sanctions for legal persons. By analyzing the existing theoretical and legislative models of criminal liability of legal persons, it has been concluded that there are three fundamental distinctive material-legal features that depend on their content. The main question is whether the criminal responsibility of a legal entity is performed or autonomous, whether it is subjective or objective and is ultimately subsidiary or cumulative. In most of the criminal law regulations, a model of realized responsibility of legal persons was accepted in which the liability of a natural person is accounted for by a legal person. However, it is increasingly penetrating, both in theory and in legislation, a model of autonomous accountability. In order to make the liability of a legal person independent of the guilt of a natural person, it was necessary to create new criminal law institutes that correspond to the delinquent behavior of a legal entity, among which the most well-known responsibility is due to defects in the organization and misdiagnosis.

LITERATURE

[1] M. Simović, Criminal Proceedings, Third and Modified Edition, Banja Luka, 2009. year.
[2] M.Simović, Criminal Proceedings, Introduction and General Part, Bihać, 2009. year.
[3] Lj. Filipovic, V.Ikanovic: Educational Model "Criminal Procedure Against Legal Persons", High Judicial Prosecutorial Council.

SAFETY PROTOCOLS IN E-BANKING

Almedina Hatarić, MA, email: almedina_tr@hotmail.com,
Imran Kasumović-student, email: imran.kasumovic@gmail.com

***Abstract**: Safety Information System includes actions, measures and procedures in order to protect data and information system from unforeseen events with undesirable consequences. In this direction is the increasing need for disabling any accidental or deliberate distortions and prevent the functions of computer systems. We should also create the necessary conditions for the proper use of predefined functions of information systems. As a basis for finding a satisfactory answer to the question of protection of information systems, we start from the classification of threats that can jeopardize the same accident, crime and error. On the basis of this classification,there are given four answers to questions where a partial response is received, and by their synthesisis receiveda fuller response: the value of hardware and software; versatility of computer systems; characteriatics of computer systems.*
First, it is necessary to define the purpose of the protection system, that any system of protection has meaning only if something, somewhere, and for some reason needs to be protected, and in order to achieve the goal, we need to execute something in some way on the function. The solution of these set goals is that question is possible with logical units, and according to the "golden questions" of criminology, the corresponding "golden questions" of information protection and which require full answers.

***Keywords:** Protocol, security, information systems, banking, technologies*

1. INTRODUCTION

E-commerce is a modern form of business organization that involves the intensive application of information technology and especially Internet technology. E-commerce is the conduct of business on the Internet, which does not only mean buying and selling, but also for the care of clients and business partners, as well as the organization of business in its online company and organization of business towards clients. From the definition, it can be seen that the basis for electronic commerce consists of information communication technologies that merges into the Internet that makes the global multimedia infrastructure. Today's development of the Internet has enabled new dimensions of organizational and business processes that are created by creating opportunities provided by:
A new, interactive way to access the market and business partners, both locally and globally.
Possibility to perform certain business processes outside the company.
Accessibility to a multitude of information, with powerful search elements and automated analysis.
New modalities of business association, financial transactions and business processes.

Business has always depended on technology, but today it is more pronounced than ever. It could be said that technology today manages all human life and work, and not just production facilities and service activities. Technology has changed the way we are doing jobs today, the very nature of jobs and the reasons why we are doing it. Today, customers want access to products and services at any time from 0 to 24 hours a day. Firms that provide the most functional, reliable and user-friendly product or service have the greatest prospect of success in the long run. Investing in technology is inevitable in order to find a way to create new business opportunities, to mend trends in the shortening of the product life cycle, and to speed up the acquisition of new markets. Business moves in sometimes unimaginable directions and performs in ways that could not be assumed in the near past. The best example that confirms this is the Internet that today sets a business strategy in the world's largest companies, but also in those small ones who are aware of both its advantages in application and inevitability for that application, all for the sake of business sustainability.

Areas where the most commonly used e-business:
Online sales of their own goods and services,
electronic trading,
online entertainment and recreation,
electronic banking and online financial transactions and
electronic publishing.

2. INTERNET AS A PLATFORMA OF ELECTRONIC BUSINESS

Internet is a global multimedia network that connects computers around the world. It consists of the infrastructure of network servers and communication channels between them that are used to transport information between client PCs and WEB servers, as well as the creation of the servers themselves. Internet is a network of all

networks that all interact with each other in an agreed language called the protocol. This protocol is known as the TCP / IP (Transmission Control Protocol). There are literally millions of networks that are connected to Internet, and it continues to grow steadily.

The basic concept of an internet operation is client / server architecture. This concept is based on the fact that any user can request a network server from a service, and this server provides it, if he has the right to access that service. Each computer within the network, which has some information that it may wish to provide in its own memory to other users on the network, is called a server.

While on the other side, each user device (such as a user PC or workstation in a local area network) that can request and accept data from a server is called a client. The most significant feature of the client / server architecture is that users do not need to take care of where the information is in the network system, where the form is stored, and which communications paths (telecommunication lines) will reach it. What the client needs to know is that there are many standard and non-standard network (internet) services (services) that will initiate the search and obtain information, or perform some information business (data transfer and processing).

3. SECURITY IN E-BUSINESS

Data security and data transmission is an old problem. The simplest form could be crawling - only one person gets the information, and others do not know the content of the message. The advantage is simplicity, and the shortage is the short distance that can be transmitted through this way of communication. The emergence of the letter opened new possibilities, primarily sending messages to the messenger at, at that time, arbitrary distance.

The biggest application was for military purposes, which brought greater danger to the messenger and message. The messenger could save a lot of speed or combat skills, but once mastered, then the message comes to hand to the enemy. The simple trick of the Romans was to write the message on a tape wrapped around a stick of exactly a certain diameter, so such a message could be understood only by the owners of such a stick. The enemy received only a tape with an incomprehensible sequence of characters, and the message was not even known to the messenger.

Once it is learned that the message is protected in this way, it is relatively easy to try to reach the appropriate size rod. Another way is, for example, to replace each letter with someone else. The recipient and sender of the message must have the same replacement table in order to write the message or read it. No one can try it, but for thirty letters there are 30! (factorial) of possible tables.

The disadvantage of this kind of protection is that some table must also be sent, so if the enemy is lucky to have intercepted a messenger with a table, he can read all the messages in the future. Moreover, he can write himself a encrypted message, and send a false messenger. If the recipient of the message knows the handwriting, at least the sender's signature, he will know that the message is fake. It can also ask the

messenger to identify, for example, a special ring of medallions, and best personal potency. With the advent of mass communication, especially internet, the need for secure transmission has grown sharply. It is now needed, not only to generals and rulers, but also business people, and ordinary citizens. Whether it's a military industrial secret, a credit card number in a love letter, data protection has become an everyday need. As we mostly do not know which way our data travels and through which hands pass, secure data transfer is necessary for every job where privacy is sought.

3.1. SSL protocol

Secure Sockets Layer (SSL) is a secure messaging (communication) protocol via Internet, which allows you to send confidential data (such as a credit card number) through Internet in encrypted and secure formats. The SSL protocol provides a special communication layer, which is placed on a trusted transport layer (eg TCP / IP), while an application layer is placed on the SSL.

It receives the message from the application layer, disassembles it into smaller parts suitable for encryption, adds a control number, encrypts, possibly compresses, and then sends those parts. The recipient receives parts, decompresses, decrypts, checks the control numbers, compiles the message sections, and submits them to the application layer. In this way, a secure channel of transmission through the network is realized through SSL. If the client and the server are inactive for a long time or conversation with the same security attributes takes too long, the attributes change.

The SSL protocol was designed and built by Netscape Communications Corporation to be used with Nescape Navigator. The first version, 1.0, was developed in 1994, however, it was just a trial version of the use within this corporation. Version 2.0 was the first to be released to the public and shipped with Netscape Navigator, versions 1 and 2.

The SSL protocol was created in response to the growing demands for secure data transmission on the Internet. Due to timely emergence, and because of the market role of Netscape Communications, the creator of this protocol, SSL has become very extensive. SSL, apart from being approved as standard by the www consortium (www.w3.org), has become a de facto standard.

With SSL, other solutions that secure secure data transmission across the network were developed. The success of SSL is further emphasized by the lack of other good solutions that would replace it. S-MIME is one of the other solutions. 3.1.1. S-MIME

Secure-MIME protocol has been developed by RSA and is an extension to an already existing MIME protocol. It uses the public key system as the basis for validation and encryption. Algorithms for encrypting and working with certificates are identical to those used in SSL, so the same certificates can also be used in this protocol. MIME users, SMIME, provide the same protection described by SSL in this work.

4. PUBLIC KEY SYSTEM

Through computers on Internet, numerous data are continuously passing, and in normal situations, the owners of these computers do not check their content. But there are many data that require protection from the dangers that lurk from a global network. With the task of protecting data in such conditions, a technique called the Public Key Criptography was established, which accomplishes the following protection tasks: Encryption and decryption allows two participants in communication to hide the content sent to each other. The sender encrypts the data before sending them, until the recipient decrypts them after receiving them.

Encryption represents the process of transforming data into a form that is incomprehensible to all but the intended recipients. Decryption is a reverse process, transforming encrypted data into an understandable form. The encryption algorithm was determined by a suitable mathematical method. Often, two linked methods are used, one for encryption, and the other for decryption. In the latest encryption methods, a series of alphanumeric characters are used, called the key, which use the algorithm to encrypt the data. Decryption with the corresponding key is simple, while without it it is very complex, that is, it is usually impossible for all practical applications. By separating the algorithm from the key, it allows everyone to be familiar with the algorithm, but without the key data the data is still incomprehensible.

4.1. Key length and protection strength

The protection power depends on the complexity of the key detection. The easiest way is to get the key directly from the owner, by stealing it or by some way of compelling it to convince him to give it to us. By such techniques, we are in danger of being identified and endangering ourselves. Another way is to calculate the key based on the encrypted data, which freely pass through the network. The complexity of this task depends on the length of the key and the encryption algorithm. The protection force is often described by the length of the key being used, and in general the following applies: a longer key - better protection.

The key length is measured in bits. Thus, when using an SSL protocol, you can also find the use of a 40-bit key, but also a 128-bit, which provides significantly better encryption with the same algorithm. The algorithms used are based on mathematical methods that have the characteristic that make it difficult, almost impossible, to decipher without knowing the key. Different algorithms for encryption can require different key lengths.

4.2. Confirmations

A certificate is an electronic document that identifies an individual, computer, company, or other entity that owns a private key. A certificate with the name of the entity also contains its public key. As an ID card, driver's license or other document is used for identification, certificates in computer communications provide evidence of the identity of the respective

entity. Certificates are used to protect against imitation, representation as someone that the entity actually does not. Receipt of confirmation is based on the same concept as the confirmation in the real world - certain conditions must be met. In order to obtain an identity card, we have to report to the police to determine our identity, take the fingerprint, the address of the dwelling and determine the time of validity of the ID. If a driver's license is to be obtained, a driving test must be passed first to prove the ability to drive a vehicle of the appropriate category.

Working with digital certificates as used by the SSL protocol is organized in a very similar way. As each person in his wallet has different documents (certificates) for different purposes (personal, health, driver ...), and for identification via the network, according to purpose, appropriate certificates are used. Slanderers are the institutions that verify the identity of other entities and issue certificates about it.

These may be either independent entities in the communication of the two entities, that is, a third party, or the subject in communication, who also issues certificates (for example, the bank checks the identity of its clients with its own certificates). The method for verifying identity depends on the policy of the particular issuer of the certificate, just as it is in a different way in the real world - it depends on its use. In any case, prior to the issuance of the certificate, its issuer must conduct its identity verification procedure of the person to whom it is issued. This procedure is published so that anyone who receives such a confirmation can determine whether this is a sufficient sigma method for his needs.

The significance of a digital signature is comparable to the significance of a personal signature used to sign papal documents. In some situations, a digital signature may be as correct as a personal signature. With the public key and name of the identity, the certificate contains the date to which the certificate is valid, the name of the issuer of the certificate, the serial number and some other information. The certification itself that travels over the network can be an attack object. That's why it is digitally signed. As the issuer of the certificate enjoys our trust, all offers of the affirmative issue can be trusted.

4.3. Identity authentication methods

In communicating with identity verification data, there is a reliable mutual identification of two subjects in communication. This can be done in several ways, where the use of certificates is one of them. In a network environment, they communicate with the most common client (for example, some communication software on a personal computer) and the server (for example, software and hardware that contain web pages). Client identification refers to confirming the identity of a client by the server, or checking the person who is supposed to use the client software. Server identification refers to confirming the identity of a server by a client, or identifying an organization that is assumed to be responsible for the server (at the appropriate network address).

Client identification is one of the basic elements of security in the communication

network. There are two types of customer identification:

4.3.2. Identification using certificates

Identification by certificates is considered more appropriate than password-based identification because it is based on:
something that the user has (private key);
something the user knows (a code that keeps his private key);

It is very similar to identifying ATMs where the user has to have a card and know the secret number. However, it is necessary to emphasize that these two assumptions are true only if the user's computer and password are protected from unauthorized access. The code is required to access the private key that stores the client software.

4.4. Types of certificates

There are several types of certificates. Confirmations can also be used in other situations, not only within the SSL protocol, but their use goes beyond the scope of this work.

4.4.1. Client SSL certificates

They are used to identify the client through the SSL protocol. It is common to identify the client's identity with a person. Except for identifying people when accessing a server, client certificates can be used for other purposes, e.g. for digitally signing digital forms.

Examples: 1. The bank gives the client a client SSL certificate that enables the bank server to identify the users and allows the use of a bank account. 2. An enterprise may provide each new employee with a client SSL certificate, which allows access to the enterprise server.

4.4.2. Server SSL certificates

They are used to identify the server by the client through an SSL protocol. Server identification is mandatory in the SSL protocol to achieve secure data transfer while client identification is not. Example: Internet business, e.g. online stores, most often use server identification through server SSL certificates to establish a secure SSL connection and convince users that it is the appropriate enterprise with which the user wants to do business. Encrypted SSL connections ensure that sensitive data sent across a network, such as credit card numbers, is protected.

4.4.3. Certificates of the issuer's certificate

They are used to identify the issuer's certificates. Client and server software uses certificates of the issuer's certificate to determine which other certificates can be trusted. This simplifies the work of both the client and the server, because it is sufficient to administer the work with only one certificate issuer, and it can be accessed by servers whose certificates are part of the system of that single certificate issuer. An example of the certificate of the issuer's certificate kept by the client decides which client will believe. The information system administrator within the company can organize a secure communication policy based on certificates from each user in the company. Examples of other types of certificates are S / MIME certificates that are used for digital signing and encryption

of e-mail, then certificates for signing objects that can serve as a confirmation that the software is sent via Internet, we are creating the product of the corresponding company.

4.5. Content confirmation

The content of the certificate used in the SSL protocol is organized according to the X.509 v3 specification for the certificates produced by the ITU. Users do not have to be overloaded with the content of the certificate, because the handling of them most often goes automatically. The primary task of the certificate is to verify the relationship between the public key and a specific entity (for example, individuals or businesses) designated by its own name. Thus, one of the more important data is the name of the holder of the certificate (distinguishedname). The name of the certificate holder is a structured set of attributes that uniquely describes the entity that identifies the certificate.

Typical confirmation: Each X.509 certificate consists of two parts: data and signature.

The data part contains:

- The serial number of the certificate that is unique to each certificate issued by that certificate issuer.
- Information about the user's public key, using the algorithm and the key itself.
- Name of the issuer of the certificate (structured as well as the name of the certificate holder).
- Validity period (eg between 1:00, 15/11/1998 and 1:00, November 15, 1999).
- The name of the entity, the bearer of the certificate.
- Additional, optional, data can provide useful information to either the client or the server.

The certificate signature part contains:

- The encryption algorithm, used by the publisher of the certificate for its digital signature.
- A digital signature, made on the basis of the control number obtained from all the data in the certificate, is encrypted with the private box of the issuer of the certificate.

5. CONCLUSION

Information technologies represent a very important factor (resource) in the process of strategic positioning of companies. The process of transition, which includes the processes of globalization and market integration, provides companies from our area to enter the foreign market, but at the same time it opens the boundaries of our country for the inflow of foreign capital, investments and products. In such an environment, enterprises, like the country and the economy themselves, must be transformed. A large number of information must be provided to the management team of the company in order to carry out the processes in the company at the optimum level.

Knowing the problem of protection of information systems through protection objects, threats, consequences, measures and risks are a precondition for the successful organization of the security of the information system itself by persons

dealing with this issue. So far, in all major conventions on the issue of security on the internet network, the most important problem is the man as a user, who is insufficiently addressed in the possibilities of using the security service, better education of users of information systems is necessary, and through organizational measures (an example that every employee has a pass ECDL and the like) and education in the basics of security, what this work contains in itself.

In addition to the above, the aim of this paper was to point out the obligation of data protection that is transmitted through the computer network and show the basic mechanisms for their protection. This work provides only the framework of cryptography, the use and significance of applied algorithms without specific examples of mathematical operations. As a science that is developing rapidly, with the development of computers, it is expected to upgrade and implement it in the security measures of modern information systems.

[1] Wirtz, J., Lwin, M.O., Williams, J.D .: Causes and consequences of consumer privacy online concern, International Journal of Service Industry Management, Vol. 18, No. 1 4, 2007, pp. 327.
[2] SSL protocol, http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt (November 2016)
[3] McRobb, S., Rogerson, S .: Are they really listening ?: An investigation into published online privacy policies at the beginning of the third millennium, Information Technology & People, Vol. 17, No. 1 4, 2004, pp. 443
[4] http://www.slideshare.net/majatodorovic980/zatita-i-sigurnost-u-elektronskom-poslovanju, (November 2016)

IMPACT OF NEW TECHNOLOGIES TO PROTECTION AND ROAD SAFETY

Prof. dr. sc. Sinan Alispahić, email: sinan.alispahic@iu-travnik.com; Doc. dr. Tihomir Đurić, email: mrdjtiho@teol.net; Hata Mušinović, hatka95@hotmail.com; Irfan Zec, irfan.zec@outlook.com

Abstract: *The purpose of this paper is to point out the importance of the impact of new technologies on protection and road safety. The use of certain technological solutions in practice has many advantages, but also shows a number of problems and phenomena that negatively reflect on the protection and safety in road traffic. The consequences of the application of new technology and communications solutions today are reflected in a growing problem distraction, and distraction to driving. The problem is present in all the frequent use of various technological devices, whose use during driving can be dangerous, affecting the safety of driving. Most often when driving using mobile devices to talk or write and read messages. A number of relevant research on the dangers of using mobile phones while driving a vehicle, which are discussed in the paper, indicating their deleterious effects on road safety. Implementation of new measures to protect participants, and first and foremost the driver while driving a vehicle requires a minimum standard and the adoption of the legislation, which will affect the reduction in risk and increase protection and security during driving.*

Keywords*: New technologies, communication devices, distraction, hazards, safety and security*