виробничих майстернях несе вчитель, який керує цією роботою [4].

Майстерні навчального закладу використовуються під час проведення занять з трудового навчання і поділяються на навчальні майстерні для трудового навчання молодших школярів; навчально-виробничі майстерні, у яких здійснюється трудове, допрофільне навчання і допрофесійна підготовка учнів середнього шкільного віку; навчально-виробничі майстерні загальноосвітніх навчальних закладів системи загальної середньої освіти для трудового і виробничого навчання та профільної, допрофесійної і професійної підготовки учнів старшого шкільного віку. Приміщення майстерень навчальних закладів, розміщення в них обладнання і механізмів повинні відповідати вимогам до освітлення, опалення і вентиляції, з безпеки праці до обладнання, електробезпеки, пожежної безпеки. Вчитель навчає учнів безпечного поводження з наявним у майстерні обладнанням, а також безпечних методів виконання робіт; забезпечує дотримання вимог безпечного проведення навчально-виховного процесу; несе відповідальність за збереження обладнання майстерні, справність засобів пожежогасіння; стежить за своєчасним проведенням технічного обслуговування та ремонту обладнання майстерні; здійснює навчання та інструктаж учнів з охорони праці, безпеки життєдіяльності; здійснює першу допомогу у разі нещасних випадків, що сталися з учнями в майстерні [2].

Усі напрацювання Д. О. Тхоржевського втілюються в практику і в наш час, завдяки ним активізується процес трудового навчання учнів старших класів, стає можливим вирішення проблем безпеки трудового навчання підлітків. Саме науковометодичні комплекси, розроблені Дмитром Олександровичем зумовили характерні тенденції розвитку та становлення трудового навчання школярів у закладах загальної середньої освіти України.

Список використаних джерел

1. Дебре О. С. Практичне використання безпеки життєдіяльності на уроках трудового навчання. Безпека життя і діяльності людини: теорія та практика *: збірник наук. праць Всеукр. наук.-практ. конф., присвяченої Всесвітнім Дням цивільної оборони та охорони праці,* (Полтава, 23–24 квітня 2020 р.) / упоряд., і ред.: В. П. Титаренко, А. М. Хлопов. Полтава : ПНПУ імені В.Г. Короленка, 2020. С. 94–98.
2. Про затвердження Правил безпеки під час занять у навчальних і навчально-виробничих майстернях навчальних закладів системи загальної середньої освіти. Наказ Міністерства освіти і науки України від 13 серпня 2007 року N 730. URL: https://ips.ligazakon.net/document/RE14257?an=444
3. Пшеничний М. Педагогічна спадщина Д.О. Тхоржевського у контексті проблем трудового навчання другої половини XX ст. в Україні. URL: https://library.udpu.edu.ua/library_files/psuh_pedagog_probl_silsk_shkolu/24/visnuk_27.pdf
4. Тхоржевський Д. Вимоги до уроку трудового навчання. *Радянська школа.* 1976. №8. С. 60–68.
5. Тхоржевський Д. О. Система трудового навчання. Київ : Радянська школа, 1975. 200 с.

CRYPTOCURRENCIES IMPACT ON BUSINESS TRANSACTION SECURITY

Дебре Віктор Сергійович
Харківський національний університет радіоелектроніки
Debre Viktor Serhiyovych
Kharkiv National University of Radio Electronics Kharkiv

Annotation*. This article discusses the security of business transactions. This topic is very*

important because the online transaction market is growing at an incredible rate, and it is extremely important to protect them from hacker attacks. Cryptocurrencies are one way to solve this problem. In addition, recently, more and more areas of life are moving to a remote form of financial flow, and with increasing market size, this topic will remain relevant. As a result, the integration of the blockchain system into the banking and investment systems is inevitable. Therefore, structuring and further studying a given topic are extremely necessary.

***Key words**: blockchain, smart contract, cryptocurrency, transaction security, bitcoin, ethereum, Cryptocurrency Security Standards, business transaction.*

Introduction. With the development of new technologies and information space, the question of business security of new forms of online work is urgent. One of the newest and safest technologies, which introduces new levels of protection to personal accounts and money transfers, is the blockchain. A new type of interaction and establishment of business transactions allows you to do without intermediaries and enter into smart contracts with minimal fees and protection against unauthorized access to the accounts of the originators.

Aim. Over the last decade, the number of crimes related to online money transfers has increased, and many businesses and individuals have online or unprotected online accounts. Direct transfers of banks to another account are not always secure. To provide the necessary level of protection, they have to spend significant resources on the secure operation of servers and systems that serve them. Due to this, the price of the transfer commission increases significantly. Cash transfers require resources for transportation and longer order processing. Therefore, the only alternative to these methods is the blockchain system.

Materials and methods. Blockchain technology is commonly used to create cryptocurrencies. Cryptocurrency security encompasses everything you need to know about the potential dangers of cryptocurrency and the fundamentals of what you can do to make your setting related to your crypto investments or trades safer and safeguard your crypto assets.

The method transactions are recorded in «blocks», and the blockchain describes as time-stamped. It's a lengthy, complicated procedure, but the result is a secure digital ledger of cryptocurrency transactions that hackers can not influence. Transactions also necessitate a two-factor authentication process. While security measures are in place, this does not mean that cryptocurrencies are immune to hackers [1].

Also, as cryptocurrency sees increased adoption, state, local, tribal, and territorial (SLTT) governments are encountering malware designed to steal or mine cryptocurrency. Their systems are held for ransom payable only via cryptocurrency. Bitcoin (BTC), the first cryptocurrency to see widespread use, emerged in 2009. Today, there are hundreds of alternatives to Bitcoin. Popular alternatives include Litecoin (LTC), Ethereum (ETH), Bitcoin Cash (BCH), and Monero (XMR). Most cryptocurrencies are decentralized, operating without the oversight of trusted authority and instead relying upon the security of cryptographic algorithms and ledger distribution commonly achieved through blockchain technology. This independence grants company and individuals the freedom to transfer funds directly to one another.

Even if it provides high security and independence for cryptocurrency, it has risks that arise while engaging in the crypto sector:

The first risk is that people can leave cryptocurrency on exchanges. It especially happens when they first start trading cryptocurrencies. If funds and crypto coins are readily available for transactions, hackers, unfortunately, take the possibility to get all money by getting access to an account on the exchange. Moreover, exchange hacking is not confined to other parties, employees and even exchange founders who can commit significant fraud.

The second risk is in contrast to leaving seed phrases in centralized cloud storage. Several examples of seed phrases are backed up on local devices, and if it is subsequently lost or stolen or the password is forgotten, you can not contact support. The problem with local storage is that it's easy to misplace it or for someone to track you down and steal it.

But advanced authentication in cyber security provides another layer of defense that helps

ensure that when a user is accessing your network, they are that person. By following the next rules [2], using cryptocurrencies can become protected.

Limit login attempts practice is a standar00d network authentication technique that not everyone implements. Limiting login attempts should not be possible to brute-force an account through your web user interface. There are a few different ways to limit login attempts. You can block users who perform too many incorrect logins by IP address, lock down accounts that receive many false login requests, and notify the account holder in question. You can also do both.

In general, Cryptocurrency Security Standards (CCSS) have ten points that are fulfilled while setting up cryptocurrency security systems [3]. It is 10-step security put up on three levels. Thus the standard is followed by most cryptocurrency exchanges. The following are the steps that most blockchain companies and organizations follow, and investors must invest in the services of companies following the Cryptocurrency Security Standards:

−Key/seed generation
−Wallet Creation
−Key Storage
−Key Usage
−Key Compromise policy
−Keyholder Grant/ Revoke Policy and Procedures
−Third-party audits
−Data Sanitization Policy
−Proof of Reserve
−Log Audits

Security considered ‘level one’ proves that assets are protected with strong policies and procedures, while those deemed ‘level three’ exceed security expectations and provide strictly enforced policies. Users should consult the CCSS to identify the best cryptocurrency systems to use and keep their currency safe.

Businesses using cryptocurrency can adopt file sanitization to ensure no chance of malicious code running in the background. Proactive cyber security solutions, such as content disarm and reconstruction (CDR), help organizations be one step ahead of cybercriminals. CDR ensures that no malicious malware exists within a file by scanning it and re-building it to the known good manufacturer’s specification.

Results and discussion. By analyzing data about the growth of cryptocurrencies in the 2021 year, we can assume that capitalization is increasing. According to data [4], the cumulative market capitalization of cryptocurrencies grew around 300% year over year to $758bn in 2020, as investors flocked to crypto coins in times of economic uncertainty caused by the pandemic. The combined value of all crypto coins soared by 220% in the 2021 year, reaching $2.43trn in May. Even above the market cap reached in 2017, this was considered the break-out year for Bitcoin and other digital coins. However, 2021 witnessed even more impressive growth, with many major crypto coins reaching their all-time highs. Bitcoin, the biggest digital currency, accounts for 45% of the global crypto market cap.

The following data [5] show its price rallied over 100% this year alone, helping its market cap hit $1.1trn last week. Compared to $178bn in 2020, this represents a massive 515% increase in a year. However, the latest boost in the cryptocurrency market has been equally driven by impressive Ethereum growth. In 2020, the combined value of all Ethereum coins amounted to $23.4bn. Over the next twelve months, this figure soared by 1,656%, three times the growth rate of Bitcoin.

Conclusions. Therefore, the development of the crypto market and its execution in business processes will decentralize and ensure the safe use of these processes. The general trend of rising capitalization of cryptocurrencies indicates an increasing role in this area in the future. As the impact of cryptocurrencies boosts, transaction security will increase significantly. Therefore, research and implementation of new systems to protect personal data and accounts is an integral part of human development in a post-industrial society.

References

1. Shetty N. Cryptocurrency Security: How To Protect Your Digital Investment URL: https://www.finextra.com/blogposting/20477/cryptocurrency-security-how-to-protect-your-digital-investment (дата звернення: 12.03.2022)
2. Matthews K. What to know about user authentication and cyber security URL: https://www.information-age.com/what-to-know-about-user-authentication-cyber-security-123487818/ (дата звернення: 22.03.2022)
3. Bhalla A. Complete Guide on Cryptocurrency Security URL: https://www.blockchain-council.org/cryptocurrency/complete-guide-on-cryptocurrency-security/ (дата звернення: 11.02.2022)
4. Milan Fintech Summit URL: https://www.milanfintechsummit.com/crypto-currency-global-market-2021/ (дата звернення: 21.01.2022)
5. Coin Market Cap URL: https://coinmarketcap.com/currencies/bitcoin/price-estimates/ (дата звернення: 02.04.2022)

ЗАГРОЗА ПОШИРЕННЮ ІНФЕКЦІЙНИХ ЗАХВОРЮВАНЬ В РЕАЛІЯХ ВІЙСЬКОВОГО СЬОГОДЕННЯ: МІКРОБІОЛОГІЧНІ АСПЕКТИ

Дерев'янко Тетяна Василівна, Звягольська Ірина Миколаївна, Полянська Валентина Павлівна
Полтавський державний медичний університет

Анотація. *У статті розглянуто чинники поширення і розвитку інфекційних захворювань як серед цивільного населення, так і військовослужбовців ЗСУ в умовах військових подій, які склалися на території України в 2022 році. Наведено приклади інфекційних хвороб різної етіології, їх шляхи передачі, які становлять загрозу щодо поширення в умовах надзвичайної ситуації військового характеру і є порушенням нормальних умов життя та діяльності людей.*

Ключові слова: *інфекційні захворювання, військові події.*

Протягом усієї історії становлення людського суспільства інфекційна патологія завжди домінувала в структурі захворюваності людей. Незважаючи на численні науково-практичні здобутки в галузі медицини минулого і теперішнього століть проблеми інфекційної патології і на сьогодні не втратили своєї актуальності [1].

На жаль, у зв'язку з військовими діями 2022 року в Україні може скластися вкрай важка ситуація з поширенням і розвитком багатьох інфекційних захворювань як серед цивільного населення, так і військовослужбовців ЗСУ. Тому, проблеми інфектології не лише не відійшли на другий план, а, навпаки, піднялися на вищий рівень актуальності.

В умовах природного, а для людини і соціального середовища, між чутливим макроорганізмом і патогенним мікроорганізмом історично виникли певні взаємовідносини, які визначаються як інфекційний процес, крайнім проявом якого є інфекційне захворювання. Види інфекційного процесу різняться за проявами і характером перебігу, за характером зараження і поширенням мікроорганізму та його токсинів в макроорганізмі. Найважливішою особливістю інфекційних захворювань є те, що безпосередньою причиною їх виникнення є проникнення в організм будь якого мікроорганізму (патогенного, умовно-патогенного і навіть непатогенного), який, розмножуючись, викликає ті чи інші порушення в ураженому організмі, виділяється в навколишнє середовище, створюючи небезпеку зараження інших людей. Тож основними факторами інфекційного процесу є патогенний мікрорганізм, чутливий макроорганізм і умови довкілля.

Процес поширення інфекцій в людському колективі (епідемічний процес) – безперервний процес взаємодії мікро- і макроорганізмів на популяційному рівні, який