АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION AND COMMUNICATION TECHNOLOGIES

АҚПАРАТТЫҚ ЖҮЙЕЛЕР
ИНФОРМАЦИОННЫЕ СИСТЕМЫ
INFORMATION SYSTEMS

DOI 10.51885/1561-4212_2024_2_114
МҒТАА 44.29.01

Ж.К. Алимсеитова[1], А. Оган[2]
Сәтбаев университеті, г. Алматы, Казахстан
*[1]E-mail: zhuldyz_al@mail.ru**
[2]E-mail: atkeldi@mail.ru

ЦИФРЛЫҚ КРИПТОВАЛЮТА НАРЫҒЫНЫҢ ҚЫЗМЕТТЕРІ ҮШІН АҚПАРАТТЫҚ ҚАУІПСІЗДІК МӘСЕЛЕЛЕРІ ЖӘНЕ ТЕХНОЛОГИЯЛЫҚ ТӘУЕКЕЛДЕР

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕХНОЛОГИЧЕСКИЕ РИСКИ ДЛЯ СЕРВИСОВ РЫНКА ЦИФРОВЫХ КРИПТОВАЛЮТ

INFORMATION SECURITY ISSUES AND TECHNOLOGICAL RISKS FOR DIGITAL CRYPTOCURRENCY MARKET SERVICES

Аңдатпа. *Тәуекелдерді бағалау үшін қолданылатын әдістер мен модельдерге, оның ішінде ақпараттық қауіпсіздікке, Цифрлық криптовалюта нарығының сервистеріне және тиісті биржалық алаңдарға шолу және талдау жасалды. Цифрлық криптовалюта нарығына қызығушылық салыстырмалы түрде аз уақыт ішінде тез өсетіні көрсетілген. Сонымен қатар, бүгінде көптеген мемлекеттер мен олардың қаржы ұйымдары, мысалы, банктер, несиелік және сақтандыру компаниялары өз активтерінде Цифрлық криптовалютаға ие. Цифрлық криптовалюта нарығының мұндай даму қарқыны кәсіби хакерлерден бастап, цифрлық криптовалюта нарығын қорғауда әлсіз жақтарды іздейтін әртүрлі алаяқтарға дейін әртүрлі зиянкестерді қызықтырды. Криптовалюта биржаларының қызметін қамтамасыз ететін электрондық сервистердің ақпараттық қауіпсіздікті қамтамасыз ету міндетін шешудің аралас әдістерін дамытуды көздейтін бағыт перспективалы болып табылады.*

Түйін сөздер: *Ақпараттық қауіпсіздік, цифрлық криптовалюталар, криптовалюта биржалары, тәуекелдерді модельдеу, тәуекелдерді бағалау.*

Аннотация. *Выполнен обзор и анализ методов и моделей, применяемых для оценки рисков, в том числе, связанных с информационной безопасностью, сервисов рынка цифровых криптовалют и соответствующих биржевых площадок. Показано, что интерес к рынку цифровых криптовалют стремительно возрастает на протяжении относительно небольшого отрезка времени. Причем сегодня уже многие государства и их финансовые организации, например, банки, кредитные и страховые компании, имеют в своих активах цифровые криптовалюты. Такие темпы развития рынка цифровых криптовалют заинтересовали и различных злоумышленников, начиная от профессиональных хакеров и заканчивая разного рода мошенниками, ищущих слабые места в защите рынка цифровых криптовалют. Установлено, что перспективным является направление, предусматривающее развитие комбинированных методов решения задачи обеспечения инфрмационной безопасности электронных сервисов, обеспечивающих деятельность криптовалютных бирж.*

Ключевые слова: *Информационная безопасность, цифровые криптовалюты, криптовалютные биржи, моделирование рисков, оценка рисков.*

Abstract. *A review and analysis of methods and models used to assess risks, including those related to information security, services of the digital cryptocurrency market and relevant exchange platforms has been carried out. It is shown that interest in the digital cryptocurrency market is rapidly increasing over a relatively short period of time. Moreover, today many states and their financial organizations, for example, banks, credit and insurance companies, have digital cryptocurrencies in their assets. Such a pace of development of the digital cryptocurrency market has also interested various intruders, ranging from professional hackers to various kinds of scammers looking for weaknesses in the protection of the digital cryptocurrency market. It has been established that a promising direction is the development of combined methods for solving the problem of ensuring the information security of electronic services that support the activities of cryptocurrency exchanges.*

Keywords: *Information security, digital cryptocurrencies, cryptocurrency exchanges, risk modeling, risk assessment.*

Кіріспе. Цифрлық криптовалюта нарығының (бұдан әрі – ЦКВ) даму ретроспективасын қарастыра отырып, осы нарыққа деген қызығушылық салыстырмалы түрде аз уақыт ішінде тез артып келе жатқанына тез көз жеткізуге болады. Осы уақыт аралығында ЦКП-ға тек ынтағерлер қызығушылық танытты [1, 2], содан кейін бұл нарық инвесторлардың өте кең ауқымына қызығушылық танытты [3, 4]. Сонымен қатар, бүгінде көптеген мемлекеттер мен олардың қаржы ұйымдары, мысалы, банктер, несиелік және сақтандыру компаниялары өз активтерінде ЦКВ бар [4]. Көптеген мемлекеттер мен олардың қаржы ұйымдары ЦКВ-ны толыққанды төлем құралы ретінде толық тану туралы мәселені талқылайды және сәйкесінше ЦКВ үшін толыққанды төлем жүйелерін мемлекеттер деңгейінде дамыту идеясын алға тартады. Бүгінде әлемде мамандандырылған криптовалюта биржалары белсенді жұмыс істейді. Мұндай биржалар жеке инвесторлар мен ЦКВ-ны заңды төлем құралдары ретінде танитын жеке компаниялар арасында сауда-саттықты жүргізуге ықпал етеді [5-7]. Классикалық биржалық қызмет пен ЦКВ-мен мәмілелермен айналысатын биржалар арасындағы белгілі бір ұқсастық туралы айтуға болады.

Криптовалюта биржаларында ақпараттық қауіпсіздіктің жағдайдың өзгеруі, тек жағдайды және ақпараттық қауіпсіздікті бақылаудың неғұрлым қатаң тетіктері пайда болған жағдайда ғана мүмкін болады, тиісті сауда алаңдары мен олардың электрондық сервистері пайда болған жағдайда ғана мүмкін болады. Бұл жаңа зерттеулер жүргізуді талап етеді.

Осылайша, бұл жұмыстың мақсаты – тәуекелдерді бағалау үшін қолданылатын әдістер мен модельдерге, соның ішінде ақпараттық қауіпсіздікке (АҚ), ЦКВ нарығының қызметтеріне және тиісті биржалық алаңдарға талдау жүргізу.

Әдеби шолу. Криптовалюта биржалары (бұдан әрі-КВБ) қандай да бір өнімді сатып алумен/сатумен айналысатын ұқсас биржалар сияқты аппараттық-бағдарламалық қамтамасыз етудің үлгілік жиынтығына ие. Мысалы, бұл пайдаланушыларды тіркеуге арналған бағдарламалық қабықшалар, сонымен қатар жаңалықтар арналары, чаттар, аналитика және т. б.

Крипто-валюталық тәуекелдер – бұл ЦКВ сату/ сатып алу процесінде инвесторлардың қаржылық шығындарының ықтималдығы. Технологиялық крипто-валюталық тәуекелдерді, ең алдымен, ЦКВ-мен операциялардың ақпараттық қауіпсіздігін (АҚ) қамтамасыз етумен байланысты қарастырамыз.

КВБ-ны бұзуға байланысты алғашқы фактілер алғашқы сауда алаңдары ашылған кезде тіркелді. Ең танымал бірі 2011 жылы MtGox (Жапония) биржасын бұзу болды. Хакерлік факт тіркелгенімен, тиісті қорытынды жасалмады.

2016 жылы АҚШ-тағы Bitfinex биржасы бұзылды. Бұзу Bitcoin курсының құлдырауына әкелді. Шын мәнінде, бұл сауда қызметтерін тікелей бұзу ЦКВ бағамына тікелей әсер еткен екінші жағдай. Жағдайдың ауырлығына АҚШ FBI мамандары терғеуге қосылғаны куә болды.

Қазақстанда криптовалюта саласы белсенді дамып келеді – 2021 жылы майнерлер Қытайдан белсенді кете бастады, бұл саланың ілгерілеуіне айтарлықтай әсер етті. Bitriver мәліметтері бойынша, Қазақстан криптовалюта майнингі бойынша ең ірі елдердің ондығына кіреді.

Profinvestment сарапшылары Қазақстан үшін криптовалюта биржаларын қарап, цифрлық активтерді ұлттық валюта теңгемен сатып алуға немесе сатуға мүмкіндік беретін платформалардың рейтингін жасады. Олардың пікірінше, бүгінгі таңда Қазақстан нарығында жұмыс істейтін ең қауінсіз және сенімді биржаларға Bybit, Binance, OKX және басқалары (барлығы 15 криптобиржа) жатады.

Binance криптобиржасына жүргізілген талдау жұмыс барысында оған бірнеше шабуылдар сәтті жүргізілгенін көрсетті, олардың арасында фишинғтік шабуылдар да бар. Мысалы, 2019 жылдың мамырында Binance криптовалюта биржасы шамамен 7000 BTC зардап шекті. Хакерлер Binance-ті бұзу үшін фишинг пен зиянды бағдарламаны қолдана алды. Зиянкестер 40 миллион долларлық биткоиндермен қашып кетті. Нәтижесінде Binance өзінің қауінсіздігін арттыруға уәде берді. 2022 жылдың қазан айында Binance криптобиржасы хакерлер жалпы сомасы 570 миллион долларды құрайтын токендерді ұрлағаннан кейін блокчейн желісін уақытша тоқтатты. Оның BNB токендер тізбегімен байланысты брандмауэрге шабуыл жасалды, бұл хакерлерге токендерді желіден тыс жылжытуға мүмкіндік берді.

Blockchain-нің пайда болуымен хакерлер шабуылдар мен хакерлік техниканы жаңа бағытқа бағыттады. Мәселен, мысалы, Blockchain үшін төлем (вирусы-вымоғатели) вирустары, трояндық бағдарламалар, жалған сайттарды қолдану принциптері қайта қаралды.

Биржаларға, цифрлық қызметтерге және ЦКВ саудасымен айналысатын ойыншыларға бағытталған фишинғтік шабуылдар әлі де өзекті болып қала береді. Фишинғтік шабуылдар пайдаланушылардың жеке деректерінің бұзылуына байланысты қауіптерді жасырады. Мұндай ағып кетудің бір мысалы Leger (Франция) крипто әмияндарын қолдауға арналған аппараттық платформадан 270 000-нан астам крипто әмияндарына қатысты деректердің ағып кетуі болды [4, 8-11]. Мұндай ағып кету бір уақытта шабуылдаушыларға дивидендтер төлемеуі мүмкін, бірақ олар ақпараттың бір бөлігін хакерлер қосымша шабуылдар кезінде қолдана алатындығына ықпал етеді. Өділеттілік үшін, барлық фишинғтік шабуылдар шабуылдаушы тарап үшін нәтиже бермейтінін ескеріңіз. Өйткені, пайдаланушылар жаңа сілтемелерге әлдеқайда мұқият бола бастады. Көбінесе мұндай шабуылдар салдарсыз өтеді. ЦКВ-мен байланысты қаржылық цифрлық қызметтерге (крипто биржаларына) жасалған шабуылдар әлдеқайда үлкен қауін болып табылады. Міне, [9]-да келтірілген осындай шабуылдардың шағын тізімі.

Ең үлкен тәуекелдер 51 % шабуылмен байланысты. Шабуылдаушылар үшін мұндай шабуыл оны жүзеге асыруға өзінің қаржылық инвестициияларын жоғалту қаупімен байланысты. Шабуылдың бұл түрі шабуылдаушылар үшін ең қымбат болып табылады, өйткені шабуылдаушылар жабдықты сатып алу (жалға алу) үшін айтарлықтай шығындарға ұшырауы керек. 51 % шабуыл proof-of-Work алгоритміне сәйкес жұмыс істейтін блокчейндерге тән екенін ескеріңіз.

Bitcoins (BTC) жағдайында шабуылдаушыларға желінің қалған қуатынан асып түсетін есептеу қуатын алу мүмкін болмайтынына қарамастан, бұл кішігірім ЦКВ-ге қатысты өте жақсы жүзеге асырылады. Мәселен, мысалы, BTC-мен салыстырғанда, альткоиндер (Near, Polka dot, TXT, Dodge, Monaco, Luna және т.б.) блокчейнді қорғау үшін жеткілікті төмен хэш жылдамдығымен сипатталады. Демек, олардың желісінде 51 % шабуылдар болуы мүмкін.

1-кесте. ЦКВ-мен айналысатын криптовалюта шабуылдарының салдары

Жыл	Крипто биржасы (Страна)	Шығындар, млн. долларов США
2018	CoinCheck (Жапония)	534
2019	Coinbene (Сингапур)	105
2020	KuCoin (Қытай)	280

Жоғарыда айтылғандардың бәріне қарамастан, мұндай шабуылдар сирек емес. Мысалы, 2018 жылы осындай шабуыл тіркелді, оның барысында ЦКВ ZenCash шабуыл жасады. Шабуыл кезінде қос шығындар 550 мың АҚШ долларын, ал шығындар шамамен 33 мың АҚШ долларын құрады. Осындай шабуылдар КВ Verge, Bitcoin Gold және electron EU m-де тіркелді [4].

ЦКВ нарығына көптеген ықтимал шабуылдар тек ғипотетикалық түрде мүмкін, сондықтан оларды жүргізу бұзышудан үлкен ресурстарды қажет етеді. Дегенмен, DDOS және фишинғтік шабуылдар сияқты дәстүрлі шабуылдар ЦКВ курстарының орнықсыздыққа әкелуі мүмкін. Бұл өз кезегінде Форексте қолданыла алады, онда қысқа позицияларды ашуға, мәмілелерді тез ашуға және тәуекелдерді хеджирлеуге болады. Шабуылдаушыларға бір тиімді шабуыл жасау жеткілікті, сондықтан ЦКВ арзандайды. Жарқын мысал - Mt.Gox, қаскүнемдер биржадан 650 мың BTC-ні абайлап алып шыққан кезде. Жоғарыда айтылғандардың барлығы ЦКВ нарығының киберқауінсіздігін бағалаудың жаңа әдістері мен модельдерін дамыту бағытында жаңа зерттеулердің өзектілігін анықтайды, мысалы, нейрондық желілерді, ойын теориясын және бұлыңғыр логиканы қолдану негізінде.

ЦКВ нарығындағы тәуекелдерге арналған басылымдарды талдау [2, 3] мәміленің инвесторы үшін сәттілік пен кірістілік негізінен әлеуетті тәуекелдерді, соның ішінде биржалық қызметтердің ақпараттық қауінсіздігіне байланысты түсіну мен көзқараспен анықталатынын көрсетті. ЦКВ-мен байланысты мәселелерді зерттеудің бұл аспектісі зерттеу міндеттері аясында ерекше қызығушылық тудырады. Тиісінше, қазіргі зерттеу аясында жан-жақты зерттеуге лайық.

Материалдар және зерттеу әдістері. ЦКВ нарығындағы тәуекелдердің өзіндік практикалық және теориялық маңызы бар. Тәуекелдер басқару теориясы мен тәжірибесінің маңызды құрамдас бөлігі болғандықтан.

ЦКВ нарығымен байланысты тәуекелдер, соның ішінде технологиялық тәуекелдер-күрделі құбылыс. ЦКВ нарығының тәуекелдерінің негізінде көптеген сәйкес келмейтін және көбінесе қарама-қарсы нақты факторлар жатыр. Бұл ЦКВ нарығы үшін тәуекелдердің әртүрлі анықтамаларының болуын және нарықтың әр түрлі қатысушыларының позициясын анықтайды.

Жұмыста келтірілген тәуекелді түсіндіруді талдау [2] келесі сипаттамалық ерекшеліктерді анықтауға мүмкіндік берді:

– ЦКВ нарықтарына тән белгісіздіктің болуы;

– ЦКВ нарығындағы ойыншылар үшін инвестициялаудың балама нұсқаларының мүмкіндігі;

– мәміле бойынша нәтижелерді алдын ала талдау мүмкіндігі;

– мәмілелер бойынша шығындардың пайда болуының жеткілікті жоғары дәрежесі;

– жоғары пайда алу ықтималдығы;

– және т.б.

ЦКВ нарығында мәмілелерді жүзеге асыру кезінде тәуекелдерді бағалау мәселелерін қозғаған басылымдарды талдау негізінде [1, 3] ЦКВ-мен мәмілелер бойынша тәуекелдерді бағалау үшін қолданылатын жекелеген математикалық әдістер мен модельдердің артықшылықтары мен кемшіліктерін қамтитын келесі жиынтық кесте құрылды, 2-кестені қараңыз.

2-кесте. ЦКВ нарығындағы операцияларға тән тәуекелдерді бағалауға арналған әдістер мен модельдерді салыстырмалы талдау.
Автор құрастырған ([2, 3, 12-20] мәліметтері бойынша)

№	Әдіс/Модель	Артықшылықтары	Кемшіліктері
1	2	3	4
1	ЦКВ инвестициялау тәуекелдерін талдаудың статистикалық әдістері мен модельдері	1) ЦКВ нарығындағы мәміле нұсқаларын талдауға және бағалауға және бір тәсіл шеңінде көптеген тәуекел факторларын ескеруге мүмкіндік береді; 2) ғылыми әдебиеттерде жақсы зерттелген және сипатталған.	1) ықтималдық сипаттамаларын пайдалану қажеттілігі; 2) ойыншы талдау объектісіне қатысты статистикалық ақпараттың жеткілікті көлеміне ие болған жағдайда ғана қолдануға болады және ақталады.
2	Шығындардың (инвестициялар-дың) орындылығын талдауға негізделген әдістер мен модельдер	1) осы әдіске және тиісті үлгілерге сәйкес тәуекел деңгейлерін айқындау ЦКВ-мен мәмілелер кезінде тәуекелдердің әлеуетті аймақтарын сәйкестендіруге бағдарланған; 2) ғылыми әдебиеттерде жақсы зерттелген және сипатталған.	1) тәуекел шамасы тұтас шама ретінде қабылданса, тиісінше мәміле тәуекелінің көп құрамдас бөлігі қаралмайды; 2) ЦКВ нарығында барлық тәуекел факторларын ескейтеңгейлі есепке алу бойынша мүмкіндіктер жоқ.
3	Сараптамалық бағалау әдістері	1) іске асырудың қарапайымдылығы; 2) әдістеме жақсы пысықталған және бағалауды жүргізуге арналған бағдарламалық құрал бар.	1) субъективті сипатқа ие; 2) тәуекелге сараптамалық зерттеу жүргізудің барлық кезеңдерін дайындауға және іске асыруға үлкен уақыт шығындары; 3) сарапшылар арасында коммуникацияның болмауы қиын жағдайларда сарапшылардың пікірлерін келісу кезінде қателіктерге әкелуі мүмкін.
4	Аналогтарды қолдану әдісі	1) қарапайымдылық және жылдам нәтиже; 2) прецеденттерге сүйенеді; 3) прецеденттердің көбеюі тәуекелдерді талдауға үлкен негіз береді.	1) Жаңа ЦКВ үшін аналогтарды табу және бағалау қиын; 2) Егер аналогтар болмаса, онда ЦКВ нарығында барлық тәуекел факторларын ескейтеңгейлі есепке алу мүмкіндігі жоқ.

2-кестенің жалғасы

1	2	3	4
5	ЦКВ нарығындағы тәуекелдерді бағалаудың аналитикалық әдістері	Үлкен әртүрлілік, бұл оларды тәуекелдерді бағалау үшін қолданылатын әртүрлі бағдарламалық платформалар үшін тартымды етеді.	Көптеген модельдер ЦКВ нарығында оқытылмаған ойыншылардың қабылдауы үшін жеткілікті күрделі.
5.1	Ықтималдық	1) ЦКВ нарығында сценарийлердің толық спектрін талдау мүмкін; 2) теңдестірілген тәсілдер; 3) ЦКВ нарығының элементтері арасындағы өзара тәуелділіктер айқын түрде ескеріледі; 4) белгісіздіктердің тәуекелдерді қорытынды бағалауға әсерін сандық түрде анықтауға болады.	1) тәуекелдерді талдау кезінде үлкен еңбек шығындары; 2) үлкен белгісіздік салдарынан бірқатар жағдайларда қолайлы нәтижелерді алу қиын.
5.2	Детерминистік	1) тәуекелдердің барлық аспектілері айқын түрде қаралады; 2) осы әдіс шеңберіндегі әдебиеттерде жақсы сипатталған модельдер.	1) есептеу ресурс тарына қойылатын ар тық талаптар; 2) нарықтағы ойыншы лардың әрекеттеріне тәуелділікке байланыс ты кейбір мәселелер шешілмеген; 3) тәуекелдерді есеп теу кезіндегі белгісіз діктер жүйелі түрде талданбайды.
5.3	Шешім ағашы	1) тәуекелдерді бағалаудың барлық бөлшектерін дәл ғрафикалық түрде ұсыну қамтамасыз етіледі; 2) мәселені шешудің ең жақсы жолдарын анықтауға болады.	1) талдау қиын 2) үлкен ағаштар; 3) шешім ағашының диа-ғраммасын қолда ну көбінесе ЦКВ нары ғындағы жағдайды тым жеңілдетуге әкеледі.
5.4	Имитациялық модельдеу	1) тәуекелдерді талдау кезінде нәтижелерді қарапа йым қабылдау; 2) әдістер мен модельдерді кіріс деректерін кез келген үлестіруге бейімдеу мүмкіндігі; 3) тәуекелге әсер ететін факторлар арасындағы кез келген өзара байланыстар мен өзара іс-қимылдарды ескеру мүмкіндігі.	1) тәуекелді модельдеу үшін статистикалық деректерді жинау қиын; 2) есептеулерде пайдаланы-латын айнымалыларды бөлу функцияларын таңдау кезіндегі түсініксіздік; 3) барабар модельдеу моделін жасау қиын; 4) шешімнің дәлдігі Итераңия санына тура пропорционал; 5) пайда болу ықтималдығы өте жоғары немесе төмен оқиғаларды барабар модельдеу мүмкін емес.

2-кестенің соңы

1	2	3	4
5.5	Бұлыңғыр логиканы (БЛ) қолдануға негізделген тәуекелдерді бағалау	1) тәуекелдерді бағалаудың қолданыстағы әдістерінің кемшіліктері мен шектеулерін еңсереді; 2) анық емес кіріс деректерімен де, лингвистикалық критерийлермен де жұмыс істеуге болады.	1) тиістілік функцияларын таңдау және тәуекелдерді бағалау кезінде анық емес енгізу қағидаларын қалыптастыру кезіндегі субъективтілік; 2) арнайы бағдарламалық жасақтаманың қажеттілігі.

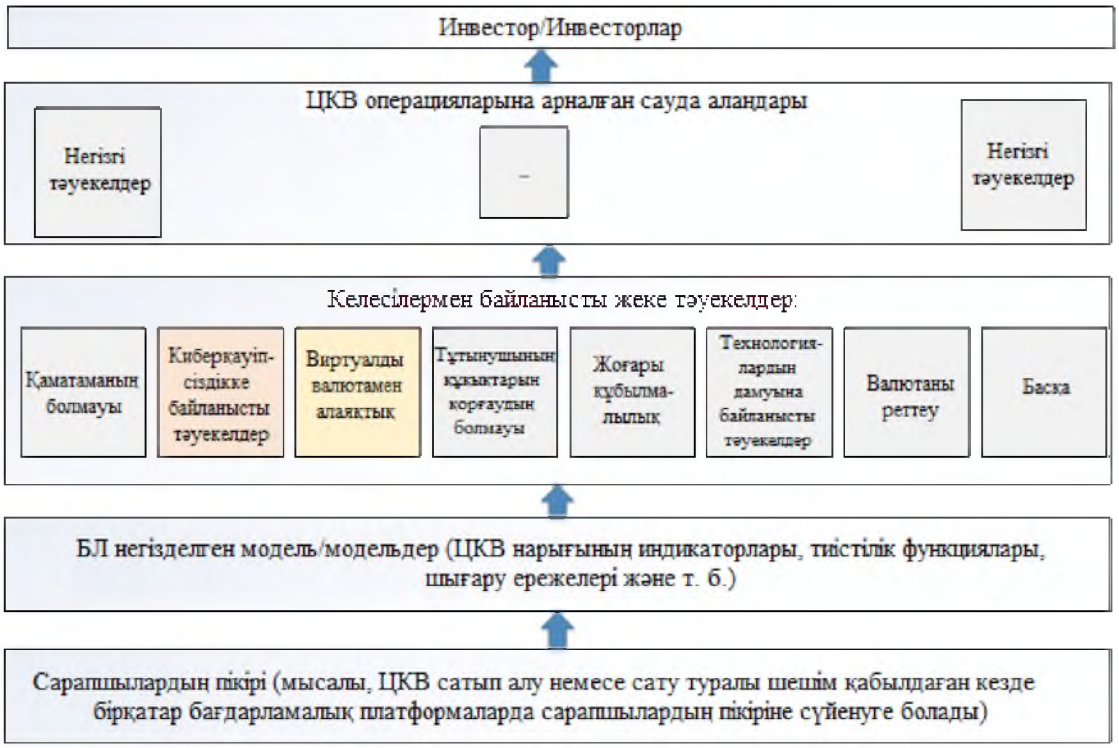
2-кестеде жүргізілген талдау көрсеткендей, тәуекелдерді бағалау жүйелері мен модельдері, соның ішінде БЛ аппаратын қолдану негізінде құрылған ЦКВ нарығы үшін логикалық және жоғары тұрақтылықпен сипатталуы мүмкін. Бұл, әсіресе, инвесторлар үшін тәуекелдерді талдау нарықтағы жағдай туралы бастапқы деректер мен білімнің жетіспеушілігі жағдайында жүзеге асырылатын ЦКВ нарығына тән жағдайлар үшін өте маңызды. Бұл жағдайда НЛ аппараты сарапшыларға ЦКВ-ға инвестициялау тәуекелдерін бағалаудың мәніне назар аударуға мүмкіндік береді. Өз кезегінде, мұндай талдау нарықтың негізгі факторлары, жеке көрсеткіштер мен факторлар арасындағы себеп-салдарлық байланыстарды қарастыруды қамтиды.

Нәтижелері және оларды талқылау. Мысалы, 1-суретте БЛ математикалық аппаратын қолдануға негізделген ЦКВ биржасы қызметтерінің ақпараттық қауіпсіздігінің тәуекелдерін қарапайым талдау схемасы келтірілген.

1-суретте көрсетілген құрылым жоғары көтермелі болып табылады. Бұл құрылымның негізінде ЦКВ нарығына тән жеке тәуекелдер жатыр. Содан кейін анықталған тәуекелдер (және мұндай анықтау, мысалы, сараптамалық әдістерді қолдану арқылы алынуы мүмкін) ЦКВ саудасымен айналысатын жеке биржалар деңгейінде топтастырылады. Бұл ЦКВ-ға инвестициялауға байланысты АҚ-ның негізгі тәуекелдерін анықтауға мүмкіндік береді. Дәл осы тәуекелдерге ЦКВ нарығындағы трендтерді болжауға маманданған жеке инвесторларға да, талдаушыларға да назар аударуға болады.

1-суретте көрсетілген нарықтағы АҚ тәуекелдерін бағалаудың иерархиялық құрылымы қаржы нарықтарына тән тәуекелдердің басқа түрлерімен салыстырылуы мүмкін. Егер ЦКВ нарығындағы тәуекелдердің әрқайсысының әсерін талдау кезінде қолданылатын өлшем бірліктерін бірыңғай параметрге бейімдеу мүмкін болса, мысалы, дұрыс емес инвестициялау стратегиясын таңдағанда және АҚ тәуекелдерін ескермегенде инвесторға зиян келтіру немесе қаржы ресурстарын жоғалту ықтималдығы.

БЛ аппаратының тәуекелдерін бағалау үшін пайдаланылған жағдайда, жиынтық залалдар анық емес жиындарды анық емес сандарға түрлендіру нәтижелері негізінде болжануы немесе анықталуы мүмкін (мысалы, ойын моделін пайдалану кезінде). Бұлыңғыр логикалық модельдер АҚ-ке қауіп төнген жағдайда және хакерлер КВБ үшін қызметтерді қорғаудағы олқылықтарды пайдаланған жағдайда ЦКВ-дағы инвесторлардың жалпы шығындарын сипаттай алады. Сонымен қатар, ЦКВ-ға инвестициялауға бағытталған қаржы ресурсын жоғалтудың негізгі тәуекелін анықтаудан басқа, сіз БЛ аппаратының көмегімен белгілі бір тәуекелдің себептерін сипаттай аласыз, мысалы, 1-суретте көрсетілген тәуекелдер тобынан. Бұл ақпаратты өз тәуекелдерін азайтуға тырысатын әлеуетті инвестор басшылыққа ала алады.



1-сурет. ЦКВ-мен операцияларға тән тәуекелдерді бағалаудың құрылымдық схемасы (автор сараптамалық әдістер мен БЛ аппаратын біріктіру негізінде әзірлеген)

КВБ-ны бұзудан басқа, зиянкестер әлеуметтік инженерия әдістерін жиі қолдана бастады. Бұл көбінесе нәтиже береді, әсіресе киберқылмыскерлерге ЦКВ нарығындағы жаңадан келген ойыншы қарсы болған кезде.

Мұндай шабуылдардан қорғану өте қиын және ең сенімді әдіс-нарықтағы ойыншылардың сауаттылығын арттыру және ЦКВ-мен операциялар жасау кезінде әдеттегі қырағылық.

КВБ-ға бағытталған шабуылдардың саны артуы мүмкін, өйткені шабуылдаушылар сәтті шабуылды жүзеге асыру барысында өте үлкен сыйақы ала алады.

Киберқауіпсіздік саласындағы жетекші компаниялар әзірге КВБ қызметіне байланысты киберқауіптердің жаңа ландшафтын қалыптастыра бастағанын ескеріңіз. Ал КВБ жасаушылар ЦКВ-пен мәмілелер бойынша жылдам пайданы артық көре отырып, ДБ АҚ-ға инвестиция салуға әлі дайын емес.

Қорытындылар. Осылайша, жұмыста осындай негізгі нәтижелер алынды:

1) тәуекелдерді бағалау үшін қолданылатын әдістер мен модельдерге, оның ішінде ЦКВ ақпараттық қауіпсіздігіне байланысты және тиісті КВБ-ға шолу және талдау жасалды;

2) бұл нарыққа деген қызығушылық салыстырмалы түрде аз уақыт ішінде тез өсетіні көрсетілген. Сонымен қатар, бүгінде көптеген мемлекеттер мен олардың қаржы ұйымдары, мысалы, банктер, несиелік және сақтандыру компаниялары өз активтерінде ЦКВ-ға ие;

3) КВБ қызметін қамтамасыз ететін электрондық сервистердің АҚ қамтамасыз ету міндетін шешудің аралас әдістерін дамытуды көздейтін бағыт перспективалы болып табылатыны анықталды.

Әдебиеттер тізімі

1. Ertz, M., & Boily, É. The rise of the digital economy: Thoughts on blockchain technology and cryptocurrencies for the collaborative economy // International Journal of Innovation Studies, 2019, no. 3(4). – Pp. 84-93.
2. Bunjaku, F., Gjorgieva-Trajkovska, O., & Miteva-Kacarski, E. Cryptocurrencies–advantages and disadvantages // Journal of Economics, 2017. – No. 2(1). – Pp. 31-39.
3. Sapovadia, V. Legal issues in cryptocurrency // In Handbook of Digital Currency Academic Press. 2015. – Pp. 253-266.
4. Haynes, A., & Yeoh, P. Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues // Taylor & Francis. 2020.
5. T. Zoumpekas, E. Houstis, and M. Vavalis, Eth analysis and predictions utilizing deep learning // Expert Systems with Applications, 2020. – Vol. 162. – P. 113866.
6. Mallqui, D. C., & Fernandes, R. A. Predicting the direction, maximum, minimum and closing prices of daily Bitcoin exchange rate using machine learning techniques // Applied Soft Computing, 2019. – No. 75. – Pp. 596-606.
7. Mannaro, K., Pinna, A., & Marchesi, M. Crypto-trading: Blockchain-oriented energy market // In 2017 AEIT International Annual Conference IEEE. 2017, September. – Pp. 1-5.
8. Kim, C. Y., & Lee, K. Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats // In 2018 international conference on platform technology and service (PlatCon) IEEE. 2018, January. – Pp. 1-6.
9. Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., Wallace, D., & Veron, J. F. An investigative study of links between terrorist attacks and cryptocurrency markets // Journal of Business Research, 2022. – No. 147. – Pp. 177-188.
10. Caporale, G.M., Kang, W.Y., Spagnolo, F., & Spagnolo, N. Cyber-attacks and cryptocurrencies // CESifo Working Paper. 2020. – No. 8124.
11. Аксенова, Н.И., & Спиридонова, Е.А. Криптовалютный рынок: потенциал, риски и драйверы развития // Закономерности и тенденции формирования системы финансово-кредитных отношений, 2021. – С. 4-23.
12. Alkhalifah, A., Ng, A., Kayes, A.S. M., Chowdhury, J., Alazab, M., & Watters, P.A. A taxonomy of blockchain threats and vulnerabilities. In Blockchain for Cybersecurity and Privacy // CRC Press. 2020. – Pp. 3-28.
13. Alvarez-Ramirez, J., Rodriguez, E., & Ibarra-Valdez, C. Long-range correlations and asymmetry in the Bitcoin market // Physica A: Statistical Mechanics and its Applications, 2018. – No. 492. – Pp. 948-955.
14. Ding, Y., & Chen, W. Probing the Mystery of Cryptocurrency Exchange: The Case Study Based on Mt. Gox // In 2022 International Conference on Service Science (ICSS) IEEE. 2022, May. – Pp. 297-304.
15. Boireau, O. Securing the blockchain against hackers // Network Security, 2018. – No. 2018(1). – Pp. 8-11.
16. Hu, J., Luo, Q., & Zhang, J. The fluctuations of bitcoin price during the hacks // International Journal of Applied Research in Management and Economics, 2020, no. 3(1). – Pp. 10-20.
17. Astrakhantseva, I., Astrakhantsev, R., & Los, A. Cryptocurrency fraud schemes analysis // In SHS Web of Conferences. EDP Sciences. 2021, Vol. 106. – P. 02001.
18. Andryukhin, A.A. Phishing attacks and preventions in blockchain based projects. In 2019 International Conference on Engineering Technologies and Computer Science (EnT). IEEE. 2019, March, pp. 15-19.
19. Aggarwal, S., & Kumar, N. Attacks on blockchain // In Advances in Computers, 2021, Vol. 121. – Pp. 399-410.
20. Mrazek, K., Holton, B., Cathcart, C., Speirer, J., Do, J., & Mohd, T. K. Risks in Blockchain–A Survey about Recent Attacks with Mitigation Methods and Solutions for Overall // In 2022 IEEE International Conference on Electro Information Technology (eIT), IEEE. 2022, May. – Pp. 5-10.

References

1. Ertz, M., & Boily, É. The rise of the digital economy: Thoughts on blockchain technology and cryptocurrencies for the collaborative economy // International Journal of Innovation Studies, 2019, no. 3(4). – Pp. 84-93.

2. Bunjaku, F., Gjorgieva-Trajkovska, O., & Miteva-Kacarski, E. Cryptocurrencies-advantages and disadvantages // Journal of Economics, 2017. – No. 2(1). – Pp. 31-39.
3. Sapovadia, V. Legal issues in cryptocurrency // In Handbook of Digital Currency Academic Press. 2015. – Pp. 253-266.
4. Haynes, A., & Yeoh, P. Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues // Taylor & Francis. 2020.
5. T. Zoumpekas, E. Houstis, and M. Vavalis, Eth analysis and predictions utilizing deep learning // Expert Systems with Applications, 2020. – Vol. 162. – P. 113866.
6. Mallqui, D. C., & Fernandes, R. A. Predicting the direction, maximum, minimum and closing prices of daily Bitcoin exchange rate using machine learning techniques // Applied Soft Computing, 2019. – No. 75. – Pp. 596-606.
7. Mannaro, K., Pinna, A., & Marchesi, M. Crypto-trading: Blockchain-oriented energy market // In 2017 AEIT International Annual Conference IEEE. 2017, September. – Pp. 1-5.
8. Kim, C. Y., & Lee, K. Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats // In 2018 international conference on platform technology and service (PlatCon) IEEE. 2018, January. – Pp. 1-6.
9. Almaqableh, L., Reddy, K., Pereira, V., Ramiah, V., Wallace, D., & Veron, J. F. An investigative study of links between terrorist attacks and cryptocurrency markets // Journal of Business Research, 2022. – No. 147. – Pp. 177-188.
10. Caporale, G.M., Kang, W.Y., Spagnolo, F., & Spagnolo, N. Cyber-attacks and cryptocurrencies // CESifo Working Paper. 2020. – No. 8124.
11. Aksenova, N.I., & Spiridonova, E.A. Kriptovalyutnyj rynok: potencial, riski i drajvery razvitiya // Zakonomernosti i tendencii formirovaniya sistemy finansovo-kreditnyh otnoshenij, 2021. – C. 4-23.
12. Alkhalifah, A., Ng, A., Kayes, A.S. M., Chowdhury, J., Alazab, M., & Watters, P.A. A taxonomy of blockchain threats and vulnerabilities. In Blockchain for Cybersecurity and Privacy // CRC Press. 2020. – Pp. 3-28.
13. Alvarez-Ramirez, J., Rodriguez, E., & Ibarra-Valdez, C. Long-range correlations and asymmetry in the Bitcoin market. // Physica A: Statistical Mechanics and its Applications, 2018. – No. 492. – Pp. 948-955.
14. Ding, Y., & Chen, W. Probing the Mystery of Cryptocurrency Exchange: The Case Study Based on Mt. Gox // In 2022 International Conference on Service Science (ICSS) IEEE. 2022, May. – Pp. 297-304.
15. Boireau, O. Securing the blockchain against hackers // Network Security, 2018, no. 2018(1). – Pp. 8-11.
16. Hu, J., Luo, Q., & Zhang, J. The fluctuations of bitcoin price during the hacks // International Journal of Applied Research in Management and Economics, 2020, no. 3(1). – Pp. 10-20.
17. Astrakhantseva, I., Astrakhantsev, R., & Los, A. Cryptocurrency fraud schemes analysis // In SHS Web of Conferences. EDP Sciences. 2021, Vol. 106. – P. 02001.
18. Andryukhin, A.A. Phishing attacks and preventions in blockchain based projects. In 2019 International Conference on Engineering Technologies and Computer Science (EnT). IEEE. 2019, March. – Pp. 15-19.
19. Aggarwal, S., & Kumar, N. Attacks on blockchain // In Advances in Computers, 2021, Vol. 121. – Pp. 399-410.
20. Mrazek, K., Holton, B., Cathcart, C., Speirer, J., Do, J., & Mohd, T. K. Risks in Blockchain–A Survey about Recent Attacks with Mitigation Methods and Solutions for Overall // In 2022 IEEE International Conference on Electro Information Technology (eIT), IEEE. 2022, May. – Pp. 5-10.