UDC 004.056 **doi: 10.26906/SUNZ.2022.4.122**

O. Shefer, E. Nikitchenko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

CYBER PROTECTION OF ENERGOIL ENTERPRISES

Abstract. This article is about providing comprehensive protection of the oil refining and distribution company ENERGOIL. This protection includes components such as encryption, anti-virus software, and user access matrices. Within the access delimitation system, a dispatcher must be used, which performs access delimitation. This dispatcher is an employee of the security department. Access is restricted in accordance with the authority of employees. A request for employee access to a specific computer is sent to the database management and event registration unit. The authority of the employee and the characteristics of the object are analyzed by an employee of the security department. The first basic step for organizing work computers at the enterprise will be the creation of user accounts. For this, we create our own account for each computer A user access matrix was developed for the ENERGOIL enterprise, divided by information departments. It is necessary in order to clearly understand which users have access to which. The Triple DES algorithm was used for encryption. The essence of the algorithm is to use the Data Encryption Standard, or simply DES, published by the US National Bureau of Standards (NBS). First, the data is encrypted with the first key, decrypted back with the second key, and re-encrypted with the third key. Since as many as three keys are used, their total length is actually 3 * 56 = 168 bits. The encryption speed is also lower than that of the DES algorithm, but the reliability leaves no doubt. It takes a billion times more attempts to break this encryption than simple DES. Avast and Microsoft Windows Defender antiviruses were used to protect against malicious software, and an access matrix with user accounts and their permissions was created to limit access on work computers.

Keywords: cyber security, encryption, algorithm, Triple DES, access.

Introduction

Information protection is one of the eternal problems. Throughout human history, the ways to solve this problem were determined by the level of technological development. In today's information society, technology plays the role of an activator of this problem – computer crimes have become a characteristic feature of today.

Crimes related to interference with the work of a computer and crimes in which computers are used as necessary technical means are called computer crimes.

Among the causes of computer crimes and related theft of information, the following are the main ones:

- rapid transition from the traditional paper technology of information storage and transmission to the electronic one, at the same time lagging behind technologies for protecting information recorded on machine media;
- widespread use of local computer networks, creation of global networks and expansion of access to information resources;
- constant complication of software tools, which causes a decrease in their reliability and an increase in the number of vulnerabilities. [2]

Today, no one can give an exact figure for the total losses from computer crimes, but experts agree that the relevant amounts are measured in the billions of dollars.

Among the main articles, the following should be highlighted:

- losses caused by the situation when employees of the organization cannot perform their duties due to system (network) failure;

According to the Law of Ukraine "On the Protection of Information in Automated Systems", information protection is a set of organizational and technical measures and legal norms to prevent harm to the interests of the owner of the information or OS and persons who use the information. Related terms

- monetary value of stolen and compromised data;
- costs of restoring the system, checking its integrity, fixing vulnerable areas, etc.

The importance of the problem of data protection in enterprises cannot even be doubted due to the fact that with the knowledge of technologies and opportunities to rob the company – someone will definitely take advantage of it - either internally or externally.

It is also worth considering the moral and psychological consequences for users, staff and owners of IC and information. As for the violation of the security of so-called "critical" applications in state and military administration, atomic energy, medicine, the rocket and space industry, and in the financial sphere, it can lead to serious consequences for the environment, the economy and the security of the state, health and even for people's lives.

Economic and legal issues, private and commercial secrecy, national security – all of this dictates the need to protect information and IS.

Ensuring the security of information technologies is a complex problem that includes legal regulation of IT use, improvement of technologies for their development, development of the certification system, and provision of appropriate organizational and technical conditions for operation. Solving this problem requires significant costs, so the first priority is to correlate the level of necessary security and the costs of its support. To do this, it is necessary to determine potential threats, the probability of their occurrence and possible consequences, choose adequate means and build a reliable corporate threat protection system [2]. "information security" and "information technology security" are also used in the literature [2].

Application of cryptography

Nowadays, cryptography is used everywhere and is considered the most advanced means of protecting information. What causes it? Ciphers work at the lowest level of protocols - the bit level. New ways and methods of protecting information from changes and unauthorized interference during transmission, processing and storage are being developed every day, and ciphers are the most common means of keeping information safe.

Modern cryptography is based on mathematical methods of information protection. Its task is to use mathematical transformations or algorithms to reconstruct the text of the message (plaintext) into a disordered and meaningless (ideally, completely random) sequence of symbols, or ciphertext, which can be transmitted over an open channel. To reproduce the plaintext, the recipient performs decryption - the reverse transformation of the received ciphertext.

The encryption algorithm is generally considered open, that is, known to everyone. Secrecy of the procedure is ensured by the use of cryptographic keys - a set of symbols that act as parameters of mathematical transformations. The key is used for both encryption and decryption of the message. Depending on the type of encryption algorithm, the sender's and receiver's keys can be interdependent, correlated (with symmetric encryption) and different (with asymmetric, i.e., open encryption).

A set of encryption and decryption algorithms and all possible plaintexts, ciphertexts and keys is called a cryptosystem. Cryptography is closely related to cryptanalysis - the art of deciphering, or "breaking", ciphertext. This requires a reliable security system, which is unique for each company, otherwise it would be easy to hack them.

Violation of the procedure for cryptographic protection of information by business entities, institutions, organizations, positions. persons, citizens shall be punished in accordance with the legislation of Ukraine [5].

The main part of the article

A modern private enterprise is faced with the issue of ensuring the protection of information that circulates in the enterprise. The analysis of scientific publications gives reason to claim that in connection with the increase in information flows at the enterprise, it is necessary to create an information protection service. Currently, the protection of information is more and more relevant to business entities that need to protect themselves from the leakage of their information.

Comprehensive protection of information in information and telecommunication systems involves the use of special legal, physical, organizational, technical and software and hardware means of information protection. Control over the above measures, responsibility for their implementation and implementation is entrusted to the information protection service of the enterprise. legal norms of information security [6].

Company description. ENERGOIL (Fig. 1) is a private oil refining company specializing in the production and distribution of oil in Ukraine. Petroleum products are extracted and stored in the company's warehouses, while the head office handles the main important components of the business, such as management, accounting (spent and received) and delivery logistics. The main office is located in the city of Ivan-Frankivsk, Berehova street, bldg. 34.

Fig. 1. ENERGOI

The company provides the following services:

- supply of oil and products of its processing;
- management and calculation of oil consumption;
- effective conversion of oil into electricity;
- development of oil production methods;
- management and efficient sale of oil.

General cyber protection plan. The facility's security system is created to prevent unauthorized access to the territory. The object on which work with confidential information is conducted has a hierarchy of protection boundaries (territory – building – premises – information carrier – program – confidential information).

Scheme of computers arrangement (Fig. 2). In total, the building will have 64 computers, switches and all the necessary server equipment to provide the company's own server network.

Protection of the territory and premises of the company. First of all, protection of the premises itself and the equipment located in it is created. The main components that will be installed to protect the enterprise from possible threats:

- security alarm designed to detect attempts to enter the protected territory;
- engineering structures designed to create obstacles to the penetration of intruders (reliable doors, bars on windows);
- means of continuous surveillance implemented with the help of television video surveillance systems;
- organization of control of access to the territory of the object by identification using cards.
- soundproofing of premises
- installation of a backup power supply unit

Protection of information within the premises of the company. Access to information on specific computers will be limited as follows. The following persons have access to the computer of ordinary employees:

- the employee himself;
- head of the security department;

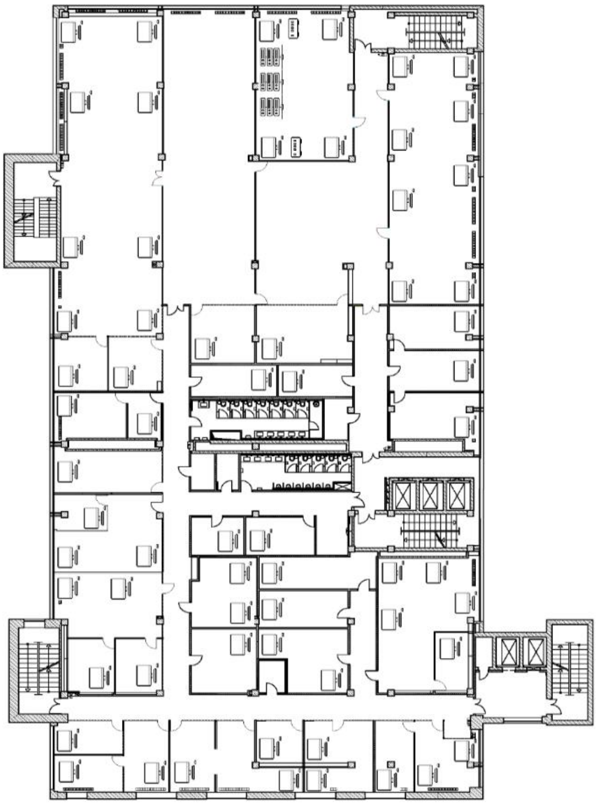


Fig. 2. Building scheme

- chief system administrator;
- company director.

Server room computers have access to:

- system administrator;
- head of the security department;
- company director.

Only the director himself has access to the company director's computer.

Within the access delimitation system, a dispatcher must be used, which performs access delimitation. This dispatcher is an employee of the security department. Access is restricted in accordance with the authority of employees. A request for employee access to a specific computer is sent to the database management and event registration unit. The authority of the employee and the characteristics of the object are analyzed by an employee of the security department. As a result, it gives a signal of permission or denial of permission ("Allow", "Reject"). If the number of "Refuse" signals exceeds a given level (for example, three times), which is fixed by the head of the security department, the dispatcher gives the "Unauthorized access" signal. Based on this signal, the system administrator blocks access to the computer until the reasons for unauthorized access are determined (Table 1).

Duties of employees to protect information at the enterprise:

- Responsible for alarm management: Security department.
- Responsible for unlocking and locking doors: Security department.
- Responsible for checking the backup power supply unit: Security department.

Table 1 – **User accounts of enterprise workers**

Office	Login	Password
IT Department	server1	5454322
Secretary	sek1	it13u22
Director	dir	it2rt322
Accounting	buhg3	it3re322
Human Resources Dept	kadr4	it4wf322
Dept of economists	ekon5	it53rr22
Lawyer	yuris1	sedfse77
Storage	stora32	gnid235
Sales dept	prod1	madir55
Logistics dept	progn1	bsdfh1sa
Planning dept	plan23	ssdhy234
Security dept	secr2342	bfsd432c
Cooperation dept	coopewl1	auh5sde

- Responsible for access restriction: Dispatcher from the security department.
- Responsible for product distribution: Logistics department.
- Responsible for cryptological protection of information: IT department.
- Responsible for checking the functionality and security of work computers: System administrator of the IT department.

Accounts of all users at enterprise (Table 2)**.** The first basic step for organizing work computers at the enterprise will be the creation of user accounts. For this, we create our own account for each computer

A user access matrix was developed for the ENERGOIL enterprise, divided by information departments. It is necessary in order to clearly understand which users have access to which.

At the enterprise, the access matrix has a division of information into types (6 of them in total) and the type of access to it. Types of access are used:

- R – More viewing information;
- RW – View and change information.

Data encryption at the enterprise. Although it is officially known as the Triple Data Encryption Algorithm (3DEA), it is more commonly referred to as 3DES. This is because the 3DES algorithm uses the Standard Encryption Standard (DES) cipher three times to encrypt its data.

DES is a symmetric key algorithm based on the Feistel network. As a symmetric key cipher, it uses the same key for both the encryption and decryption processes. The Feistel network makes both of these processes almost identical, resulting in a more efficient implementation of the algorithm [3].

DES has a 64-bit block and key size, but in practice the key provides only 56-bit security. 3DES was developed as a more secure alternative due to the short length of DES keys. In 3DES, the DES algorithm is performed three times with three keys, but it is only considered secure if three separate keys are used.

As the security weaknesses of DES became more apparent, 3DES was proposed as a way to increase its key size without building an entirely new algorithm. Instead of using a single key like DES, 3DES runs the DES algorithm three times, with three 56-bit keys.

- The key one is used to encrypt plain text.

Table 2 – **Accounts of all users at enterprise**

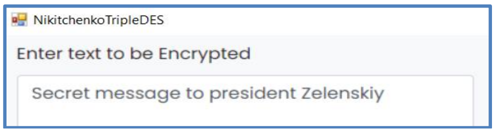
Department	Types of information					
	Not secret	Secret			Official use	
	General	Private	Financial	Legal	Technical	Personnel
IT Department	RW	RW	RW	RW	RW	RW
Secretary	RW	R	-	RW	-	RW
Director	RW	R	R	-	-	R
Accounting	R	-	-	-	RW	RW
Human Resources	R	-	-	-	RW	R
Economists	R	-	-	-	RW	R
Lawyer	R	-	-	RW	RW	R
Storage	R	-	-	-	RW	R
Sales dept	R	-	-	-	RW	R
Logistics dept	R	-	-	-	RW	R
Planning dept	R	-	-	-	RW	R
Security dept	R	-	-	-	RW	R
Cooperation dept	R	-	-	-	RW	R

- The second key is used to decrypt the text that was encrypted by the key.
- Key three is used to encrypt the text that was decrypted with the third key.

Encryption algorithms use keys to add data that will change the final result of the process. If DES only involves steps like permutation and S-boxes (permutation is explained below, while S-boxes are covered in the Substitution section), all an attacker has to do is reveal the details of the algorithm and then do each step in reverse order to reveal the original message [7].

Presentation of the application

After starting the program, we see a window where you can immediately start working with encryption. We enter the text that we want to encrypt (Fig. 3).



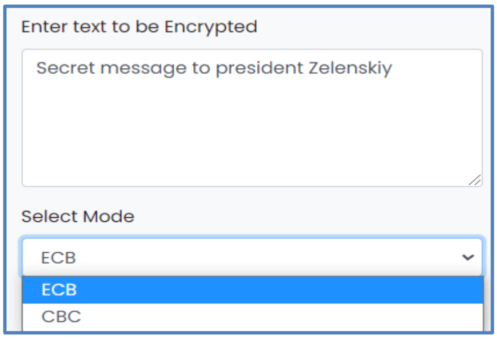
NikitchenkoTripleDES

Enter text to be Encrypted

Secret message to president Zelenskiy

Fig. 3. Enter the text to be encrypted

Then choose the ECB or CBC encryption type. (Fig. 4). ECB stands for Electronic Code Book, while CBC stands for Cipher Block chaining. ECB is suitable for encryption small messages, while using CBC we can encrypt a large message. Usuallyit is used the CBC encryption at the enterprise, but this time it will be enough to use ECB.



Enter text to be Encrypted

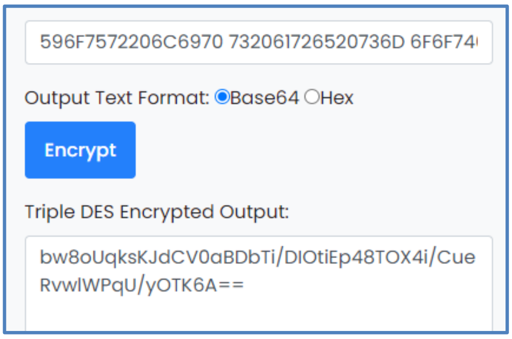
Secret message to president Zelenskiy

Select Mode

ECB

Fig. 4. Selection of entering the type of keys for encryption

We enter the encryption key and the type of cipher text at the output (it is not so important which one we choose, so we leave Base64). In Triple DES, it consists of three sets of keys. It can be three different sets, 2 the same and one different, or three identical sets of characters. The most effective is a set of three different keys, so we will use it (Fig. 5). To decrypt the received text, we take our pre-encrypted message and insert a field to decrypt the text, and specify the type of the entered encrypted message (in this case, Base64) (Fig. 6). Set the same settings and necessarily the same key that was used to encrypt the initial message. (Fig. 7).



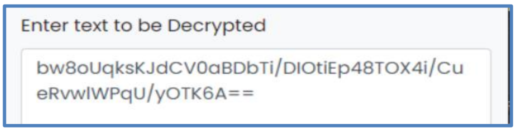
596F7572206C6970 732061726520736D 6F6F74

Output Text Format: ●Base64 ○Hex

Triple DES Encrypted Output:

bw8oUqksKJdCV0aBDbTi/DIOtiEp48TOX4i/CueRvwlWPqU/yOTK6A==

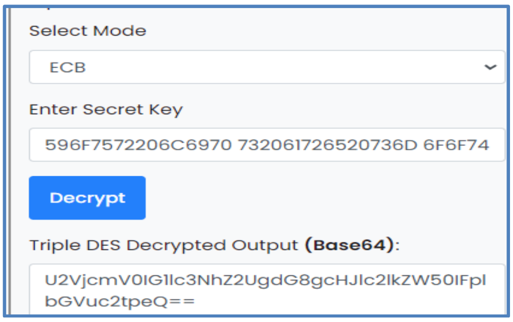
Fig. 5. The message is encrypted with the TDES algorithm



Enter text to be Decrypted

bw8oUqksKJdCV0aBDbTi/DIOtiEp48TOX4i/CueRvwlWPqU/yOTK6A==

Fig. 6. Decryption text field



Select Mode

ECB

Enter Secret Key

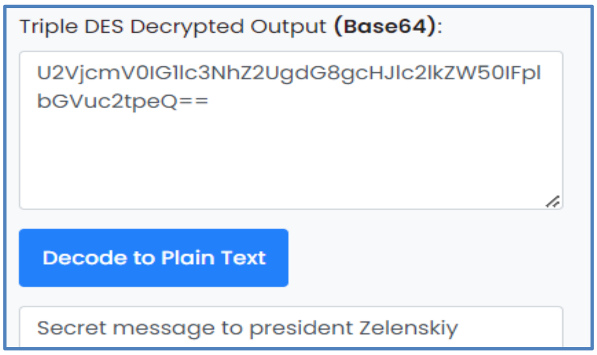
596F7572206C6970 732061726520736D 6F6F74

Triple DES Decrypted Output **(Base64)**:

U2VjcmV0IG1lc3NhZ2UgdG8gcHJlc2lkZW50IFplbGVuc2tpeQ==

Fig. 7. Decryption settings

At the output, we have a message that, after being translated into plain text, is displayed on the screen and also written into a separate text file named "TripleDESdecrypted.txt" (Fig. 8).



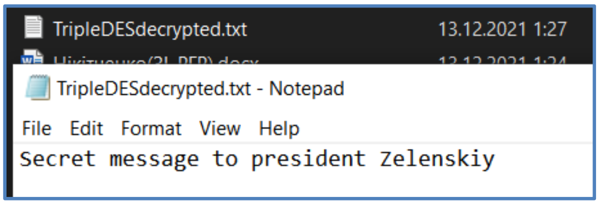
Triple DES Decrypted Output **(Base64)**:

```
U2VjcmV0IG1lc3NhZ2UgdG8gcHJlc2lkZW50IFpl
bGVuc2tpeQ==
```

Secret message to president Zelenskiy

Fig. 8. The message is decrypted

At the end, this decryption is written to a file in the form of a simple message (Fig. 9).



TripleDESdecrypted.txt 13.12.2021 1:27

TripleDESdecrypted.txt - Notepad

```
Secret message to president Zelenskiy
```

Fig. 9. The decrypted message is written to the file

Conclusions

The organization of information protection at the ENERGOIL enterprise is all the measures taken to prevent the leakage of information that should not be known to outsiders. They concern both software and hardware. For the enterprise, a system has been created so that access to each specific computer is only available to a limited number of persons, such as employees in their own positions and system administrators. A password system and mandated access model were created. Information protection was also ensured at the registration levels with the help of basic programs understandable to ordinary users.

To protect against virus threats, the appropriate antivirus was selected, taking into account such characteristics as price, quality for its price, downloads to working machines, program efficiency and the size of virus databases, as well as their update frequency. For data encryption, an application based on the TDES algorithm was created, it was tested for encryption and decryption of a simple message. Triple DES cannot be called the best of all encryption algorithms in our time, but it is easy to use and quite reliable, because it is a complex version of another DES algorithm, which was previously accepted as a standard.

All comprehensive security measures for the ENERGOIL enterprise have been taken into account to provide adequate protection of information to the enterprise.

References

1. Data encryption using the XOR cypher G. Golovko, A. Matyashenko, N. Solopikhin - journal "Control, Navigation and Communication Systems". 2021. 81 p.
2. Technologies of information protection (UZHNU), URL - https://www.uzhnu.edu.ua/uk/infocentre/get/4186
3. TripleDES class and its implementation, URL - https://learn.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.tripledes?view=net-6.0
4. Triple data encryption algorithm, URL - https://wikicsu.ru/wiki/triple_des
5. Cryptography (Encyclopedia of modern Ukraine), URL – https://esu.com.ua/search_articles.php?id=1576
6. Requirements for information protection services at enterprises, URL - http://pyuv.onua.edu.ua/index.php/pyuv/article/view/607
7. Analysis of the TDES encryption algorithm, URL - https://instagalleryapp.com/informacijna-bezpeka/shho-take-shifruvannja-3des-i-jak-pracjue-des/

Received (Надійшла) 05.09.2022
Accepted for publication (Прийнята до друку) 09.11.2022

Кіберзахист підприємства ENERGOIL

О. Шефер, Є. Нікітченко

Анотація. У статті йдеться про забезпечення комплексного захисту компанії по переробці та дистрибуції нафти ENERGOIL. Захист включає в себе такі компоненти, як шифрування, антивірусне програмне забезпечення та матриці доступу користувачів. У системі розмежування доступу обов'язково використовується диспетчер, який здійснює розмежування доступу. Запит на доступ співробітника до конкретного комп'ютера надсилається до підрозділу управління базами даних та реєстрації подій. Повноваження співробітника і характеристики об'єкта аналізуються співробітником служби безпеки. Першим основним кроком для організації роботи комп'ютерів на підприємстві буде створення облікових записів користувачів. Для цього створюється свій обліковий запис для кожного комп'ютера Для підприємства «ЕНЕРГОІЛ» розроблена матриця доступу користувачів, розділена на інформаційні підрозділи. Це необхідно для того, щоб чітко розуміти, які користувачі до чого мають доступ. Для шифрування було використано алгоритм TripleDES. Суть алгоритму полягає у використанні опублікованого Національним бюро Стандартів США (NBS) стандарту шифрування даних Data Encryption Standard, простіше кажучи DES. Спочатку дані шифруються за допомогою першого ключа, розшифровуються назад другим ключем та зашифровуються повторно третім. Оскільки використовуються аж три ключі, фактично їхня сумарна довжина 3 * 56 = 168 біт. Швидкість шифрування також менша ніж у алгоритму DES, зате надійність не залишає ніяких сумнівів. Для взлому такого шифрування необхідно в мільярд разів більше спроб, ніж для простого DES. Для захисту від шкідливого програмного забезпечення було використано антивіруси Avastта Microsoft Windows Defender, а а для розмежування доступу на робочих комп'ютерах, було створено матрицю доступу з аккаунтами користувачів та їх дозволами.

Ключові слова: кібербезпека, шифрування, алгоритм, TripleDES, доступ.