CREATING AN INFORMATION SYSTEM FOR A POLICE OFFICE AND CRYPTOGRAPHIC PROTECTION OF ITS INFORMATION

Ilhan Istikbal Ibryam
Konstantin Preslavsky University of Shumen, Faculty of Mathematics & Informatics, Republic of Bulgaria
i.ibryam@shu.bg
Byulent Mustafa Mustafa
Konstantin Preslavsky University of Shumen, Faculty of Mathematics & Informatics, Republic of Bulgaria
byulent_mustafa@abv.bg
Atti Rashtid Mustafa
Konstantin Preslavsky University of Shumen, College in Dobrich, Republic of Bulgaria atti_mustafa@abv.bg

Abstract: Information systems for the service of the small settlements in the Republic of Bulgaria and their adjoining territory are not designed and integrated everywhere at the Ministry of Interior (MOI). Therefore, this article considers an option for building such an information system that would be useful for the activity of a micro-district police office.
After the analysis, we have come to the conclusion that the manual information processing is not efficient with regard to the processing time and at the same time a greater number of human resources are involved in the process. By creating such an information system, the time spent on storing and processing information would be significantly shortened. Undoubtedly, this would have a positive impact on the workload of police officers in smaller settlements. The integration of the information system in regions does not mean that it will result in state cuts. On the contrary - the tasks of the corresponding staff would be redistributed and the officers would do much more of their duties and they would do them more efficiently. By means of the modern information technologies, an optimal solution to arising problem situations is sought, namely in such services to the Ministry of Interior (MOI). A detailed analysis of the documents, by means of which this information is processed, is done. It includes requests such as document validation forms, requests for access to information, etc. According to the DB-Engines chart for November 2017, the Microsoft Access database management system ranks eighth (that is, the top 10) compared to the other 337 systems. Another IT Career Success rating also identifies Microsoft Access in the top 10 of database management systems. In this chart it is in ninth position. The capabilities of Microsoft Access 2016 have been analyzed compared to the previous versions of the information systems design. This environment is discussed in greater details in the discipline of Databases and Applications and it is namely this that is used to build the information system described in the article. In order to limit data from unauthorized access, we have used cryptographic protection. It has been created with a PHP scripting language with a syntax based on C and Perl. The algorithm of the encryption and decryption software that we have used is effective and successfully passed the statistical tests with the National Institute of Standards and Technology (NIST) for resistance to attacks.
Keywords: information systems, databases, cryptographic protection, encryption, decryption

1. INTRODUCTION

The development of police as an institution in Bulgaria starts after Turnovo Constitution was acceted /16.04.1879/. With Decree № 1 of Alexander I of July 5th 1879 The Ministry of Inner Affairs was created as a part of the first Bulgarian government. The first Bulgarian minister of inner affairs was Todor Burmov.
The basic spheres of activity of this ministry are: inner affairs and administration, people's health; veterinary affairs, post offices and telegraph management. The police functions are fulfilled by an administrative-police department in the Ministry of Inner Affairs and the connected institutions. In the beginning the ministry used to be loaded with tasks not typical for it, e.g. veterinary affairs that are removed in 1893; post offices management that ends in 1882; and social affairs in 1885. [1]
Undoubtedly during the years since its creation the activities of its officers have been overloaded in administrative aspect. Processing and storage of a large volume of documents at that time had probably been time consuming process taking months, may be years of hard work. When information technologies penetrate these structures of the country information processing becomes a much faster process. This process is dependent on technology which can be used, the remote access to information and risks in relation to its completeness and secrecy. According to the National Statistical Institute of the Republic of Bulgaria about the Bulgarian population as of 31.12.2016 is 5 204 385 people. [2]. This population is not evenly distributed in the territory. The majority of people inhabits

bigger administrative cities. The reason for this is the opportunity for better paid job and the better living conditions. But there are also found more crimes. Accordingly in the Police Stations in the bigger cities there are integrated information systems connected to the internet in order to provide opportunities for more adequate reactions in concrete situations. On the other hand this does not allow us to maintain that in the little towns and villages (population under 20 000 people) there are not crimes. On the contrary, on paper there are stored registered crimes of the following types:

- ✓ crimes against property;
- ✓ crimes against personality;
- ✓ crimes connected to services;

In order to receive reference about a crime fulfilled information about a person connected to a presumable crime, it is necessary to research a great number of files full of documents which is difficult for the officers in the police stations in the small and far away places and regions in the country. In this article we present a variant of infrmation system for a police station that will be useful if introduced in the small and far away regions.

2. EXPOSITION

For creating the information system (fig. 1) we have used a Microsoft product – MS Access. In the abstract we have motivated the choice of this medium for database management systems. The tables store information about:

- ✓ staff (including ID number, names, address, contact telephone number, position, service region, determined by him (code of the crime, date of crime fulfillment));
- ✓ crimes (including code of the crime, type of the crime);
- ✓ region-microregion (code of the region, location, code of the area); etc.

Figure 1. Information System *Police Station* created by means of MS Access

After performing data normalization (the data attributes are grouped in tables), the corresponding relations between the tables in the system are performed. In the information systen the majority of relations are of the type "one to one" (1:1), "one to many" (1:M) and "many to many" (M:N). For access to the information in the database we have created forms by means of the object "Forms". For all references concerning the information system it is necessary to build the corresponding requests to the database. Most applications for work with database provide the user with relative easy ways for creating data extracts comprehensible for him/her, collected from a few tables. [3]. In this case we have used requests in a few criteria as well as parametrical requests. Microsoft Access gives opportunities for these requests‘ performance result to be provided in the form of reports that can be safed on an electronic device as well as printed out on paper by means of the print buttons created in the forms. They have to be well defended no matter of the store type (electronic device or paper). Tha hard (paper) copy can be stored in various types and sizes

of safes. For the safety of the electronic reports (fig. 2) we offer a varient for crypting it. The cryptographic algorythm is a mathematical function (one of which parameters is called a key), which is used for crypting and decrypting. In order to crypt an open text, a crypting algorythm is applied to it. In order to crypt a ciphered text, a decrypting algorythm is applied to it. [4]. For generating keys we use a Tinkerbell's cart, which is recursively defined as (1):

$$u_{m+1} = u_m^2 - v_m^2 + au_m + bv_m$$
$$v_{m+1} = 2u_m v_m + cu_m + dv_m \quad (1)$$

where $a = 0.9$, $b = -0.6013$, $c = 2.0$ and $d = 0.50$.

By means of this method we provide a more reliable way of defending information.

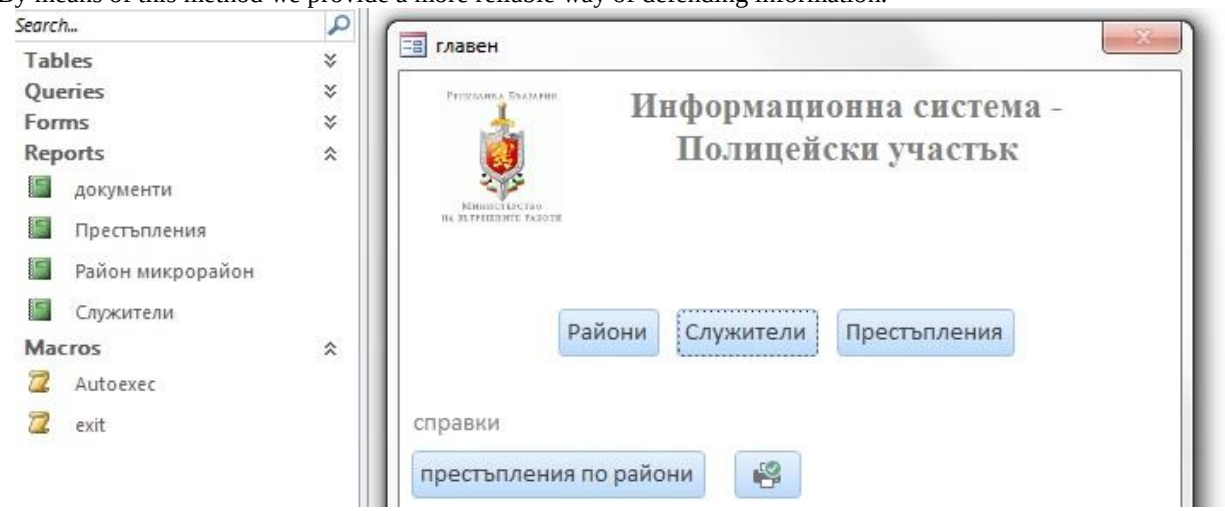


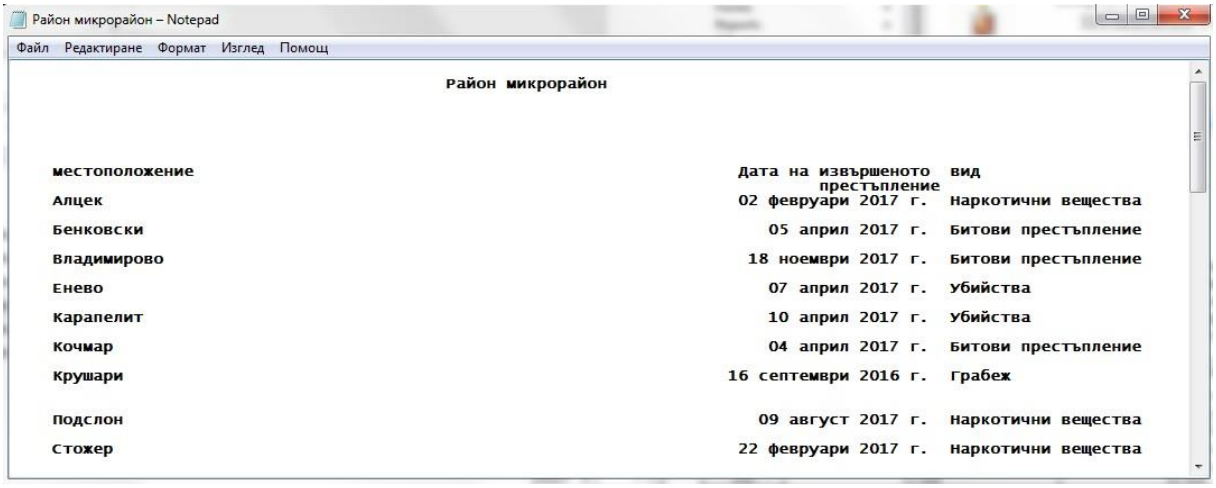
Figure 2. Reports from the information system

The reports created by means of Microsoft Access 2016 can be exported in excel, rtf, pdf or xps files, text files, xml file and html document. The report Region-Microregion is exported in the formats rtf, pdf, xps, txt, xml and html. A comparative charasteristic of the size of the file in its various formats is made before and after crypting it. The length of time necessary for the cryptographic algorythm is analyzed. The best results are reached when the file is exported in txt format (Table 1).

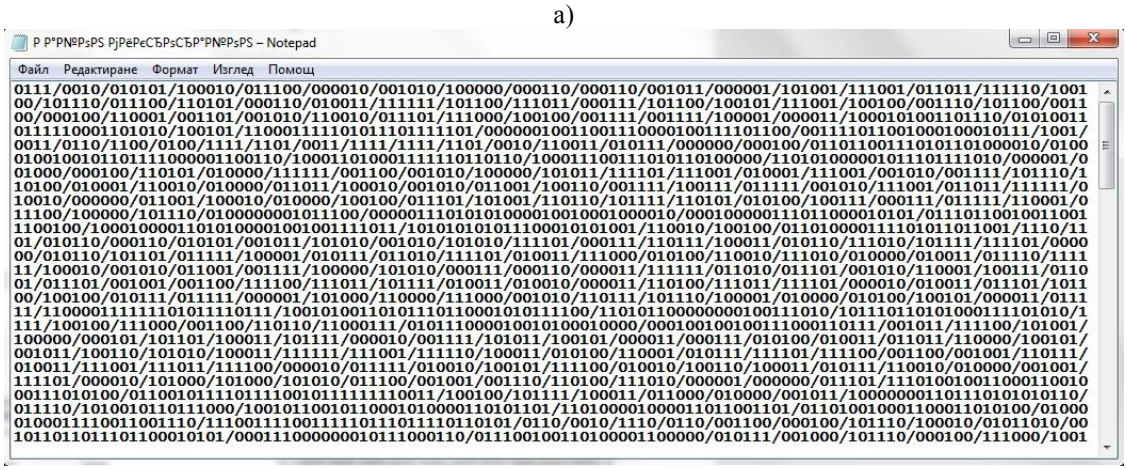
Table 1.

File format	Size of the file before cripting it	Size of the file after cripting it	Times more
html	8 KB	59 KB	7,38
pdf	93 KB	746 KB	8,02
rtf	6 KB	38 KB	6,33
txt	2 KB	11 KB	5,50
xml	11 KB	82 KB	7,45
xps	99 KB	784 KB	7,92

Figure 3 a) presents the report after exporting it in a txt format and Figure 3 b) – also in txt format, but with changed content. In the second case the file is already crypted.



a)



b)

Figure 3a) Data exported from report of database and a crypted variant of the file – 3 b).

The diagram on Figure 4) shows the initial content of the symbols (in red), and the crypted variant is shown in green.

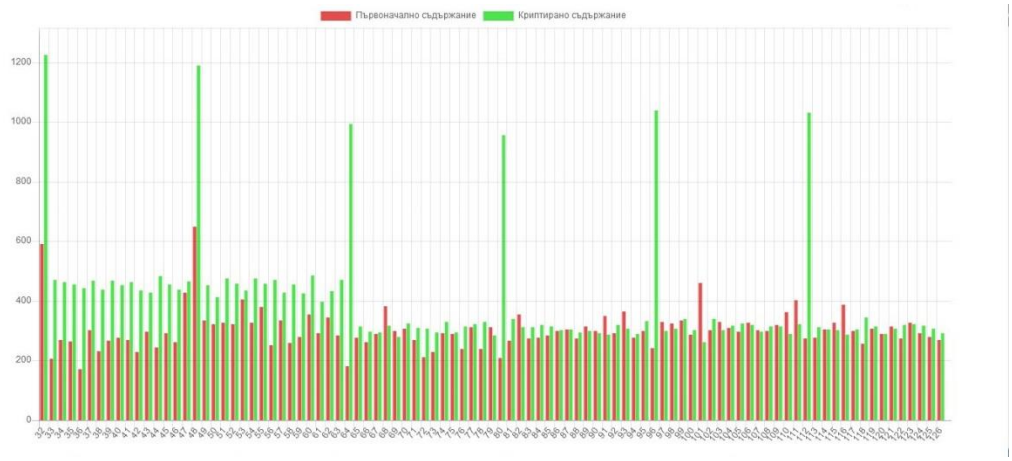


Figure 4) Diagram with initial and crypted content of the symbols

3. CONCLUSION

- ✓ Creating an information system for the needs of The Ministry of Inner Affairs in the small regions requires detailed analysis of the documentation, the parameters of the personal computers and the opportunities of the technical facilities available. Last but not least, they have to possess the corresponding licenced software.
- ✓ The management of the information security concerns all organizations, icluding the structures of The Ministry of Inner Affairs The Ministry of Inner Affairs.
- ✓ For information defence various cryptographic algorythms can be used. They have to be tested for stability agains attacks by means of statistical tests of the National Institute of Standards and Technology (NIST), Statistical Package for Social Science (SPSS), etc.

REFERENCES

[1] https://www.mvr.bg
[2] http://www.nsi.bg
[3] Роман, С. Access бази данни. Проектиране и програмиране., Издателство „O'REILLY", стр. 51, София, 2003.
[4] Целков, В., Стоянов, Н. Защитени криптографски приложения в компютърните системи и мрежи, поредица"Защита на информацията", Издателство "Нова звезда" стр. 31, София, 2009