Институт информационных и вычислительных технологий МНВО РК

МАТЕРИАЛЫ

VII международной научно-практической конференции
"Информатика и прикладная математика",
20 октября - 21 октября 2022, Алматы, Казахстан

Алматы 2022

УДК 378 (063)
ББК 74.58
И74

И 74 **Информатика и прикладная математика:** Мат. VII Межд. науч. конф. (20 октября -21 октября 2022 г.). Алматы, 2022. – 404 с.

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные ученными Республики Казахстан, стран ближнего и дальнего зарубежья. (Кыргызской Республики, Российской Федерации, Турции и др.)

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

DEVELOPMENT OF A MODEL OF AN INTEGRATED INFORMATION SECURITY SYSTEM AT THE ENTERPRISE

Akhmetova A., Shayakhmetova A., Sultangazieva A., Zhamuratova M.
e-mail: asemshayakhmetova@mail.ru

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2] Astana International University, Astana, Kazakhstan
[3] Satbayev University, Almaty, Kazakhstan

Abstract. *Decision-making in all spheres of life of an enterprise or organization is increasingly based on information processes. The analysis of these processes with the subsequent development of control solutions is carried out on the basis of information models based on modern information and telecommunication technologies. Therefore, the protection of information is an independent component of the security of the enterprise as a whole, the importance of which increases every year. In this regard, many solutions are being implemented. One of them is an IoT-based implementation, i.e. systems of objects mounted on sensors and software installed for data collection and exchange, with the possibility of remote monitoring and control in automated mode. The article implements the development of a model of an integrated information security system at an enterprise based on a leak sensor and a fire sensor*

Keywords. *IoT, information security, integration system, ESP 32 controller, fire sensor*

1. Introduction

The modern stage of informatization, now digitalization, is associated with the creation of personal electronic computers, telecommunications systems, computer networks and IoT systems. There is an increasing need to develop and apply effective solutions in the information sphere. He is engaged in technical and software, production of information technologies for obtaining new knowledge [1].

At a certain stage in the development of the information industry, there is an information society in which many employees work by producing, storing, processing and implementing information, i.e. creative work is aimed at intellectual development and knowledge acquisition. The information community of people not divided into national borders [2].

The formation of the information society is based on the latest information, telecommunication technologies, communication technologies and now on IoT systems [4]. New technologies that have led to the accelerated spread of global information networks, which opens up fundamentally new opportunities for international information exchange. The formation of the information society implies the formation of a conceptual and practically global information space [5].

The development of the information society, along with creative opportunities, leads to an increase in security threats associated with the violation of established modes of use of information and communication systems [6]. The rights of citizens, the spread of malware and the use of modern information technologies for hostile, terrorist and other criminal activities. To create a unified information chain of an enterprise, an Ios system is needed that accumulates information about incidents from various sources, warns the security service

about existing and potential threats and takes into account patterns between different threats [7].

The problem statement is formed as follows: automation of the integrated security system model at the enterprise based on IoT.

To implement the task, it is necessary to perform the following tasks:

To analyze complex security systems at the enterprise;

Development of IT security system at the enterprise;

Development of an algorithm for an integrated enterprise security system;

Development of a model of an integrated enterprise security system.

To begin with, we will give a generalized architecture of the functioning of the system (Fig.1).

2 Development of the algorithm and architecture of the system

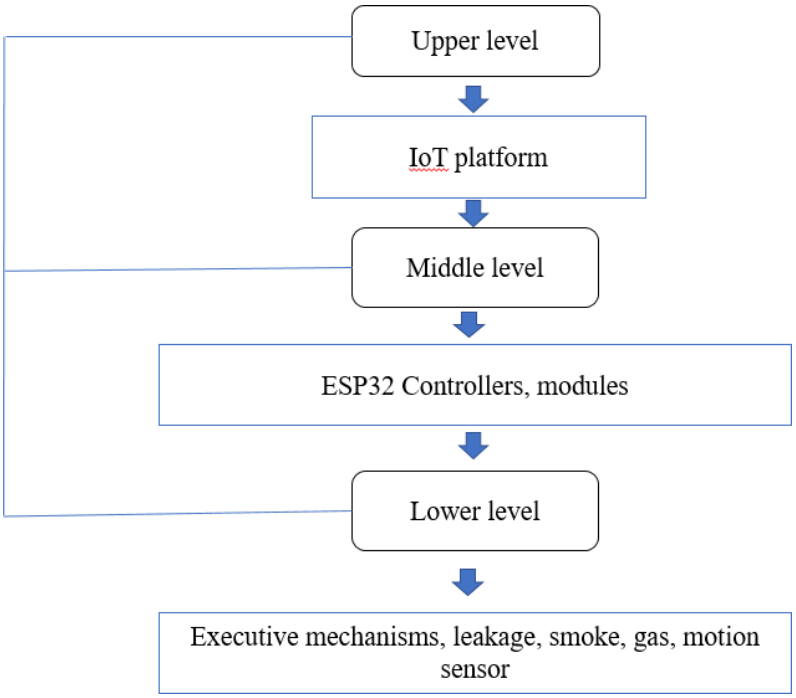

Fig. 1. Architecture of system

The system outlines the principle of interaction of three levels. The upper level is represented by the Ios platform, the middle level is represented by the ESP 32 controller and modules, the lower level consists of an actuator, a leak sensor, smoke, gas and motion.

Next, we present the algorithm for the functioning of the system (Fig.2).

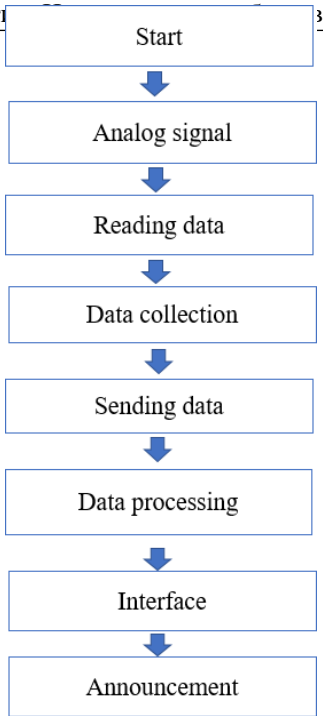

Fig. 2 The algorithm of the system

Step 1. Information from the external environment is perceived and converted into an analog signal.

Step 2. Data is being read.

Step 3. The data collection process is underway.

Step 4. The collected data will be sent.

Step 5. The received data is processed.

Step 6. The result is displayed as a message via the interface.

Automation of the integrated information security system model at the enterprise

Figure 3 shows the board used in the automation of the integrated enterprise information security system model.

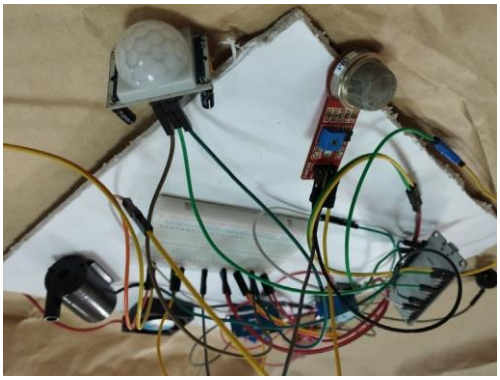

Fig. 3. Board

The water sensor used in the automation of the integrated information security system model at the enterprise is shown in Figure 4.

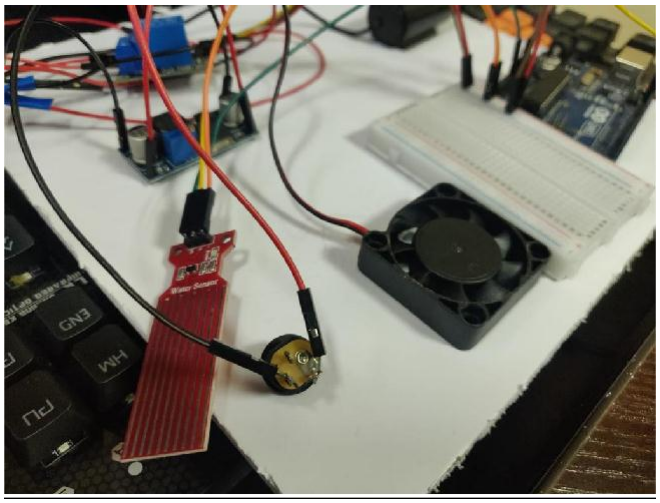

Fig 4. Water sensor

Figure 5 shows the preparation of the model during the automation of the integrated information security system model at the enterprise.

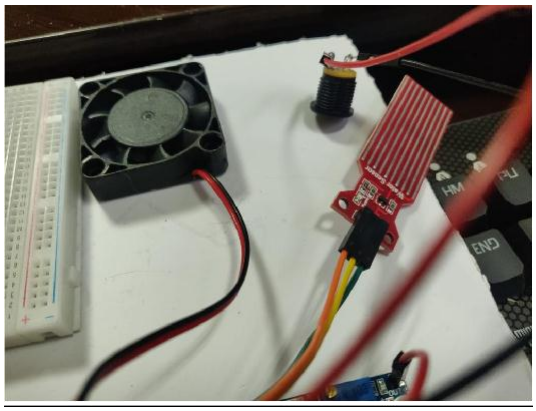

Fig 5. The process of preparing the model

3.1 The program of the integrated information security system at the enterprise

The program view of the integrated information security system program at the enterprise in the Arduino environment is shown in Figure 6.

Fig 6. Program view

When water gets on the water sensor, a change occurs as a result of the program, as shown in Fig. 7.

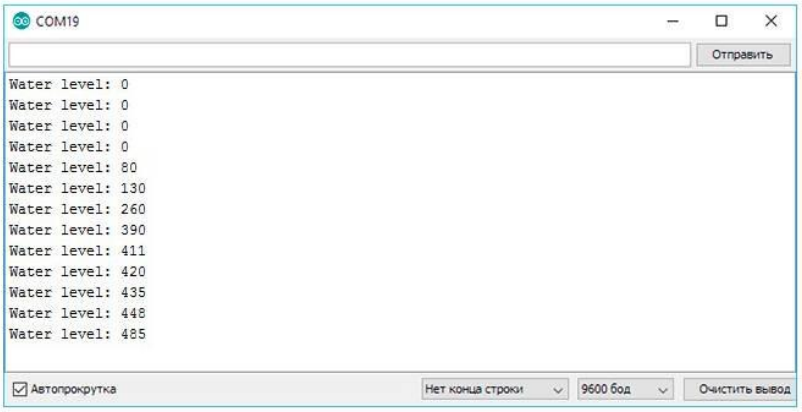

Fig 7. Result

The principle of operation of the integrated information security system model at the enterprise is shown in Figure 8.

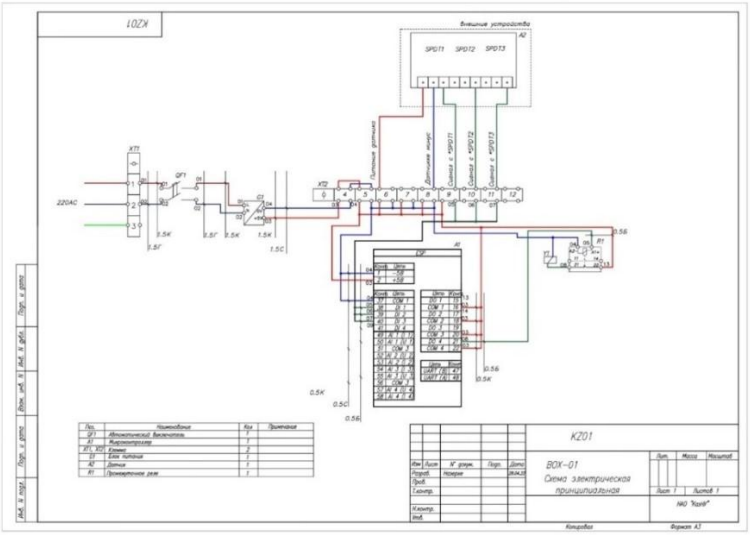

Fig 8. The principle of operation

3.2 The result of the integrated information security system model at the enterprise

The result of the integrated information security system model at the enterprise is shown in Figures 9 and 10.

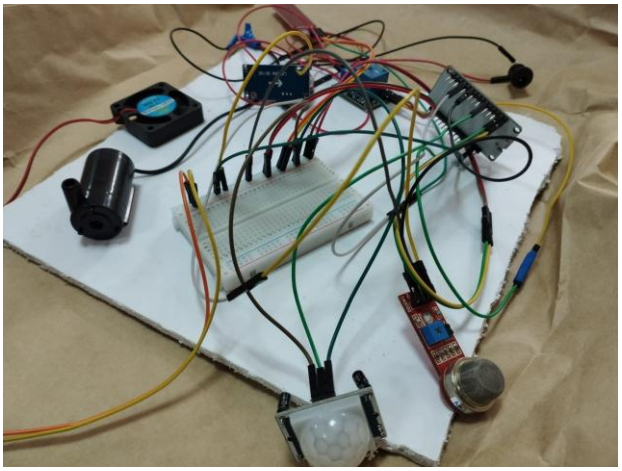

Fig 9. The result of the work

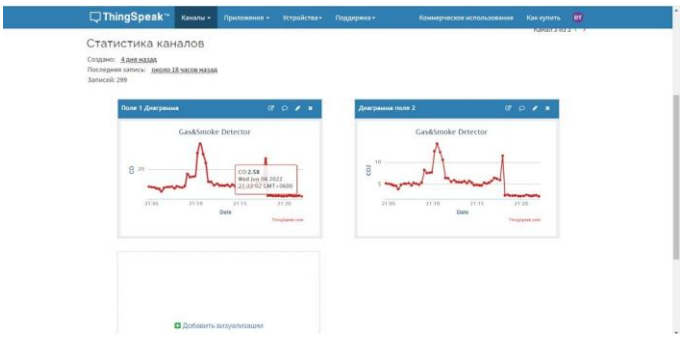

Fig 10 Graphical representation of the result of the work

This figure shows a diagram of the observation results of the MQ135 sensor on the Ios platform. It can also be tracked via the mobile app version. Additionally, you can view the announcement of the motion sensor via telegram bot.

3. Conclusion

A comprehensive information security system at an enterprise or organization includes ensuring the security of important processes carried out in accordance with the requirements of regulatory authorities (regulators). Maintenance and security of information systems include the implementation of legal, organizational measures, as well as the introduction of comprehensive engineering, software and hardware protection.

As a result, a model of an integrated information security system at the enterprise was created based on a leak sensor and a fire sensor. Thus, designing an effective alarm system is a complex multidimensional task that cannot be solved without an IoT system with a deep and comprehensive knowledge of its device, functionality and operating principles, taking into account the software and hardware means of its protection from pests.

References

1. [1] Azizova M.I. Innovatsionnyye tekhnologii v tsifrovoy ekonomike / Uchebnoye posobiye. – SP: «Nihol print», 2022. 184 p.
2. [2] Yasenev V.N., Dorozhkin A.V., Sochkov A.L., Yasenev O.V. Informatsionnaya bezopasnost'. Nizhniy Novgorod: Nizhegorodskiy gosuniversitet im. N.I. Lobachevskogo, 2017. 198 p.
3. [3] Mel'nika L.G., Bryukhanova M. V. Sotsial'no ekonomicheskiye problemy informatsionnogo obshchestva: monografiya. Sumy: Universitetskaya kniga, 2010. 896 p. ISBN 9789666804993
4. [4] Zinov'yeva Ye.S. Razvitiye informatsionnogo obshchestva: problemy bezopasnosti. J.CiberLeninka. 130-135.
5. [5] Gribunin V.G., Chudovskiy V.V. Kompleksnaya zashchita informatsii na predpriyatii: Uchebn. posobiye. M.: Akademiya, 2009. 416 p.
6. [6] Serdyuk V. A. Organizatsiya i tekhnologii zashchity informatsii: obnaruzheniye i predotvrashcheniye informatsionnykh atak v avtomatizirovannykh istemakh predpriyatiy. M.: GU-VSHE, 576 r, 2013. ISBN 978-5-7598- 0698-1.
7. [7] Zavgorodniy V.I. Kompleksnaya zashchita informatsii v komp'yuternykh sistemakh / Uchebnoye posobiye. M.: Logos; PBYUL N.A. Yegorov, , 2001. 943 r.

МАТЕРИАЛЫ
VII международной научно-практической конференции
"Информатика и прикладная математика",

20 октября - 21 октября 2022, Алматы, Казахстан

Подписано в печать 18.10.2022 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 21,72.
Тираж 200 экз. Заказ № 006900.
Отпечатано в ИИВТ МНВО РК.
Алматы, ул. Шевченко, 28