# Journal of Digital Science

ISSN 2686-8296

Volume 1 Issue 1 December 2019

**CONTENTS**

# Secure i-Voting Scheme with Blockchain Technology and Blind Signature

Mahmoud Al-Rawy[1] and Atilla Elci [2]

[1] Ark IT, Tirana, Albania
[2] Electrical Electronics Department, Aksaray University, Aksaray, Turkey

https://doi.org/10.33847/2686-8296.1.1_1

Received 25.09.2019/Revised 30.10.2019/Accepted 11.12.2019/Published 22.12.2019

**Abstract.** In the last four years, blockchain technology affected largely all aspects of our lives. Blockchain started to launch a new technological revolution of storing digital transactions over the Internet, verifying the authenticity, licensing and providing the highest degree of security and encryption. Blockchain usage started with digital currency then its implementation extended to many industries such as voting, health records, copywriters, real estates and so on. However, it is time to upgrade the election scenario from practicing paper-based elections to use modern technologies in order to facilitate our lives. The fact that the blockchain technology has demonstrated almost infinite immutability and high resistance against hacking, lends credit to employ it in securing election data from fraud by saving every single piece of data, record or transaction with unchangeable history. In this paper, we propose and test implement a robust online voting system based on blockchain in order to prevent election forgery and ease the voting process for citizens. The essence of our research lies in abandoning alterable traditional databases and replacing them with two private blockchains that use the peer-to-peer network. Along with the blockchains, we utilized blind signature to maintain vote/voter privacy in order to safeguard voter eligibility validation against manipulation and forgery. Lastly, we discuss a threat model, and suggest solutions overcome it; we also suggest a solution to identity impersonation and vote-selling problems.

**Keywords:** Blockchain, Internet Voting, Vote/Voter privacy, Blind Signatures, Public-Private Key algorithm anonymization.

## 1. Introduction

For hundreds of years, traditional elections based on the principle of accepting a ballot paper at a specific polling station have been practiced. The cost of this process, of each ballot paper, trustee, preparation of a polling station, and other high costs not to mention the time spent, difficulties faced by disabled people, repeatedly encountered problems due to fraud, manipulation of results and influencing voters are all factors to consider against traditional/paper-based elections. History is littered with examples of elections being manipulated to influence their outcome; scammers and rulers have developed means of manipulating votes to achieve personal agendas, which is considered a violation of the core principle of democracy.

With the advent of the ever-expanding Internet, many researchers have devoted effort to find the easiest, economical and most importantly a secure way to achieve a fair online election by using an i-Voting system aimed to overcome all problems faced by the traditional elections. The i-Voting system, alternately called the Internet Voting, may be defined as an election system constructed on cryptographic techniques allowing voters to cast their ballots for their favorite candidates and transmitting their votes over the Internet from anywhere in the World while the voting and tally processes run entirely anonymously. In 1981, David Chaum introduced the first electronic voting system [25], where he used public-key cryptography to maintain solid anonymity of voters/votes as well as utilizing Blind

Signature to ensure disconnectivity between voters and their ballots. Since then, the evolving of cryptography inspired several academicians to show interests in Internet voting [20, 21, 26 – 29]. Yet, due to the fact that Internet voting systems run over the Internet, significant challenges such as voters' authenticity and eligibility, ballot privacy, process completion, the immutability of the results and fairness have been obstacles for decades.

Despite the concerns mentioned above, Estonia introduced for the first time in the history online voting system to be the first country in the world to put in place an Internet voting. In the most recent online elections, over 30% of the Estonian participators cast their ballots online [1, 5]. Similarly, over 280,000 votes were submitted through iVote in New South Wales, and 70,090 Norwegian votes submitted online in 2013. Security vulnerabilities in voters' client devices, systems servers, and voter authentication process have been demonstrated by security analysis on these systems [12, 13].

In 2008, Nakamoto introduced his by-now famous white paper [3], which revolutionized the world of cybersecurity. He combined some encryption algorithms in a brilliant way to obtain immutability of data and provide sufficient protection to transfer and store the data in a distributed ledger with the well-known technology called "Blockchain." Blockchain technology, initially known as the cryptocurrency transaction log, helps keep data resistant to tampering with ever-growing linked data ledgers and allows secure exchange transactions of valuables such as votes, funds, stocks or data access rights.

Achieving fair election without running the risk of rigging and manipulation of the results was and still difficult [11]. However, with the emergence of the blockchain which provided many possibilities that inspired researchers to investigate and reach to the proved conviction through their research to suggested that blockchain is a suitable base for Internet voting, besides, it could have the prospect to make e-voting more acceptable and reliable in the society [4].

Fundamentally, blockchain uses data distribution principle (i.e., distributed replication or decentralization). Therefore, it operates as an electronic transaction log-cum-record system that allows all parties to track information through a secure network without requiring verification by a central authority.

Eventually, the most important advantages of using blockchain-based i-Voting has become the following:

i) Anonymity
ii) Accuracy
iii) High performance, particularly against Denial of Service (DoS) and Distributed DoS Attacks
iv) Strong integrity (immutability) by replicating many copies of the same identical data over many nodes, but none is the golden copy.

It is fundamental that a proposed e-voting scheme contributes to preventing any violation of voter-ballot anonymity, and the absence of any possibility to manipulate the results. The main challenges usually i-Voting systems have faced are highlighted below:

**Vote Privacy**. Voter's choices must be anonymous (secret ballot). Non-observance of the secrecy of the ballot leads to attempts to influence the voter by either intimidation or through potential vote-buying.

**Identity Theft (ineligibility)**. Impersonation and multiple vote casting were real issues in the past with traditional-based voting systems. Deceptive voters used to register themselves multiple times or manipulate their eligibility of voting. In Australia, 217 ineligible voters cast votes in 1996 elections, and in 2010 elections, a family cast more than 150 votes by impersonating others. The security analysis of the Estonian Internet Voting System demonstrated that attackers can plant malware in the voter's client and read the National-ID card's PIN, then impersonate an eligible

voter to cast an unqualified vote as they desire. In fact, due to the lack of biometric devices (online) electronic voting machines can allow identity theft. A biometric device would not be available in every home on the polling day, and, supplying such equipment for each house is very expensive and unpractical. Therefore, there must be a solution to overcome this issue.

**Immutability**. The biggest election concerns lie in the immunity of the electoral system from manipulation and counterfeiting [17].

In this paper, we first illustrate the problem and then propose the solution approach. In section two, we will compare traditional databases and blockchain. In section three and four, we will describe our scheme in further detail in term of authentication and voting processes.

## 2. Problem and Solution Approach

In online voting systems, privacy must be preserved to dispel the election concerns highlighted above. This paper proposes a novel i-Voting architecture to properly facilitate digitalized elections maintaining vote and voter privacy while preventing fraud through employing firstly the blockchain technology to ensure result immutability, secondly, through the RSA public-private key algorithm (PKI) [2] to prevent identity theft, lastly, we will be using the Blind Signature algorithm to allow only eligible voters to cast a ballot.

The proposed voting scheme uses the blockchain technology to store the cast votes and electronic IDs, thus it can act as an immutable database. As usual, the current Web-based system uses HyperText Transfer Protocol Secure (HTTPS) yet there is the need for a further configuration affected by the system administrators to secure the connection between servers and client's computer, therefore preventing devastating attacks such as Logjam and FREAK attacks. Disabling the support for TLS (Transport Layer Security) export cipher suites and using a 2048-bit Diffie-Hellman group also disable other cipher suites that are known to be insecure, thus enable forward secrecy to obtain the desired server immunity [14, 15].

Moreover, it is necessary to relinquish the use of third-party servers that used to read and verify votes by voters. Studies proved that not doing so opens the door to different opportunities for privacy violations as in the cases of elections in Australia and some other countries. So, any kind of reading the vote or overriding it in our scheme is prevented just as in traditional paper-based voting [16].

The major challenge in this work is allowing people to cast their votes right from their home, without the need of going to the polling stations. Usually, digital voting systems rely on the use of standalone electronic voting machines (EVM) which also perform user (/voter) verification as well as the entire election process. In this proposal, we give up on needing such machines and allow the voters to use just an Internet browser to cast ballots and votes.

Our design of the blockchain-based digital voting system is explained below in terms of the processes involved, such as, voter logging in, digital ID creation, re-logging, Electoral Authority preparation, vote casting, and vote tallying; but first we introduce the differences between traditional databases and blockchain to better highlight the advantages of the latter.

## 3. Structural Differences between Traditional Database and Blockchain

In this section, we will review the main reasons behind adopting blockchain over the traditional database in our voting system architecture. In fact, a blockchain is a form of a distributed database, both used for data storage, but there are many fundamental differences in their structures. The traditional database has a central authority (Administrator) to maintain, control, distribute read/write privileges to other

authorities, also, it often uses the client-server network. Blockchain is a digital ledger that receives, encrypts, distributes and stores data without requiring a trusted third party (i.e. Disintermediation), such as Bitcoin, considering ledger crypto-currency. Blockchain storage method produces a linear series of blocks, where each is connected to the previous one, that provides high data immutability and confidentiality. Let us consider the superior features of blockchain with respect to serving as a base for data.

### *3.1. Immutability of Blockchain*

In contrast to centralized databases, data stored in the blockchain is not erasable and almost impossible to be modified, unlike the traditional databases which perform Create, Read, Update and Delete operations (C.R.U.D. Operations) according to the given user permission by the administrator. A blockchain is a secure, distributed, and immutable database shared by all parties (nodes) in a distributed network. A blockchain block contains transactions stored and linked to each other through the so-called Merkle root, for example, see Fig. 1; and, each block is connected to the previous block's "hash" to form an interconnected chain.

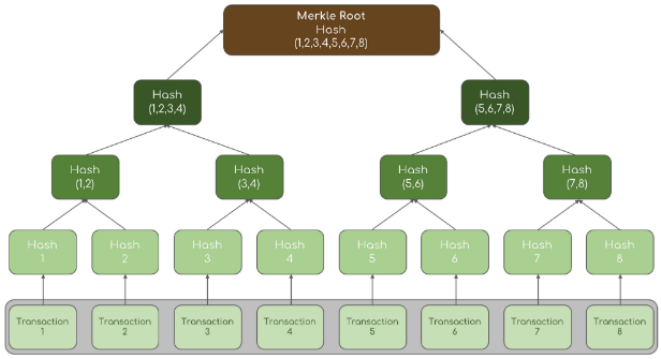

Fig. 1. Merkle root tree example.

A Merkle root is the hash of all the hashes of all the transactions contained in a block; it provides the ultimate encryption for the transactions tree included in a block. This means that any change in any transaction within the block leads to not only a change in the Merkle root hash but so too the block hash will change, thus breaking the chain; as the result, the immutability provided by the blockchain is almost infinite.

***1.*** **Performance**

Traditional databases are very fast compared to the blockchain for the latter uses the cryptography to link its blocks, also employs consensus principle that provides full-distribution by allowing a majority of peers agree on the outcome of transactions in order to accept it into the chain. Every node (aka, computer) in a blockchain network contains a copy of the full data ledger, so any node experiencing failure will be shut out and the network completes its work with the remaining nodes. In the case of distributed databases, the trust factor between the parties must be significantly guaranteed to preserve the integrity of data. Blockchain is quite the opposite operationally; it repeals the trust factor to allow an independent transfer of transactions, even though transacting parties are anonymous. In conclusion, traditional databases are fast but not fully distributed. As for permissionless blockchains that use the principle of consensus, which makes it slow; however, permissioned blockchains are relatively fast, while not exactly fully-distributed.

***2.*** **Decentralization Aspect to Secure Data:**

Instead of using a single repository of data to upload to a server, blockchain distributes data across the entire network to be stored in every node's digital ledger.

Thus, data loss is almost reduced to zero, because if one or more nodes go down, the data will not be affected, unless the entire node network fails, and this is of an extremely low probability. This in its entirety, cutting out the middle-man, the central authority and need to trust a third-party in processing data create a distributed immutable ledger of data records, as shown in Fig.2.

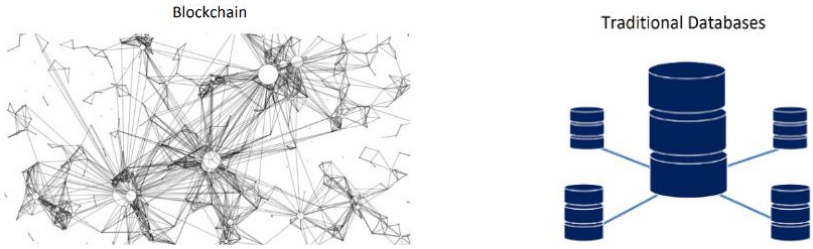


**Fig. 2.** Blockchain structure vs traditional database structure.

## 4. Authentication Structure of the i-Voting System

In this section, we will propose a voter/user authentication process applied before casting a ballot in i-Voting System. The user authentication process requires that voters must establish and sign an electronic identity after secure logging into the system, as described below.

### *1.* The Access Authorization

Let us assume that the country where a digital voting based election will be held has its own e-government system where every single citizen is recorded and has his/her own individual private e-number. Therefore, it is possible to make the very first voter's authentication stage via TLS client authentication [19] starting with asking the voter full name (F-Name), National ID number (NIDN), and e-number. Subsequently, a session token is computed as follows which will be used to identify that user then on:

$$\mathbf{Hash} = \{\mathrm{eNumber} + (\mathrm{F-Name}) + \mathrm{NIDN}\}_{\mathrm{Enc}} \quad (1)$$

Web applications that use cookies are known to be vulnerable to XSS (Cross-Site Scripting) Attacks [18], so voter's privacy might be violated by unauthorized accesses; thus, we strongly recommend cutting out the use cookies and replace it with session tokens. Additionally, using HTTPS protocol is insufficient for an attacker requesting a page with HTTP gets served user cookies in the unconcealed form. Overcoming this gap requires sending system pages only in response to HTTPS calls before starting the session.

### *2.* Digital ID Card Creation

As the voters would identify themselves in the login step, they must have first created an electronic identification (eID), consisting of an ID and digital signature. "eID" is an electronic identification solution of citizen [7]. The idea behind creating a digital ID card is to prove voter identity while using it in the voting processes and to be verified by Electoral Authority's Representative (EAR, more on this below).

In the public-private key algorithm, the user needs a set of two complementary keys: one of them is published for use by the public, and the other is kept secret by the individual for personal use. If a piece of data is encrypted by using the public key, only the person who has the second prime of the key (private key) will be able to decode it. On the other hand, if the person uses his private key to encrypt a piece of data, anyone who has the public key can decrypt it. This process also makes sure the signer (encryptor) is the owner of that key pair. Usage of the public-private key algorithm provides high protection of the data from being modified as well as authenticating the private key owner.

After a voter logs into the system, a public-private key pair will be automatically

generated. The public key will be stored in the system, open to the public. The second key (a private one) will be conveyed to the user, kept hidden and can be used only by the user. Indeed, the private key must not fall into the hands of others, because it might be used to impersonate the voter or used for signature purposes elsewhere. After the creation of the key pair, some information about the person will be requested to be matched with the stored information in the system's database, in order to verify the voter's credibility. The requested information consists of the following fields:

1. Voter's National Identification Number and its expiration date (NIDED).
2. Images of the voter, captured right from the system using the device's webcam: one of the voter himself/herself and two others of both sides of the national identification card (IMGs).
3. Voter's full-name and phone number (V-NO).

The voter's personal identification card number is requested for the second time for confirmation purpose. In order not to depend on the availability of usable biometric devices (fingerprint, eye print), it is necessary to invoke another solution, such as these required images can be photographed, encrypted and stored in the database to prove that the voter has created own electronic identity.

Voter's phone number will be used in processing the time-based one-time password. It will be used while logging into the system, also in every process after that including casting a vote in order to verify the voter's identity. Finally, all the requested data fields are combined and encrypted with the voter's public key to obtain a verifiable eID hash as follows:

$$\mathbf{eID} = \{(\mathrm{F-Name}) + \mathrm{NIDN} + \mathrm{NIDED} + \mathrm{IMGs} + (\mathrm{V-NO})\}_{\text{Voter's Public Key}} \quad (2)$$

Eventually, the voter will create a unique signature by using his private key, allowing others to check the validity of the signature using his public key for the purpose of verification [8]. The voter, in order to prove ownership of the private key without requiring to reveal it, will use the signature to sign the ballot.

$$\mathbf{Signature} = (\mathrm{eID})_{\text{Voter's Private Key}} \quad (3)$$

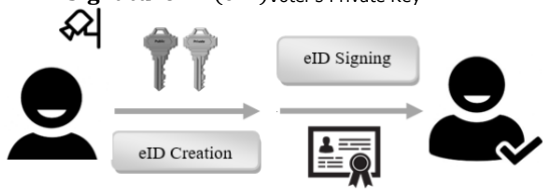


**Fig. 3.** Voter authentication structure.

### *3.* Re-Login

It should be possible to keep the election system running live and open to the public some number of days before the election in order to allow voters to login and establish their eIDs. In this way, the EAR will have enough time to correct voter data if there will be any mistakes. Meanwhile, voters will get familiar with the election system and check whether someone else used their data to create fake eID; if so, they can inform the EAR to receive the necessary assistance. Even after establishing the eID, attackers who hack the eID of an eligible voter and change the phone number to redirect the privileges to his favor will be exposed. The moment that voters try to log into the system for the second time, their eID will be corrupted, due to the fact that his data has been changed, thus they can easily report to EAR immediately. As the voter successfully completes establishing his/her eID, he can log out of the system, and re-login during the polling day in order to vote.

Protecting voter data from being used by others must be given serious consideration; time-based one-time password algorithm [9] may be used to preclude this issue. In the time-based passwords, time synchronization is very important, a secret key and a timestamp will be defined, and everything will be synchronized via

a standard protocol such as network time protocol. Once the password token will be created, it can be used in a limited duration just to ensure that the voter is using his own data in the login process, or the ongoing operation is within his knowledge because he is the one who receives the verification code on his phone.

Once a voter logs into the system (for the second time) in order to vote, the system will check whether his electronic identity has been successfully established or not. In case that everything has been done in proper order, the voter will receive a time-based verification code on his phone. The code could last for, say, two minutes. Also, the voter must confirm his identity using his own private key.

### *4.* Summary

So far, we have described the use of the eID and electronic signature instead of relying on the database management system's self-created IDs to increase the e-voting system's security level. Now, let us summarize our accomplishments of this approach in this section as follows:

Obligating the voters to capture photos of themselves and their ID card is part of the system's processes. These images allow the EAR to verify whether a voter has established own eID or there are impersonations, especially impersonating a deceased person. Those images will be converted to binary format, encrypted and stored in the database. In addition, it will be part of the eID hash, so it will be impossible to decrypt, change or manipulate images.

- Nowadays almost every individual has his own cell phone, which gives us the possibility to use it to secure the voters' data from being exposed. Otherwise, supposing that we did not use the time-based verification code method, and someone's private key got exposed anyone who has the private key and the individual's information can re-login into the system and cast a vote as he desires. That is why the verification code is used to add another level of protection. Even though an individual's information and the private key could fall into other's hand, they will not be able to open the system unless the verification code can be received in time.

## 5. Voting, Verification and Tallying Processes

Basically, in any election employing 'secret ballot-open counting', the following points must be considered: (1) Vote by secret ballot: a vote's originator must be unknown. More clearly, the voter's ballot shall not be violated by anyone anyhow, which means it must be completely concealed whether it is directed to a candidate or it is null. (2) The voters must be marked in the electoral registry that they voted to prevent duplicate voting or cheating and to allow only the legitimate voters to cast a ballot. (3) Open counting: the outcome of the election should be determined by an open verifiable counting of the votes.

Our design is unlike the Bitcoin [19], which uses a single public blockchain; the proposed scheme uses two private/permissioned blockchains. The reason behind preferring permissioned blockchains is twofold: firstly, it prevents unauthorized nodes/parties from joining the network, which in return prevents Sybel Attack; secondly, it provides significant resistance against today's security problems by using robust cryptography features and limited access to the ledger, without affecting the transparency aspect of blockchain technology.

I-Voting Scheme employs two blockchains. Let us call the first blockchain as BL-v, the voters' identities and the second one as BL-b, the encrypted ballots. The purpose of using permissioned blockchain is to limit the parties who can read the information, also, restricting the nodes and separating it in different locations around the country. Now let us dive into the vote casting process as the following:

- **Addresses.** Every transaction requires candidates' new addresses in order to keep the vote-voter anonymity every single time voter cast a vote [10]. The recipient to receive the ballot credit will specify the generated address.

Sending a checksum with an address permits to verify that address was not manipulated by preventing any possibility of a Men-In-The-Middle Attack via making the communications between voter and candidate going through a secure channel using a handshake protocol (see Fig. 4).

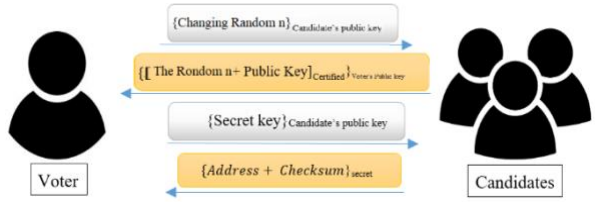


Fig. 4. Voter-candidate authenticated communication.

- **Transactions and Blocks**. Each voter has the right to cast only one countable vote. Once the voting starts, voters have to sign their ballots from the EAR anonymously using the blind signature in order to verify their eligibility. The blind signature scheme is described as follows:

EAR owns a signing function $S'_{EA}$. The corresponding publically-known inverse $S_{EA}$ satisfies $S_{EA}(S'_{EA}(s)) = s$, but gives no clue about $S'_{EA}$. To obtain EAR's signature of the transaction (t) without revealing it, voter will depend on a computing function $C_{Voter}$ and its inverse $C'_{Voter}$, both of which belong to him/her only, and satisfy the condition that $C'_{Voter}(S'_{EA}(C_{Voter}(s))) = S'_{EA}(s)$ while $C_{Voter}$ and $S'_{EA}$ give no clue about (s). The signing scheme is presented as follows:

1. Voter sends $C_{Voter}(t)$ to the EAR.
2. EAR receives $C_{Voter}(t)$, checks the eligibility and signs it using $S'_{EA}$ to obtain $S'_{EA}(C_{Voter}(t))$, then sends $S'_{EA}$ $(C_{Voter}(t))$ back to the voter.
3. The voter uses $C'_{Voter}$ to obtain $S'_{EA}$ (t) according to $C'_{Voter}(S'_{EA}(C_{Voter}(t))) = S'_{EA}(t)$.

The steps above demonstrate how voters could obtain $S'_{EA}$ for the transaction ID (TxID), without revealing the transaction. After a voter signs the ballot, the voter will specify a candidate/party and cast the vote. Every voter has one value credit (Signed Ballot) to be spent once by giving it to a specific candidate. Now, BL-v transaction containing the fields shown in Table 1 is created and submitted to the transaction pool.

Table 1. BL-v transaction content.

| Block element | Dummy example | Description |
|---|---|---|
| TxID | f4184fc596403b9e17e450rd63 | Formed by encrypting the transaction data twice with the SHA-256 algorithm |
| Version | 1.0 | Block version |
| Size | 8 bytes | Block Size |
| Timestamp | 1565259135 | Epoch Unix Time Stamp |
| Prev-Out | J9f74g4h4566f8kl9h985025r6 | Presents whether the voter has voted before or not |
| Out | {Recipient Address} Recipient Public Key | Specified candidate's address |
| $S_{EA}$ | [Transaction Signature] EAR | Contains the $S'_{EA}$(TxID) |

The BL-v transaction is created by including Transaction version, Transaction size, Prev-out, and the Out. The Out contains the recipient wallet address encrypted with the recipient's public key. However, the recipient will prove that he is the owner of the private key; only then, he gets the vote. After all, TxID established by including all the transaction stuff together, encrypted with SHA-256 twice.

As for the BL-i transaction, it will include (Prev-out, and the Out), as shown in Table 1. The Out contains the recipient wallet address encrypted with voter's public key to conceal it.

Table 2. BL-i transaction content.

| Block element | Dummy example | Description |
|---|---|---|
| TxID | 8h5d8i905r4de34y7i8v4z33c5 | Formed by encrypting the transaction data twice with the SHA-256 algorithm |
| Version | 1.0 | Block version |
| Size | 8 bytes | Block Size |
| Timestamp | 1565259135 | Epoch Unix Time Stamp |
| Prev-Out | 5tf43w6i80hf56831s3vs3st67 | Presents whether the voter has voted before or not |
| Out | {Recipient Address} $_{\text{Voter's Public Key}}$ | Specified candidate's address |
| $S_{EA}$ | [Transaction Signature] $_{\text{Voter's Private Key}}$ | Contains the S'EA(TxID) |

Eventually, the transactions will be posted with the one-value credit to the transaction pool waiting to be validated and appended to the blocks. Let us summarize this stage as follows:

1. A voter's first cast transaction will include no Prev-Out of the BL-i transaction and false value in Prev-Out of the BL-v transaction. After that, if there is an overwriting vote, it will consist of the previous TxID in the BL-i transaction as well as in BL-v transaction block.
2. BL-v does not have any clue leading to the voter.
3. BL-v must include only signed transaction by EAR.

- **Vote Tallying**. Vote tallying will be one of the responsibilities of the EAR for that constituency. EARs are (virtual agent) persons or institutions permissioned by the network and directed by the state to perform audit and certification of the votes/voters. An EAR could be assigned for every polling station or even one per district.

Candidates/parties will get a summary ballot tallying just the votes received; furthermore, the summary will be fully vetted by the EARs. That is how the vote tallying will happen automatically. EAR will verify both of the blockchains, also counting or listing all voters thus verifying who did cast his vote and who did not.

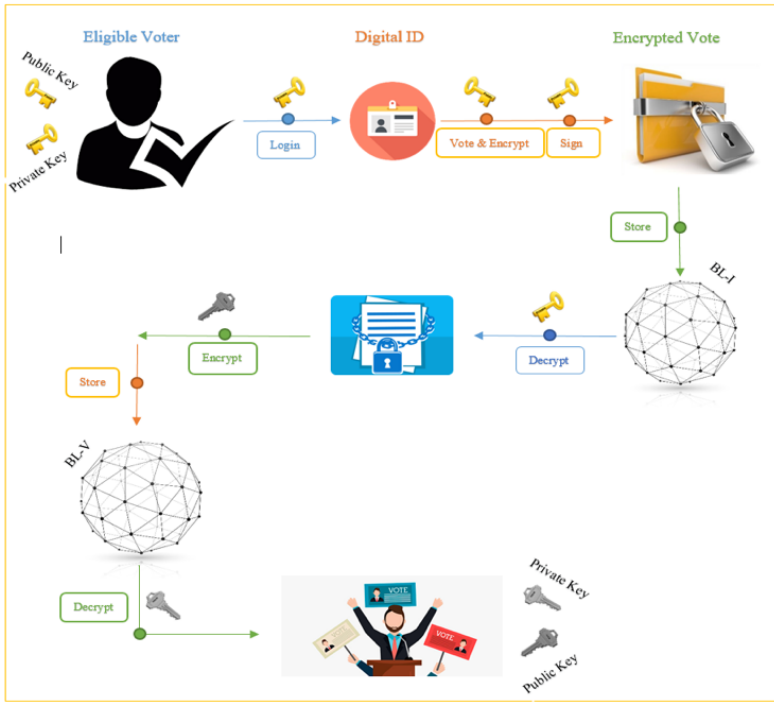


Fig. 5. Secure i-Voting architecture.

## 6. Threat Model

Maintaining sufficient security of the e-voting paradigm requires overcoming many difficult problems in cybersecurity, especially, with existing technology, a small lapse can affect the election result's integrity. Undesirable experiences in different places around the World (New South Wales, Estonia, India, etc.) in real-world have come up in online voting examples which demonstrated many security issues. There are many kinds of attackers (foreign countries, deceptive voters, funded criminals, etc.) who demonstrated realistic threats; many of these threats must be taken as an example while designing or setting online voting. Let us identify some potential attacks and any exposures that might exist to highlight the way to avoid and overcome them.

### *1.* Cross-Site Scripting (XSS)

An XSS vulnerability is a type of injection, simply attacker who can exploit an XSS attack could gain the ability to act like the victim. Moreover, both the voter and the vulnerable system often will not be aware of the attack. Using the well-known practices below all together considered as a great way to defeat the majority of XSS vulnerabilities [23]. Let us outline these methods below:

**Escaping**. Escaping data means ensuring that the data is secure before rendering it to the end-user. So escaping user input and key characters prevent received data from being interpreted in any malicious way.

**Validating Input**. Input validation prevents voters from inserting any special characters, instead of rejecting the request.

**Sanitizing**. Assuring the input data will not do any harm to users and database by cleaning the data from any potentially harmful markup, moreover, changing untrusted user inputs to an acceptable format.

### *2.* FREAK Attack

The SSL/TLS vulnerability (Factoring Attack on RSA-Export Keys) may allow attackers to decrypt secure communications between vulnerable clients and servers (intercept HTTPS connections) and force them to use older and weaker encryption, also known as the export-grade key or 512-bit RSA keys [24]. Let us highlight the necessary precautions against the FREAK attack by:

- Disable the support for TLS export cipher suites.
- Disable the support for insecure known ciphers (not only RSA export ciphers),
- Disable support for ciphers with 40- and 56-bit encryption,
- Enable forward secrecy.

### *3.* Malware

Malicious attackers who tend to manipulate systems to have more access by promoting their privileges can install Trojans or backdoors by using pre-existing botnets and target a specific country or region [22]. In this case, it would be easy for them to fully control data of the infected voters' computers.

Voters must be very careful and familiar with the computer protection instructions to be able to protect their own computer (or smart terminal device such as a cellphone, tablet, so on). Some of the common critical steps to protecting voters' computers are listed below:

- Installing a firewall
- Installing security software from a reliable company.
- Setting the operating system and the web browser to update automatically.
- Making sure that the web browser's security setting is high enough to detect unauthorized downloads.

## 7. Conclusion

This paper is an extended version of the older version of A Design for Blockchain-Based Digital Voting System [30]. The paper proposes a novel e-voting architecture to properly facilitate digitalized elections maintaining vote and voter privacy while preventing fraud. The key processes of the architecture, namely, voter ID creation, voting, vote verification and vote tallying are introduced in explaining the logical design of the digital voting system i-Voting. The key technologies used in affecting such results are the distributed ledger of Bitcoin, namely the blockchain

technology and RSA public-private key system. As well as in this new extended version we utilized blind signature in authorizing eligible votes and preventing multi-vote cast by a voter. Moreover, solutions to overcoming many server- and client-side attacks faced by earlier elections were indicated.

Fundamentally, the blockchain technology's ledger decentralization and blocks serialization provide great tools against result manipulation. Therefore, using the proposed blockchain-based architecture leads to achieving sound and fair election. Let us not forget the issue of impersonation. By deliberately opening the system sometime before the election, voters will be allowed to establish their identity. If there is any impersonation, it will be discovered. In addition, an eID's legitimate owner only will be able to use it due to the employed time-critical one-time password algorithm.

Furthermore, an effective approach proposed to address the issue of vote-selling by making vote vendors unreliable is one of the most important solutions to this structure. Several ways and possibilities allow a candidate/party to buy a voter's ballot. Firstly, by taking all login information of the voter and logging into the system in the legitimate voter's place during the polling day and casting a vote. Secondly, asking a voter to attend a specific place and make him cast his vote for them remotely. Thirdly, a voter can be asked to video himself his vote during the voting process. Our proposed approach allows voters to cast a vote unlimited times, whereas only the first vote cast will be accepted with subsequent ones disregarded due to the fact that the structure of the blockchain in itself prevents double voting.

It should be noted that the proposed scheme permits absentee ballot due to its web-based nature allowing remote vote casting; however, mail-in ballot (postal vote) and proxy voting are not permitted. The identified approach involves tradeoffs and may not be suitable for all. Some citizens, especially older ones, may not be able to cope with the complexity of digital voting: eID creation, PKI use, or even using a browser. It can be solved by posting guidance videos or preparing help centers to guide voters who have difficulty following the voting procedures. As a stopgap measure, postal and proxy vote may be authorized in advance in certain exceptional cases, such as inability and incapacity to reach the polling station.

**References**


1. Brightwell, I., Cucurull, J., Galindo, D., Guasch, S.: An overview of the iVote 2015 voting system, New South Wales Electoral Commission, Australia, Scytl Secure Electronic Voting, Spain (2015)
2. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, February (1978)
3. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, (2008)
4. Glaser, F.: Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. Hawaii International Conference on System Sciences, Goethe University Frankfurt, Hawaii, (2017)
5. Kizhakkedathil, N.: A Study Into The Prospects Of Implementing End-To-End Verifiability In Estonia Voting. Tallinn University Of Technology, Faculty of Information Technology, Department of Computer Science, Tallinn (2016)
6. Zyskind, G., Nathan, O., Pantland, A.: Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE CS Security and Privacy Workshops, (2015)
7. Lyon, D.: National IDs in a Global World: Surveillance, Security, and Citizenship. Case Western Reserve Journal of International Law Cleveland, Ohio, vol. 44, pp. 607–623, (2010)
8. Johnson, D., Menezes, A.: The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, Dept. of C&O, University of Waterloo, Canada (1999).
9. M'Raihi, D., Machani, S., Pei, M., Rydell, J.: TOTP: Time-Based One-Time Password Algorithm, Internet Engineering Task Force (IETF), (2011)
10. Dunphy, P., Adleman, L.: A First Look at Identity Management Schemes on the Blockchain. IEEE, VASCO Data Security, (2018)
11. Hastings ,N., Peralta, R., Popoveniuc, S., Regenscheid A.: Security considerations for remote electronic UOCAVA voting. National Institute of Standards and Technology, NISTIR 7770, Feb (2011)
12. Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., Halderman, J. J.: Security Analysis of the Estonian Internet Voting System, University of Michigan , Open

Rights Group, ACM New York (2014)
13. Halderman, J. A., Teague, V.: The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election, University of Michigan, University of Melbourne, arXiv:1504.05646v2 [cs.CR] Jun (2015)
14. Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thome, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Beeguelin, S., Zimmermann, P.: Imperfect forward secrecy: How Diffie-Hellman fails in practice, May (2015)
15. Durumeric, Z., Adrian, D., Mirian, A., Bailey, M., Halderman J. A.: Tracking the FREAK attack, https://freakattack.com/
16. McKay, R.: Flaws in iVote's re-vote process which attempts to defeat coercers, http://www.bigpulse.com/governmentelections#changevoteaw
17. Jones,D. W., Simons, B.: Broken Ballots: Will Your Vote Count?, Stanford University Center for the Study of Language and Information, California (2012)
18. Cross-Site Scripting, http://shiflett.org/articles/cross-site-scripting
19. Parsovs, A.: Practical issues with TLS client certificate authentication, University of Tartu, Software Technology and Applications Competence Center, Estonia (2014).
20. Moura, T., Gomes, A.: Blockchain voting and its effects on election transparency and voter confidence, Proceedings of the 18th Annual International Conference on Digital Government Research, ACM, pp. 574–575, USA(2017)
21. McCorry, P., Shahandashti, S. F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy, in International Conference on Financial Cryptography and Data Security. Springer, pp. 357–375, (2017)
22. Danchev, D.: Study finds the average price for renting a botnet, ZDNet, May (2010), http://www.zdnet.com/blog/security/study-finds-theaverage-price-for-renting-a-otnet/6528.
23. Vonnegut, S.: Preventing XSS: 3 Ways to Keep Cross-Site Scripting Out of Your Apps, Oct (2017), http://www.zdnet.com/blog/security/study-finds-theaverage-price-for-renting-a-otnet/6528
24. Vonnegut, M.: FREAK Attack: What You Need to Know, March (2015), http://www.zdnet.com/blog/security/study-finds-theaverage-price-for-renting-a-otnet/6528
25. Chaum, D. L.: Untraceable electronic mail, return addresses and digital pseudonyms, technical note programming techniques and data structures, Advances in Information Security, 7, 211-219 (1981)
26. Czepluch, J. S., Lollike, N. Z., and Malone, S. O.: The use of block chain technology in different application domains, IT University of Copenhagen, Copenhagen, (2015).
27. Jason, P. C., and Yuichi, K.: E-voting system based on the bitcoin protocol and blind signatures, E-voting system based on the bitcoin protocol and blind signatures, 10, 1, 14-22 (2017).
28. Bartolucci, S., Bernat, P., and Joseph, D.: SHARVOT: secret SHARe-based voting on the blockchain, 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg, 30-34 (2018).
29. Ayed, B. A.: A conceptual secure blockchain-based electronic voting System, International Journal of Network Security and Its Applications (IJNSA), 9, 3, 1-9 (2017).
30. Al-Rawy M., Elci A. (2019) A Design for Blockchain-Based Digital Voting System. In: Antipova T., Rocha A. (eds) Digital Science. DSIC18 2018. Advances in Intelligent Systems and Computing, vol 850. Springer, Cham, pp. 397-407.

# Social Aspects of Big Data Technology Implementation

Artem A. Balyakin[1], Sergev B. Taranenko[1], Marina V. Nurbina[1], Mikhail A. Titov[2]

[1] National Research Centre Kurchatov Institute, Moscow, Russia, 143968
[2] Lomonosov Moscow State University, Moscow, Russia,119991

https://doi.org/10.33847/2686-8296.1.1_2

Received 30.09.2019/Revised 01.11.2019/Accepted 11.12.2019/Published 22.12.2019

*That which has been, is that which is to be,*
*and that which has been done,*
*is that which will be done,*
*and there is no new thing under the sun.*
*Ecclesiastes 1:9*

**Abstract.** Big Data is supposed to be one of the main traits of new coming digital era. Its technological aspects are usually widely discussed, whereas social peculiarities are mostly neglected. We present main approaches to Big Data, and argue that despite seeming revolutionary technology, Big Data can be treated as a new tool to produce knowledge. That means, it generates the same risks and challenges as other breakthroughs we witnessed previously. To our viewpoint, cultural aspects should be as counted as a main issue in Big Data implementation. Since the inability to control big data through prohibiting some peculiar features it possesses, we argue that one should focus on such practical steps as terminology improvements, and the evaluation of societal outcomes of the new technology.
**Keywords:** Big Data, Cultural Aspects, Scientific Infrastructure, Megascience, Research and Innovation Policy, Socio-Economic Challenges.

## 1. Introduction

With the pace of nowadays technology development digital aspects of everyday life become inevitable, and such a term is widely used to describe forthcoming a global information infrastructure. Experts predict the rise of "Internet of Things" that will rise from the current "big data", artificial intelligence and other similar technologies. As a whole, the most important thing is to put existing data in prescribed order, and in case it is duly collected, structured, and processed, the information would enable the society to arrive at right managerial decisions [1,2]. For instance, in the EU, the first task is to build a digital infrastructure that would ensure effective interaction between researchers and infrastructure elements [3]. In the Russian Federation, digital technologies are included in the number of breakthrough technologies, and their practical use in the future should contribute to Russia's global technological competitiveness [4].

Newly forming digital industry will be highly likely personal: it is expected to be characterized by a flexible network approach to the production process (so called network-centric approach), when each consumer turns to be a manufacturer, constructing the necessary goods upon one's purpose. In this scenario the industry of the future will be operating online, from sample designing to its production (through data exchange and numerical processing). There would be the geographical dispersion of various elements of production (i.e., production of the constituent parts of the goods). In optimistic conception, the innovation cycle would be also reduced. All these ideas are still under question, as the regulatory governmental function in the field of high technologies to increase.

With the development of electronic computer technologies and the Internet, the

role of the management of large amounts of data is becoming increasingly prominent. The issues of transferring, processing and storing information from purely practical tasks of building hardware and software are transformed into a problem of infrastructure organization, and data handling issue is moving from technological solutions into the field of economics, sociology and public administration. Moreover, the evolution of "big data" technologies gives an impetus to the development of a number of specialized scientific areas, including dual purpose ones. In particular, we are talking about the creation of a system of highly specialized artificial intelligence (i.e., intelligent big data processing systems), the development of mechanisms for optimizing data selection using a statistical-probabilistic approach, and the creation of new methods for in-depth analysis of large amounts of data, methods for solving multidimensional incorrect problems.

The most common approach is to consider the Internet as a source of "big data", and, more narrowly, - to regard social networks as the only big data origin [5]. However, other areas of human activities, such as science, retail, and medicine play an important role in "big data" formation [1,6-8]. The apparent diversity of "big data" sources is being neglected by similar approaches in collection, storage and analysis of the gathered information. Hereby, the algorithms used in the scientific field can be transferred to other areas of knowledge.

Main feature of digital technologies development (and related areas) is a serious heterogeneity in its introduction and implementation into everyday life; at the same time, the dynamics of the information technologies dissemination in world regions does not meet optimistic expectations [9], the last ultimately leads to the emergence of new socio-economic and political challenges, the response to which requires increased attention of society, with the involvement of experts in various industry areas. Thus, one of the possible consequences is the information (digital) spatial inequality, which is irremovable in the short term [1].

In particular, one of the problems requiring a scientific approach is the legal implementation of processes of the "big data" circulation and the development of a common (more likely – cultural) approach to "big data" that takes into account the socio-economic and moral-ethical dimensions of new technologies.

In this paper, we consider the current situation of perception of "big data": in the first section a general description of the problem of "big data" is given, with corresponding definitions and concepts. The second section describes some features of the legal regulation of the "big data" circulation and existing practices, and shows the important role of the cultural aspect of the considered problem. In the third section, we postulate the idea of non-uniqueness of "big data", we provide parallels with already existing technological innovations in human history. Finally, in conclusion, a number of practical steps are proposed in the field of "big data" regulation.

Our main position is that the novelty of the practical use of "big data", as well as the problems produced by them, is very exaggerated: most of the difficulties have already arisen in human history throughout scientific and technological progress, thereby, we are able to assume (predict) the main consequences new technology can produce, and strive to take the most optimal management decisions in this area.

Based on the proposed approach, the conclusion contains brief summary and recommendations on the need and the possibility of "big data" regulating.

## 2. Conception of "Big Data"

The term "Big Data" does not have a conventional definition. Some researchers even exclude the technology of "big data" as an independent area, considering it as "…a title that includes a large number of technologies that are actively used in everyday life, related to the various areas of activity and do not have signs of innovation…" [1].

Previously, the main criterion for referring to "big data" was the amount of information processed, "the size of which exceeds the capabilities of typical databases

for writing, storing, managing and analyzing information" [10], and the "big data" themselves were determined by specifying the following main characteristics of the operated data, usually referred as "Three Vs" (see Fig.1):

1) large volume (Volume),
2) diversity of data (Variety), and
3) high rate of their change (Velocity) [2].

In a broader sense, "big data" was understood as a socio-economic phenomenon associated with the emergence of technological capabilities to analyze huge amounts of data, in some problem areas - the entire volume of worldwide data, - and with the resulting transformational consequences [11].

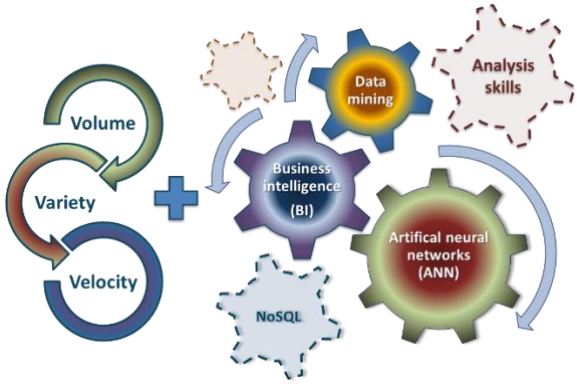


Fig.1. Big Data and Technologies

Gradually, the limitation of computing capacity for information processing began to wash out from this definition, and the main emphasis was placed on the methods and approaches to the processing of initial/raw data. By now, the main software methods used for the processing of "big data" are the means of mass-parallel processing of vaguely structured data, first of all, database management systems of the NoSQL category, MapReduce algorithms and software frameworks with corresponding libraries implementing the Hadoop project [12]. A variety of information technology solutions further began to be attributed to a series of big data technologies, to a greater or lesser extent, providing similar characteristics to the possibility of processing extra-large amounts of data. Fig. 1 illustrates the key technologies involved in "big data" operation, as well as main characteristics of "big data" as a process (Three Vs).

Since "big data" involves a combination of information, methods of its processing and obtained results (of the erroneously counted as new "knowledge"), the question of the source of data arose. Onwards we will utilize the term "data lake", that refers both to all the initial unstructured information in general, and the infrastructure that makes it possible to operate the "big data".

Fig. 1.

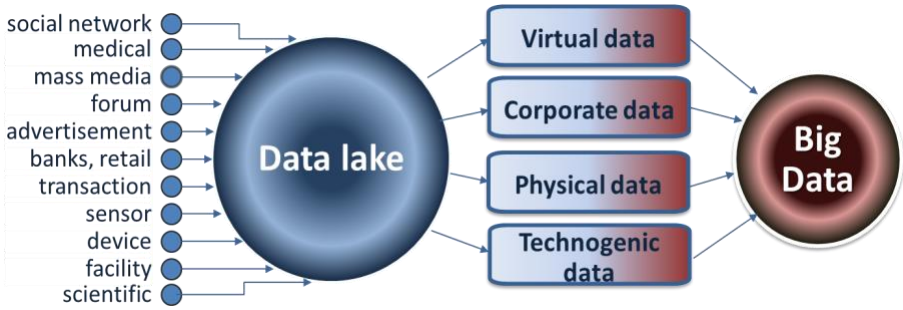


Fig. 2. Main approaches to Big Data. The current state-of-the-art

Since in the practical aspect the commercial use of "big data" is considered to be the most significant, we propose following classification according to the nature of original data (where from "data lakes" are formed/filled), represented in Fig. 2:

- virtual data (e.g., Internet: social networks, forums, electronic media, etc.);
- corporate data (e.g., banks, advertisement, retailers - it is, usually, customer data and currency transactions);
- physical data (e.g., data from sensors, detectors, measuring tools and other devices);
- technogenic data (information exchanged between devices during operation; auxiliary information).

As it is seen, the resulting data set relates to various areas of human society: social (e.g., electronic data), economic (e.g., data of corporations and banks), medical (e.g., collection of personal data and a number of corporate data), scientific (e.g., physical data from scientific facilities) - which, in turn, leads to different prioritization in data handling and processing. Thus, for electronic data, the size (volume) aspect is important, for corporate data - the emphasis is put on variability (dynamics of data), while the data itself is often initially structured. For medical data, such parameters as volume and dynamism are important, but there is also a clearly postulated parameter "value of human life" (i.e. social and cultural aspect).

Practically, manipulation with "big data" requires the structuring information into categories (tags), and the corresponding accompanying information (answering to questions what, where, how, by whom, etc.) is often comparable in volume to the original one. Consequently, the rapid growth of the data archives leads to problems with scalability, efficiency of the monitoring system and delays in receiving a response to external requests. At the physical level, this results in the fact that working with "big data" means [partial] segmentation of data on tasks (in accordance with the metadata model adapted to the requirements of the system: monitoring of terrorist activity, updates in the Facebook, analysis of scientific data, etc.)[1].

The requirement for computational efficiency (e.g., minimizing the amount of data processed in memory while generating a report) leads to the need to generate reports at different levels of detail [8]: in fact, "big data" is a data model with stepwise aggregation (in the limit – infinite recursion, and thus, fractal).

In the future, we will consider "big data" as a kind of entity with the following properties and meeting the following criteria[2]:

- The initial data set is considered to be some "data lake": unstructured, dynamically changing, heterogeneous and loosely coupled.
- "Big data" is the result of applying some methods (models) of selecting data from the all information available in the "data lake", and includes both the data itself with corresponding categories, and the mechanism (algorithm) of their selection and analysis.
- "Big data" is a dynamic, non-stationary system that is in constant process of filling, updating and adjustment[3].
- Inside the "big data" is embedded the algorithm of their processing, issuing a response upon some request. In this case, a feedback mechanism is implemented[4]: the data obtained, in turn, modify the "big data" and/or the mechanism of their selection from the data lake[5].

[1] To obtain more advanced position, investors/shareholders may have the interest to assess more detailed and structured information extracted from "data lakes". This is especially crucial for technology-oriented industries supposed to be capable to convert R&D expenditures into innovative products. This can be a key driver of competitive advantage and hence the financial performance of the organization. For instance, meaningful patent indicators can be an interesting proxy for assessing a firm's capability to innovate and to gain competitive advantage. Lexis Nexis can be cited as an example of a company that evaluates the competitive advantages and vulnerabilities of firms using a big data analytical platform [13].

[2] As an example of "big data" handling a one can refer to "data lakes" operating chart at Tinkoff Bank (see for details [14])

[3] Any arbitrarily large structured data is just a large database.

[4] Data should be continuously updated or modified (including its structure).

[5] In practice, it can be said that the data at the time of its retrieval from the "data lake" is ALREADY outdated.

• Any "big data" is scientific in the sense that it is measurable, selected by the chosen model, processed in advance by given methods and algorithms.

Towards the creation of a digital infrastructure that uses large amounts of data, several problems are highlighted, both of technical and institutional nature, in particular [15]:

• Data encoding;

• Elimination of "garbage", data "noise" management (e.g., filtering out unnecessary information, extracting useful information, evaluation of data adequacy);

• Addressing issues of the long-term content preservation, the development of new storage devices, backup technology;

• Compatibility of data from different periods of time (methods of data writing and encoding are different today and 10 years ago). Compatibility of data from different fields of science;

• Numerous duplications and repeatability of data, information redundancy;

• The need for continuous data verification and its "repackaging" (saving in a more compact form and/or more accessible). Data reduction (for writing) and their recovery (for adequate performance on request);

• Data presentation (visualization);

• The problem related to the creation of metadata: the transition from simple records to complex ones, having external and internal references for navigation (e.g., the analogy to the Internet); metadata structure development;

• Organization of data search and retrieval: formalization of search queries, caching of search data, allocation of servers for storage depending on the tasks and stored information. Organization of multi-level data access (e.g., the analogy with the library);

• Compliance with the legal issues of storing information, which is related to different countries (jurisdictions);

• Resolving the issue of territorial distribution of stored information.

Thus, we can distinguish "big data" issues in following aspects:

- man-made (problems associated with the technical evolution of storage devices, communication channels, etc.);
- structural (associated with duplication, redundancy of information, the creation of metadata, and TP);
- organizational and legal.

In our opinion, the most important problem to date is not technical difficulties, but issues of regulating "big data" circulation, providing for both following national interests and ensuring the protection of human rights (in case of using and processing personal information). In that question, science provides examples of both the appearance of the first difficulties of the legal regulation of "big data" and the emergence of moral and ethical problems, as well as possible ways of addressing them.

## 3. Cultural Approach to "Big Data"

The fact is that modern science and technology are inseparable from the socio-economic and political life: all areas of activity are so intertwined that it is impossible to separate technological progress from changes in social norms. In the formal language of title deeds, this led to the fact that, for example, in the European Union, the basis of decisions made is the need to solve social and humanitarian challenges in all their manifestations [3,15]. With respect to the "big data" in the EU there is a discussion about the ways of their management and regulation; Biomedicine (Artificial Intelligence for Decision Making) was selected as the first field of application:

metadata is now being collected and ethical principles relating to the regulation are being developed.

In the United States, the first concerns are not about controlling the circulation of "big data", but about the technical access control: the so-called "neutral" Internet involves changing the physical parameters of access to information and its processing in accordance with its content; in practice, data and users of these data are ranked due to their status. In the United States, issues with the protection of private information and its transfer to third parties for analysis and processing also led to a number of serious scandals with social network companies, but it was not possible to formulate clear definitions of permissible information disclosure (a discussion of existing legislative initiatives is given in [16]).

In Russia, the topic of "big data" has not gone beyond the highly specialized approach yet: thus, it raises the question of the need to create a public operator, allowing private sector participation, who would manage information about users' social data (e.g., user preferences on the Internet, social connections, the circle of communication, etc.) [17]. At the same time, legal issues are mainly limited to the regulation of access to personal user data by third parties [5,18] or the use of collected information to solve legal problems (e.g., user localization on the basis of geo-tracking of his mobile phone) [19]. Evidently, "big data" are a key interest for financial authorities, who are eagerly striving to get access to private users' information in order to streamline taxation[6].

The first problem that arises in the field of "big data" circulation is connected with personal data protection. Main issue is the necessity of personalized consent (confidence agreement) that includes the information to which extent the consent is given, and the procedure for its use. Practically, this leads to the emergence of a new segment of "big data" (the volume of regulatory legal documents, with the details of the base to be regulated, is comparable with the initial volume, i.e., it is also "big data" in volume). On the other hand, the set of all available data is so large (the size of data lakes is significant) that even without their personalization it becomes possible to identify the individual without any doubt, i.e., "data protection" function becomes useless. A way to break this vicious circle could be classifying "data lakes" as "natural" (i.e., data with no possessor, belonging to anyone), as suggested by the McKinsey report [21].

It is also important to note that the existing legal restrictions on the processing of personal data solely in accordance with the originally stated processing objectives, as well as the inadmissibility of combining different databases with originally stated and incompatible processing objectives, contradict with the existing technology and business practices, since it eliminates the advantages provided by "big data" technologies [22].

Note that a superficial way on the issue of regulating "big data" circulation leads to the thesis about the prohibition of social networks or their artificial restriction by introducing forbidden words, topics, etc. However, this approach is doomed to failure according to the above concept of "data lakes" and "big data": the initial data per se can be any, and their selection and analysis play the most important role (nor its origin or content). As practice shows, while maintaining and enhancing the existing attitude to the information regulation, "big data" technologies will increasingly migrate towards DarkNet, thus, exiting from the legal field. Thereafter, it should be about regulation at a level higher than the formal prohibition of certain words and/or pictures.

For example, in the EU, the concerns expressed about the recently expanding requirements for the protection of personal data will lead to the suspension of work in the field of "big data". As an example, the General Data Protection Regulation (EU)

[6] The last attempt of "big data" regulation was undertaken in newly proposed draft law on the creation of a single information resource for all citizens of the Russian Federation and persons residing in the territory of the Russian Federation [20].

is provided (2016/679, EU GDPR) [23]. This block of laws is aimed at giving citizens the control over their own personal data, at the same time suggesting the simplification of the regulatory framework for international economic relations by unifying regulation within the EU. The law expands the concept of personal data, introduces the concepts of "cross-border data transfer", "pseudo-anonymization", establishes the "right to oblivion", introduces the role of a security officer. The continuation of this policy is the recently adopted directive on the protection of copyright (EU Copyright Directive).

Another problem is the task of storing and accessing "big data". In general, a more capacious data warehouse, an improved search system, maximum complementarity and coherence of information are offered. In order to obtain maximum results and implement the right of equal access, the EU actively implements the principles of open science: thus, 779 organizational declarations governing open access were noted in the ROARMAP report for 2016. Of these, 133 were prepared by investors, 636 were formulated by scientific organizations. The "open science" movement in the Russian Federation has not become one of critical technology yet, but the creation and promotion of "open" principles for building digital infrastructure is included in the number of recommendations for adjustments to the scientific and technological priorities of research and development. Thus, in the foreseeable future, it is planned to implement a system of distributed remote access to both unique scientific facilities and databases, the development of systems for cloud computing and information storage.

This, in turn, leads to the fact that "big data" creates the illusion of knowledge, when the quantity replaces the quality. Easily accessible information leads, for example, to the desire to launch an "unconditional digital income", which contradicts to the fact that most of the information is useless and is never used (e.g., the CISCO report indicates that the "data lakes" themselves are growing at an enormous rate and according to expert estimates, at present, up to 90% of lakes are useless, since they are overfilled with information collected for some unknown purposes [1]).

## 4. Big Data: Totally New Deal?

The list of issues stated above are dangerous, challenging, but in fact nothing new for the society has come into life: such concerns, as can be easily seen, have already arisen in human history. The key point can always be reduced to the inquiry, if new technology introduces new knowledge, or just provide the new solution (assess)? If "big data" challenge is unique? Our answer is "sure not". We recall, for example, the invention of typography and the change in the status of monasteries at the end of the Middle Ages, when they lost their functions of knowledge accumulation and preservation.

The first issue is connected with the volume of information. It puts the question of data preservation and transference, rather than the extraction of new knowledge. In fact, we are witnessing the return to the present of the difficulties and problems of the middle ages: how to properly organize the functioning of libraries? Storage and preservation of manuscripts? How we can sure that their rewriting by literate monks?

The amount of data (information) can increase, but quantity doesn't turn into quality. For "big data" it is widely accepted the concept of easy search for correlations: we find what happens after what, while not explaining, why. We also note that data/information (not knowledge!) has become more accessible, their spread has accelerated significantly. But whether it is really new knowledge? The amount of information created today generates the same scholastic problems as before: does new knowledge exist or does the overall objective only narrow down to the correct codification of the existing one? To date, the answer is most likely negative: quantity (amount of data) does not yet turn into quality. However, there is a tendency of the

dilution of the notion of "big data", when society's demand shifts from quantity (size) to quality (algorithms and results of the technology use).

An obstacle to the development of the technology of "big data" is, in our opinion, a bias against it: the strong term is shifted from the field of scientific analysis to the field of hype. The main problem now in the field of using "big data" is the lack of a culture of handling a new tool of scientific and technological progress. Therefore, many problems and difficulties arising in the application of the "big data" technology do not have a conscious cause and malice: they result from ignorance (both the mechanisms and algorithms of the "big data" and the interaction of high technologies with the society). Another problem is associated with seemingly redundancy, accessibility and "belonging to no one" knowledge.

The lack of a culture of handling "big data" means no practices in the relevant field. Accordingly, at this stage there is no object for legislative work. In this regard, the expert community can and should form these practices.

In this case, the holistic approach is important. Currently, the most common attitude involves answers to ongoing challenges, the regulation of particulars: restrictions and prohibitions are created, which in fact are very easy to get around - this is not about lacunae, but about holes. The whole experience of mankind shows that such an approach is doomed [to failure]: an attempt to manage "big data" "piece by piece" creates new "big data" that governs the original "big data": it turns out to be a vicious circle.

We argue that it is required to perceive "big data" as a new tool of conceiving the world, carrying both positive and negative sides. This leads us to the conclusion that it is necessary to manage the social dimension of high technology. "Big data" technology accompanied with "open science" approach create endless "data lake" set. It brings us to the need to find a new way to data flows regulating. We propose to focus on "props of meaning" (main concepts, ideas, algorithms, physical basis of "big data" technology such as Data-centre), rather than on virtual space with unformed social communication practices.

In addition to this "from above" approach, the induction method is also possible. For example, one of the options for resolving such problems is the case law, which fixes the established tradition. Practically, society is waiting for some event to happen (e.g., the Cambridge Analytica data scandal) in order to begin to regulate this field. Until a certain moment, there is a fear of the new and unknown, to which unique (dangerous) features are attributed. It does not take into account the fact that similar problems have already arisen earlier, and it is just required to adapt them, "translating" from the old language and terminology into a contemporary perspective. As an example, we recall the dispute about the responsibility of artificial intelligence used in self-driving cars. It is proposed, for example, to use the Roman approach and to consider AI as an analogy for a slave (servile) in Roman law, i.e., not a subject, but an object of law. In such interpretation, there is no need to expand the concepts and introduction, as some researchers suggest, of a new - digital personality (which AI would be endowed with).

As the authors see it, the development of "big data" technology still raises more questions than answers, which is why it is now important to promote the development of new technologies with taking into account their social consequences. It is, in our opinion, the equivalent to the formation of the scientific culture of using digital infrastructure. Those are people who write the rules and set the language of the future. Its symbols are the digital infrastructure, but the logic of the organization of communication will be set by human. This is a hermeneutic approach: a well-formed language structure solves half of the problems.

This idea can be regarded as a possible treatment of approaching Digital Age, as well as a format of social science in the Digital Age. We suggest it to be a kind of a New Deal with regards to "big data" technology and its application.

## 5. Conclusion

In our opinion, the problem of "big data" represents an important task of modern social science: the versatility of methods and approaches in the technology of "big data", the "trans-border nature" of their consequences, the level of impact on the society - all this makes us consider new technologies both as an opportunity and as a serious challenge at the same time.

Big Data technology is an inevitable tool for digital economy that is being formed now. Its implementation requires the solution of both technical and social tasks: moreover, socio-economic impact of big data is often neglected, and needs to be addressed. With this regard it is extremely important to apply to previously arisen problems, adapting former answers for modern risks and challenges.

By now we witness the serious overestimation of the "big data" technology, when it appears to be something revolutionary that drastically changes human nature. In our previously published work [24] we stressed that the novelty of big data technology is mostly semblant, and the human society has already undergone similar problems earlier. We argue that this misconception is rooted in "trendy" perception of digital science as a whole and big data particularly. In fact, much of the moral and ethical issues have already arisen to humanity in the past, and the most important way to solve them was not partial prohibitions, but an understanding of the problem as a whole, developing a culture of dealing with a new phenomenon.

The authorities have 3 ways to influence the development of big data technology: to regulate it (via standards, etc.), to prohibit it (the most adequate example – GDPR introduced in EU [23]), and to stream it via infrastructure development (i.e. constructing data centers, etc.).

The role of experts' community is to raise questions of probable socio-economic issues in advance, to find the very position of big data technology in a whole structure of digital society. As for the practical steps, authors would suggest:

First, the coordination and promotion of a single glossary in the field of "big data", taking into account the experience from various fields of activity.

Second, the rejection of attempts to control the information used by "big data", and move the emphasis on the result of their use. It means the shift of the focus from "data lakes" to other objects (the conclusions drawn from "big data" technology, the regulation of data centers, etc.).

Third, bridging the gap between the technologies themselves and the consequences of their use. This requires taking into account social and economic effects of high technologies.

Neglecting social outcomes of new digital approaches could be the main problem in Big Data technology implementation. Reducing all problems solely to technical issues should be avoided, and emerging digital society should take complex form of advantageous combination of high-tech solutions and high-tech culture (i.e. culture of handling new technological solutions based on previous experience).

**Acknowledgments**

This work was supported by RFBR grant № 18-29-16130 MK.

**References**

1. Hype Cycle for Emerging Technologies (2015), URL: https://www.gartner.com/doc/3100227/, last accessed 2019/03/31
2. Lynch, C.: How do your data grow? Nature 455, 28-29 (2008).
3. Florio, M., Sirtori, E.: Social benefits and costs of large scale research infrastructures. Technological Forecasting and Social Change 112, 65-78 (2016).
4. The decree of the President of the Russian Federation. About the strategy for the development of the information society in the Russian Federation for 2017-2030. No. 203, 09.05.2017

5. Almyrzaeva, A., Kostyuk, V., Nevredinov, A.: The role of Big Data in modern society. Journal of Economy and entrepreneurship 9 (3), 580-582 (2017).
6. Yuchinson, K.: Big Data and Legislation on Competition. Law. Journal of the Higher School of Economics, issue 1, 216-245 (2017).
7. Grigorieva, M., Golosova, M., Ryabinkin, E., Klimentov, A.: Exascale Store for Scientific Data. Open Systems. DBMS. 23 (4), 14-17 (2015).
8. The Global Information Technology Report. The World Economic Forum (2016), URL: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf, last accessed 2019/03/31
9. Zobova, L., Shcherbakova, L., Evdokimova, E.: Digital spatial competition in the global information space. Fundamental research, issue 5, 64-68 (2018).
10. Manuka, J., Chui, M., Brown, B., Bughin, J., Hobbs, R., Roxburgh, C., Byers, A.: Big data: The next frontier for innovation, competition, and productivity / McKinsey Global Institute (2011).
11. Mayer-Schönberger, V., Cukier, K.: Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt (2013).
12. Making Sense of Big Data. PwC Tech Forecast, issue 3 (2010).
13. H. Ernst, N. Omland The Patent Asset Index – A new approach to benchmark patent portfolios: World Patent Information 33 (2011) 34–41.
14. https://habr.com/ru/company/tinkoff/blog/259173/
15. Balyakin, A., Mun, D.: Formation of an open science system in the European Union. Information and Innovations. Proceedings of the conference "Scientometrics and Bibliometrics", pp.33-37 (2017).
16. Net Neutrality 2019 Legislation. National Conference of State Legislatures (2019), URL: http://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2019-legislation.aspx, last accessed 2019/03/31
17. Hu, J., Zhang, Y.: Discovering the interdisciplinary nature of Big Data research through social network analysis and visualization. Scientometrics 112(1), 91-109 (2017).
18. Sokolova A.: The impact of big data analysis technologies (big data) on personal data legislation. In the collection : Jurisprudence 2.0: a new look at the right materials of the interuniversity scientific-practical conference with international participation. Russian University of Peoples' Friendship . Moscow , 2017. pp. 282 -285.
19. Bulgakova E.V. Methods for analyzing big data in solving legal problems. In the collection : Law and Information: Questions of Theory and Practice, a collection of materials of the international scientific-practical conference. Ser. "Electronic legislation" of the FSBI Presidential Library named after B. N. Yeltsin. 2017. pp. 90 -96.
20. Order of the Government of the Russian Federation of July 22, 2019 No 1627-p On submitting to the State Duma of the Federal Assembly of the Russian Federation a draft federal law "On a single federal information resource containing information on the population of the Russian Federation", http://government.ru/dep_news/37452/, last accessed 2019/07/30.
21. Digital Russia: a new reality (2017), http://www.tadviser.ru/images/c/c2/Digital-Russia-report.pdf, last accessed 2019/03/31.
22. Savelyev, A.: The Issues of Implementing Legislation on Personal Data in the Era of Big Data. Law. Journal of the Higher School of Economics, issue 1, 43-66 (2015).
23. The EU General Data Protection Regulation (GDPR), https://gdpr-info.eu, last accessed 2019/03/31.
24. Balyakin A.A., Malyshev A.S., Nurbina M.V., Titov M.A. (2020) Big Data: Nil Novo Sub Luna. In: Antipova T. (eds) Integrated Science in Digital Age. ICIS 2019. Lecture Notes in Networks and Systems, vol 78, pp. 364-373. Springer, Cham.

# State regulation of the introduction of digital technologies in the oil and gas complex of Russia

Zhanna Mingaleva[1] and Elizaveta Sevidova[1]

[1] Perm National Research Polytechnic University, Perm, 614000, Russia

https://doi.org/10.33847/2686-8296.1.1_3

Received 05.10.2019/Revised 04.11.2019/Accepted 11.12.2019/Published 22.12.2019

**Abstract.** Using digital technologies for the oil and gas production requires the organization of a generalized network of wireless interaction of components, continuous data collection from various sensors and sensors, the collection and exchange of information in order to detect complex events and critical moments, their analysis and detailed description based on the situation. However, the digitization of basic technological processes and operations in the Russian oil and gas complex is proceeding more slowly than in many other areas of production. Government assistance can stimulate the process of digitization of the oil and gas industry. The government authorities form and develop a regulatory framework in the field of and digital transformation of oil and gas production. This article presents a scheme of government regulation for the digital transformation of oil and gas production.

**Keywords:** Sustainability development, Government regulation, Competitiveness of enterprises, Digital technologies.

## 1. Introduction

One of the most important problems of the development of oil and gas production in Russia is a decrease of the oil recovery factor due to an increase in the residual hard-to-recover oil. In the main areas of oil production in Russia (in Western Siberia, the Volga-Ural, North Caucasus regions) hard-to-recover reserves are more than 50 % and in some areas more than 80 %. This can be explained by the specific geological peculiarities of the main areas of oil production and leads to a decrease in the economic efficiency of oilfields. In such conditions, relying on modern trends in the development of the economy and society further development of hydrocarbon production should be aimed at significantly reducing operating costs through digital upgrading. "Today's market and industry outlook are forcing O&G companies to re-examine core business capabilities, and explore new ways to execute business strategies in a dynamic and volatile marketplace. Whether large or small, national or international, digitalization of key operational workflows in O&G companies will be critical for success in the years to come" [1, p.2]

The significance of the digitization of the oil and gas industry was recorded in 2017 at the World Economic Forum, where the oil and gas industry's digital transformation initiatives were discussed and adopted [2]. An expert analysis of the prospects for the development of the oil and gas industry on the basis of the coverage of the digital transformation of all its enterprises conducted by the staff of the World Economic Forum showed the prospects for the development of the industry and humanity in general.

"The digital transformation in the Oil and Gas industry could unlock approximately $1 trillion of value for oil and gas firms, with another $640 billion for its customers and wider society" [2, p.5]. This figure includes approximately "$170 billion of savings for customers, roughly $10 billion of productivity improvements, $30 billion from reducing water usage and $430 billion from lowering emissions" [2, p.5].

Another important advantage of digitalization industry - reduction of environmental damage: "environmental benefits include reduced emissions of CO2-equivalent (CO2 e), savings of about 800 million gallons of water, and avoiding oil spills equivalent to about 230,000 barrels of oil" [2, p.5].

As a result, the total estimated benefit from digitization of the industry may increase to $2.5 trillion [2, p.5].

Despite technological advancements, oil and gas companies have been slow to seize the opportunity presented by digitization. As emerging technologies continue to reshape the landscape of other legacy industries, the oil and gas industry has generally been more cautious and slower to embrace change.

However, as many experts note, "Despite technological advancements, oil and gas companies have been slow to seize the opportunity presented by digitization" [3]. This is unusual because "oil and gas companies were pioneers of the first digital age in the 1980s and 1990s. Long before phrases such as big data, advanced analytics, and the Internet of Things became popular, oil executives were making use of 3-D seismic, linear program modeling of refineries, and advanced process control for operations. The use of such technologies unleashed new hydrocarbon resources and delivered operational efficiencies across the value chain" [4].

This requires a change in the conditions for the introduction of digital technologies in the industry. The government of each country can and should regulate the process of introducing modern digital technologies at all stages of the operation of enterprises in the oil and gas sector.

## 2. Theoretical and methodical background

The concept of digital upgrading is increasingly being developed in modern scientific literature. Foreign researchers from universities and research centers of large corporations are developing these issues over the course of the current decade. At the same time, most of the studies, like 30 years ago, are dedicated to assessing the possibilities of applying various methods and tools for processing big data to control various production processes. This is the development and introduction into production of optimization methods for various equipment in gas storage systems [5], including in underground gas storage systems [5] and in natural gas transportation systems [7-8]. This is a numerical simulation for various types of well drilling [9], selection of evaluation methods of enhanced-oil-recovery [10], digitization of drawings of complex engineering structures [11], development and implementation of RN-Lab information system for core and reservoir fluid laboratory study [12], prediction and modeling of damage to the reservoir oil field [13].

Russian researchers are studying the results of digital modernization of oil and gas companies (Rosneft oil company, Bashneft) [14-15], analyzing the digitalization trends of the Russian oil and gas complex and the features of its modernization [16-17]. Also, Russian researchers analyze the results and possibilities of implementing the innovation strategy for the development of the Russian oil and gas complex and the fundamental foundations of innovative technologies in the gas industry [18-19].

Digital upgrading of oil and gas production is the process of transforming oil and gas activities through intellectualization, super computerization, opticalization and robotization by changing the vision of its development. "The access to intelligent insights, analysed in real-time, is crucial to an industry that's global network is vast in both size and scope" [3]. Companies that successfully employ automation can significantly improve their bottom-line operations. Experts of Forbes note: "We expect to see dramatic cost savings and significant improvements in productivity and revenue" [20].

Digital upgrading of production means revolutionary changes in business models based on the use of digital platforms in order to ensure a significant increase in market volumes by increasing the competitiveness of business activity [21]. The

rapid progress of technology such as big data and analytics, sensors, and control systems offers oil and gas companies the chance to automate high-cost, dangerous, or error-prone tasks [7]. "Digital transformation creates unprecedented opportunity" [1, p.3]. And as the researchers note, "while it may appear as though digital transformation is passing oil and gas companies by, the industry is working towards digitisation, albeit at a more gradual rate" [3].

Digital upgrading of production involves the organization of the introduction of modern innovative technologies, the adaptation and development of new business models in the digital economy, which will entail a qualitative improvement in business processes, including the production of products and services. Particular emphasis in this area of research is done on minimizing energy costs for various enterprises of the oil and gas sector [22], on minimizing environmental damage from the activities of enterprises in this industry [23]. At the same time, most researchers note that the harnessing Big Data remains the priority for enterprises in the industry. "The difficulties arise as the data is often scattered across various oil fields and off-site collection centres, and a multitude of software is being used to interpret it. In recent years, however, advancements in data processing and communications have made large volumes of data more manageable, simpler to process and to stream between machines" [3].

In the last 2 years, works have appeared on analyzing the problems of the oil and gas sector related to the use of digital technologies and management methods [24]. "As emerging technologies continue to reshape the landscape of other legacy industries, the oil and gas industry has generally been more cautious and slower to embrace change" [3].

The main research method is bibliographic analysis. The main bibliographic sources used were federal laws and regulations of the Russian Federation (Federal Law "On Environmental Protection" No. 7-FZ [25]; Federal Law "On Industrial Policy in the Russian Federation" No. 488-FZ [26]; Federal Law "On Production and Consumption Waste" No. 89-FZ [27]; The Federal Law "On Standardization in the Russian Federation" No. 162-FZ [28]; Tax Code of the Russian Federation [29]), regulatory documents of oil and gas production enterprises, modern scientific research, including materials from journals "International Journal of Oil, Gas and Coal Technology", "Pipeline and Gas Journal", "Neftyanoe Khozyaystvo - Oil Industry", "Oil. Gas. Innovations", "Oil and Gas Science and Technology", "Oil and Gas Journal" and all.

All major consulting firms and major automation vendors have been actively offering their own IoT platforms for more than 5 years, which are focused on providing services for the oil and gas enterprises. These are: predictive analytics, Big Data analytics, cloud services, remote monitoring, big data analysis and cybersecurity, which is of paramount importance in the oil and gas industry.

Also, all major consulting firms offer digital products, solutions and services to reduce operating and maintenance costs, increase efficiency, increase profitability, increase productivity, optimize enterprise performance. Analytical information of the largest consulting firms and major automation vendors as IBM Corporation, McKinsey & Company, Deloitte Consulting LLP, Insight Consultants was also used in this study.

## 3. A legal regulation of the digital transformation

Digital upgrading leads to a massive change in the models of the oil and gas business and production, the best of which are transferred to the entire oil and gas sector. This implies not only changing the conceptual model of business, but also compliance with legal requirements.

The provisions of the Federal Law of Russia "On environmental Protection" [25] form the legal basis for the transition of oil and gas companies to the concept of modern digital technologies. The law formulates the concept of best available technologies (BAT), establishes standards for areas in which their use is necessary,

provides for the development of information-technical journals for specific areas of application of the best available technologies, provides for state support for their implementation [30]. The conditions and procedure for the application of information-technical documentation are regulated by the legislation on standardization (Federal Law of Russia "Standardization in the Russian Federation" [28]). The introduction of the best available technology journals in the oil and gas sector is starting in 2019. This will contribute to a more active transition of Russian oil and gas enterprises to the principles of modern digital technologies.

Article 17 of the Federal Law of Russia "On environmental Protection" names the measures and a sequence of government support for the activities of enterprises implementing the best available technologies in their industries. They are:

- monetary funds may be allocated from the federal or regional budget to enterprises;
- privileges on payment of taxes and fees may be granted;
- enterprises may receive benefits on environmental charges levied in order to compensate for the consequences of their negative impact on the environment.

According to Article 10 of the Federal Law "On Industrial Policy in the Russian Federation" oil and gas enterprises intending to upgrade their production facilities by means of new technologies can receive government subsidies and expect on their financial support. The transition to modern technologies is connected with the Federal Law of Russia "On Energy Saving and Improving Energy Efficiency" that determines relations in the development of the efficient use of energy resources. At the same time, tax exemptions are established for objects and technologies with high energy efficiency including an investment tax credit (Article 67 of the Tax Code of the Russian Federation) and the use of special raising coefficients to the depreciation rate in relation to the corresponding fixed assets similar to those established during the implementation best available technologies (Article 259.3 of the Tax Code of the Russian Federation).

The standards for the introduction of new technologies are established in Article 11 of the Federal Law of Russia "On Production and Consumption Wastes". Paragraph 2 of which states that legal entities and individual entrepreneurs operating buildings, structures and other objects should introduce the best available technologies.

The above regulatory acts have formed certain incentives for the introduction of modern innovative technologies. Their use will contribute to minimizing the negative impact of oil and gas enterprises on the environment and improving the efficiency of the Russian oil and gas industry.

## 4. The main ways of development of digital technologies of the oil and gas complex of Russia

The introduction of digital technologies in the oil and gas complex of Russia is directly connected with artificial intelligence systems. This is machine learning and in-depth machine learning; botosphere, including: robotization, bots, drones; and virtual reality of objects: improved reality, digital twin, etc. Digital upgrading models used in oil and gas companies are similar in nature.

The cost of hydrocarbon production technologies can be decreased by digital upgrading of production that will make oil and gas more available for the customers. The main ways of digital technologies' development in the oil and gas complex of Russia is presented on Fig. 1.

Using of digital sensors will make it possible to record the processes of production in the oil and gas industry more effectively. The information received by means of the embedded processors can help in making decisions independently, regardless of the central control system of the production process in the current conditions.

The difference between cyber-physical systems is based on the function of two-way communication between computerized computing facilities and physical

production processes. The process of collecting, exchanging, processing, analyzing information will allow diagnostics of the state of the production system, forecasting, comparing and selecting options for decisions, automatic tuning and adaptation of equipment. Elements of cyber-physical systems can be located either in a single production zone or remotely from each other, and their interaction takes place at all stages of the production process.

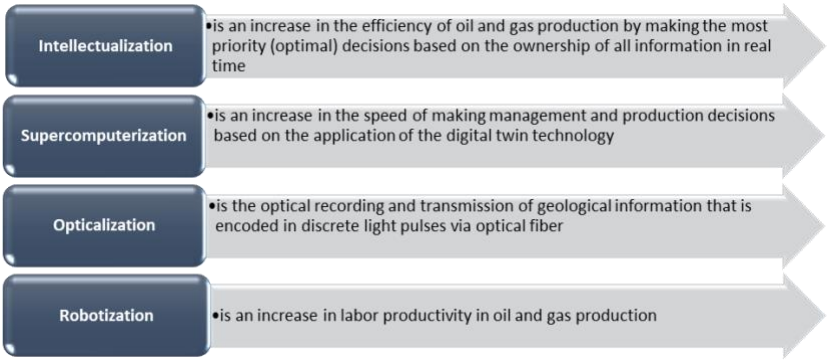


Fig. 1. The main ways of development of digital technologies in the oil and gas complex of Russia

*Source: own processing*

Automation offers many potential benefits of the value chain associated with exploration, development, production and transportation, as well as great opportunities to improve safety, security and decreased downtime [8]. Expanding their digital capabilities, companies will have more opportunities for the formation of informative and intellectual understanding. Companies that successfully employ automation can significantly improve their bottom-line operations [8].

However, despite the fact that all the main areas of digital modernization of the oil and gas complex of Russia (from artificial intelligence to cloud computing, robotics and 3D scanning technologies) are taken into account in digital modernization programs, development of comprehensive security systems to protect these newly-connected, software-driven operations have lagged behind. "To solve the current security challenges facing the oil and gas industry and take advantage of the capabilities promised by Industrial IoT, a new vision for security must be innovated" [31].

## 5. The government support of the digital transition of enterprises in the oil and gas complex of Russia

The Russian system of stimulating the transition of the oil and gas sector of the economy to modern technologies, the prerequisites for the introduction principles of BAT are formed. But it is necessary to implement a number of measures to make this mechanism work more effectively. For example, it is now assumed that the introduction of the best available technologies should be carried out by enterprises on a voluntary basis, while in the practice of the European Union, enterprises are obliged to implement them at the level of their financial capabilities.

To implement the transition to the best available technologies algorithm it is necessary to create an effective interaction between government agencies and oil and gas enterprises through regulatory and information support is required (see Fig. 2).

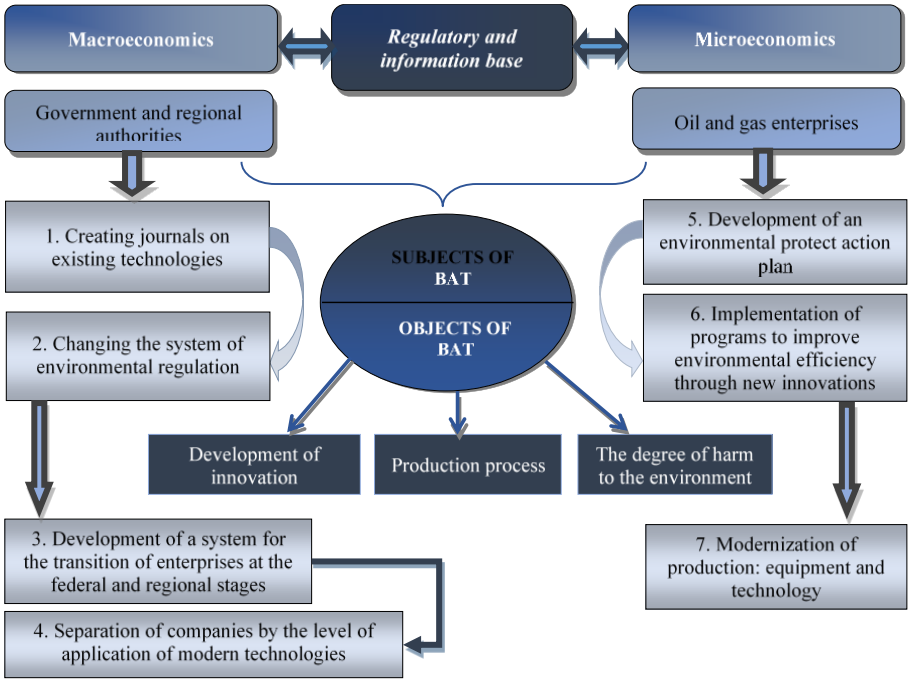


Fig. 2. The algorithm of modernization enterprises of the oil and gas complex of Russia on the basis of modern technologies

*Source: Compiled by the authors according to [32-33].*

In order to maintain the trend of using modern technologies at oil and gas enterprises, the government can use the following incentive measures (see Fig. 3). In order to carry out upgrading and transition to its principles until 2020, it is planned to allocate 0.21 trillion rubles from the budget to the oil and gas complex, what will form up to 7 % of the total government support for the introduction of modern technologies in Russian industries.

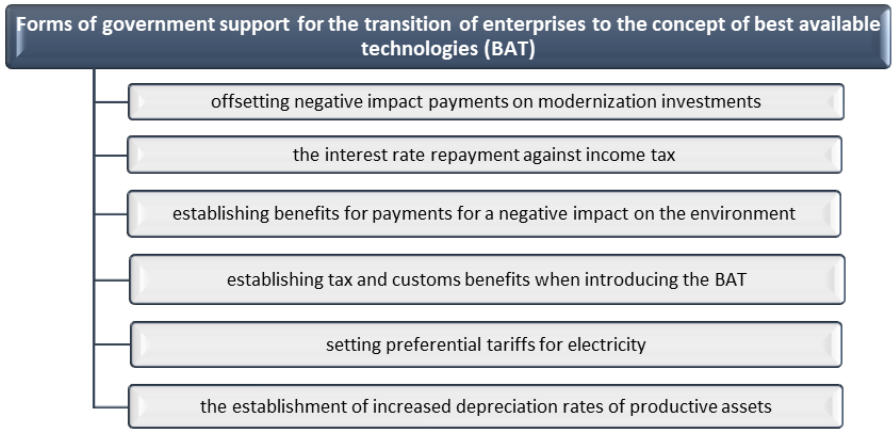


Fig. 3. The government measures to stimulate enterprises of the oil and gas industry of Russia to use modern technologies

*Source: Compiled by the authors according to [32-33].*

The current state of the oil and gas complex of Russia requires modernization, implementing introduce innovative technologies, creating new approaches to solving existing problems, as well as support from the side of fundamental science. The state must contribute to support innovation and investment processes in the sphere of oil and gas complex of Russia. It is important to create additional opportunities for its participants and stimulate the development of oil and gas complex.

## 6. Conclusion

The research has proved what the main ways of development and introduction of modern digital technologies in the oil and gas complex of Russia are directly connected with artificial intelligence systems. This is machine learning and in-depth machine learning; botosphere, including: robotization, bots, drones; and virtual reality of objects: improved reality, digital twin, mixed reality. Digital upgrading models used in oil and gas companies are similar in nature.

The government authorities form and develop the framework in the field of ecology and digital transformation of oil and gas production. The oil and gas companies, on the one hand, create tools to facilitate the introduction and increase the effectiveness of new technologies. While on the other hand, they are modernizing their production processes to increase environmental friendliness through the development of new technologies.

The oil and gas complex of Russia form one of the most efficient investment multiplication effects. It creates high demand on the production of neighbor branches of industry. This can be explained by the multiplication index, which characterize the development of industries. In the developed countries the amount of this multiplication index is: in the USA – 2,1, Norway – 1,7, Australia – 1,8-2,4. In Russia, multiplication index is 1,9, that means that Russian oil and gas complex is practically at the level of industrially development countries.

Based on research, it can be confirmed that the algorithm of implementation of modernization of the enterprises of the oil and gas complex will contribute to the effective transformation of existing production plants. This, in turn, will reduce the negative impact of oil and gas companies on the state of the environment; improve the economic, energy and environmental performance of industrial facilities of this complex.

Researchers point out that "undeniably digital has, and will continue to, lower the industry's operating costs, but there is a much bigger category of $3.4 trillion in net property, plant, and equipment—or the productive capital—which is nearly untouched by existing digital solutions" [34]. Therefore, our future research will be connected with the analysis of the possibilities of digitization of production technologies and equipment, in particular - drilling equipment.

**Acknowledgment**

This work is carried out based on the task on fulfilment of government contractual work in the field of scientific activities as a part of base portion of the state task of the Ministry of Education and Science of the Russian Federation to Perm National Research Polytechnic University (topic # 26.6884.2017 /8.9 "Sustainable development of urban areas and the improvement of the human environment").

**References**

1. Digital transformation in oil and gas. How innovative technologies modernize exploration and production. IBM Chemicals and Petroleum. IBM Corporation, NY (2017).
2. World Economic Forum. Digital Transformation Initiative Oil and Gas Industry, 2017. http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-oil-and-gas-industry-white-paper.pdf, last accessed 2019/04/26.

3. How Digital Technology is Reshaping the Oil & Gas Industry. https://www.fotech.com/2018/07/11/how-digital-technology-is-reshaping-the-oil-gas-industry, last accessed 2019/04/24.
4. Choudhry, H., Mohammad, A., Tee Tan, K., Ward, R.: The next frontier for digital technologies in oil and gas. URL, https://www.mckinsey.com/industries/oil-and-gas/our-insights/the-next-frontier-for-digital-technologies-in-oil-and-gasry, last accessed 2019/04/27.
5. Warchoł, M., Świrski, K., Ruszczycki, B., Wojdan, K.: The method for optimisation of gas compressors performance in gas storage systems. Int. J. Oil, Gas and Coal Technology 17(1), 12–33 (2018).
6. Wojdan, K., Ruszczycki, B., Michalk, D., Swirski, K.: Method for simulation and optimization of underground gas storage performance. Oil Gas Sci. Technol. – Rev. IFP Energies nouvelles 69 (7) (2014).
7. Jami, S., Shah, V.: Digitization and automation of crude transport operations for improved safety and security. Society of Petroleum Engineers - SPE Oil and Gas India Conference and Exhibition 2019, OGIC 2019, paper Code 148101 (2019).
8. Rios-Mercadoa, R.Z., Borraz-Sanchez, C.: Optimization problems in natural gas transportation systems: a state-of-the-art review. Applied Energy 147, 536–555 (2015).
9. Zhang, X., Liu, X., Geng, D., Yu, W., Shi, L.: Numerical simulation on the flow field of self-propelled multi-orifices nozzle for ultra-short radius radial jet drilling. International Journal of Oil Gas and Coal Technology 17(1), 1-11 (2018).
10. Trujillo, M., Mercado, D., Maya, G., Castro, R., Soto, C., Pérez, H., Gómez, V.: Selection methodology for screening evaluation of enhanced-oil-recovery methods. In: SPE Latin American and Caribbean Petroleum Engineering Conference Proceedings, 2, pp. 1249-1258 (2010).
11. Moreno-García, C.F., Elyan, E., Jayne, C.: New trends on digitisation of complex engineering drawings. Neural Computing and Applications 31 (6), 1695-1712 (2019).
12. Kuzenkov, V.Z., Kashirskikh, D.V., Ramazanov, Yu.A., Paromov, S.V., Serkin, M.F.: Development and implementation of RN-Lab information system for core and reservoir fluid laboratory study. Neftyanoe Khozyaystvo - Oil Industry (3), 98-101 (2018).
13. Rostami, A., Shokrollahi, A., Shahbazi, K., Ghazanfari M.H.: Application of a new approach for modeling the oil field formation damage due to mineral scaling. Oil Gas Sci. Technol. – Rev. IFP Energies nouvelles 74, 62 (2019).
14. Lazeev, A.N., Timashev, E.O., Vakhrusheva, I.A., Serkin, M.F., Gilmanov, Y.I.: Digital core technology development in rosneft oil company. Neftyanoe Khozyaystvo - Oil Industry 11, 18-22 (2018).
15. Shishkin A.N. Timashev E.O., Solovykh V.I., Kolonskikh A.V.: Bashneft digital transformation: from concept design to implementation/ Neftyanoe khozyaystvo - Oil Industry 3, 7-13 (2019).
16. Abukova, L.A., Dmitrievsky, A.N., Eremin, N.A.: Digital modernization of Russian oil and gas complex. Neftyanoe Khozyaystvo - Oil Industry (10), 54-58 (2017).
17. Eremin N.A.: Digital Trends in the Oil and Gas Industry. Oil. Gas. Innovations 12, 17-23 (2017).
18. Dmitrievsky, A.N.: Resource-innovative strategy for the development of the Russian economy. Neftyanoe Khozyaystvo - Oil Industry 5, 6-7 (2017).
19. Dmitrievsky, A., Lyugai, D., Markelov, V.: Fundamental basis of innovative technologies in gas industry. In International Gas Research Conference Proceedings 3, 2758-2770 (2014).
20. Bertocco, R., de Graauw L., Naberezhnev D.: How Digital Technology Will Change Oil And Gas Companies. URL, https://www.forbes.com/sites/baininsights/2016/06/24/how-digital-technology-will-change-oil-and-gas-companies /#5f9568630aa6, last accessed 2019/04/27.
21. Automation in Oil and Gas: Innovations and benefits. URL, https://www.insightconsultants.co/oil-and-gas/automation-oil-gas-innovations-benefits, last accessed 2019/04/22.
22. Zhang, X., Wu, C.: Energy cost minimization of a compressor station by modified genetic algorithms. Engineering Letters 23(4), 258–268 (2015).
23. Mingaleva, Z.: Exploitation of Oil Fields and Sustainable Development of the Environment. Recent Adv Petrochem Sci. 4(1), 555628 (2017).
24. Melo L., Mastella L.S.: Os desafios do setor de O&G para potencializar o uso dos dados na era da transformação digital (The challenges of the O & G sector to leverage data use in the digital transformation era). TN Petróleo 119, 34-39 (2018).
25. Federal Law "On Environmental Protection" dated January 10, 2002 No. 7-FZ. URL, http://www. consultant.ru/document/cons_doc_LAW_34823, last accessed 2019/04/16.

26. Federal Law "On Industrial Policy in the Russian Federation" dated December 31, 2014 N 488-FZ. URL, http://www. consultant.ru/document/cons_doc_LAW_173119, last accessed 2019/04/16.
27. Federal Law "On Production and Consumption Waste" of 06/24/1998 N 89-FZ. URL, http://www. consultant.ru/document/cons_doc_LAW_19109, last accessed 2019/04/16.
28. Federal Law "On Standardization in the Russian Federation" of 06/29/2015 N 162-FZ. URL, http://www. consultant.ru/document/cons_doc_LAW_181810, last accessed 2019/04/16.
29. Tax Code of the Russian Federation. Federal law of July 31, 1998 N 146-FZ. URL, http://www. consultant.ru/document/cons_doc_LAW_19671/, last accessed 2019/04/16.
30. Best Available Technologies Bureau. URL, http://burondt.ru/informacziya/dokumentyi/, last accessed 2019/04/24.
31. Arutyunov, R.: The Next Generation of Cybersecurity in Oil and Gas. Pipeline and Gas Journal 245 (6) (2018).
32. Concept of implementing the transition to the principles of the best available technologies and the introduction of modern technologies in the industrial sector of the Russian Federation. March 2018. URL, https://www.gost.ru/portal/gost/_home/activity/NDT/sovet, last accessed 2019/04/16.
33. On financial mechanisms for introducing the best available technologies in Russia. URL, http://www. mnr.gov.ru/docs/latonova.pdf, last accessed 2019/04/16.
34. Mittal, A., Slaughter, A., Bansal, V.: From bytes to barrels. The digital transformation in upstream oil and gas. A report by the Deloitte Center for Energy Solutions. – 28 p. URL, https://www2.deloitte.com/insights/us/en/industry/oil-and-gas/digital-transformation-upstream-oil-and-gas.html, last accessed 2019/04/16.

# An Educational Model of Graduation Project for Students at Automation and Computer Engineering

Sebastian Rosca[1], Simona Riurean[1], Monica Leba[1], Andreea Ionica[1]

[1] University of Petrosani, 20 University str., Petrosani, Romania, 332006

https://doi.org/10.33847/2686-8296.1.1_4

Received 10.10.2019/Revised 01.11.2019/Accepted 11.12.2019/Published 22.12.2019

**Abstract.** The upcoming engineers, students at Automation and Computer Engineering, acquire, during four years of education, a tremendous theoretical information in different areas connected with their educational field of study. From solid mathematical backgrounds to electronics and automation and many other subjects become a stock of incredible useful database for future engineers. The lack of adequate practical work that allow them to connect and get aware on how to use information acquired, lead, in most of the situation, to a useless database of information. This paper presents a model of a good practice work and aims to be a useful example for students in the last year of study on how to handle and realize, starting from one idea and finishing with a working prototype, their graduation project. The example here is a low cost, handy, a real time data acquisition and duplex wireless data communication system. It consists of two modules. The first one is a glove used by an operator, equipped with an Arduino board with a gyroscope, accelerometer and full duplex communication parts that sends movements commands to a mobile robot. The mobile robot is equipped with a camera sending video streaming related to the immediate space and a network of sensors with the aim to acquire environmental data and sent them remotely to the first module.
**Keywords:** network sensors, hazardous environments, underground spaces, wireless communication

## 1. Introduction

From an idea to a final, functional prototype and a good written, valuable graduation project, is a long and difficult way to travel on for a student, when no guiding marks to follow, are on the way. Any software, hardware or an embedded system project includes requirements analysis, system design, simulation, implementation and final testing. Starting with the initial idea, all the way through to system analysis, hardware and software design, simulation of the system, execution and testing are important stages to be well achieved to be able to continue with the next one for a valuable final graduation project. The students have opportunities to use the knowledge they have gained in different courses as well as during practical teamwork [1].

First of all, a detailed and comprehensive literature review is essential as a first development stage in order to complete a high quality project. The detailed literature survey on the subject has to be realized by the student, not only to increase his/her knowledge but to improve the understanding of the particularities related to the project's subject and be aware of all up-to-date situation connected to the project's topic [2]. This paper presents step by step, the main stages to be completed for a well appreciated final project (Fig. 1) with an example of a remote guiding robot that acquire environmental information from difficult or forbidden to access places.

The hazardous environments such as underground spaces (coal, salt, minerals mines), research laboratory or test centers are dangerous to work in, especially because of air quality, small and difficult to access spaces and in some cases highly explosion hazard due to instant events, such as combination of explosive gases or

substances. Environmental data acquisition and wireless communication prior to human access in these spaces or sometimes instead of human access, is life savings.

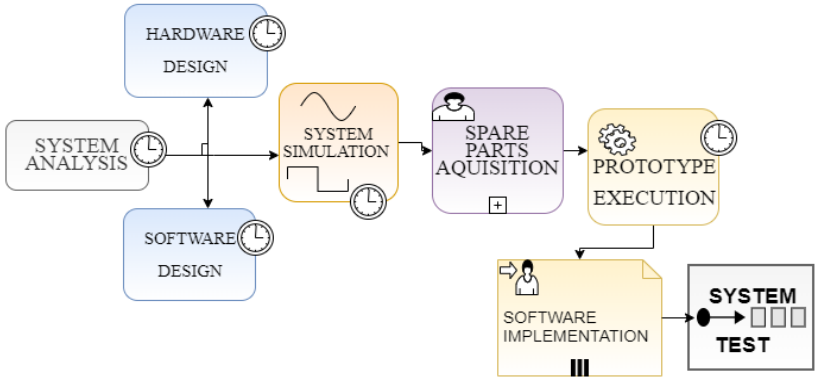


Fig. 1. Stages to complete for a successful project

The robot designed is remotely controlled by an operator with one hand by means of an accelerometer. As an implementation, it would be useful in any areas where flexible one-handed guiding and controlling is required. Depending on the sensors added to it, the robot can be created for different missions such as rescue or exploring hard-to-reach spaces. The prototype designed and presented in this work is a low-cost with off the shelf components, therefore prototype's quality is minimal [3].

All the parts from which the robot is made, are Arduino type or compatible with it. The given robot consists of two parts: the part of the data transmitter that has the role of remotely controlling the movement of the second one, according to the inclination of the operator's hand. The movement is controlled by a sensor type Gyroscope MPU6050, that consists of a gyroscope, accelerometer and a data converter from Digital to Analog. In other words, the data will be taken from the accelerometer due to data generated according to hand's inclination relative to the earth. The gyroscope is connected by an Arduino board. The Arduino board also connects a radio module nRF24L01 that will transmit wireless information to the second module.

The second module of the system is a mobile robot made up of a kit with 2 motors and a platform on which other parts are placed. The Arduino board with a radio module nRF24L01 is used to receive data from the transmitter. In order to control the two engines, a L298N engine module is added to the system.

The software part is created in Arduino IDE and likewise, it is made up of 2 parts: Module I and II. In the Module I, the source code is shorter because it is only necessary to initialize the gyroscope and the radio module, to enter the data generated by the gyroscope in a multidimensional variable and to transmit this variable through the radio module to the second part of the robot. The data receiver code will be a little longer since the received data will be converted by a power formula of the left and right engines and then by several decision instructions, setting them to fulfill certain commands according to the received data.

## 2. Hardware and software design

The system is composed of two modules as shown in the block diagram. The first module, remotely sends, according to the operator's hand, a series of movements

(forward, backward, left or right) to the second module.

The block diagram (Fig. 2) shows the connection diagram of our kit based on Arduino microcontroller used for the acquisition of streaming video for real-time monitoring purposes either on a personal computer or on an Android-based device.

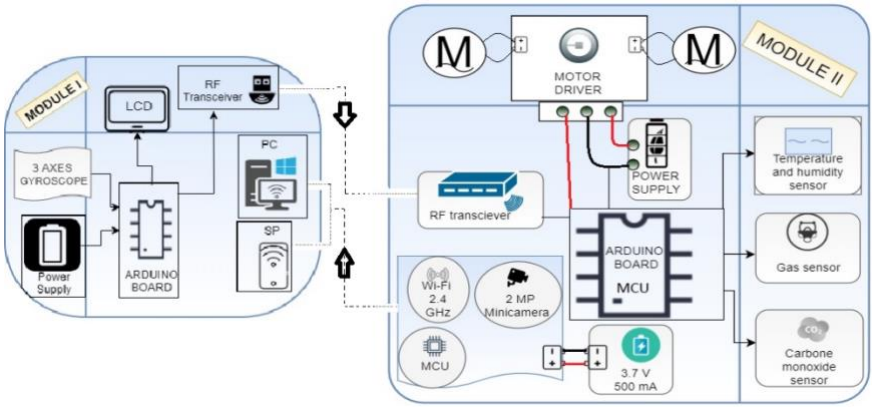


**Fig. 2.** Block diagram – the monitoring system

The other module (module II), a robotic mobile platform, is responsible for data acquisition based on a network of sensors that are capable of acquiring sensible environmental data from special areas considered to be either hazardous due to emissions of natural gas, or forbidden to be accessed because of dangerous substances into the workspace. A 2MP mini-camera has been added to the second module in order to avoid any obstacle into the environment explored.

In order to achieve our goal, we used two Arduino microcontroller boards, both for prototyping the robot remote control system, that is built around an ATmega328P chip and offers the programmer everything necessary to achieve an automation system. It provides a 16 MHz ceramic resonator for dealing with time issues, a series of digital in/out pins can be used to control a wide range of motors such as: DC motor, servo, stepper motor based on PWM modulation or an RF transceiver or a Wi-Fi module for communication purpose and a series of analog pins that can be used to acquire data from sensors such as: environmental parameters or orientation of an object in space using a gyroscope [4]. All of these can be programmed based on C language using the USB interface integrated on any ordinary computer to load the program developed by user into embedded microcontroller [5].

The mobile robot provides a relatively simple mechanical implementation with only 3 wheels, of which only two are driven by DC gear servomotors, the third wheel being useful when turning left or right because it can also move on the horizontal axis. Research in the field shows that in order to maintain optimum contact with the soil, especially in the case of uneven surfaces, the required number of wheels is three, additionally with a suspension system to achieve a higher performance [6].

With the purpose of controling the direction and speed of the robot a driver motors based on a H-bridge Dual Motor Controller is used. Based on the PWM signal received from the Arduino board microcontroller, it drives the two servomotors in the same time. The driver motors based on H-bridge is useful because it is a current amplifier that converts a low current control signal into a higher current signal [7] since the Arduino board microcontroller can supply a maximum output current of 40 mA per pin [8] and a current between VCC and GND pins limited to 200 mA [9], which proves to be insufficient to control the servomotors.

The supply voltage required for Arduino-based robot operation can be provided directly from an external power source based on a battery that ensure a voltage of 9

V because the Arduino board has a built-in voltage regulator that limits the voltage to 5V required for most modules compatible with Arduino [10]. In order to have a single power supply for the robot, we have powered the Arduino Board from the driver motors by connecting the voltage input pin - VIN on the Arduino board to the + 5V pin supplied from the driver motors [11].

### *2.1 Arduino software – IDE*

The Arduino Integrated Development Environment (IDE) or Arduino Software contains a code-writing editor, a message area, a text console, a toolbar with common function buttons and a series of menus.

The Arduino IDE is a cross-platform application written in Java which is derived from the IDE made for the Processing programming language and the Wiring project. It is designed to introduce programming to any new programmer unfamiliar with software development. It includes a code editor with features such as syntax highlighting, brace matching, and automatic indentation, and is also capable of compiling and uploading programs to the board with a single click.

The Arduino IDE comes with a C / C++ library called "Wiring", which makes many common input/output operations much easier. Arduino programs are written in C/C++ [12].

### *2.2 The Network of Sensors*

Real-time acquisition of sensible data of environmental factors that may be present at a particular time in the workspace from special underground areas is a priority to be considered in risk management to be able to act properly in accordance with the field acquiring data to prevent the errors that may arise during the decisional measures in case of rescue operations. Therefore, we propose to implement within our mobile robot a network of wireless low cost environmental sensors compatible to Arduino able to monitor: temperature and humidity, presence of carbon monoxide, and flammable gases, especially methane, the presence of sources of ignition that can generate a fire.

The sensor used to detect temperature and humidity is a hybrid sensor that operates at low energy (3V-5V) like most Arduino compatible modules, it can measure the humidity based on the resistor and the temperature based on the Negative Temperature Coefficient (NTC) component, offers a fast response in time, is immune to interferences, and the fact that it is provided with a single analog data pin for the acquisition of both environment parameters represent an advantage for Arduino board pins management [10]. With respect to the range of measurement values, the sensor can measure temperatures in range of 0 to + 50 °C and humidity in a range of +/- 5.0% RH [11].

In order to detect gas leakage, in special in underground spaces, we implement into the mobile robot a low cost gas sensor that is designed for industrial or domestic environment monitoring, useful to detect gasses such as: propane, butane, methane, alcohol and hydrogen. This sensor is also useful in our monitoring process since is smoke sensitive [12]. From the constructive point of view, this sensor is based on a component that contains an adjustable resistor and a protective resistor integrated on board that can detect target gas leakage based on the variation of the resistance of the sensitive component [13]. The gas sensor operates at +5V with a low current consumption of just 40 mA, making it ideal to be used with an Arduino board as a digital or analog data input. An important advantage is that the methane emissions can be detected with high accuracy between 300 and 10,000 ppm according to the datasheet provided by the manufacturer [14].

Because of lethally potential represented by the presence in the air of the carbon monoxide that can present at a time in particular due to an accident in special underground spaces that evolving an incomplete combustion of any organic materials

such as: wood, butane, propane and other natural gasses or even by underground machinery malfunction such as air compressor that supply fresh air in workspace, was also necessary to implemented on the robot a carbon monoxide detection specialized sensor that can accurately measure the concentration of this gas in the air which if it remain undetected it present potential to harm the human health because it's particularity that it present: carbon monoxide gas is odorless, colorless, tasteless and nonirritating and is lethally after 1-3 minutes at a concentration in the air between 12-13,000 ppm or after an hour at a concentration of 1,600 ppm [15].

With regard to the construction details of this type of sensor, the sensing component of the measuring circuit consists of two parts: the heating circuit on one side providing the time control function and the output signal circuit that responds to changes of resistance detected on the surface of the sensor [16].

In case of the gas sensor, the carbon monoxide sensor can be connected for supplying data output to any digital or analogue pin from Arduino board and it operates at a +5V with a low current consumption at only 40mA and has a high sensitivity for carbon monoxide detection ranging from 20 ppm to 2000 ppm [17].

### *2.3 The module with gyroscope*

In order to be able to control the robot, we use the method that allow to replicate the hand's orientation in space and to transpose it into control commands that we can use in robotics for locomotion purposes in accordance with visual data acquired in real time from the camera kit. The glove with this intelligent sensor can be integrated into our application developed with Arduino. It is based on an I2C motion processor with 6-axis that incorporates a 3-axis gyroscope and a 3-axis accelerometer along with a Digital Motion Processor (DMP) all on one system-on-chip device. The MEMS motion tracking device features programmable gyroscope and accelerometer designed for fast and slow movements precision tracking.

The motion processing unit incorporates Motion Fusion algorithms which will also access external sensors and magnetometers through the auxiliary master I2C bus. The possible applications of this type of intelligent component can to include: development of device that based on wearable sensors or development of smart applications in case of tablets or smartphones in specially for counting steps operations by a mobile processor to display the numbers of calories burned or the quality of sleep and up to could play intelligent games that is dependent for acquired data from sensors. The Platform extracts the motions that are associated and unload the sensor management from the operating system to provide an Application Program Interface (API).

### *2.4. Video Streaming and Communication*

In order to remotely control the mobile robot, a real-time video camera is used with the aim to send information from workspace to the user. For this purpose, a low cost special kit based on Arduino microcontroller is used. It is mounted directly on the mobile robot frame and offers video streaming capabilities based on a mini camera that can be connected as a daughter card on the board using GPIO pins header and that can capture 2MP full resolution JPEG still image, even stream low resolution at fairly framed video over network via WI-FI module embedded on board which operates at a frequency of 2.4GHz.

The kit is suitable for portable application, it can be powered from micro-USB or using battery and has built in lithium battery charging circuits with of capacity of +3.7 V and 0.5A maximum current.

The special kit based on Arduino present a series of key features: 32bit microcontroller with low power consumption and RISC type architecture [18]; operate at a high frequency clock speed of 80 MHz and can be boost at a frequency of 160 MHz when Real Time Operation System (RTOS) is enabled [17]; supports Arduino

sketch script to be programmed and is suitable for android application [19].

### *2.5. NRF module*

Transceiver NRF uses the 2.4 GHz band and it can operate with baud rates from 250Kbps up to 2Mbps. If used in open space with lower baud rate its range can reach up to 100 meters. The radio modules include a 2.4 GHz RF transceiver and a logic that supports a high-speed SPI interface for data connection and exchange.

The module can use 125 different channels which gives a possibility to have a network of 125 independently working modems in one place. Each channel can have up to 6 addresses, or each unit can communicate with up to 6 other units at the same time. Power consumption of this module is just around 12mA during transmission, which is even lower than a single LED. The operating voltage of the module is from 1.9 to 3.6V, but the other pins tolerate 5V logic, so easily we can connect it to an Arduino without using any logic level converters. So, once we connect the NRF modules to the Arduino boards we are ready to make the codes for both the transmitter and the receiver [20].

## 3. System simulation

Due to bidirectional communication benefit our solution can receive environmental data from sensors network that are placed on the receiver module directly on the transmitter module to analyze and display them.

To demonstrate the functionality of the proposed system we also performed a simulation (Fig.3) into an environment specialized in design and testing of the embedded system of the two modules handled in this paper for monitoring of a special underground environment.

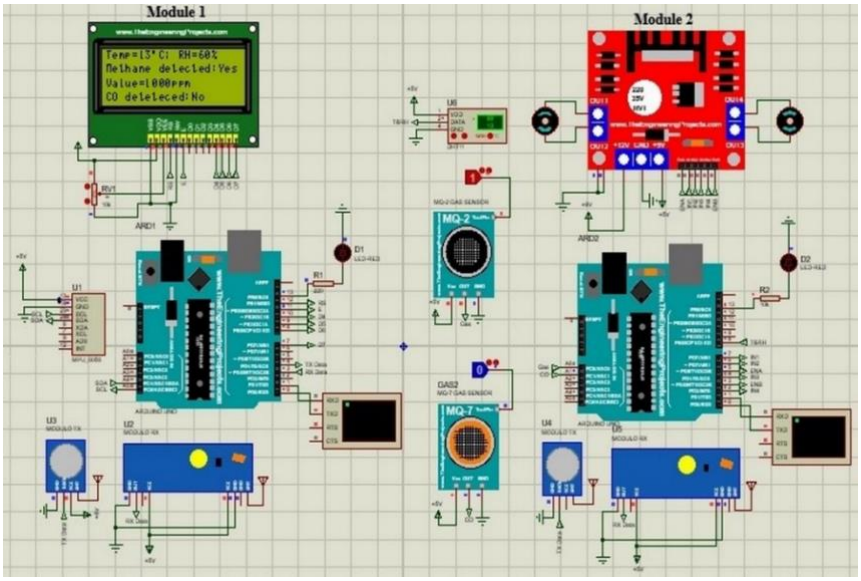


Fig.3. Simulation of the monitoring system applied in a salt mine

## 4. Prototype execution and software implementation

In order to achieve our goal of monitoring in the real-time the potentially hazardous environment to prevent unpredictable or fatal events that may occur at a time in the workspace we implemented all that was necessary for a good integration powered by C/C++ programming language of both modules to be able to supply the

one hand a bidirectional communication required for control operations and the other hand for data acquisition related to existent environments parameters.

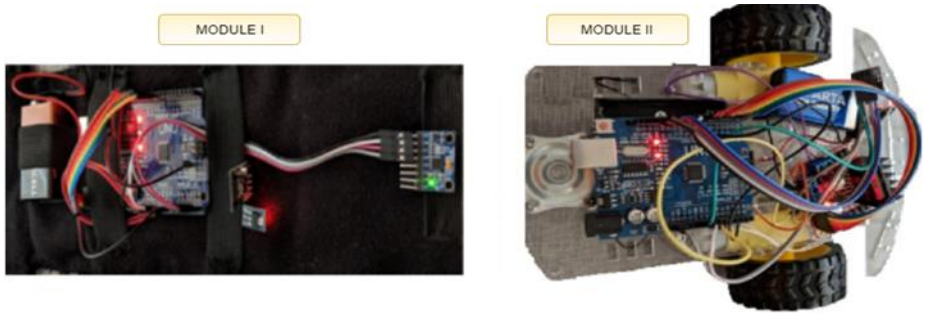


Fig. 4. The prototype developed

To get visual stimuli from the environment, the software solution implemented, allows video streaming to be captured and send based on a Wi-Fi network using the HTTP protocol. It provides support in order to control the robot from a safe distance, so that the operator is not exposed to the hazards or unanticipated harmful events.

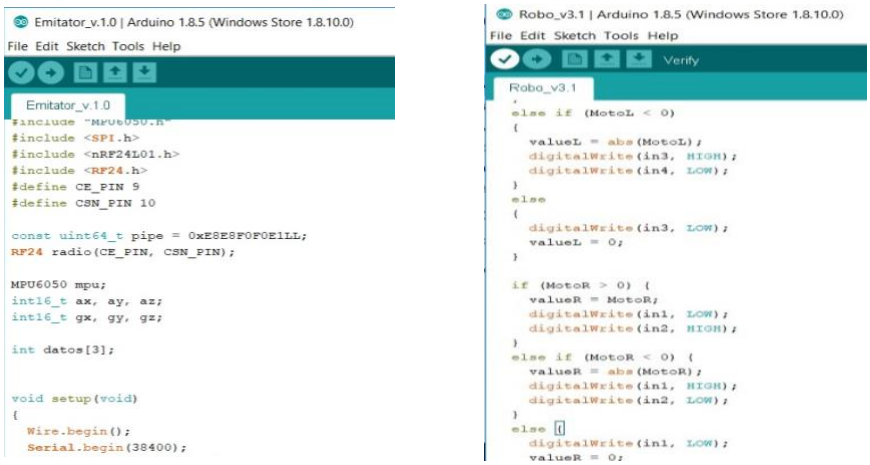


Fig. 5. Software implementation

Regarding radio-frequency based wireless communication between modules we developed a software solution by implementing the SPI communication protocol that can check the status of connection between of the modules and can transmit commands from the transmitter module based on gyroscope that will generate data depending on its position in space and give certain commands to DC gear servomotors that assists the robot to change the movement's direction or to turn.

## 5. Testing the system

Once the code has been load on both Arduino boards, tests were done and noticed that the turns were performed too quickly, as well as after tilting the hand in any direction, the robot reacted too fast. To solve this problem a function in the code was written, to decrease the values of the two motors, MotoL and MotoR, as well as to slow down these values after tilting the hand:

```
int MotoLN = ValY - (ValX / 1.3);
int MotoRN = ValY + (ValX / 1.3);
MotoL = MotoLN / 1.3;
```

MotoR = MotoRN / 1.3;

Similarly, for the slower transfer, the coefficients from 1.2 to 1.3 have been increased in the first formula when dividing *ValX*. Another observation was that sometimes the robot stopped for 1-2 seconds and did not perform any command, because one of the radio modules or even both had small errors.

Following few test, the sources of inconsistencies have been identified and planned to be removed by software improvement or, some low-cost spare parts to be replaced with others with higher quality.

## 6. Conclusions

Time is short, project is difficult to realize and high demanding when no idea of reducing the development time, increase throughput and improve the accuracy of the graduation project, are available to students as guiding pillows on the way.

This work presents the stages to be followed by students to accomplish the most important task before graduation, the final project. A mobile robot driven by gestures with Arduino and a gyroscope has been used as an example. The prototype is built as the mobile robot to be driven by user's gestures with one hand. The system is made by a kit with two engines, two Arduino boards, two radio modules, a gyroscope and two voltage stabilizers. According to its position in space, the gyroscope sends data to the mobile robot in order to perform specific movements. The possible commands integrated in the system are back and forward acceleration, turn left and right and according the gyroscope angle of inclination, the mobile robot's speed can be controlled by user.

This model of a graduation project describes necessary steps to be taken in order to develop a preformat prototype. It also describes a low-cost, handy system, designed for data acquisition and duplex wireless communication with duo-module. One is managed with one hand by a remote operator and the other one sends video streaming of spaces, acquire and sends environmental data as well. A different possible approach is to local save data acquired from environment, directly on a SD/TF card. The data acquired by a network of sensors can be temperature and humidity, gasses (propane, butane, methane, alcohol and hydrogen) and carbon monoxide, as well.

## References


1. Blicblau AS, Naser J.: Developing Engineering Students' Communication and Information Retrieval Skills Utilizing Capstone Projects. International Journal of Quality Assurance in Engineering and Technology Education (IJQAETE), 4(3):1–20, (2015).
2. Yilmaz, M., Tasel, F.S., Gulec, U., Sopaoglu, U.: Towards a process management life-cycle model for graduation projects in computer engineering. PLOS ONE 13(11): e0208012. DOI: 10.1371/journal.pone.0208012, (2018).
3. Rosca S., Riurean S., Leba M., Ionica A.: A Reliable Wireless Communication System for Hazardous Environments. In: Antipova T., Rocha A. (eds) Digital Science. DSIC18 2018. Advances in Intelligent Systems and Computing, vol 850, 235-242. Springer, Cham (2018).
4. Pan, T., Zhu, Y.: Designing Embedded Systems with Arduino: A Fundamental Technology for Makers. Springer (2017).
5. Sweatt, M., et al.: WiFi based communication and localization of an autonomous mobile robot for refinery inspection. In: Robotics and Automation (ICRA), IEEE International Conference on. IEEE, p. 4490--4495 (2015).
6. Taha, I.A., Marhoon, H.M.: Implementation of Controlled Robot for Fire Detection and Extinguish to Closed Areas Based on Arduino. TELKOMNIKA, 16.2: 654--664 (2018).
7. Behera, S., Muduli, P. K.: Remote Speed Control of Brushless DC Motor with Display. International Journal of Automation and Smart Technology, 8.2: 65--71 (2018).
8. Nayyar, A., Puri, V.: A review of Arduino board's, Lilypad's & Arduino shields. In: Computing for Sustainable Global Development (INDIACom), 3rd International Conference on. IEEE, 2016. p. 1485-1492 (2016).

9. Arduino Playground, https://playground.arduino.cc/Main/ArduinoPinCurrentLimitations
10. Ollukaren, N., Mcfall, K.: Low-cost platform for autonomous ground vehicle research. In: Proceedings of the 14th Early Career Technical Conference. (2014).
11. Junior, Luiz A., et al.: A low-cost and simple Arduino-based educational robotics kit. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Robotics and Control (JSRC), December edition, 3.12: 1--7 (2013).
12. Pandya V., Shukla D.: GSM modern based data acquisition system. International Journal of Computational Engineering Research, 2(5):1662--1667 (2012).
13. Sipani, J.P., et al.: Wireless Sensor Network for Monitoring & Control of Environmental Factors using Arduino. International Journal of Interactive Mobile Technologies (iJIM), 12.2: 15--26 (2018).
14. Ünsal, E., Milli, M., Çebi, Y.: Low cost wireless sensor networks for environment monitoring. The Online Journal of Science and Technology, 6.2: 61--67 (2016)
15. Sowparanika, E. L., et al.: Wireless Communication System for Coal Mining Worker using Arduino. Journal of Chemical and Pharmaceutical Sciences ISSN, 974: (2015).
16. Al-Dahoud, A., Jannoud, I., Al-Rawashdeh, T.: Monitoring Metropolitan City Air-quality Using Wireless Sensor Nodes based on ARDUINO and XBEE (2011).
17. Olimex:https://www.olimex.com/Products/Comp/Sensors/SNS-MQ2/resources/MQ2.pdf
18. Srivastava, S.K.: Real Time Monitoring System for Mine Safety Using Wireless Sensor Network (Multi-Gas Detector). PhD Thesis (2015).
19. Ramesh, M., et al.: Solid Waste Management Using IoT, IJITEE 8(12), (2018).
20. Olimex: https://www.olimex.com/Products/Components/Sensors/SNS-MQ7/resources /SNS-MQ7.pdf
21. Gour, G. B., et al.: Helmet Sensing Speed Controller Device. International Journal of Current Trends in Engineering & Research (IJCTER) e-ISSN 2455–1392 Volume 2 Issue 5, pp.291--296 (2016).
22. Manikandan, J.: Design and evaluation of wireless home automation systems. In: Power Electronics, Intelligent Control and Energy Systems (ICPEICES), IEEE International Conference on. IEEE, p. 1-5 (2016).
23. How to Mechatronics: https://howtomechatronics.com/tutorials/arduino/arduino-wireless-communication-nrf24l01-tutorial/

# Reforming Russian legislation for crimes in the digital economy

Anna Mingaleva[1,2]

[1] GSEM, Ural Federal University named after the first President of Russia B. N. Yeltsin, Ekaterinburg, Russia
[2]Institute of Certified Specialists, Perm, Russia

https://doi.org/10.33847/2686-8296.1.1_5

Received 07.09.2019/Revised 25.10.2019/Accepted 11.12.2019/Published 22.12.2019

Abstract. The aim of this research work is to analyze Russian criminal legislation on punishment for computer crimes. The growth in the number and intensity of cyber-attacks throughout the world also leads to an increase of costs for companies and society as a whole to provide protection against cyber-attacks and to prevent losses from them. The financial sphere of the economy suffers especially. The article provides statistical and expert data on the potential damage from the suspension of the financial institution's activities, including lost profits and costs for restoring websites after cyber-attacks. A significant increase in the number of crimes committed with the help of digital devices and a multiple increase in the amount of damage from them were revealed on the basis of an empirical study. On the part of the business community, the demand for the state to toughen penalties for computer crimes is increasing. To this end, in 2018 novels were introduced into the Criminal Code of the Russian Federation, which toughened criminal liability for embezzlement of funds from bank accounts or electronic money. It is shown that the changes introduced by the legislator in the criminal legislation of Russia take into account modern threats to economic security and increase the level of protection of the financial interests of citizens, credit organizations and the state as a whole.

**Keywords:** economic losses, punishment, computer crimes, criminal punishment, stealing money, cyber-attacks

## 1. Introduction

Expanding the scope of digital technologies application in the credit and banking sector creates broad prerequisites for increasing the speed of banking operations, improving customer service, and transparency of financial transactions. However, the use of digital innovations in the financial sector of the economy carries significant criminal risks with it according to experts [1].

At the same time fraudulent actions in the field of computer information have a great public danger, as they can immediately cause damage to a significant number of citizens, as well as jeopardize the functioning of the financial and credit system due to violation of bank secrecy, destruction, blocking or modification of computer information.Cyber-attacks are ranked among the world's major threats according to the study 'Global Risks Report' prepared for the World Economic Forum in Davos.

According to the respondents' evaluation, the probability of "Cyber-attacks: Theft of data/money" increasing is 82 % (4th place in the ranking by danger level); the probability of increasing of "Cyber-attacks: disruption of operations and infrastructure" is 80 % (5th place in the ranking); the probability of increasing of "Personal identity theft" is 64 % (10th place in the ranking); the probability of increasing of "Loss of privacy (to companies)" is 63 % (13th place in the ranking) [2].

In general, according to expert estimates, the damage to the global economy from massive cyber-attacks can grow to $ 2 trillion in 2019 and to $ 3 trillion in 2020. Accordingly, companies' and society's expenses on providing protection against cyber-attacks and preventing losses from them increases. The volume of companies' global expenditures for cybersecurity will increase by 14 times by 2021 and reach approximately a trillion dollars according to forecasts of "Sberbank of Russia" [3].

In previous research we have built a macroeconomic model of the relationship between the rising cost of banking services and the rising costs of the banking sector for providing protection against cyber-attacks. Also was showed the influence of this factor on the computer security of the sector [4]. Issues of digital security in the credit and banking sphere, prospects for its development in the conditions of digitization and increased competition from new financial institutions, which are full-fledged IT companies, as well as issues of criminal punishment for computer crimes in the credit and banking sector were identified as further research directions. In this study, we will analyze the existing measures of state protection and punishment for committing computer crimes, as well as make an analysis of the necessary directions of improvement the criminal punishment for committing computer crimes in the credit and banking sector.

## 2. Theory and method of research

The study of the scientific and legal literature of foreign countries has shown that the criminal legislation of many countries has imposed penalties for computer crimes for a long time. Thus, in criminal law of Austria, Germany, Sweden and a number of other European countries computer fraud is singled out as an independent offense, which, as a rule, provides for stricter sanctions in comparison with the general rules on embezzlement.

Thus, the Swedish Criminal Code (Brottsbalk) specifies how to commit a crime as a sign of a qualified crime: "A person who, using false or incomplete information, changing programs, or by any other means, illegally interferes in automatic data processing or other automatic processes, benefits for themselves, while causing damage to the property of the owner, must be held accountable for fraud" [5].

The Austrian Criminal Code (Bundesgesetz) in article 148a provides liability for material damage caused in order to gain illegal benefits for the offender or a third person by influencing the processes of automated data processing using special programs, entering, modifying or deleting data or in any other way affecting data processing [6].

In the German Criminal Code (Strafgesetzbuch) computer crime is identified as property damage through influencing the result of data processing using special programs, incorrect or incomplete data, using unauthorized data or otherwise influencing the result of data processing (paragraph 263a) [7].

Comparative and bibliographic analysis are used as a method of research. The use of other methods of scientific research is difficult due to the lack of open information on the number of computer crimes and their size. Banks, credit and financial institutions hide such information. They do not allow the public and the press to find out information about the theft of money or customer databases, as this sharply undermines the confidence of customers in these banks and financial institutions. The police and crime investigation authorities also do not disclose information about such crimes, since they have a great public danger. Thus, the lack of complete, accurate and reliable information on the extent of computer crimes in the banking and financial sectors is a serious limitation for the analysis.

The results of several studies on the state of cybercrime in Russia are used as the data source. Also we use analytical reports of Positive Technologies "The market

of criminal cyberservices. 2018" [8], "How much is security?" [9]. The analysis of data from the National Computer Incident Coordination Center (NCCI) was conducted.

The sources of a comparative analysis for the study were materials from international organizations and forums, including the conclusions made in the Global Risks Report in the framework of the World Economic Forum.

## 3. Research

Studies in recent years have shown tremendous damage to the credit and financial sector due to the suspension for at least 1 day of work of a bank or other financial institution. Thus, it was assumed that the cost of an attack on web resources during an hour on the darknet is estimated at about $ 5, and within a day - $ 300 according to the study "How much does security cost?" of 2017 conducted by the company Positive Technologies [9, p.16].

At the same time, the damage to the financial and credit organization, which at that time could not fulfill main functions, will be hundreds and thousands of times more. Thus, the potential damage from the suspension of financial organization, including lost profits, as well as the cost of restoring websites, was estimated for certain types of cyber-attacks and the size of potential damage by institutions of credit and financial and banking sectors (see Fig. 1).

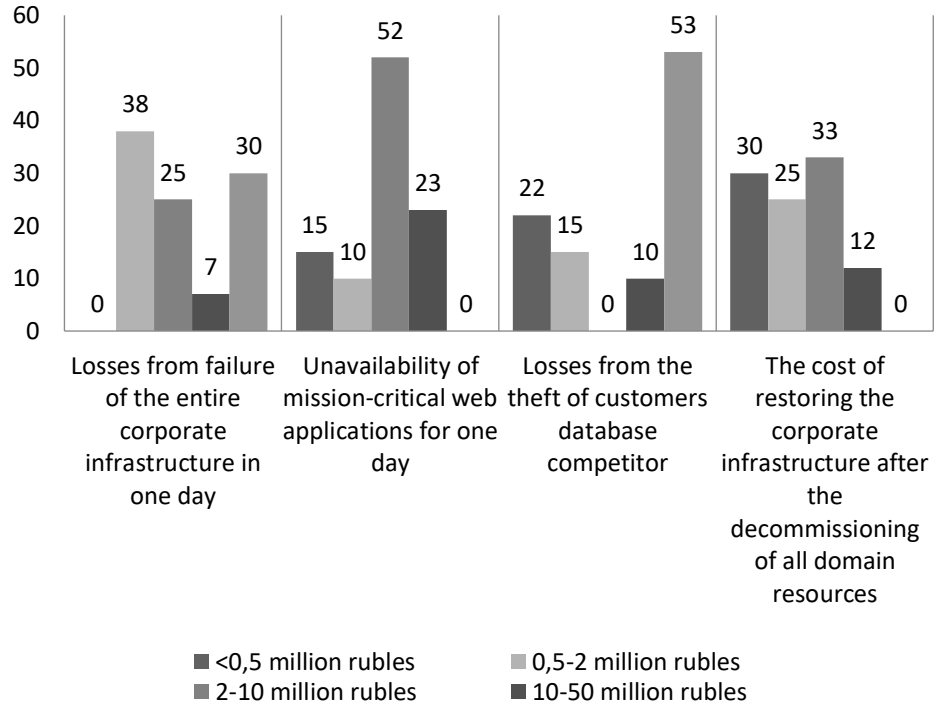


Fig. 1. Potential damage from the suspension of the financial organization, including lost profits and the cost of restoring sites

*Source. Compiled by the author [9, pp.14-16, 18]*

So, as can be seen on Fig. 1, the most significant are the losses of credit and financial institutions and the banking sector from various kinds of cyber-attacks (more than 50 million rubles) due to theft of customer databases (53% respondents) and in

case of failure of the entire corporate infrastructure during one day (30% respondents).The potential damage from unavailability of critical web applications in one day is estimated at 2-10 million rubles by the majority of respondents (52%). Additional costs of restoring the corporate infrastructure after the decommissioning of all domain resources in most cases do not exceed 10 million rubles. 88% of respondents called all this amount and less.

Thus, cyber-attacks targeting individual credit organizations together constitute a big threat to the entire financial sector of the country's economy. It was noted at the Insurance Technologies Forum "InnoIns-2018" held in Moscow on April 17, 2018, that 16 enterprises in Russia were being subjected to cyber-attacks every day. Business spends about $ 122.5 billion a year to protect information systems.

Theft of funds from bank accounts or electronic money seems to be attractive and profitable for criminals because of the absence of strict penalties for it. Other computer crimes against the financial and credit and banking sectors are attractive as well. What is more, computer scammers and hackers are finding new ways of committing crimes that prevent them from falling under criminal penalties.

Analysis of the methods of crimes committed in the credit and financial sphere showed that criminals continue to use social engineering methods along with the use of high-tech hacker schemes to gain access to banking systems. The most common form of such preparatory unlawful activity is pretexting, that means preliminary contact with potential victims by telephone, in instant messengers (Skype, WhatsApp, Viber, Telegram, etc.) or in social networks (VKontakte, Facebook and etc.) in order to obtain necessary information for access to the disposal of their funds. According to the position of the Central Directorate of Security and Information Protection of the Bank of Russia, the heightened danger of such criminal acts is determined by the gullibility and low level of financial literacy of the population. Consequently, in the near future, reducing the prevalence of pretexting as a preparatory activity for committing theft of money from bank accounts and electronic money seems unlikely [10]. Analysis of statistical data of law enforcement agencies showed that in 2018 citizens from 18 to 40 years old were increasingly becoming victims of "social engineers" [11].

Russian lawmakers made a number of changes in the criminal legislation of the Russian Federation considering the ever-increasing threat to society and people from committing cyber-attacks on the financial system and considering the experience of leading foreign countries in the field of criminal punishment for computer crimes in the financial and banking fields. The most important changes are shown in Table 1 [12-13].

Table 1. The most important changed in the field of criminal punishment

| Article of CC of RF | Old content [12] | New content [13] |
|---|---|---|
| Article 158 Criminal Code of the Russian Federation (point "g" introduced by Federal Law dated 04.23.2018 N 111-ФЗ) | This basis was absent | g) Theft from a bank account in relation to electronic money (in the absence of evidence of a crime under article 159.3 of the CC of the Russian Federation) is punished: - with a fine in the amount of one hundred thousand to five hundred thousand rubles; - in the amount of the salary or other income of the convicted person for the period from one year to three years; - forced labor for up to five years with or without restriction of liberty for up to one and a half years; - imprisonment for up to six years with a fine of up to eighty thousand rubles or in the amount of wages or other income for a period of up to six months; - or without it and with a restriction of freedom for up to six years or without it. |
| Article 159.3 CC RF | The old name of the article "Fraud with the use of payment cards" | New title of the article "Fraud using electronic payment" |
| Part1 Article 159.3 | Payment card fraud, that is, theft of another's property using a fake credit | Fraud with the use of electronic means of payment is punishable: - by a fine of up to |

| | | |
|---|---|---|
| Criminal Code of the Russian Federation | payment card or a card belonging to another person by deceiving an authorized employee of a credit, trading or other organization. Fraud is punished: - with a fine of up to one hundred twenty thousand rubles; - in the amount of the salary or other income of the convicted person for a period of up to one year; - compulsory work for up to three hundred and sixty hours; - correctional work for up to one year; - restriction of liberty for up to two years; - forced labor for up to two years; - arrest for up to four months. | one hundred twenty thousand rubles; - in the amount of the salary or other income of a convicted person for a period of up to one year; - by compulsory work for up to three hundred and sixty hours; - correctional work for up to one year; - restriction of freedom for up to two years; - forced labor for up to two years; - imprisonment for up to three years. |
| Part 2<br>Article 159.3<br>Criminal Code of the Russian Federation | Fraud with the use of payment cards, committed by a group of people by prior agreement, as well as causing significant damage to a citizen, is punished: - with a fine of up to three hundred thousand rubles; - a convict's salary or other income for a period of up to two years; -compulsory work for four hundred and eighty hours, either by correctional labor for up to two years; -by forced labor for up to five years, with or without restriction of freedom for up to one year; - deprivation of freedom for up to four years with the restraint of liberty for up to one year or without it. | Fraud using electronic means of payment committed by a group of people in a preliminary conspiracy, as well as causing significant damage to a citizen is punished: - with a fine of up to three hundred thousand rubles; - in the amount of the wages or other income of the convicted person for a period of up to two years; - compulsory work for four hundred and eighty hours; - by correctional labor for up to two years; - by forced labor for up to five years with restriction of freedom for up to one year, or without it; - imprisonment for up to five years of restriction of liberty for up to one year, or without it. |
| Part 3<br>Article 159.3<br>Criminal Code of the Russian Federation | Acts, under part 1-2 of article 159.3 committed by a person using his official position, as well as on a large scale are punished: - with a fine in the amount of from one hundred thousand to five hundred thousand rubles; - in the amount of the salary or other income of the convicted person for a period of one to three years; - forced labor for up to five years with restriction of liberty for a period of up to two years without it; - imprisonment for up to five years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of a convicted person for a period of up to six months or without it; -with restriction of freedom for up to one and a half years or not. | Acts, under part 1-2 of article 159.3 committed by a person using his official position, as well as on a large scale are punished: - a fine in the amount of from one hundred thousand to five hundred thousand rubles; - or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation liberty for up to six years with a fine of up to eighty thousand rubles; -in the amount of the salary or other income of the convict for a period of up to six months or without it; - with restriction of liberty for a period of up to one and a half years or without. |
| Part 3<br>Article 159.6<br>Criminal Code of the Russian Federation | Acts, under part 1-2 of article 159.6 committed by a person using his official position, on a large scale are punished: a fine in the amount of from one hundred thousand to five hundred thousand rubles, or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation of liberty for up to five years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of the convict for a period of up to six months or without it; -with restriction of liberty for a period of up to one and a half years or without. | Acts, under part 1-2 of article 159.6 committed by a person using his official position, on a large scale or from a bank account, as well as in relation to electronic money are punished: a fine in the amount of from one hundred thousand to five hundred thousand rubles, or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation of liberty for up to six years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of the convict for a period of up to six months or without it; -with restriction of liberty for a period of up to one and a half years or without. |

So, the analysis of the novels of the Russian criminal legislation in the field of digital crimes introduced by the Federal Law of April 23, 2018 N 111-ФЗ "On Amendments to the Criminal Code of the Russian Federation" [14] allows speaking:

1) on expanding the field of offenses in the area of computer crimes in the banking sector to the more general concept of electronic means of payment

2) shows tougher penalties for committing crimes in the field of banking and financial activities.

Thus, under article 158 of the Criminal Code of the Russian Federation ("Theft") criminal liability is provided for theft committed from a bank account and electronic money. And the title of article 159.3 was changed from "Fraud with the use of payment cards" to "Fraud with the use of electronic payment", that greatly expands the scope of its application. Also, according to article 159.3 the severity of punishment was significantly changed:

1) the punishment for fraud with the use of electronic means of payment in the form of arrest for the time up to four months was replaced by imprisonment up to three years;

2) the threshold value of a large-scale offense was reduced from one million five hundred thousand rubles to two hundred and fifty thousand rubles.

Under article 159.6 of the Criminal Code "Fraud in the field of computer information" the new law also provides reducing the threshold value of a particularly large offense from six million rubles to one million rubles. The action assessment itself is supplemented by a new qualifying sign that is an act committed from a bank account, as well as in relation to electronic cash.

The punishment for fraud with the use of electronic means of payment, committed by an organized group or on a large scale has not changed. This type of offense is punishable by imprisonment for a term of up to ten years with a fine of up to one million rubles or in the amount of wages, or other income of the convicted person for a period of up to three years or without restriction of liberty for up to two years or without [13]. According to official judicial statistics [15], 74 and 144 people in 2017 and 47 and 33 persons during 6 months of 2018 were convicted for committing acts under articles 1593 (Fraud using electronic means of payment) and 1596 (Fraud in the field of computer information) of the Criminal Code of the Russian Federation.

National Computer Incident Coordination Center was established in July 2018 to increase the level of national computer security of the country and in accordance with part 4 of article 5 and clause 2 of part 4 of Article 6 of Federal Law No. 187-FZ of July 26, 2017 "On the Security of Critical Information Infrastructure of the Russian Federation" [16].

According to the National Computer Incident Coordination Center (NCTC), in 2018 more than 4.3 billion cyber-attacks were made on critical information infrastructure, 17 thousand of which were considered the most dangerous. This is almost two times higher as in 2017 – 2.4 billion and 12 thousand respectively.

## 4. Conclusions

As it was shown in the study, cyberattacks aimed at individual credit organizations together pose a tremendous threat to the entire financial sector of Russia, and financial institutions spend annually about 122.5 billion dollars to protect their information systems from hackers and scammers.

Until 2018 there were no penalties under the Russian criminal law that were adequate to the gravity of the crimes and the amount of damage from computer crimes. The absence of strict penalties makes theft of funds from bank accounts or electronic money attractive and profitable for criminals, as well as other computer crimes against the financial and credit and banking sectors.

The Federal Law dated 04.04.2018 N 111-F3 "On Amendments to the Criminal Code of the Russian Federation" and entered into force on May 4, 2018, tightened criminal liability for embezzling funds from bank accounts or electronic money.

The changes introduced by the legislator in the criminal legislation of Russia take into account modern threats to economic security and increase the level of protection of the financial interests of citizens, credit institutions and the state as a whole.

However, the application of the new criminal law against computer crimes in the financial, credit and banking sectors during the first year has showed that the adopted criminal norms are not enough to reliably prevent crimes. In addition, computer scammers and hackers are finding new ways of committing crimes that prevent them from falling under criminal penalties.

Further research in the framework of this problem is supposed to be carried out taking into account the emergence of new methods of committing computer crimes in the banking sector, the emergence of new objects of crime (for example, cryptocurrency - bitcoins, etc.) and new types of crimes.

Also, the further studies within the framework of this problem are supposed to be conducted in the context of the most important threats to Russia's digital security, including not only the credit and banking and financial sectors, but also other areas of the functioning of society.

The main limitation of the study on these issues is the lack of complete, accurate and reliable information about the size of computer crimes in the banking and financial sectors, since this information is disrupted by banks, credit and financial institutions, and the police. Such data and information are not available in official statistics.

**References**


1. Improving criminal liability for cybercrime in the financial sector http://ormvd.ru/pubs/102/improvement-of-measures-of-criminal-liability-for-cyber-crimes-in-the-financial-sector-of-the-econom/
2. The Global Risks Report 2019, 14th Edition, World Economic Forum, Geneva. 2019.
3. The global losses from cybercrime in 2019 can reach $ 2 trillion. - [Electronic resource] - URL: https://www.banki.ru/news/lenta/?id=10404738
4. Toropova I., Mingaleva A., Knyazev P. (2020) Macroeconomic Model of Banking Digitization Process. In: Antipova T. (eds) Integrated Science in Digital Age. ICIS 2019. Lecture Notes in Networks and Systems, vol 78. Springer, Cham. doi.org/10.1007/978-3-030-22493-6_9
5. Brottsbalk (1962: 700). Regeringskansliets rättsdatabaser. Utfärdad: 1962-12-21 Senast ändrad: 2015-04-01 Uppdaterad: t.o.m. SFS 2015: 97. https://www.legislationline.org/documents/section/criminal-codes
6. Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) https://www.legislationline.org/documents/section/criminal-codes.
7. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juni 2019 (BGBl. I S. 844) geändert worden ist. https://www.legislationline.org/documents/section/criminal-codes.
8. The market for criminal cyber services. 2018. https://www.ptsecurity.com/ru-ru/research/analytics/darkweb-2018/.
9. How much is security? Analysis of information security processes in Russian companies. Positive Technologies. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf.
10. Barkhatov E.N. Features qualifications fraud in the field of computer information and its distinction from other offenses // Modern law. - 2016. - № 9. - p. 111.
11. New bank fraudsters: we are called "social engineers"! // BANKIN RUSSI. 2017 December 14th. - [Electronic resource] - URL: https://bankinrussia.ru/news/novye-bankovskie-moshenniki-socialnye-inzhenery.
12. Criminal Code of the Russian Federation. Old edition: GARANT system: http://base.garant.ru/57412609/644c26293f27715490005d21e7af011f/#ixzz5tFVlIB3l.

13. Criminal Code of the Russian Federation. New edition. GARANT system: http://base.garant.ru/57412609/644c26293f27715490005d21e7af011f/#ixzz5tFWXjg5s.
14. Federal Law of April 23, 2018 N 111-ФЗ "On Amendments to the Criminal Code of the Russian Federation" http://www.consultant.ru/document/cons_doc_LAW_296451/.
15. Summary statistics on criminal status in Russia for 2016; Summary statistics on criminal status in Russia in 2017; Summary statistics on criminal status in Russia for 6 months of 2018 // Judicial Department at the Supreme Court of the Russian Federation. - [Electronic resource] - URL: http://www.cdep.ru/index.php?id=79.
16. Order of the Federal Security Service of Russia of July 24, 2018 N 366 "About the National Coordination Center for Computer Incidents" System GARANT: http://base.garant.ru/72041506/#ixzztv1rQY2i.

# A study on market intelligence: the professional, the applicability of information technologies to innovate and gain competitive advantage

Enzo Arthur Martins da Silva[1] and Patrícia Scoralick Martins Lopes[2]

[1] Federal Institute of Minas Gerais, Sabará, Brazil, 34590-390
[2] Faculty of Sabará, Sabará, Brazil, 34555-000

https://doi.org/10.33847/2686-8296.1.1_6

Received 01.10.2019/Revised 30.10.2019/Accepted 11.12.2019/Published 22.12.2019

**Abstract.** With the evolving market of various industries, business management specialists are creating a demand for information technology to gain competitive advantage. Within this context, technology management specialists seek to innovate by creating systems that offer results with differentials. In this paper, we seek to present the connection between the study of Business Administration and Information Systems, addressing a brief history of Market Intelligence, its evolution and the importance it has for most business sectors. We have strengthened the argument why information technology is an essential investment for the success and survival of any organization today. We intend to contribute with theoretical material for future research on the subject.

**Keywords:** Market Intelligence, Information Technology, Innovation, Advantage, Data Science.

## 1. Introduction

Running a business requires that a leader prepare with professional qualification of personal nature and invest in his team. Choosing highly qualified professionals to meet quality requirements is essential for your organization to achieve the desired success.

Although technology dominates most of today's businesses, intellectual capital is in line with [1] "the most important resource of an organization, because it is the bearer of knowledge". To manage an organization and its team, you need to apply this knowledge to drive technologies toward the goals to be achieved. This role of the leader makes it necessary to elaborate a planning, which [2] states is "vital for the other administrative functions, because without planning, organization, direction and control they lose all their effect".

This management step relies on reliable data and information collection to be accurately crafted. Having [3] presented the planning at the strategic, functional and operational levels, we follow his reasoning with the steps of analyzing the current situation, defining objectives and elaborating the strategies to achieve the desired results, covering the areas of marketing, operational, human resources and information technology (IT).

Following the needs of companies, [4] says that marketing has key factors for a good market orientation, pointing out among them the surveillance of technological, social and political environments. In addition, so arise the concepts and practices of intelligences, which involves data collection, analysis and applicability.

One of these is Market Intelligence (MI), which has gained a fundamental place within organizations, especially in IT. For [5] what Customer Relationship Management (CRM) involves, it is IT that makes it possible to generate, store and

analyze data at a speed that meets the needs of companies, allowing them to elaborate competitive strategies and, consequently, generating advantages.

This paper provides information about IM, the professional responsible for applying its features, advantages of implementation in a company, exemplifying with some well-known and easily accessible systems. We want to present our analysis on the subject with the purpose of generating theoretical material and contributing to future research, presenting the following structure.

Market Intelligence:
- What is Market Intelligence (MI)?
- When did it come about and how did it evolve?
- Importance and advantages.

Market Intelligence Professional:
- What does a Market Intelligence analyst do?
- Appreciation and future prospects in the labor market.

Technologies for data extraction, storage and analysis;

Strategic Management Systems for Market Intelligence:
- How they work;
- How to put it into practice;
- Defining the key performance indicators (KPIs);

The concept of Business Intelligence and Examples of some systems:
- Business Intelligence; Google Analytics; Big Data; CRM.

Innovate for competitive advantage.

Conclusion.

## 2. Market Intelligence

### *2.1. What is Market Intelligence?*

Market Intelligence (MI) began many years ago, but in the last decade has gained its place within organizations in such a way that it has become essential to the outstanding success of the global market. In 1974, [6] argued about MI, presenting it as an organized way to collect data and analyze information, using everything relevant to the company.

Guiding decisions that affect many areas, such as marketing, sales, innovation and others, depending on each company. It involves knowing the internal market, the external market, what drives customers, analyzing competitor data and providing information for enterprise management systems, which we'll talk about later.

In a study, published in 2013, [7] says that by manipulating a set of techniques, methods and mechanisms, MI records, analyzes and works the action of disseminating information, transforming it into strategies to achieve certain goals. It uses this strategic information to make appropriate decisions in each competency, so that data analysis allows for a thorough understanding of market needs and the application of that knowledge to their advantage.

Today, these MI positions continue to prevail. If we are going to define IM now, we would just add some information that involves technological evolution. Given the value of globalization and the need to keep up with market developments in any business sector, Information Technology (IT) has become essential to the role of a Market Intelligence analyst.

### *2.2. When did it come about and how did it evolve*

When we start looking for information about IM, one of the first questions is "when did it come up?". So, we have a brief history of the context that includes this concept, also known as 'Competitive Intelligence'.

Several scholars have approached this topic differently, but what made the most sense for our study is the approach of [8], which says that military activities gave rise to what we now call MI. In analyzing the book "The Art of War" written by Chinese General Sun Tzu, [8] he says that his activities are described in detail, where he presents his military beliefs, making this the milestone where it all began, dating from the fourth century BC From this milestone, we have had several developments in military techniques until business applications arrived.

During the Cold War, which took place from 1945 to 1989, to address the need for concern for the enemy, they consolidated strategic military intelligence. They characterized their structures in analyzing the peculiarities of the current situation, personality traits of the enemy, using methods and techniques available at the time to survey the enemy's possible intentions, thereby obtaining some prestigious position that favored his army.

Only from the 1960s to the 1970s, that to meet an economic need, economists and managers began a new conception of intelligence to gain competitive advantage. With this they intended to anticipate the uncertainties, ambiguity and opportunities of national and international markets. The result of this was that from the implementation of Competitive Intelligence (CI), new perspectives emerged in relation to the old intelligence practices, which were adapted with methodologies appropriate to the business environment and technological evolution.

### *2.3. Importance and advantages*

When the company masters' tools that allow predictive analysis to be performed, it attributes its competences with a better understanding of its business, involving internal procedures within the reach of the foreign market. This is possible because the volume of data available helps in the analysis and elaboration of assertive actions. This way you can have a clear view of brand positioning, consumer behavior and other information that enable you to leverage your results with marketing, sales and customer relationship strategies.

The German Development Institute [9] conducted a study showing that the company analyzes competitiveness on four economic and social levels, namely:

- Micro level: involves companies and networks focused on improving production processes, which to be executed involve innovation and IT variables;
- Meso level: It is about the state and social factors, which involves employment policy and collaboration in favor of social learning structures. It is a level that encompasses innovation;
- Macro level: encompasses external factors that involve the company, having IT as a variable to achieve good performance and productivity;
- Goal level: It is about organizational patrons, it involves the legal and political economic scope. This level involves company decision marketing, aiming at social responsibility and strategic integration.

With proper data collection, it is possible to have a real and enlightening market analysis to achieve one of the goals of IM, which is CI, resulting in advantages for the organization. Implementing this concept provides several advantages, highlighting the following:

- enables a better understanding of the consumer profile;
- identifies possible current and future problems;
- provides solutions for future issues;
- encompasses knowledge of follow-up;
- allows you to follow your market trends and possible product coverage;
- brings information about the perception that the consumer has of the brand;
- identify possible and potential external influences;
- allows for a competitive analysis;
- assists in developing strategies focused on business opportunities.

But it's not just about having systems to gather information, it takes someone who is an IM expert to manage that content and make the tools work for the business, otherwise it becomes just data, no application. The responsible for the operation of this concept, MI that conquered the business world is the Market Intelligence Analyst.

## 3. Market Intelligence Professional

### *3.1. What is a Market Intelligence Analyst?*

The professional analyst may have several professions, all requiring theoretical and practical knowledge in certain areas. This is still a professional said as new in the Brazilian scenario, and is gaining his space and value, both personal, professional and compensation. The most common training for the position of Market Intelligence Analyst in Brazil is in Business Administration. This professional must be able to objectively and quickly monitor, investigate and analyze the market, customers, technologies on their business environment to assist in the accurate decision-making process. It is necessary to deepen the data collection and the results, to think in a wide scenario, to unify the data, to expose the failures and to know how to reproduce the information for all the sectors that depend on its work. In addition to identifying opportunities and anticipating trends.

In an article about the challenges of this professional, [10] presents a research that exposes the information that the position of MI Manager was one of the most valued in 2016, in Brazil, reaching remuneration ranging from $ 10,000 to $ 15,000. But to reach this position there is a long way to go and it requires experience that the MI analyst acquires over time. No need for mastery of information technology such as advanced programming and cutting-edge software handling, but for an analyst, mastery of mathematics and advanced knowledge in Excel is essential.

Having other knowledge is a differential, because Administrators, Advertisers, Sociologists, Journalists, Designers, can form even a team among other professionals, IT is involved in all areas and abroad knowing programming is something basic for most professionals. Having this vision, a professional who wants to reach this position, should be self-taught and invest in himself, with study and practice of IT, research and other content that covers the work of MI, as this position involves multiple sources of knowledge to obtain information and result in competitive advantage.

### *3.2. Appreciation and future prospects in the labor market*

The Robert Half Recruitment Specialist, founded in 1948 in the United States, respected worldwide in the human resources field, released the 12th 2020 Payroll Guide [11]. This material presents an annual recruitment and selection study, showing the highlighted professions for next year and with appreciation visibility. Among them, in the sales and marketing area, is the Market Intelligence Analyst (see Table 1).

Table 1. List of prominent professions in the market and sales area

| Featured Positions | Most demanded skills |
|---|---|
| Market intelligence analyst.<br>Head of Growth.<br>Account Executive.<br>Sales manager.<br>Digital Marketing Analyst.<br>Marketing manager | Familiarization with technological trends.<br>Focus on results.<br>Analytical Profile.<br>Multitasking.<br>Hunter Profile ("hunter" of new customers) |

*Source: Table adapted from [11].*

In its website [11], it presents the professions highlighted in the areas we mentioned in this paper, as shown in Table 1. It argues that the sales and marketing areas followed the technological evolution and were transformed, as a function of

optimizing and achieving always better results, thus dictating the direction of the market and future trends.

Table 2. List of prominent professions in the market and sales area

| | CARGO (JOB TITLE) | Tamanho da Companhia* | 25° | 50° | 75° | 95° |
|---|---|---|---|---|---|---|
| Marketing<br>*Marketing* | Diretor de Marketing<br>*Marketing Director* | P/M | 17.100 | 21.000 | 24.550 | 33.600 |
| | | G | 24.200 | 35.000 | 43.000 | 58.900 |
| | Head of Growth | P/M | 13.000 | 16.000 | 19.650 | 21.600 |
| | | G | 17.250 | 25.000 | 30.700 | 33.800 |
| | Gerente de Marketing<br>*Marketing Manager* | P/M | 10.350 | 15.000 | 18.450 | 20.300 |
| | | G | 15.200 | 22.000 | 27.000 | 29.700 |
| | Analista de Inteligência de Mercado<br>*Business Intelligence Analyst* | P/M | 3.450 | 5.000 | 6.150 | 6.800 |
| | | G | 6.200 | 9.000 | 11.000 | 12.100 |
| | Gerente de Trade Marketing<br>*Trade Marketing Manager* | P/M | 9.000 | 13.000 | 16.000 | 17.600 |
| | | G | 12.450 | 18.000 | 22.100 | 24.300 |
| | Gerente de Produto<br>*Product Manager* | P/M | 8.300 | 12.000 | 14.750 | 16.250 |
| | | G | 10.350 | 15.000 | 18.400 | 20.250 |
| | Coordenador de Categoria<br>*Category Coordinator* | P/M | 5.550 | 8.000 | 9.850 | 10.900 |
| | | G | 8.300 | 12.000 | 14.750 | 16.250 |
| | Analista de Marketing/<br>Marketing Digital<br>*Marketing/Digital Marketing Analyst* | P/M | 3.450 | 5.000 | 6.150 | 6.800 |
| | | G | 5.550 | 8.000 | 9.800 | 10.800 |

*Source: Table adapted from [11].*

According to Table 2, of remuneration analysis, noting that we are talking about the positions of analysts, aiming at valuation and remuneration, among the listed professions the Market Intelligence Analyst, has positioning and future perspective considered positive.

## 4. Technologies for Data Extraction

To optimize the work of a marketing manager, there are several technological tools that constantly evolve according to market demand. Marketing Information Systems (SIM), defined by [12], depend on several factors, including information technology, which is essential in the quality of data collection, storage and analysis, so as to minimize the possibility of errors, helping so in decision making. [13] analyzes Sandhusem's SIM model, (see fig. 1) and points out that the marketing manager must have access to all information about the company, the foreign market, and the business environment. In this context, data storage is linked to all information, input and output sources, being at the center of the SIM model.

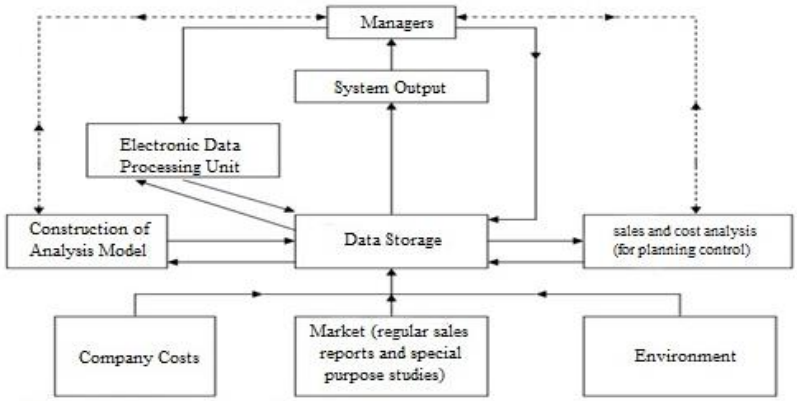


Fig. 1. Exemplifies the marketing information system
*Source: [13] adaptation.*

In the SIM scenario, as shown in Fig. 1, are Customer Relationship Management (CRM) systems, which rely on IT for proper and quality operation.

Following the evolution and market demand, technologies described in Table 3 were developed for data extraction, storage and analysis, as shown in the table below, exemplified by [13]:

Table 3. Evolution and market demand

| Step Evolution | Business Matter | Enabling Technology | Features |
|---|---|---|---|
| Data collection | What is my total income over the last 5 years? | Computers, tapes, disks | Delivery of retrospective and static data. |
| Data Acess | What is the total sales in stores in the state of São Paulo last March? | Relational Databases, SQL, ODBC | Dynamic retrospective record-level data delivery. |
| Data Warehousing & Decision Support System | What is the total sales in stores in the state of sao paulo last March? Specify the city of Sao Paulo. | Online analytic processing(OLAP), multidimensional databases, Data Warehouses | Dynamic multi-level retrospective data delivery at |
| Data Mining | What will happen to sales of units in the city of São Paulo next month? | Advanced algorithms, computers, microprocessors, massive databases. | Delivery of prospective and proactive information. |

*Source: [13] adapted from Thearling (2004)*.

Table 3 shows the evolution of some technologies used for data extraction, which we will show below how they are used in management systems.

### *4.1. Strategic Management Systems for Market Intelligence*

For [14] "Business Intelligence (BI) is a process that involves methods, techniques, technologies, people, information, information sources, metrics, tools, and Business Analytics (BA) systems, are predictive models for trying to predict events. or predict values for attributes. This type of support includes systems known as decision support systems (DSS). What-if predictions and analysis are made with BA and SAD systems. "

In his work [15], he presents the BI architecture and its functionalities by subsystems, as follows:

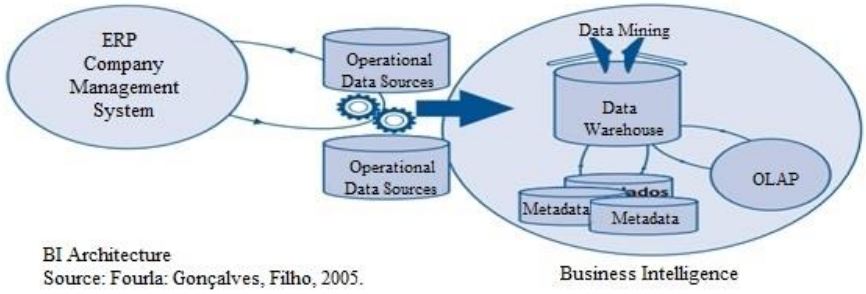


Fig. 2. Exemplifies the BI Architecture
*Source: Figure adapted from [15]*

And [15] complements the argument that subsystems play an essential role for SADs, and those that use Data Warehouse repositories use dimensional modeling from operational data and organize them into dimensions and facts to facilitate analysis. The subsystems of classical architecture are served by data mining, Data Mining, whose function is to make explicit the information that until then is implicit in the organization's databases. And goes on talking about the interface subsystem, which is represented in the BI architecture by the OLAP tool, perform the presentation and crossover of information to support the decision process steps.

*4.1.1. SIM Operation. How to put it into practice*

To make the process truly efficient, a company must follow some necessary procedures, such as defining its performance indicators, which tools will be used to gather information, and how its data will be manipulated.

To complete these steps, you need to review the available information and get accurate conclusions about the business problem in order to maintain, update, or modify the strategy you analyze. This study should be conducted periodically, updating the quality of processes allowing to stay ahead of the competition

*4.1.2. Key Performance Indicators (KPIs):*

The first step is to define your key performance indicators (KPIs). They exist to measure the effectiveness of your actions and the progress of projects and processes of the organization.

There are a number of performance indicators, [16] all of which are relevant and useful, but there are some that are global trends where each KPI integrates with a specific type of feedback and its respective functions that can be applied in a number of cases and will be important in many cases any operation. Being them:

*Turnover:* Measured as a percentage (%), it serves to measure employee turnover over a set timeframe, and can measure employee satisfaction or dissatisfaction with the organization, for example.

*Gondola Share:* This is a performance indicator that compares execution in practice to what was previously planned by BackOffice. Being able to measure the size and presence of products on shelves. Your rating may be fair by separating the area by regions, categories, or networks, depending on which plan the company decides to follow.

*Rupture:* Controls the supply of products in retail chains compared to the virtual inventory index.

*Sell out:* Measures transaction volume and product introduction. This KPI is not always feasible as it depends on the need for your retail network.

*Sell in:* Can be focused on the business process, generating information on sales promotions and retail replacements, until optimizing manufacturer costs, focusing on product registration and inventory inventories.

*Profitability:* Can provide information on final billing based on previously planned.

*Average Ticket:* This KPI would return the average unit sales value, affecting product and service promotion initiatives.

*LTV: Lifetime value, or LTV*: is a KPI that measures company billing information according to a customer's length of stay.

*CAC: Customer Acquisition Cost (CAC)*: is a KPI that tells you the success or failure of an operation. Also showing the amount invested to maintain and win new consumers.

### *4.2. The Business Intelligence Concept and Examples of Some Systems*

*4.2.1. Business Intelligence (BI)*

Second business intelligence [17] is knowing how to collect, organize and analyze data to make decisions and know the results obtained through their investments. Unlike what it seems to be, BI is not a tool. BI relies on robust software to deliver everything that is expected, but it goes beyond that, it is a set of processes that aims to deliver the right information to the right recipient at the right time, following three pillars:

Data Collection: Collect data about everything that happens in the business to determine key aspects such as productivity, seizing opportunities, bottlenecks, market reputation, etc.

Organization and analysis: Organize previously capitalized information to be presented visually to facilitate decision making.

Action and monitoring: When processing organized data, decision makers make their decisions and monitor their results and whether they match what expected.

As a practical example of BI software, we have Power BI, which is one of the leaders in the BI market and since its inception is a complete software, not only showing information visualization, but also with the creation of DW and ETL process. and the OLAP cube.

Compared to its competitors, Power BI is the most cost-effective, with a paid value of approximately $ 9.99, winning over its competitors' market, where its prices exceed $ 1,000.

Another attraction of this system is the ability to access your data through mobile operating systems, such as Android, IOS and Windows Mobile.


Fig. 3. Exemplifies the BI System
*Source: Figure adapted from [17]*

Another BI platform is SPAGOBI, it keeps competing because it is considered the best open source tool, has only one version, where it is completely free. This tool is not fully complete, but it is not a significant limitation as its developers suggest another open source tool to "complete" its functionality called Talend Open Studio.

SPAGOBI delivers the key functionality you need for your organization, providing all the analytics, which include reporting, the data mining process, and OLAP

analysis.

*4.2.2. Google Analytics*

Google analytics is not only a free tool, it is an extremely complete tool and can be applied to online stores, physical sales and service companies. Showing beyond the number of hits to your store, it returns you with detailed profile and user behavior analysis. Allowing the company to adapt to better serve its customers. Compared to its competitors, Power BI is the most cost-effective, with a paid value of approximately $ 9.99, winning over its competitors' market, where its prices exceed $ 1,000.

Another attraction of this system is the ability to access your data through mobile operating systems, such as Android, IOS and Windows Mobile.

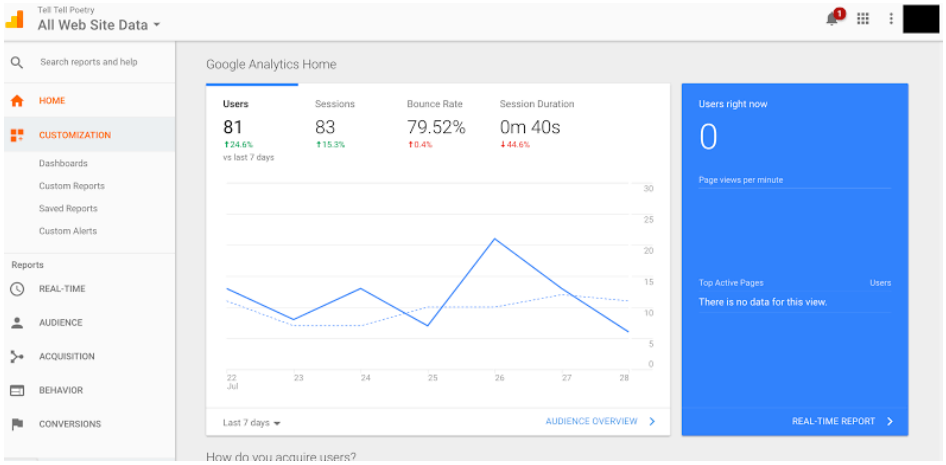


Fig. 4. Exemplifies the Google Analytics
Source: screenshot adapted from [18]

*4.2.3. Big Data*

As the name implies, big data is a concept that describes large structured and unstructured databases, essential for large companies that process large amounts of data. They are usually programmed in Python, as this language enables more assertive analysis.

*4.2.4. Customer Relationship Management (CRM)*

The Customer Relationship Management (CRM) system is software that has the ability to manage sales industry information and its means of communication with customers. It presents possible sales strategies that can be better applied to favor the current situation of the company.

The tools offered by this system allow access to data important for market intelligence, detect events in the sales sector, making an analysis of activities such as number of emails triggered, messages read, number of calls made, among other information.

**5. Innovate for Competitive Advantage**

A study by [19] shows that Brazilian companies can leverage their productivity

by investing in Research, Development and Innovation (RD&I), using simple tools already known, others that involve more technology and are used more frequently today. Points out that prior to performing Strategic Planning (PE), you must apply Technology Watch to monitor IT advances and trends, presenting the following figure, which you refer to as a mind map to aid this thinking.

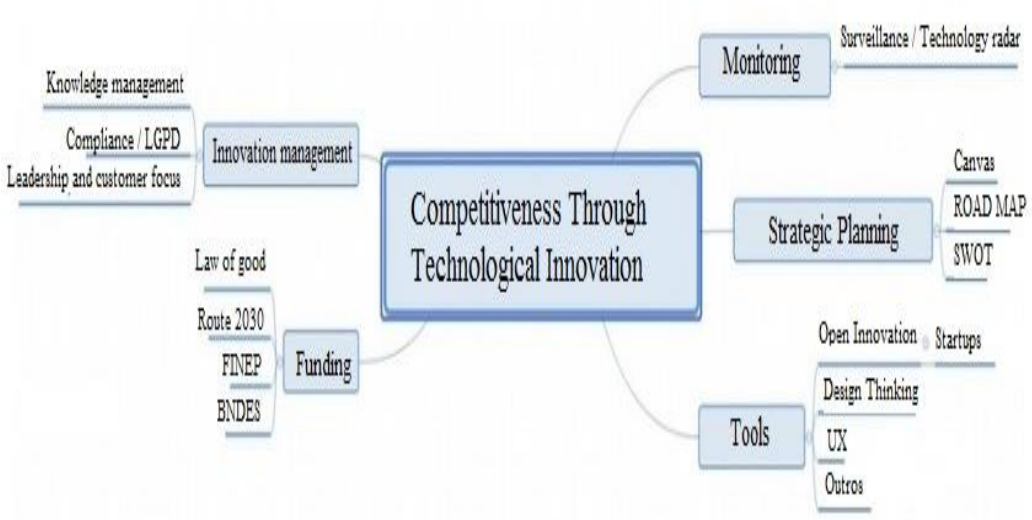


Fig. 5. Model of Mental Map
*Source: Figure adapted from [19]*

One of the strategic management tools presented by the author is Canvas, already known in the business environment, of simple execution and that helps in the creation of new projects and businesses. But here we highlight the new technological tools that have been gaining more space in companies, which are:

- UX Design: focused on analyzing and defining the problems that need to be solved and dictating which way to go. Focusing on the product, whether it is a service, website, machine or others, UX works to make usability easy, reducing users' difficulties. It relies on principles of psychology to manipulate the user to be able to perform tasks, motivating and encouraging in some way. This tool aims to achieve greater customer satisfaction and allows to have the image that has the brand, because it evaluates human behavior and proposes designer improvements.

- Open Innovation: aims at seeking knowledge for R&D processes, allows internal ideas, which would be eliminated in the closed model, have room to find place in other business models, with the participation of the company that generated the idea through licensing, royalties or spin out. The open innovation model figure exemplifies one way to create and profit from technology (Fig. 6).

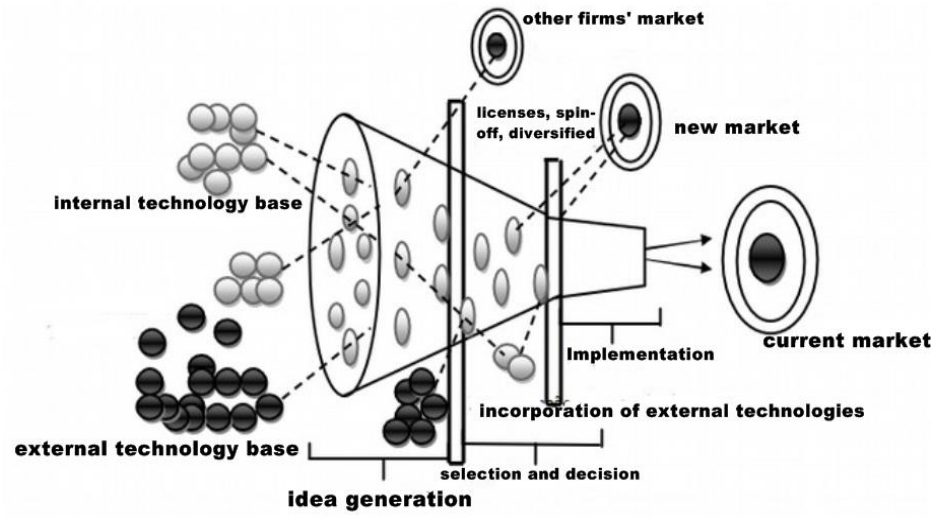


Fig. 6. Open innovation model
*Source: adapted from [19]*

- Designer Thinking: Considered an approach to inspire creativity as the name suggests, so that it is applied to solve problems, instigating innovation always focused on the user. It uses designer tools to integrate the needs and possibilities that technology can provide. It is divided into three phases which are inspiration, ideation and implementation.

These tools are used to generate inspiration in the team, so as to facilitate the creation of solutions to the problems proposed by the market intelligence analyst.

## 6. Conclusion

Market Intelligence has become essential to organizational success, as all the benefits that this department can add to the company are truly differential for those seeking not just market survival but especially growth. Investing in intellectual capital, software and technological innovation leverage competitive advantage over the competition.

Faced with the technological growth that companies face every day and can use so many tool options to their advantage to gain competitive advantage, the professional, market intelligence analyst needs to know how to deal with the team in order to apply everything available to them. achieve the goals.

We know that innovation makes any product or service more attractive, so when investing in IM, a company also needs to be prepared, with capital set aside for investing in innovation, as solutions and opportunities created by intelligence can cease to be innovative in no time since the competition is also possibly investing in that intelligence.

Companies based in Brazil, today live a scenario of opportunities, but still need to invest in technological maturity, management and strategies, such as marketing. Therefore, we emphasize the importance of a team prepared to face the challenges that market intelligence can face on a daily basis.

As described earlier, being smart for a particular industry is not just about dealing with statistical data, it is tactful to turn that data into challenges for human capital to leverage IT tools and create solutions, opportunities, and predict market trends. This attitude coupled with investment in IT puts the organization ahead of its

competitors, so that it gains advantage by investing in innovation, which today is one of the main factors considered differential by the public and the general consumer market.

Thus, we conclude with a sentence from [19] that summarizes the current scenario and future prospects for the companies in Brazil: "Without the management of technological innovation there will be no future for companies."

**References**


1. Chiavenato, I.: Introduction to General Theory of Administration. 6 edn. Campus, Rio de Janeiro (2000).
2. Chiavenato, I.: Initiation to the General Administration. McGraw-Hill (1989).
3. Facini, M., et al.: Strategic Planning. In: UniCentro Repository, Paraná (2014).
4. Moraes, C., et al.: Market intelligence: an essay under the competitiveness. In: Future Studies Research Journal, v.7, n.2. São Paulo (2015).
5. Barrionuevo, F.: Customer Relations: The Evolution of Marketing and the Presence of Technology in a Business Environment b2b, Piracicaba, (2004).
6. Kotler, P.: Marketing Direction. 2 edn. Publisher Diana. Mexico (1974).
7. Córdoba, A., Gonzales, A.: The Market Intelligence: the Competitividad Strategy. In: Management Student Essay. V. 6, Colombia (2013).
8. http://www.singularis.net.br/origem-da-inteligencia-competitiva/ last accessed 2019/11/02
9. Esser, K., et al.: International Business Competitiveness and required policies: systemic competitiveness. German Institute of Development, Berlin (1996)
10. https://www.mundodomarketing.com.br/reportagens/planejamento-estrategico/36073/os-desafios-do-profissional-de-inteligencia-de-mercado.html , last accessed 2019/11/03.
11. https://www.roberthalf.com.br/guia-salarial/vendas-marketing, last accessed 2019/11/02.
12. Kotler, P., Armstrong, G.: Principles of marketing. 7 edn. Pearson Prentice Hall, Sao Paulo (1998).
13. URL. http://www.dominiopublico.gov.br/download/texto/ea000249.pdf , last accessed 2019/11/02.
14. Loh, S.: BI in the age of big data for data scientists - going beyond cubes and dashboards in the search for whys, explanations, and patterns. Porto Alegre (2014).
15. Ceci, F.: Business intelligence: digital book. Unisul Virtual, Palhoça (2012).
16. URL, https://clubedotrade.com.br/blog/kpis-de-trade-marketing/ last accessed 2019/11/03.
17. URL, https://inteligencia.rockcontent.com/business-intelligence/ last accessed 2019/11/03.
18. URL, https://segment.com/integrations/google-analytics/ last accessed 2019/11/03.
19. Brito, A., et al.: Gain Competitiveness through Technological Innovation. In: Research and Action (2019).

**Aims and Objectives**
Published online by ICS two times a year, Journal of Digital Science (JDS) is an international peer-reviewed journal which aims at the latest ideas, innovations, trends, experiences and concerns in the field of digital science covering all areas of the scholarly literature of the sciences, social sciences. The main topics currently covered include: Digital Communications and Network; Digital Economics, Education, Engineering, Finance, Health Care.

The main goal of the journal is the effective dissemination of original incites/results generated by the human brain and presented/reflected in articles using modern information/digital technology.



**Contact information**

**Journal URL:** https://ics.events/journal-of-digital-science/

**Email:** conf@ics.events