Biodiesel or biodiesel is a liquid motor biofuel which is a mixture of monoalkyl esters of fatty acids, including waste products from the food industry. It is biodegradable, which makes it environmentally friendly. It is biodegradable, which makes it environmentally friendly.

Література:

1. Газ для авто. Каким он бывает? Матеріали сайту, 2014. Режим доступу:http://autoportal.ua/articles/chtobudetesli/27338.html.

2. Газ на авто: плюсы и минусы. Матеріалисайту, 2016. Режим доступу: http://vipgaz.ua /articles/gaz-na-avtoplyusy-i-minusy.

3. Преимущества и недостатки бензина в качестве топлива для двигателей // Режим доступу:http://www.enersy.ru/energiya/preimuschestva-i-nedostatki-benzina-v-kachestvetopliva-dlya-dvigateley.html.

4. Богдан авто. Матеріалисайту, 2019. Режим доступу: https://bogdanauto.com.ua/benzin-dizel-elektro-voden-i-gibrid-yakij-dvigun-najbilsh-efektivnij/

5. Укрпрокат. Матеріалисайту, 2020. Режим доступу: https://ukr-prokat.com/ru/blog/vydy-toplyva-dlya-avtomobylej.html

УДК 811.111

CYBERHYGIENE IN THE FINANCIAL SECTOR OF UKRAINE
КІБЕРГІГІЄНА У ФІНАНСОВОМУ СЕКТОРІ УКРАЇНИ

Жовта Н.А – *здобувач вищої освіти групи Б 3/1*

Науковий керівник – Тішечкіна К.В., кандидат філологічних наук, доцент кафедри іноземних мов МНАУ

Стаття присвячується кібергігієні як способу захисту має вищу ієрархію та більшу цінність, аніж різноманітне антивірусне програмне забезпечення

Ключові слова: *кібергігієна, фінанси, сектор, фінансовий сектор, безпека, Україна*

The article focuses on cyberhygiene as a way of protection it has a higher hierarchy and greater value than various antivirus software

Key words: *cyberhygiene, finance, sector, financial sector, security, Ukraine.*

Every day, information technology is increasingly penetrating the lives of modern man. Today, most of us have a smartphone with Internet access, which allows us to always be online. At any time, you can check your mail or messenger, buy a movie ticket or book a vacation home, and even make payments without contacting a bank branch. All these actions on the Internet involve the exchange of certain personal information or confidential data, which in case of your negligence may end up in the hands of attackers.

The number of Internet frauds, intrusions into personal information space, dissemination of false information, etc., is now becoming an epidemic, especially in the field of finance and banking. Therefore, such a concept as cyberhygiene is a common and relevant topic today.

Like personal hygiene rules to maintain good health and well-being, cyber hygiene rules and precautions can provide better protection for the user from cyber attacks and data leaks.

To ensure the protection of your personal data when working on the Internet, ESET specialists recommend following the basic rules of cyber hygiene. In turn, cyberhygiene is a security measure designed to protect user devices from infection by malicious software and possible theft of confidential information [1]. Today, cyber attacks on banking services and customer databases with complete personal data are relevant. That is why the basic rules of cyber hygiene are mandatory for everyone.

Cyberhygiene rules provide 7 steps to improve data protection [1]:

1. Security check of active accounts. (e-mail accounts and social media accounts). In particular, websites such as haveibeenpwned.com and breachalarm.com will help determine if an email password has been stolen by an attacker.

2. Program analysis - analyze already downloaded applications, delete unnecessary ones and further control the installation of each program. You should also pay attention to the permissions you provide when downloading each application.

3. Regular updates - to prevent malware infection, you should update the operating system and individual applications in a timely manner to correct vulnerabilities and bugs in the software.

4. Secure password - to prevent unauthorized access to your devices, make sure your passwords are secure. It is important to create a complex combination that contains at least 12 characters, uppercase and lowercase letters, numbers and symbols. In addition, you should use a unique password for each account.

5. Additional level of protection.- To improve the security of accounts, use two-factor authentication, which provides authentication when logging in to a particular account.

6. Regular backup - this will help to recover the necessary data in case of encryption by the requesting program or removal by malicious software.

7. Reliable protection from various threats, including extortion programs, spyware, viruses, trojans and phishing attacks.

Following all these rules will complicate the process of using gadgets. But do not forget that the profit from cyberhygiene easily eliminates any discomfort. Security of your finances and personal data above all.

Users can play an important role in ensuring the security of the digital society by raising its awareness and practicing "cyber hygiene". Qualified professionals and businesses in the field of cybersecurity should cooperate and raise user awareness about cybersecurity.

The best defense strategy is to know in advance exactly where to expect the threat and what algorithm to follow to avoid meeting with it. For example, an experienced user will never give his password to an attacker, knowing from the beginning that legitimate bank employees never make such requests.

In today's world, it is the government that sets the strategy for cybersecurity in general, the level of critical infrastructure and public corporations that need protection in the first place, and the level of private companies and groups that need state support and compliance with existing information security rules and regulations in the legislation.

Such a scheme of organizing the country's extensive defense is quite effective and allows: to distribute protection priorities, identify and neutralize potential vulnerabilities in high-level infrastructure, distribute powers: which body and what to protect, and create legislation capable of responding to cyber threats.

Today, Ukraine is trying to raise the level of awareness in this area, with the help of the educational platform of the Ministry of Digital Transformation of Ukraine Action. Digital Education. An educational series on cyber hygiene rules for civil servants is posted on this platform. It consists of 9 series lasting 3-7 minutes. This series was created with the support of the OSCE Project Co-ordinator in Ukraine and was presented on January 26, 2021 at an event in Kyiv.

Henrik Willadsen, OSCE Project Co-ordinator in Ukraine, said: “Modern governance is impossible without information technology, but it creates new risks as criminals or terrorists seek to find and exploit digital vulnerabilities to damage or disrupt public information systems. The scale of the possible damage from crimes committed with the help of information technology has increased dramatically in recent years. Informing officials about these risks and what they can and should do to increase the digital security of their institutions is a key step in shaping the country's resilience to today's threats. ”[2]

This series will help everyone to increase their level of awareness and skills in:

- rules of cyber hygiene at work and in everyday life
- secure use of the browser and Wi-Fi networks in general

- distinguishing between the use of personal and business mailboxes
- use of software
- responsible dissemination of information on social networks
- rules for safe work with mobile devices
- types of information manipulation in the cybersphere, etc. [3].

Thus, cyberhygiene as a means of protection has a higher hierarchy and greater value than various antivirus software. It is much cheaper to simply prevent infecting your device by following simple security rules (refusing to download unknown files without a signature and publisher, ignoring phishing pages, etc.) than to deal with the very consequences of that infection by relying on the power of antivirus software.

As an example, treating or removing a virus can be costly and time consuming, and even for a short period of time in the device, the virus can cause significant damage and find out your personal information.

Література:

1. Основні правила захисту даних — кібергігієна для активного Інтернет-користувача. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya#

2. Освітній серіал, створений за підтримки ОБСЄ, популяризуватиме кібергігієну серед держслужбовців України. URL: https://www.osce.org/uk/project-coordinator-in-ukraine/476542.

3. Освітня платформа Міністерства цифрової трансформації України *Дія.Цифрова Освіта.* URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

УДК 811.112

TECHNOLOGISCHE PROZESSE DER JOGHURTPRODUKTION (ТЕХНОЛОГІЧНІ ПРОЦЕСИ ВИРОБНИЦТВА ЙОГУРТІВ)

Зелінська Е.В. *– здобувач вищої освіти групи ХТ 2/1*

Науковий керівник – Пономаренко Н.Г., кандидат педагогічних наук, ст. викладач кафедри іноземних мов МНАУ

Більше 4000 років молочні кислотні бактерії були використані для виготовлення кислих молочних продуктів, але в той час нічого не було відомо про забруднювач. Про