies.

I have been dealing with computers since 1983 straight and I am deeply submerged into this topic. And he is basically a humanities-minded person, and his view of IT can hardly be deeper than mine. What use has the idea of teaching Sberbank employees a mathematical tool of artificial intelligence at your university, for example?! I engaged in artificial intelligence technology in 1988-1989 a little and I know very well that you must first study mathematical analysis, linear algebra, probability theory, mathematical statistics, modeling methods, algorithmic methods... and then you can come near the basics of artificial intelligence! Not every excellent student with a strong technical education can comprehend such a topic, and even more so a soft scientist: it's like teaching a sailor of the Revolution times the differences in the painting technique of the Impressionists.

Nevertheless, I began to acquaint myself with what bitcoin is, and came to a sad conclusion. Why was it sad? The majority happily tell us: “Everyone goes there, everyone earns money there!"” But unlike most, I know,

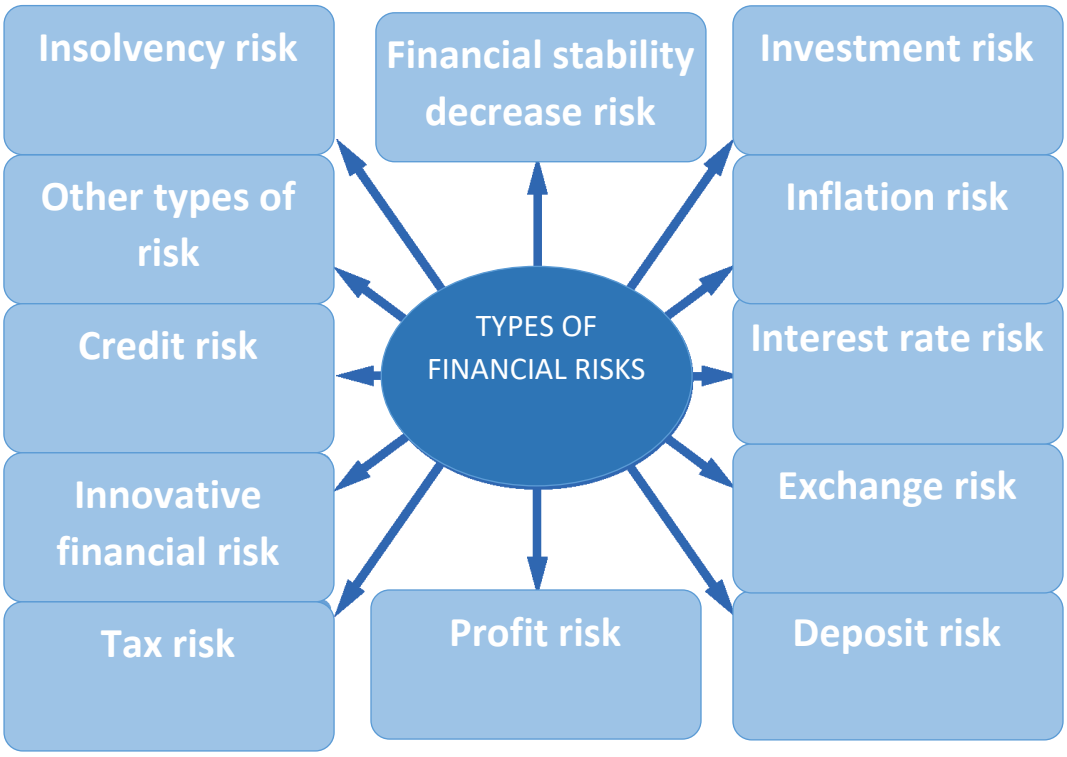
WHAT RISK MANAGEMENT IS

I will try to explain this concept to you in the most popular way, not going deep into the profile subtleties. Take the insurance business, for example. How are car theft insurance premiums formed? Insurers look at the statistics of the theft of a particular car brand over the past year. Let's say 3% of cars were stolen... They offer a 4% rate and know that if they insure 100 cars, three cars will be stolen, and they will withhold the premium on the fourth one, and they will still earn enough to buy a car. This is the essence of risk assessment - knowing the amount of risk as accurately as possible. And if, after receiving nice bonuses, you also try to “persuade” the car thieves not to engage in thievery, this is already risk management.

In the banking business, risk assessment is usually presented in the form of interest rates. When a potential borrower comes to a bank, bankers calculate their risks: the country risk costs this much, the risk to the legal system costs this much, the risk to the economic sector, the risk to the owner, the risk to the development of technologies ... All these risks add up to form the final loan rate - for example, 12.5% per annum. And the client is shown why exactly it costs this much, and not, for example, 10% and not 15%.

Risks in new technologies should also be considered like this. When financial experts and / or IT specialists “enter” a new area in a professional sense, they surely create the new area risk management: a hypothetical book, where the table of contents is a list of risks, and each chapter is a description of the risk as such, its boundary values and methods for its minimization.

Let's see how similar situations have been handled before. For example, to manage credit risks, bankers hired lawyers, developed long loan agreements, then realized that they needed to have a security for these credit risks.... Lending in its current form did not appear all at once! Banks are only 400-500 years old as institutions, and such instruments as legal support of loan agreements, collateral options, guarantees, sureties, pledges, etc. have been invented in these 500 years.



There are estimated risks. To overcome them, the companies involved in making estimates are licensed. Not everyone is engaged in settlements en masse, but only those whom the Central Bank is regularly keeping an eye. When they came up with checks, they made a whole legislation around them. As they did for letters of credit, and escrow accounts.

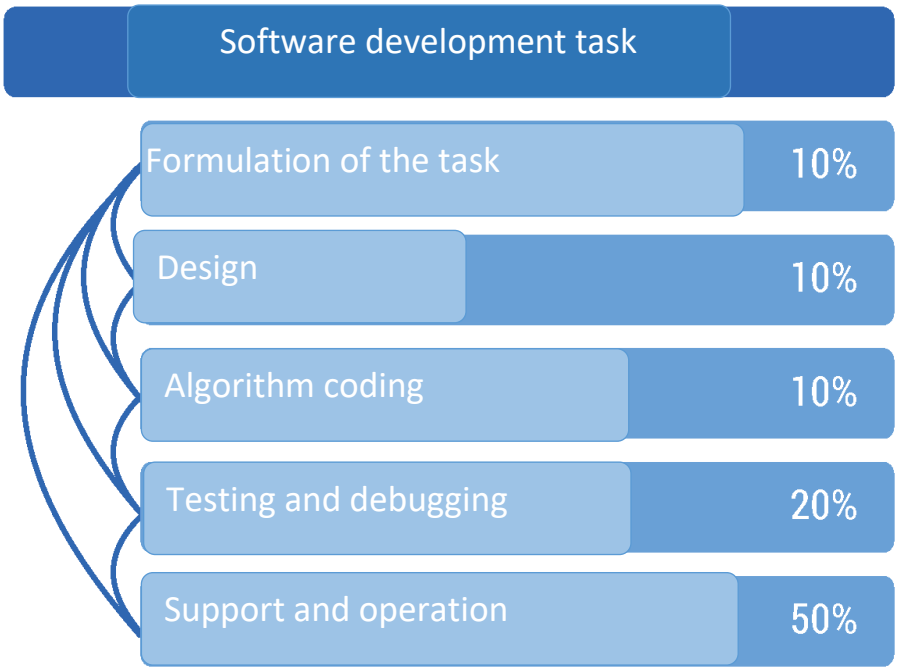
The history of the credit and settlement risks management creation shows that it is quite possible to solve the issues of blockchain, bitcoin and other cryptocurrency risk management. And the solution is three-stage as ever: listing of risks, description of risks (threat model), work on finding methods to minimize them.

Where we are in cryptocurrency risk management now

First of all, in Russia and worldwide, there is little understanding of the origin of this technology and the goals pursued by its creators. Natalya Kasperskaya told a little about the American origin of bitcoin, but most people, in principle, do not understand who created it and for what reason. What was the technical task for its development, if this was the result obtained? Why did the creators choose these technological principles from the huge variety of options at their disposal?

The issue of an ignorant assessment of the impact of technology on life often lies in maximalistic assumptions stemming from the fact that such an ignorant assessor does not even have the slightest idea of what he is talking about. There is one assessment: our whole life is going to change globally, because blockchain has emerged. And there is another: you shouldn't meddle with it, because cryptocurrencies are an organized fraud. Can you imagine

the gap? It's not even a situation where you walk into a dark room and don't know if there is an elephant or a cat. This is a situation where you are not sure if you are in the room at all.



Software development stages

WHAT PLANE DO THE RISKS OF CRYPTOCURRENCY LIE IN?

This is why, when I began to study cryptocurrencies, I looked exactly at the list of risks... And I discovered that not just that there are many, but that they also lie across three large different planes: IT risks, economic risks, legal risks. And it is almost impossible to find one universal specialist who would understand all these areas at once. There is not more than a dozen of such people in the country, and it is unlikely that they work officially.

Thus, in the scheme of things, before dealing with cryptocurrencies, you need to make a list of all the possible risks, and divide them into professionally oriented risk groups, where each of them will be analyzed by an appropriate specialist. The legal risk group is for a lawyer, the economic risk group is for an economist, and so on. Because when an economist starts talking about IT risks, nothing good comes of it. This is the main problem of all digital currencies: everyone talks about their own, and it never occurred to anyone that everyone who wants to engage in this needs to gather together, create a society consisting of profile departments, which would attribute each risk to the competence of the relevant department.

The first conclusion is that the main problem of analyzing blockchain technologies requires an extensive competence in different areas.

What areas?

First, it is basic electronics, or understanding how computers work in general. You need to understand why it is based on the binary number system (namely ones and zeros), and not, relatively speaking, on twos or threes.

Then the most state-of-the art electronics is very important, the so-called electronics of "closed" areas, first of all - military electronics, in which special algorithms are used. After all, there are no purely peaceful technologies. If a person invents something, this invention is first used to kill all rivals.

An extensive competence (including many years of experience) in various areas is required:

- General electronics
- Electronics of "closed" areas
- Public law jurisprudence
- Private (commercial) law jurisprudence
- Macroeconomics

There are very few specialists who are competent in all of the above areas at the same time. There are no officials with the right to prepare or make decisions in all of the above areas simultaneously.

The main problem of blockchain technology analysis

When humanity managed to split the atomic nucleus, 300 thousand people were killed in Hiroshima and Nagasaki to begin with. I think that the ape took the stick for the first time not to knock the fruit off a tree, but to knock on the head of another ape.

The same is true for electronics – be assured, everything that we see in the peaceful area was used in the military first. For example, mobile communications are a field communication grid developed in the mid-20th century for military use. Some of this technology was declassified and it became available to ordinary subscribers. The Internet was originally called ARPANET and connected several hundred military institutions and businesses in the United States. It was declassified, transferred to the public domain - now we send each other emails, watch news and visit other sites.

So, in order to analyze the blockchain technologies, you need at least basic knowledge of two field of electronics.

Then comes jurisprudence. It is necessary to know both public law: how cryptocurrencies, money, settlements are regulated by the state, and private (trade) law, that is, how two equal persons (legal or physical) can exchange them.

And, of course, macroeconomics.

Try imagining how many people are knowledgeable in all these industries well enough? Personally I was lucky, I have these three educations: electronic (Moscow Institute of Electronic Engineering), financial (Financial Academy[1]) and legal (law department of Moscow State University).

And the top-level problem is not even finding multidisciplinary universal specialists. The problem is to find such universal officials, because they are the ones who must regulate

processes at the state level, in the field of public law, but in macroeconomic interests, and relying on knowledge in the field of electronics.

LET'S CONSIDER THE MACROECONOMIC RISKS FIRST

The first risk is the risk of insufficient literacy of top managers. An example. A speaker holding a very responsible position spoke at one a specialized conference, who said that blockchain and bitcoin are completely different things that need to be approached in different ways. The thing is, Bitcoin was created based on blockchain technology. And what is interesting, no one objected, rebelled, no one shushed him...

Another risk is the underestimation of future damage arising from the emergence of new threats due to the development of technologies used for criminal purposes. The extent to which we do not understand future risks can be illustrated by this example. About five years ago, everyone clamored: "The bank-client system will change our lives, people will send payments to the bank using their mobile phones from home, and everything will be fine". And no one warned that at the same time there would be hackers who would hack accounts, go there instead of the client, and make money transfers somewhere else. This is described by Nassim Nicholas Taleb in his book "Antifragile": "people always talk about the height of the mountains, based on the knowledge of the tallest mountain they saw. But that doesn't mean they won't find a mountain even taller". No one assesses the probability of the risk that these cryptocurrencies, God forbid, will be stolen, in a correct and professional manner. Recently, I came across information that 10% of the money collected at the ICO was stolen by hackers. And this is just the beginning. The percentage of funds stolen will rise because hackers are improving rapidly.

Risks	Example	Details
The risk of insufficient knowledge of top managers. Requires simultaneous detailed knowledge of IT, legal affairs and finance	A major speaker declared that Bitcoin and blockchain are different technologies and different entities, a major banker identified the existence of an opportunity to train soft scientists in the body of mathematics of Artificial Intelligence	
Underestimating future damage arising from the emergence of new threats due to the development of technologies used for criminal purposes	Online banking, bio-identification	No one estimates the extent of the threat of financial networks hacking has grown after the operation to steal cyber weapons from an isolated CIA network. Existence of a hacking technology of a fundamentally new class, unknown to society, is possible. The Termen problem was sorted out only after 10 years passed.

Choosing an authoritative but inappropriate decision	SET 1995	You can invest in something that will not work well
Support	Blockchain	Lack of economic support
Recognition of a technology as licensed or prohibited for use and storage, as was the case with drugs, weapons, alcohol during Prohibition	Bitcoin, other payment methods to anonymous beneficiaries	Wanna Cry, which caused damage to the health and lives of real people through British hospitals, exists only because of Bitcoin and other anonymous payment technologies
Alternative money circulation, not controlled by the state	Any cryptocurrencies	
Uncertainty of taxation of circulation and capital gains		

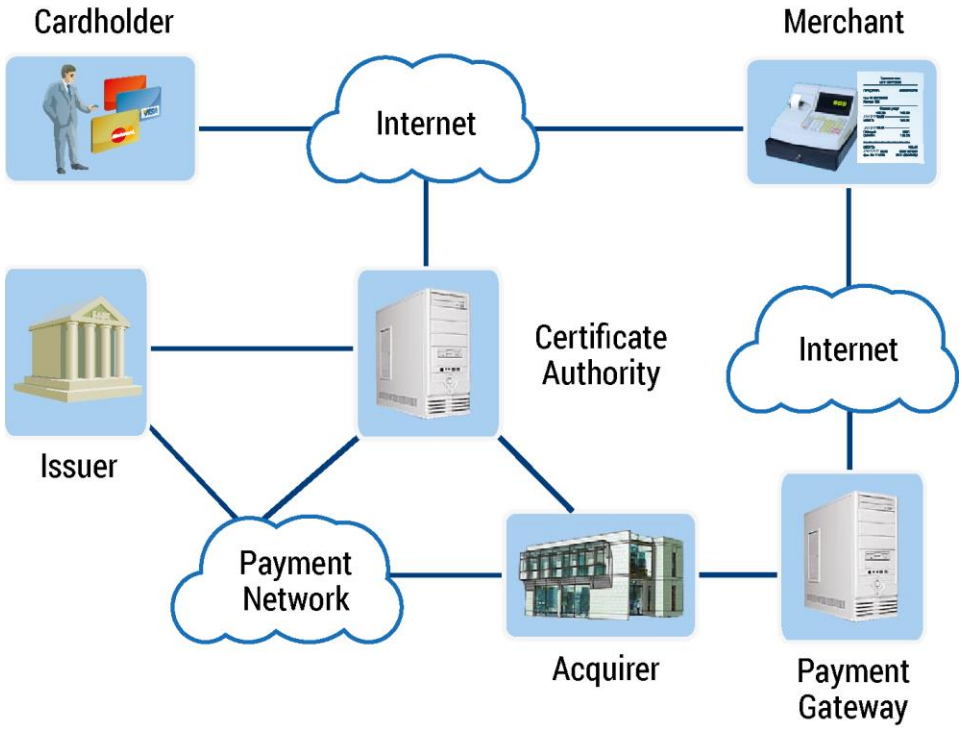
Another example. The United States is a highly developed country that creates cyber weapons to protect its interests. And to develop these weapons, the CIA has developed a separate top-secret network that is not physically connected to the rest of the Internet. And these weapons were stolen from this network! A reasonable question arises: if hackers were able to hack into an isolated top-secret CIA network in the high-tech US, how can they really fail to hack the Central Bank? And cryptocurrencies do not even have a unified registrar!

There is a very telling story of the consequences of underestimating the risks of technologies no one knows about yet. A Russian inventor, Lev Termen, invented the "Zlatoust" eavesdropping system, which worked for Russia against the Americans[2] for 10 years.

Once an American ambassador went to Artek to look at the pioneers, and they gave him a gift - an eagle carved from wood. A beautiful eagle, thought the ambassador. I'll hang it in my office, it's a symbol of America. And it’s absolutely made of wood, there are no wires sticking out of it, the power supply is nowhere to be seen- there can be no eavesdropping devices there! So the eagle hung in his office for 10 years. And when they already knew for sure that there was an eavesdropping device somewhere in his office, and dismantled everything, they decided to look at this eagle as well. They took it apart and found some little wires. And it turned out that if this eagle is targetedly flooded with a certain radio frequency, then the wires act as a voice modulator, which overlay the sounds on this frequency. And this modulated frequency is taken from the air in another place and what is said in the office can be heard.

This technology was not known to anyone for the first ten years of its existence and use. Can you imagine how many technologies exist now that we do not know about, but they do, and they work! It would be good if they were ever open and we were allowed to use them. For example, you think you bought a mobile phone and it's yours. And Natalya Kasperskaya speaks quite frankly[3]: “Your smartphone is no longer your device. They give it to you so you can play

with it yourself. But in fact, this is a device belonging to completely different people, whom we warmly greet". By extension, we do not understand the risks of new secret technologies, precisely because they are secret, but we are told - take it and use it all you want. And 10 years have not yet passed, almost no time at all.



SET components and Participants

Another macroeconomic risk is the risk of choosing an authoritative but inappropriate decision.

In 1996, the behemoths of the economy - Microsoft, IBM, Visa, Mastercard - gathered and decided to develop a single solution for electronic payments. When developed, it was named SET (Secure Electronic Transaction). Visa said: great, we will live with this solution. And the competent people who knew about IT immediately realized that it was very cumbersome, inconvenient, and no one, relatively speaking, would go to a bakery in a truck. And those who did not understand IT (and at that moment it was Alfa-Bank), took and bought the SET solution for about a million dollars[4] But a year later, they realized that a truck was a really inconvenient car to go to a bakery, and Visa suddenly left this association, and IBM said - sorry, we made a mistake...

This was a situation where everyone decided on the solution, one of them invested in it, and then the others unanimously said - oh, it won't do. Alfa-Bank had a long fight with Visa. It all ended with them accepted to some kind of a supervisory board as a consolation.

What's important in this story is that even the most experienced people can make wrong decision. And who provided us with evidence that Bitcoin is the right decision if there are already several thousand cryptocurrencies on the market? And Bitcoin no longer even holds a controlling stake among them!

All these are macroeconomic risks, which should be assessed, but by who? By Central Bank, Ministry of Economic Development, Ministry of Industry and Trade and other state bodies.

Another macroeconomic risk is the recognition of a technology as licensed or prohibited for use and storage, as was the case with drugs, weapons, alcohol during Prohibition. At one time, I wondered which currency was the best. I typed "the best currency" in Yandex... and you know what it produced? The first link? "The best currency is cartridges. One cartridge - one life".

In a number of places which are at war, it is so. And our special forces, who fought in Chechnya, understand this as well. Where there is no law, weapons are the best currency. But as soon as the law is established, the free circulation of weapons is prohibited. There is a list of items which free circulation is limited in the civilized world: drugs, weapons, missiles, certain chemicals... It also happens that something that was legal for a long time suddenly becomes illegal. Suffice it to recall the history of Bayer Company: it began with the legal production and sale of cocaine. There were even cocaine nasal drops - People's Commissar of Health Nikolai Semashko prescribed them to members of the Council of People's Commissars. Bayer flourished, and then cocaine was banned from legal sale. Then they started producing heroin[5] until it was also banned.

In such area as the circulation of money, which is very carefully monitored by the state, a situation where something legal can become illegal is extremely likely. It is obvious that cryptocurrency will be recognized as legal in some countries, but won't in others. In some countries, it has already been banned. And even if we may still have a whole Telegram channel dedicated to advertisements for the sale of apartments, cars and even titanium deposits for bitcoins and other cryptocurrencies, the question of the legal registration of such transactions remains open. How can the transaction be recognized as occurred, that the money were transferred from the buyer to the seller? And purely legal risks arise - recognition of the transaction as illegal, illegal, failed, or even worse –as false.

Not so long ago, the WannaCry encryption virus swept the world, causing real human casualties, because it also encrypted the computers responsible for maintaining life support of people in British clinics. Where did it come from? The first decoders worked based on canceling this cipher, subject to payment via SMS. And when this payment channel to the ransomware was closed, hackers stopped sending these viruses, stopped using this tool. We can say that WannaCry is based on the existence of anonymous cryptocurrencies: if there were no Bitcoin, there would be no economic sense to launch an encryption virus. Thus, if humanity wants to protect itself from encryption viruses, anonymous cryptocurrencies will have to be abolished. After all, there are so many devices you can infect with these decoding viruses, from smartphones to ventilation systems! And if, God forbid, someone tries to intimidate the whole world with such viruses, the issue of banning cryptocurrencies will arise in an instant. And these decisions are made by people who benefit from making politically beneficial populist decisions.

Another macroeconomic risk is alternative money circulation, not controlled by the state. The Chairman of the Central Bank of the Russian Federation Elvira Nabiullina and the Deputy Minister of Finance Aleksei Moiseev have already mentioned this: no normal state will allow

currency circulation on its territory, if it is not controlled by it. To some extent, no one pays attention, but as soon as circulation volumes increase, the situation changes.

Uncertainty in the taxation of cryptocurrency circulation and capital gains. Even tomorrow, the state can introduce any taxes on cryptocurrency, and such a risk must also be foreseen.

CRIMINAL RISKS

There are many.

Any cryptocurrency is at risk of being used for non-compliance with legislation on combating legalization (laundering) of proceeds from crime and financing of terrorism (AML / CFT).

Another risk is anti-state social engineering. What is it? Let's say people receive an anonymous email with a call: “Come to Bolotnaya Square at the said time, you will receive 1/10 bitcoin”. How many people will come? A very large crowd gather. Let's imagine - these people came and then received a new message: “Now cross the bridge and reach the Red Square”. Or go to Manezhnaya. Anyone with this technology in their hands can remotely manipulate a crowd of greedy and stupid people.

Risks	Example	Details
Use for non-compliance with AML / CFT legislation	Any cryptocurrencies	There is no single emission center, the payer and beneficiary are not identified
Anti-state social engineering	Any cryptocurrencies	Payment for color-coded revolutions
Using inconsistencies with current legislation for fraudulent purposes	Blockchain	Smart contracts do not correspond to the concept of equivalent handwritten signature in the Civil Code of the Russian Federation
Theft or publicity of commercially significant information and trade secrets or personal data	Blockchain	By definition, all information about all transactions and parties is known
Theft	Hundreds of millions of cryptocurrencies were stolen from exchanges	Guarantees from law enforcement agencies for the safety of funds, as well as from the Central Bank responsible for money circulation in the country, are required
At the same time, we will not be able to ensure the absolute		

reliability of transactions due to the fact that if, for some reason, the 50% +1 cryptocurrency validators say that the transaction has taken place, but in fact it did not exist, we will not have any opportunity to refute this, - Moiseev explained	

Criminal risks. Analysts: Ministry of Internal Affairs, FSB, Federal Financial Monitoring Service, Central Bank

The third risk is the use of inconsistencies with current legislation for fraudulent purposes. For example, smart contracts that form the base for the transactions, are not described in the Civil Code at all. The electronic digital signature is described, it is called equivalent handwritten signature. And from a legal point of view, no one knows what smart contracts are, and if you come to court with this, the court has no legal basis, or even more so the practice on to base the court decision on. You exchanged cryptocurrencies, yes, but by definition there is no judicial support of this decision. What is this risk equal to? We must evaluate, weigh it. Because the rules of the game can be invented so that your investment in cryptocurrency will be depreciated instantly.

Another risk: theft or publicity of commercially significant information and trade secrets or personal data. This is where the issue with all blockchain technology lies. Everyone knows about all transactions at once. You know everyone's personal data. This directly contradicts the law “On personal data”.

We discussed the risk of theft above – it’s the same 10%. Yet. As Mr. Moiseev said: “We will not be able to ensure the absolute reliability of transactions due to the fact that if, for some reason, the 50% +1 cryptocurrency validators say that the transaction has taken place, but in fact it did not exist, we will not have any opportunity to refute this”. And if these validators are also anonymous, then the risk increases significantly.

The risk of finding prohibited information in the cryptocurrency network. Any cryptocurrency validator is the keeper of the entire data archive at once. Since the overwhelming majority of validators are not professionals in the field of creating and controlling cryptographic software, they cannot even understand that the archive may contain something alien. At the same time, researchers from the Universities of Aachen and Frankfurt found that in addition to financial information, about 1,600 other files are stored on the bitcoin network. Among the detected files, seven violate copyright: they contain excerpts from various whitepapers, an RSA private key, secret software key and key for cracking DVD copy protection. Also, the Bitcoin blockchain stores wedding photos and snapshots of people with their online aliases indicated. Among the files, there were copies of US diplomatic cables, leaked through WikiLeaks in 2010, the news of a demonstration in Hong Kong in 2014, some files on the bitcoin blockchain contain illegal information and 274 links to similar resources, 142 of which lead to services located in Dark Web.[6]

Risk of containerized cryptocurrency. Any crypto-coin (token) is a crypto-container. Having received it, the user can only know the information written on the "container wall", its name and denomination. The user cannot know what is stored inside the cryptocurrency cryptocontainer precisely because of the encryption. And anything can be stored inside: instructions on terrorism or top secret information. Or malicious code.

For example, an unlimited number of people can write to a public blockchain, there is no access control, and there is absolutely no chance that any prohibited information or virus will not be sent there. And there are no certified or even trusted means to check what is inside the crypto container. In addition, many cryptocurrencies provide an open API for developers to develop their tokens based on the “base currency”. Developers have every opportunity to add illegal content to the crypto container, and it is unlikely that anyone controls the process in addition to the developers themselves.

Has there ever been a historical precedent of risks being realized in an “untested container”? Yes, it has. In the 13th century Khan Kublai launched relatively “high-speed” caravans along the “Silk Road”. Was there anyone who objected to this new and clearly revolutionary technology for the delivery of goods? Everyone was in favor of it and very happy. No one then understood that the plague virus, naturally occurring in Mongolia, did not have the time to kill caravans in the Gobi Desert, and these caravans, due to their increased speed, became carriers of the plague bringing it to Europe and China. The cost of risk realization was the death of half of the population of Europe and two-thirds of the population of China.

We do not know what kind of "infection" may be stored in these cryptocurrency cryptocontainers. It is very easy to put malware in them, stealing information or infecting critical information infrastructure. Do we understand the magnitude of critical infrastructure shutting down?

TECHNOLOGICAL RISKS

Risks	Example	Details
Inappropriateness for this use	Blockchain	Blockchain technology is essential for troops C4I system
Inconsistency with the tasks set (excessive publicity, low speed)	Blockchain	Everyone can see all transactions, processing speed is 3 (maximum 5) transactions per second and cannot be significantly increased
Non-transparent creation	Bitcoin	Nobody has ever seen the author, the source of funding of $ 20 million is unclear.
Initial use of technology	Bitcoin	Born inside Tor, with close ties to the FBI

		(http://www.cnews.ru/news/top/anonimnaya_set_tor_na_60_finansiruetsya), in a Silk Road store called Amazon or Ebay for illegal goods

Technological risks. The analysts are the largest existing integrators with extensive implementation experience, manufacturers of banking software, the Ministry of Communications. Where did blockchain technology come from? Nobody talks about it. But the blockchain technology is known not for the last five years that everyone talks about it, but for 35-40 years. And it was usually used for automated command and control systems, primarily for tactical information exchange. Imagine that you have 50 combat units engaged in combat operations. And there is a unit - for example, a helicopter, which took off, saw something important, received some information. This information must be passed on to all units of the subdivision and command, so that each of them has a complete picture of the battle. Either directly or in a chain. A transaction is considered completed only when this information has reached each authorized subscriber. Not when everyone knew about it, but precisely when they confirm the receipt. If you have 50 subscribers, the data transfer is fast enough. But as soon as their number reach thousand, problems begin... couldn't get through to one, the connection to the other was lost ... And the blockchain was originally designed for many thousands of validation nodes. The speed of this technology is 7 transactions per second maximum. What does this mean in comparison with other systems? At Cyberplat we have a nominal "firing rate" of 100 transactions per second, the peak speed is 500. In Sberbank, I suppose, the nominal speed is about 400, and the peak speed is 1500 transactions per second. How many blockchains does one need? When German Gref talks about the benefits of blockchain, I immediately start thinking - how many will he need?

The risk of inconsistency with the tasks. What are 7 transactions per second? That's about 220 million transactions per year. And we have a population of 140 million! This means that each of us can make less than TWO transactions per year! And if you need three, you have to wait another year to carry out the third one. If you need, for example, 300 transactions, I'm very sorry, but you won't live to see them completed. This is why introducing such technology in large communities is basically impossible. Large communities are served by bankers, they are interested in this. When IBM assembled the first serial hundred computers, one was bought by the Pentagon, one – by meteorologists, and the other 98 – by banks.

Photo: Hacker.ru

There was one case, where a group of developers, hearing that the speed of 7 transactions per second is not serious, assembled a thousand computers in one room, connected them with an optics cable and achieved 200-300 transactions per second. But, if this entire registry is located in one room, registry distribution becomes non-existent. Because if you want to distribute this registry across the globe, you need to use the communication system in its entirety: copper, air, etc. And a distributed, an actually distributed network, can not have such performance. Military can work with 7 transactions per second. And for bankers such speed will not be satisfactory. This technology was not originally made for this and does not fit the current form of the financial market.

We are slowly approaching the main thing. Risk of non-transparent creation. Who wrote the terms of reference for the creation of this software? Who accepted them? Who wrote the structured algorithm? Who commissioned the code? Who debugged it?

Natalya Kasperskaya was the first to publicly declare this that there was no Satoshi Nakamoto, and a group of American cryptologists is behind the blockchain creation. We already know that distributed registry technology was originally used in the automated control system by the military for quite a long time, and that is why there was nothing written about it in scientific and popular science journals. And now we find out that someone is already using this technology somewhere. And obviously they have seen it before. What place has the people who understand these things? This, obviously, is the Pentagon.

Now let's remind ourselves where bitcoin was first used? There is an anonymous network called Tor, and it had an online store called the Silk Road that sold drugs. The Tor network is funded by anonymous donations, but strange as it is, the main donor is known: it’s the US Federal Bureau of Investigation. And it goes without saying that this network cannot be hacked, because you need to hack five servers in a row ... If, of course, all these five servers are not yours to own. And if they are, all five of them, you read all this correspondence and make decisions: we lock these people for the statistics, we don’t lock these people, but we look at

who will swallow the bait, we don't lock these because they are paying us. Bad mouths say that this is how the Tor network was created - by certain people for certain people.

And the same bad mouths say about the Silk Road online store that when the FBI catches someone with drugs, it hands some things over to the state, and the rest, which was confiscated, sells on the side, but where is the most convenient store selling the confiscated goods located? An Internet store created by certain people for certain people is very convenient tool for this. If you also know that in the United States all FBI employees are officially released from responsibility for drug operations under the pretext that "they have to do this in order to infiltrate organized criminal groups," the picture becomes complete. It immediately becomes clear who and how controls the market. But, having made several cycles of "drugs / weapons – bitcoin", these people began dumping the cryptocurrency or exchanging it for apartments, cars, titanium deposits, etc. And since these people have many journalists in their arsenal, overblowing the story around all this did not require any effort.

Summing the things up. Before joining anything, let's think - how can we leave it? And if it turns out that it was laundering on an especially large scale, you are an accomplice in laundering operations involving drugs and weapons.

WHAT TO DO

Decision-making direction - division of risks by their profile

Consequently, risk analysis is carried out by dedicated specialists

"A cobbler must not go beyond his last"

You have to do risk management. The risk is described, its maximum magnitude is described, the so-called threat strategy is formed, the magnitude of this threat and the way it must be countered are described.

As you know, the most effective fighters against terrorists are the terrorists themselves - those who are counter-terrorists. They know how to carry out a terrorist attack, and can easily figure out how they can be neutralized. Any good armor maker knows perfectly well how a projectile works, otherwise he can't make armor. Why do thugs, when pushing their protection racket, call it insurance? Because it's all the same thing.

Not so long ago, a theory of the state as an institutional thug emerged, which was almost awarded the Nobel Prize. To formulate the whole theory in just one phrase - "whoever has the biggest club is the chief of this territory". The same is true with cryptocurrencies. To deal with macroeconomics, you need to go to the biggest crooks in macroeconomics - the Central Bank, the Government. To engage in crime, you have to go ... it's clear where to. Only when it becomes profitable and interesting for them will they begin to manage this process.

I y deeply believe that the real America - as we know it - began with the creation of Murder Incorporated in the 1920s. When the largest mafia clans gathered and decided that it was only possible to murder a person with the unanimous permission of the leaders of all mafia clans. Then the chaos ended, and by their internal court they sentenced who must be murdered and who must not be. From that moment, the country became civilized. Before that, cowboys shot

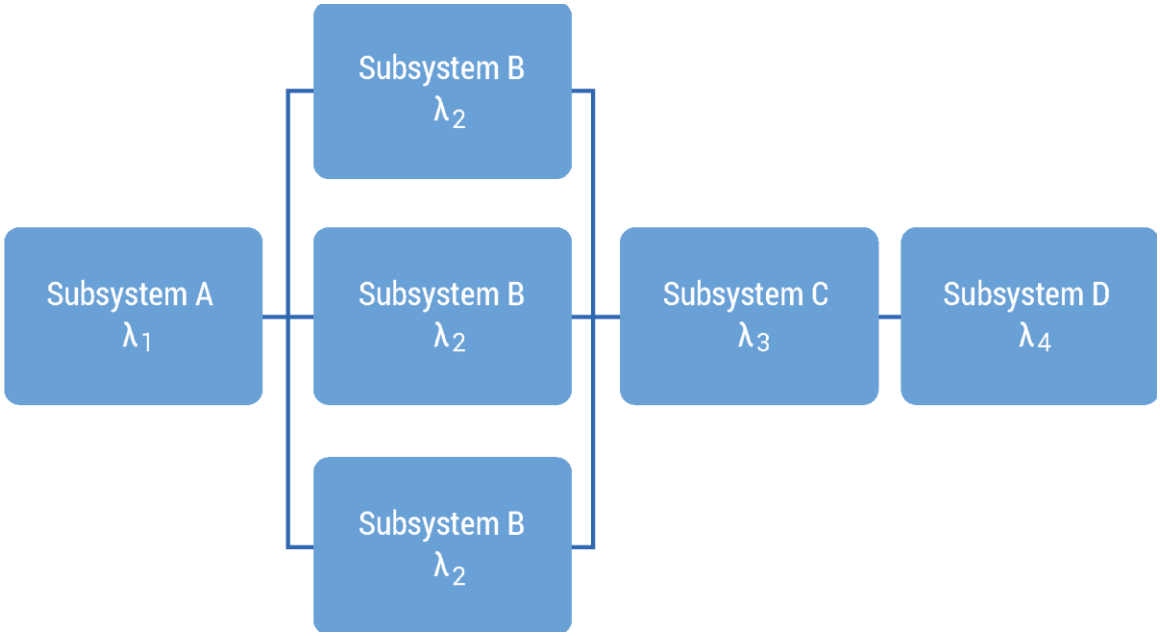
at sheriffs, and sheriffs at cowboys, and the only difference between them was the badge. But from the moment the legal proceedings appeared in illegal space, from that moment civilization in the United States began. Any risk should be considered by professional risk managers. But who these managers are... We won't write it in the open, but we understand.

Therefore, in order to determine the risks of cryptocurrencies and create cryptocurrencies risk management, all risks must be divided into groups, and each group of risks must be studied by those who understand it.

- For example, IT risks should be entrusted to the Ministry of Communications and the Academy of Sciences.
- Economic risks - to the Central Bank, the Ministry of Economic Development, the Ministry of Finance.
- Criminal risks - to the Ministry of Justice, the Ministry of Internal Affairs, the Prosecutor's Office, the security services.

And only by hearing out all the professional opinions of all groups together, you can make a joint fundamental decision.

DISASTER TOLERANCE AND SURVIVABILITY



Probability theory teaches us that two-fold failure redundancy of information infrastructure in times of peace, for example, in civil aircraft or in processing systems, is quite sufficient, and three-fold redundancy is already somewhat redundant. This parameter is called disaster tolerance. But in combat aircraft and military C4I systems, for example, critical information infrastructure failure redundancy should be 4-7-fold. For the simple reason that this device when used for combat purposes, is targeted by the enemy in order to destroy it. Therefore, in case of deliberate destruction of 2-3-4 levels of the combat information infrastructure, an aircraft or a control system must still perform their combat tasks. Therefore, the level of failure redundancy is four-sevenfold. And this is called survivability. This term is used in the

design and testing of weapons. You can hear the phrases “ship survivability”, “tank survivability”, “aircraft survivability”. But there is no such phrase for peaceful systems. Because this level of survivability is not needed in times of peace. A sevenfold level of redundancy of onboard electronics is not needed for a peaceful passenger aircraft. And a sevenfold level of redundancy is also not needed for a peaceful processing system. Unless, of course, you set yourself the task of financing terrorism, intelligence networks behind enemy lines, or the implementation of deliberately illegal acts such as selling drugs.

In blockchain technology, each “game getter” – a “miner” - duplicates almost the entire network. This is some kind of super-mega-survivability. Even if 99% of the reservation is destroyed, the blockchain does not stop functioning. But is it possible to lose 99% of the backup infrastructure in peacetime? Of course not. Then why paying for such a clearly redundant resource?

Mega-survivability of cryptocurrencies requires sacrificing additional operation of the processors of all participants, and most importantly - the transaction time. Clearly, redundant mega-survivability is the very reason for such low performance and high cost of using cryptocurrencies.

A former PayPal CEO, William H. Harris writes “It takes about an hour for a bitcoin transaction to be confirmed, and the bitcoin system is limited to five transactions per second. MasterCard can process 38,000 per second. Transferring $100 from one person to another costs about $6 using a cryptocurrency exchange, and well less than $1 using an electronic check... It takes as much electricity to create a single bitcoin — a process called “mining” — as it does to power an average American household for two years. If bitcoin were used for a large portion of the world’s commerce (which won’t happen), it would consume a very large portion of the world’s electricity, diverting scarce power from useful purposes”.[7]

In order to use the blockchain technology for peaceful purposes, it is sufficient to reduce the number of verification nodes to 10, or 20 maximum. And if you transfer these verification functions to the players responsible for the risk management of this cryptocurrency, everything falls into place. We get a super-reliable payment infrastructure in terms of disaster tolerance (and even survivability), where ministries and departments authorized by the state serve as verifiers. The risks of using such a cryptocurrency will be minimal.

Thus, the most rational development of the distributed registry technology for the creation of cryptocurrencies is the creation of a cryptocurrency with a very limited number of verifying registrars, the number, composition and responsibilities of which (primarily aimed at reducing the risks of use) will be determined by the Government. These will necessarily include the Ministry of Communications, the Academy of Sciences, the Central Bank, the Ministry of Economic Development and Trade, the Ministry of Finance, the Ministry of Justice, the Ministry of Internal Affairs, the Prosecutor's Office, and security services.

All other users will use this registry and will not keep “archives” of other people's transactions.

P. S.

As a result of reflecting and discussing the distributed registry systems for automatic command and control systems, I managed to understand that the number of not only redundancy nodes, but even of their subscribers, is very limited. First, roughly speaking, a unit fighting in the Murmansk region does not need tactical data from the Caucasus. And second, when a combat unit is captured, the enemy should not gain access to a large amount of secret data. The most interesting is that the saboteurs have the same picture. When a saboteur is captured, the local counterintelligence service should not receive much information about the whole sabotage network. The number of redundancy nodes, thus, even in the riskiest areas, does not exceed 10.

That is, empirical data allow us to conclude that more than 10-fold redundancy is not needed anywhere or by anyone under any circumstances. Not by a single user in the world. Closed interval is from 1 to 10. There is no such risk existing naturally and requiring more than 10-fold reservation.

Then who needs cryptocurrencies with thousands-fold duplicates of the entire registry?

After much consideration, I managed to identify the only type of organization that needs to know everything about everyone. No, of course, there are also journalists, but high-level cryptography with elements of technologies for automatic control of troops is “not their style”. What is clear about security services, is that if they are the organizers of the cryptocurrencies introduction, such a tool is convenient for them. Everyone gives out the entire volume of private data on themselves, wholeheartedly believing that the system is anonymous, and not wanting to think that any cryptosoft created by security services must definitely have a “backdoor”.[8]

This is regular work for the security services, they are paid to do this. But why do users need it? Even if they have such a great passion for the intelligence services of their country, you can probably find a less costly and complex method of transmitting information to them. If the secret service of another country is involved, you can find yourself in a very delicate situation, described in the Criminal Code in quite simple terms. As the poet wrote, “It’s where they eat you without salt, they seal you in an envelope, address at random, send you where the sun don’t shine”. And if a housewife can prove her firm ignorance of the foundations of the theory of reliability as part of the theory of probability, then any IT specialist who probably had to attend lectures on the theory of probability, and even passed their exams, which is evidenced by documents, will not worm their way out so easily. The argument “everyone does it” may not work, since gnoseology, the science of cognition, a part of philosophy, directly tells us that “the opinion of the majority can not be considered a criterion of truth.”

JOKING ABOUT CRYPTOCURRENCIES

Mining potatoes is the same process - spontaneous generation of liquid value as a result of multiple duplication and replication of the potato genetic code.

Currently, the potato mining process is now more profitable than Bitcoin mining. A farm and a plot of 10 decares cost the same, about 3000 USD. Ten hundred decares will yield a fork of eight tons of potato a good trader, which is equivalent to $ 2,400 at the current exchange rate

against the dollar. The payback period for the project will be 15 months. And if you overclock your farm with a little manure, you can collect all ten.

And at the same time, the process of potato mining does not involve electricity costs, and the potato mining farm itself does not lose value.

What is more, potato has a side fork called moonshine. Eight tons of potato remined into moonshine will yield 1,500 and a half liters, or $ 7,500. Bitcoin won't bring that much.

References

1. Now, the University
2. https://geektimes.ru/company/pult/blog/281704/
3. https://www.computerworld.ru/news/Natalya-Kasperskaya-zayavila-chto-bitkoin-razrabotan- amerikanskimi-spetssluzhbami
4. https://alfabank.ru/press/news/2002/2/5/ l.html
5. https://ru.wikipedia.org/wiki/repoHH
6. http://bankir.ru/novosti/20180321/issledovanie-v-seti-bitkoina-obnaruzhen-zapreshchennyi- kontent-10137403/
7. https://www.recode.net/2018/4/24/172 75202/bitcoin-scam-cryptocurrency-mining-pump-dump-fraud-ico-value
8. https://vz.rU/news/2018/7/15/932555.html

CYBERPLAT®

Passed for printing on 20.01.2020. Format 70x100/16

Cambria typeface. Offset paper. 20 conventional printed sheets

Circulation of 300 copies. Order No. 00000

Not for sale

https://www.cyberplat.ru/download/Book_Cyberplat_epub.epub

https://www.cyberplat.ru/download/Book_Cyberplat.pdf

Printed in “First Exemplary Printing House” JSC

“Chekhov Printing House” Branch

142300, Moscow region,

Chekhov, Poligrafistov st., bldg. 1

https://www.chpd.ru

e-mail: sales@chpd.ru

Tel.: 8 (499) 270-73-59