ООО «Golden Master»

Личная карточка сотрудника

Пол: Ж

Имя: Вероника

Фамилия: Куликова

Отчество: Елисеевна

Дата рождения: 15.07.2004

Семейное положение: Не состоит

Текущее подразделение: Отдел маркетинга

Текущая должность: Специалист по IT

Подразделение	Должность	Дата начала	Дата окончания	Разряд
Отдел маркетинга	Специалист по IT	08.02.2023	09.06.2024	4

Рисунок 2 — Личная карточка сотрудника

Штатное расписание

Подразделение Производственный отдел

Название должности	Мин. разряд	Макс. разряд	Количество ставок
Инженер по производству	2	5	1
Менеджер по качеству	2	5	3

Рисунок 3 — Штатное расписание подразделения

Заключение. Проведенное тестирование программы позволяет сделать вывод о полной работоспособности программы. В разработке данного приложения было сделано не только то, что соответствует данному заданию, но и многое другое для удобного использования. Благодаря удобному и понятному интерфейсу среды программирования Visual Studio с применением WPF удалось создать красивый и удобный интерфейс приложения.

Список цитируемых источников

1. Трудовые ресурсы [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Трудовые_ресурсы . — Дата доступа: 05.05.2024.

2. *Мазалевич, О. Д.* Автоматизированная система сопровождения базы данных отдела кадров / О. Д. Мазалевич, О. И. Наранович // Содружество наук. Барановичи-2013 : материалы IX Междунар. науч.-практ. конф. молодых исследователей, Барановичи, 23—24 мая 2013 г. : в 2 кн. / редкол.: А. В. Никишова (гл. ред.) [и др.]. — Барановичи : РИО БарГУ, 2013. — Кн. 2. — С. 103—105.

UDC 004.056

E. M. Pakhalyuk

Rostov branch of the state government educational institution of higher education "Russian Customs Academy", Rostov-on-Don, Russian Federation

PROBLEMS AND WAYS TO IMPROVE CYBERSECURITY OF THE FEDEREAL CUSTOMS SERVICE OF THE RUSSIAN FEDERATION

Introduction. Currently, cybersecurity is a key area in the Russian Federation, the development of which is being carried out by the state. Thus, after the start of a special military operation in Ukraine, cyber attacks began to occur more frequently on Russian state security systems, in particular, information security systems

The Russian Federal Customs Service (FCS) suffered one of the most dangerous hacks in recent times.

Thus, for the FCS of Russia there is a threat of disruption of interaction with participants in foreign economic activity (FEA) and cooperation with other government bodies, because with the help of automated software, customs authorities implement their main function — fiscal (replenishing the state budget with customs revenues). Even a small cyber attack can result in the leakage of valuable data that is difficult or impossible to recover.

The purpose of this article is to determine the mechanism for the functioning of customs authorities to ensure the safety of confidential information stored in automated software. The object of the study is the cybersecurity of the customs authorities of the Russian Federation.

Main part. Cybersecurity is the security of sensitive information in cyberspace, a complex environment that results from the interaction of humans, software and the Internet and is distributed by connected networks and information and communication technologies (ICT).

There are many interpretations of the concept of cybersecurity. Cybersecurity is also a set of activities aimed at organizing the collaboration of computing devices and personnel developing specific guidelines and risk management approaches in accordance with security policies, protecting the assets of the organization and users. Thus, a number of actions are used aimed at protecting cyberspace and preventing unauthorized access, as well as damage to data contained on information platforms [1, p. 4, 5].

The state uses cyberspace to improve the socio-economic environment of society. Thus, by increasing the revenue side of the state budget with its help, introducing new technologies and developments, the State Government increases the productivity and profitability of enterprises, and in general the level of well-being of the country's population increases. ICT is developing rapidly and is accelerating the transition to a virtual space where innovation is concentrated and there is the opportunity to interact through mobile technologies.

The rapid spread of digitalization, on the one hand, provides benefits for humanity, and on the other hand, leads to conflicts due to damage to the infrastructure of cyberspace. Nowadays, the polarization of countries is noticeably increasing, and this leads to a breakdown in cooperation between them, and within the framework of cyberspace, political conflicts are being tried to be "solved" by illegal means, namely by inflicting cyber attacks [2, p. 72]. Attempts are being made against the computer security of information systems: attackers gain access to confidential information and, by remotely controlling hacked systems, contribute to their destabilization.

According to the Russian Ministry of Foreign Affairs, the number of cyber attacks on Russia has increased in recent years. The public sector has become a particularly targeted area. In connection with the intelligence activities of foreign states against Russia, hackers and so-called "hacktivists" were hired IT specialists who were recruited mainly from the territories of NATO member states, the EU and Ukraine through telegram channels to carry out web attacks on government agencies. The main goal they pursue is leaking user data and limiting access to used resources through the use of malware, where the type of "encryptor" was used to a greater extent.

The boom in hacktivist activity predicted by Positive technologies experts, which was aimed at government institutions, was confirmed in 2023 [3, p. 4].

On April 10, 2023, a large-scale cyber attack was committed on the IT resources of the FCS of Russia, which led to the failure of the functioning of the Unified Automated System of Customs Authorities until April 12, 2023.

Customs officials have had to face a number of negative consequences. First of all, this is a time-consuming restoration of information systems. Thus, customs inspectors at checkpoints were engaged in processing customs declarations on paper, but this measure was forced.

The work of the official website of the FCS of Russia was suspended, and access to the "Personal Account" of a FEA participant was limited for use outside the Eurasian Economic Union. A positive aspect was the fact that crossing the customs border by individuals was not suspended, work was carried out as usual [5, 6].

Customs services of the FCS of Russia began to be subject to cyber attacks since March 2022, up to 3—4 times a day. By May 2023, there were "1,200 DDoS attacks" on the Russian FCS, prompting calls for help from external organizations to assist in the cybersecurity of their IT systems, such as "Sberbank" and "Kaspersky".

Let's consider the activities of criminal groups (Figure 1).

Figure 1 — Criminal groups committing cyber attacks on government information systems [4; 7; 8]

Let's take a closer look at the operating patterns of the hacker groups Sticky Werewolf and Dark River, which were identified during cyber attacks on the FCS of Russia — they send out phishing emails containing viral information.

Sticky Werewolf is a group (registered in April 2023) that sends letters to the official emails of government employees with reinforcements as attachments of PDF or Word files, after opening which the software of government information systems is instantly infected.

The strategy of the Dark River group is similar to Sticky Werewolf, but there is a significant difference - the resource controlled by criminals is loaded after the user opens the editing mode of a ".docx" file sent from an unknown address in an attachment. The group was most active in its activities from August to September 2022. A spe-

cial feature is good backdoor camouflage. Many of its samples are equipped with a real digital signature, and the names of the executable files are similar to the names of legitimate software. Developers, using different types of packagers, compress files, hiding harmful code in such a way that it is almost undetectable.

It should be noted that the protection of information systems of the FCS of Russia seems possible through the coordination of actions of specialists in the field of cybersecurity and software users who will apply organizational and legislative measures (Table 1).

T a b l e 1 — Measures to minimize the occurrence of cyber attacks on information systems of the Federal Customs Service of Russia

№	Measure	Characteristic
1	Ensuring software updates and protection	Installing anti-virus software, regularly updating the firewall
2	Implementation of multi-level protection	Data encryption, authentication, firewalls
3	Training of civil servants	Conducting seminars on information security for government officials on the existence of possible threats and protection from cyber attacks
4	Network activity analysis	Monitoring to identify “suspicious traffic”
5	Information backup	Creating backup copies of data to restore information in case of its destruction
6	Access control	Providing civil servants with access to information systems depending on their job responsibilities
7	Adherence to international information security standards	Compliance with the requirements established by ISO/IEC 27001

Conclusion. One of the most effective practices for preserving confidential customs data is data encryption. When a legal crypto gateway certified by the Federal Security Service of the Federal Service for Technical and Export Control is used, the fight against leaks of strategic information is most effective. According to experts, avoiding cyber attacks cannot be completely eliminated, but it is recommended not to activate letters sent from an unknown address [7; 8].

To summarize, it is important to summarize that timely response to problems in working with information systems and compliance with cybersecurity rules by users of computer programs is a necessity. It is also worth mentioning the consolidation of cybersecurity policy by regulations, because in the Russian Federation there is no separate concept of state cybersecurity. So, only in 2010 a project document for such a concept was formed, but it was not approved, and the project was not implemented. The development of new practical security systems and the approval of the project on “Cybersecurity” will allow regulation in cyberspace not only at the federal, but also at the international level [1, p. 7; 9].

Reference list

1. Cybersecurity strategies [Electronic resource] : Analytical report. — Mode of access: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf . — Date of access: 02.05.2024.

2. *Yakovlev, A. V.* CYBER SECURITY AND ITS LEGAL REGULATION (Foreign and RUSSIAN EXPERIENCE) / A. V. Yakovlev [Text] // . — St. Petersburg: Socio-political sciences. T. 11. № 4, 2021. — P. 70-81.

3. *Berova, D. M.* CYBER ATTACKS AS A THREAT TO INFORMATION SECURITY / D. M. Berova. — Moscow: Gaps in Russian legislation. Legal Journal, 2, 2018. — pp. 186-188.

4. TADVISER: official website / State. Business. Technologies. / Number of cyber attacks in Russia and in the world. [Electronic resource]. Mode of access: https://goo.su/d5mOJ5r . — Date of access: 08.09.2023.

5. TASS: Russian news agency / FCS inspectors switched to paper-based customs operations due to a cyber attack. [Electronic resource]. — Mode of access: https://tass.ru/ekonomika/17494915 . — Date of access: 04.11.2023.

6. Federal Customs Service of Russia: official website of the Federal Customs Service of Russia / Attention to participants in foreign trade activities [Electronic resource]. — Mode of access: https://customs.gov.ru/document/text/328444 . — Date of access: 02.28.2024.

7. Seldon.NEWS: official website / Russian government organizations are being attacked by a new hacker group, Sticky Werewolf. [Electronic resource]. — Mode of access: https://news.myseldon.com/ru/news/index/297411982 . — Date of access: 13.10.2023.

8. RIA NEWS: official website / Positive Technologies discovered a cyber group attacking the company. [Electronic resource]. — Mode of access: https://ria.ru/20230927/kibergruppirovka-1898852578.html . — Date of access: 09.27.2023.

9. LOGIRUS: official website / FCS cybersecurity will be strengthened by external contractors. [Electronic resource]. — Mode of access: https://logirus.ru/news/custom_and_ved/kiberbezopasnost_fts_ukrepyat_vneshnie_podryadchiki.html . — Date of access: 05.03.2024.