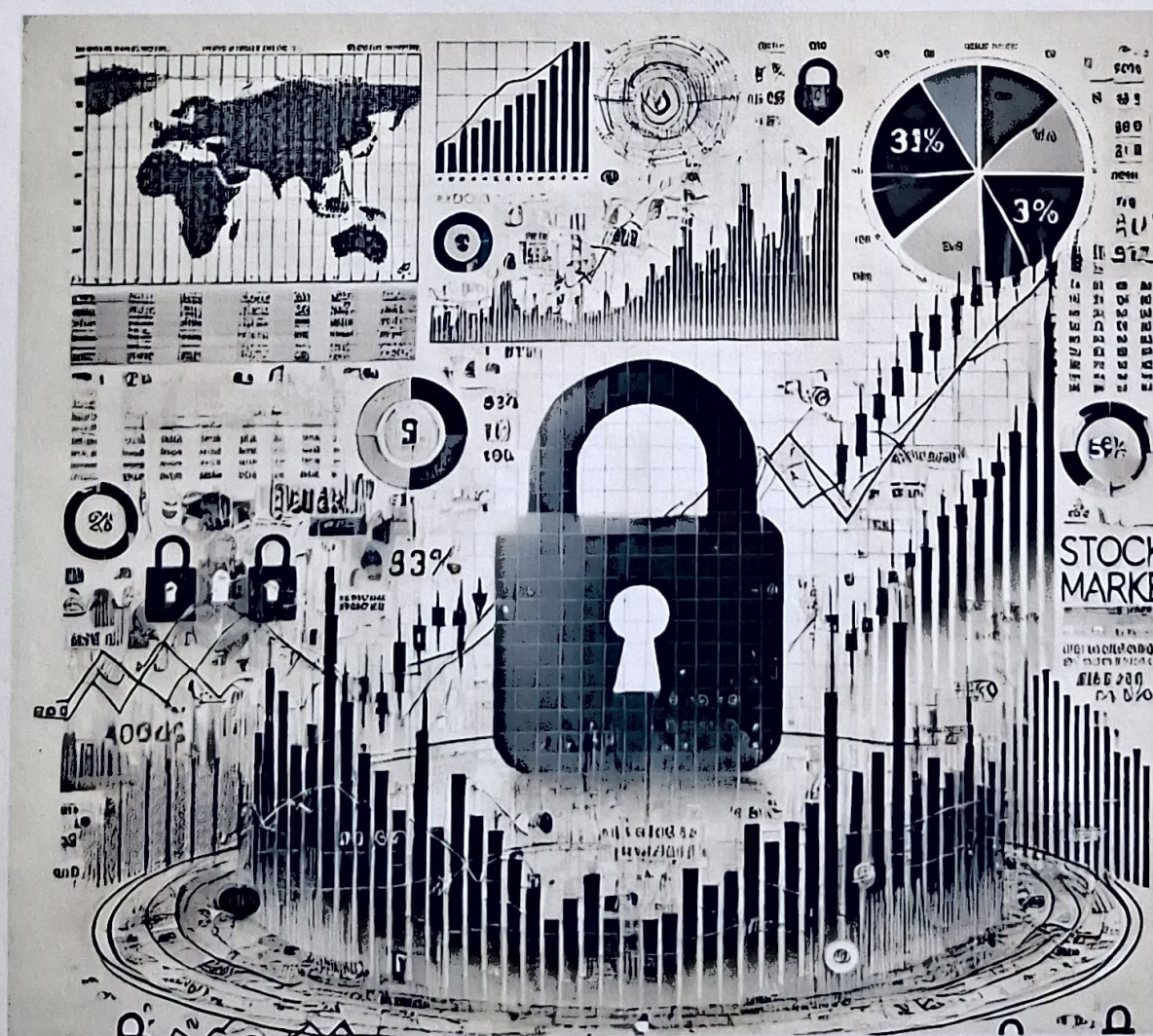


ИСАЕВА Г.К.

КИБЕР ҚАУІП-ҚАТЕРЛЕР ЖАҒДАЙЫНДА КОМПАНИЯЛАРДЫҢ ҚАРЖЫ ЖӘНЕ ИНВЕСТИЦИЯЛЫҚ САЯСАТЫН ЖЕТІЛДІРУ



**ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ
ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

М.ӘУЕЗОВ ат. ОҢТҮСТІК ҚАЗАҚСТАН УНИВЕРСИТЕТІ

Исаева Г.К.

**КИБЕР ҚАУІП-ҚАТЕРЛЕР ЖАҒДАЙЫНДА
КОМПАНИЯЛАРДЫҢ ҚАРЖЫ ЖӘНЕ
ИНВЕСТИЦИЯЛЫҚ САЯСАТЫН ЖЕТІЛДІРУ**

Монография

Шымкент, 2025

ӘОЖ 336:004
ББК 65,26:32.973
И83

М.Әуезов ат. Оңтүстік Қазақстан университетінің Ғылыми кеңесімен баспаға ұсынылған (хаттама № 8, 30.01.2025 ж.).

Пікір жазғандар:

Есиркепова А.М. – М.Әуезов атындағы ОҚУ «Экономика» кафедрасының меңгерушісі, э.ғ.д., профессор

Куралбаева А.Ш. – Орталық Азия инновациялық университеті «Бизнес және туризм» кафедрасының профессоры, э.ғ.д.

Купешев А.Ш. – «Мирас» университетінің профессоры, э.ғ.д.

Исаева Г.К.

И83 Кибер қауіп-қатерлер жағдайында компаниялардың қаржы және инвестициялық саясатын жетілдіру: Монография – Шымкент: GOLDDYES, 2025. – 112 бет.

ISBN 978-601-7787-99-8

Бұл монография кибер қауіп-қатерлердің компаниялардың қаржылық тұрақтылығына, нарық құнына және инвестициялық саясатына әсерін зерттеуге арналған. Жұмыста кибершабуылдар кезінде компаниялардың аномальды кірістілігі (CAR) анықталып, осы оқиғаларға деген нарықтың реакциясы Event Study және Difference-in-Differences заманауи эконометрикалық әдістерді қолдана отырып зерттелді.

Монографияның теориялық, әдістемелік және практикалық маңызы бар және жоғары оқу орындарының қызметкерлеріне, магистранттар мен докторанттарға, қаржы нарығының қызмет ету ерекшеліктеріне қызығушылық танытатын ғылыми қызметкерлерге арналған.

ӘОЖ 336:004
ББК 65,26:32.973

ISBN 978-601-7787-99-8

© Исаева Г.К., 2025

МАЗМҰНЫ

Кіріспе	4
Тарау 1. Кибер тәуекелдерді басқарудың теориялық негіздері және олардың компанияның қаржы және инвестициялық саясатына ықпалы	8
1.1 Корпоративтік ортадағы кибершабуылдардың классификациясы	8
1.2 Компаниялардың инвестициялық саясаты және оның кибершабуылдарға осал болу факторлары	14
1.3 Киберқауіпсіздік тәуекелдерін басқару жүйесін құрудың негіздері	20
Тарау 2. Компаниялардың қаржылық көрсеткіштеріне және инвестициялық саясатына кибершабуылдардың әсерін талдау	28
2.1 Компаниялардың қызметіне кибершабуылдардың әсерін талдаудың әдістемелік негіздері	28
2.2 АҚШ компанияларының мысалында кибершабуылдардың қаржылық салдарын талдау	49
2.3 Event study әдісі арқылы кибершабуылдардың компания құнына әсерін талдау	61
2.4 Компаниялардың инвестициялық стратегиясына кибер қауіп-қатерлерінің әсері	80
Тарау 3. Кибер қауіп-қатерлер жағдайында компаниялардың қаржылық тұрақтылығын қамтамасыз ету тетіктері	86
3.1 Қаржылық менеджменттің элементі ретінде киберқауіпсіздік тәуекелдерін бағалау әдістерін жетілдіру	86
3.2 Компаниялардағы киберқауіпсіздік стратегиясын оңтайландыру жолдары	93
Қорытынды	99
Пайдаланған әдебиеттер тізімі	101
Қосымша А - CAR орташа мәнінің үлестірілуі	108
Қосымша В - t-тестінің нәтижелері	109

КІРІСПЕ

2019 жылдың 29 шілдесінде американдық Capital One Financial банкінің 100 миллионнан астам клиенттерінің жеке мәліметтері көпшілікке жария болды. Нәтижесінде, келесі күннің өзінде компания акцияларының құны шамамен 6%-ға төмендеді, ал деректердің жария болуынан туындаған компанияның қосымша шығындары 100 миллион доллардан асты [1]. 2019 жылдың желтоқсанында Travelex компаниясы өзінің хакерлік шабуылдың құрбаны болғанын жариялады. Қылмыскерлер пайдаланушылардың жеке деректерін, соның ішінде шот иесінің аты-жөні мен несие картасы туралы мәліметтерді жарияламау үшін компаниядан қомақты қаржы талап еткендігі мәлім болды. Бұл Travelex компаниясына 25 миллион фунт стерлинг көлемінде шығын әкелді [2]. Бұл, кибершабуылдардың компанияларға айтарлықтай үлкен қаржылық шығындар әкелетінін көрсететін мысалдар. 2020 жылы кибершабуылдардан туындаған жалпы шығын 2019 жылмен салыстырғанда 600 миллион АҚШ долларға артып, 1,8 миллиард АҚШ долларын құрады [3].

Кибершабуылдар саны белсенді цифрландырудың арқасында өсуде. Қазіргі уақытта кез келген компания деректердің желіге ағып кету қаупіне тап болуы мүмкін, сондықтан кибершабуылдар компаниялардың қызметіне және олардың қаржылық көрсеткіштеріне қалай әсер ететінін зерттеу маңызды.

Соңғы жылдары кибершабуылдардың компаниялардың нарық құнына әсерін талдауға арналған зерттеулер көптеп жүргізілуде. Дегенмен, кибершабуылдардың компаниялардың операциялық, инвестициялық және қаржылық шешімдеріне қалай әсер ететініне жеткілікті көңіл бөлінбей жүр. Бұл жұмыс кибершабуылдардың компаниялардың ерекше сипаттамаларына байланысты (мысалы, компанияның өлшемі мен саласы) жиынтық аномальды кірістілікке (CAR) қалай әсер ететінін зерттеуге арналған. Сонымен қоса, монографияда компаниялардың кибершабуылдарға қалай жауап беретіні, компаниялардың инвестициялық және қаржылық стратегияларын қалай соған сәйкес беімдейтіні зерттеледі.

Мәселенің зерттелу деңгейі. Campbell et al. (2003), Garg et al. (2003a, 2003b), Novav & D'Arcy (2003, 2004), Cavusoglu et al. (2004) и Kamiya (2018) жүргізген зерттеулері кибершабуылдар

компанияның нарық құнын төмендетуі мүмкін екенін көрсетті [4-10]. Сондай-ақ, Cavusoglu et al. (2004), Novav & D'Arcy (2003), Novav et al. (2017) кибершабуылдардың салдары бұзушылықтың түріне және компанияның ерекшеліктеріне байланысты екенін анықтады [11-13]. Gordon et al. (2003), Mukhopadhyaya et al. (2013), Low (2017), Kamiya (2021), Garg (2020) кибершабуылдардың компаниялардың кірістеріне, пайдасына, беделіне және қаржылық саясатына әсерін анықтады, бірақ бұл нәтижелері анық болмады [14-18]. Бұл жаңа деректерді ескере отырып және бұрынғы зерттеу тәсілдерін негізге ала отырып, кибершабуылдардың компаниялар қызметіне, инвестициялық және қаржылық стратегиясына әсерін толығырақ зерттеудің маңыздылығын көрсетеді.

Зерттеудің мақсаты – киберқауіпсіздіктің бұзылуы компанияның құнына, оның қаржылық және инвестициялық саясатына қалай әсер ететінін анықтау.

Осы мақсатқа жету үшін монографияда бірнеше гипотеза қарастырылды:

- бірінші гипотеза кибершабуылдар компания акцияларының кірістілігін төмендетеді, теріс жиынтық аномальды кірістілікті (CAR) тудырады деп болжайды;

- екінші гипотеза мұндай шабуылдарға нарықтың реакциясы компанияның түріне және оның ерекше сипаттамаларына байланысты екенін тұжырымдайды;

- үшінші гипотеза компанияның көлеміне байланысты шабуылдардың әсер етуі айтарлықтай ерекшеленеді, яғни ірі және шағын компаниялар үшін олардың салдары әртүрлі болады деп болжанады;

- төртінші гипотеза кибершабуыл түрлері акциялар кірістілігіне әртүрлі әсер етеді деп болжайды;

- бесінші гипотеза кибершабуылдар компанияның қызметіне, инвестицияларына және қаржылық саясатына әсер етіп, оның стратегиясында өзгерістер туғызады деп тұжырымдайды.

Бұл зерттеуде кибершабуылдардың жиынтық аномальды кірістілікке (CAR) қалай әсер ететінін зерттеу үшін «Event Study» әдістемесі пайдаланылған. «Difference-in-Differences» әдісі осындай оқиғалардың компаниялардың операциялық тиімділігіне, инвестициялары мен қаржылық саясатына әсерін бағалау үшін қолданылды. Компания түріне, фирма көлеміне және бұзушылық

түріне байланысты CAR қалай өзгередінін анықтау үшін *t*-тесті жүргізілді. CAR көрсеткішіне әсер ететін факторларды анықтау үшін OLS (Ordinary Least Squares) регрессиялық талдауы жүргізілді.

Зерттеуге арналған деректер Audit Analytics дерекқорынан жиналды, ал акциялардың құны мен нарықтағы кірістілік туралы ақпарат The Center for Research in Security Prices (CRSP) дерекқорынан алынды. Компания қызметінің жылдық көрсеткіштері Compustat деректер базасынан сұралып, пайдаланылды.

Зерттеу нәтижесінде қол жеткізілген нәтижелер:

1. Кибершабуылдар компаниялардың қаржылық және инвестициялық саясатына қалай ықпал тигізетіні талданды. Зерттеу нәтижелері алдыңғы жұмыстардың қорытындыларын растап берді. *t*-тест талдауы кибершабуылдардың фирма құнына айтарлықтай теріс әсер ететінін дәлелдеді. Әсіресе, шағын компаниялар акцияларының нарық құны кибершабуылдардан кейін айтарлықтай төмендеуге бейім екендігі байқалды.

2. Жүргізілген *t*-тест кибершабуылдарға деген нарық реакциясы компанияның саласы, көлемі немесе шабуыл түрі сияқты факторларға байланысты болмайтынын көрсетті.

3. «Difference-in-Differences» тесті шабуылдарға дейін және одан кейін компаниялардың қызметінде айтарлықтай өзгерістерді анықтаған жоқ.

4. Зерттеу нәтижелері компаниялар шабуылдан кейінгі бірінші жылы ғылыми-зерттеу және тәжірибелік-конструкторлық шығындарды, екінші жылы сатылым көлемін және үшінші жылы ұзақ мерзімді міндеттемелерді көбейтетінін көрсетті.

5. Бизнестің цифрлық трансформациясы жағдайында компаниялардың инвестициялық саясатын жетілдіру бойынша ұсыныстар әзірленді.

6. Компаниялардың стратегиялық жоспарлау жүйелеріне біріктірілген киберқауіпсіздік стратегияларын оңтайландыру әдістері ұсынылды.

Жұмыста әзірленген ұсыныстарды қолданыстағы корпоративтік басқару жүйелерінде пайдалануға болады. Бұл тәуекелдерді азайтуға мүмкіндік беріп, компаниялардың кибершабуылдарға қарсы қаржылық тұрақтылығын нығайтады.

Сондай-ақ, әзірленген ұсыныстар өсіп келе жатқан киберқауіптер жағдайында басқару тиімділігін арттырудың негізі бола алады. Монографияда ұсынылған зерттеу әдістемесі жаңа заңнаманы енгізу, салық жеңілдіктерін енгізу, компания менеджерлерін ауыстыру және басқа да оқиғаларды талдау кезінде пайдаланылуы мүмкін. Жұмыс экономика және қаржы саласындағы магистранттар мен докторанттар үшін, сондай-ақ стратегиялық шешімдерді әзірлеу мақсатында қаржы менеджерлері үшін де практикалық маңызға ие.

ТАРАУ 1. КИБЕР ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ ЖӘНЕ ОЛАРДЫҢ КОМПАНИЯНЫҢ ҚАРЖЫ ЖӘНЕ ИНВЕСТИЦИЛЫҚ САЯСАТЫНА ЫҚПАЛЫ

1.1 Корпоративтік ортадағы кибершабуылдардың классификациясы

Цифрландыру дәуірінде біздің әрқайсымыз үшінші тарап бағдарламалық құралын орнату немесе іздеу жүйесін өзгерту сияқты жүйеге қажетсіз өзгерістер енгізетін кибершабуылдың қандай да бір түріне тап болудамыз. Мұндай кибершабуылдар браузерде қосымша терезелердің кездейсоқ пайда болуы түріндегі шағын зиян келтіруі, немесе қатты дискіні пішімдеу түріндегі айтарлықтай зиянға да ұшыратуы мүмкін. Осылайша, кибершабуылдар сипаты мен келтіретін зиян түріне қарай әр түрлі болады.

Кибершабуылдар — компьютерлер арқылы компьютердің ақпараттық жүйесіне, веб-сайтқа, дербес компьютерлерге қарсы жасалған және компьютердің және онда сақталған деректердің тұтастығын, қолжетімділігін және құпиялылығын бұзатын шабуылдар. Осылайша, әртүрлі зиянды бағдарламаларды пайдаланатын кибершабуылдар осал жүйені бұзу арқылы ақпаратты ұрлауы, өзгертуі немесе жоюы мүмкін. Кибершабуылдардың нысанасы компаниялар да, тұтас елдердің жүйелері де болуы мүмкін.

Кибершабуылдардың мынадай түрлері белгілі:

Backdoors (жасырын есіктер) — шабуылдаушы бағдарламалық жасақтаманы орнату үшін жасырын есіктерді пайдаланып кіреді, яғни ол жүйеңізге жасырын кіруді қамтамасыз ететін киберқауіптің бір түрі. Бұл бағдарламалық құрал ақпаратты ұрлауға, файлдарды өзгертуге, қажетсіз бағдарламалық құралды орнатуға немесе тіпті бүкіл компьютерді басқаруға мүмкіндік береді.

Әдепкі құпия сөздер, оларды пайдаланушы өзгертпесе, *backdoors* ретінде жұмыс істей алады. Кейбір бағдарламаларды орнату қызметтері, егер олар шығарылым нұсқасында жойылмаса, жасырын есік ретінде пайдаланылуы мүмкін.

2014 жылдың қаңтарында Backdoors бағдарламалық құралы Galaxy құрылғылары сияқты кейбір Samsung Android өнімдерінде табылды. Осылайша, олар құрылғыда сақталған деректерге қашықтан қол жеткізуді қамтамасыз етті. Атап айтқанда, Samsung IPC (Inter-Process Communication) протоколы арқылы модеммен байланысты өңдеуге жауапты Samsung Android бағдарламалық құралы қашықтағы файл сервері (RFS - Real File Simulator) пәрмендері деп аталатын сұраулар класын пайдалану арқылы backdoors операторы қашықтан енгізу операцияларын, мысалы модем арқылы қатты дискіде немесе басқа жадыда қашықтан енгізу операцияларын орындауға мүмкіндік береді. Модем Samsung компаниясының меншікті Android бағдарламалық құралын іске қосатындықтан, ол қашықтан басқару құралын ұсынады, сондықтан оны кейін RFS пәрмендерін шығару және құрылғыдағы файлдық жүйеге кіру үшін пайдалануға болады.

Denial-of-Service Attack (DoS - қызмет көрсетуден бас тарту шабуылы) желіге шабуыл жасап, интернетке қосылған негізгі құрылғыға әсер ететін пайдасыз трафикпен оны толығымен бұзады. DoS шабуылы серверлерде орналастырылған веб-сайттарға немесе қызметтерге бағытталған. Шабуылдың бұл түрі банк серверлері мен несие картасының төлем шлюздерін нысанаға алады.

Direct-access Attack (тікелей қол жеткізу шабуылы) компьютерге немесе оның бір бөлігіне физикалық қол жеткізуді қамтамасыз етеді және қауіпсіздікті бұзу үшін әртүрлі функцияларды орындайды немесе әртүрлі құрылғыларды орнатады. Шабуылдаушы вирустары бар бағдарламалық құралды орнатуы немесе маңызды ақпаратты жүктеп алуы мүмкін.

Eavesdropping (жасырын тыңдау) желідегі хосттар арасындағы сөйлесулерді жасырын тыңдауға мүмкіндік береді. Тыңдау үшін Carnivore және Narus Insight сияқты әртүрлі бағдарламалар пайдаланылуы мүмкін.

Spoofing (жалған деректер) – жүйеге заңсыз қол жеткізу үшін жалған деректер жасау арқылы адам немесе бағдарлама басқа біреудің кейпіне енетін кибершабуыл. Мұндай қауіптер әдетте мекенжайы жалған электрондық хаттарда кездеседі.

Tampering (бұрмалау) - бұл URL-дағы (Uniform Resource Locator) белгілі бір параметрлер клиенттің хабарынсыз өзгертілетін

веб-шабуылы және клиент сол URL мекенжайын енгізген кезде ол дәл солай көрінеді және көрсетіледі. Жалған веб-сайт жасауды негізінен хакерлер мен қылмыскерлер жеке деректерді ұрлау және ақпаратқа заңсыз қол жеткізу мақсатында жүзеге асырады.

Repudiation Attack (бас тарту шабуылы) пайдаланушы өзінің белгілі бір әрекетті жасағаны немесе транзакцияны бастағаны фактісін жоққа шығарған кезде орын алады. Пайдаланушы транзакция немесе байланыс туралы білуден бас тартып, содан кейін мұндай транзакция немесе байланыс ешқашан болмаған деп мәлімдей алады.

Information Disclosure (ақпаратты жария ету) қорғалған деп саналатын ақпараттың қолжетімді болуын білдіреді.

Privilege Escalation Attack (артықшылықты көбейту шабуылы) – пайдаланушыға бастапқыда рұқсат етілмеген желіге көбірек қол жеткізуге мүмкіндік беретін желіге ену түрі. Шабуыл жасаушы бағдарламалық жасақтама қателерін пайдаланады және желіге қолжетімділікті арттырады.

Exploits – негізінен жүйедегі осалдықты пайдалануға арналған бағдарламалық құрал болып табылады. Шабуыл жасаушы компьютер жүйесіне оңай қол жеткізуді және бақылауды алуды жоспарлайды, сол арқылы артықшылықтарды көбейтуге мүмкіндік алады немесе DoS шабуылын жасайды.

Social Engineering (әлеуметтік инженерия) - атақты адамды пайдалану арқылы шабуыл. Олар ірі шабуыл үшін құпия сөздерді немесе да басқа қажетті ақпаратты алу үшін пайдаланылады.

Malware (зиянды бағдарламалық құрал) жүйені зақымдау немесе қажетсіз әрекеттерді орындау үшін әзірленген. Зиянды бағдарламалық құрал компьютердің қатты дискісіне зиян келтіруі мүмкін вирустар, құрттар, трояндық аттар және т.б. сияқты түрде болуы мүмкін. Олар кейбір файлдарды немесе каталогты жоя алады немесе пайдаланушы білместен деректерді жай ғана жинай алады.

Adware (жарнамалық бағдарламалық құрал) – ішіне жарнамасы енгізілген бағдарламалық құрал. Бағдарлама іске қосылғанда, ол жарнамаларды көрсетеді. Бағдарламалық құрал компьютерлерді вирустармен жұқтыру үшін жарнаманы пайдалануы мүмкін.

Боттар - бұл қарапайым және қайталанатын сипаттағы автоматтандырылған тапсырмаларды орындайтын бағдарламалық қосымшалар. Боттар зиянды болуы немесе болмауы мүмкін, бірақ олар әдетте Интернетті пайдалану кезінде DoS шабуылын бастайды.

Ransomware (ақша талап ететін бағдарламалық құралдар) — компьютер жүйесіне кіруді шектейтін, содан кейін шектеуді жою үшін төлемді талап ететін киберқауіптің бір түрі.

Phishing — құпия сөздер, пайдаланушы аты-жөні және басқа деректер сияқты құпия ақпаратты алуға әрекеттенетін киберқауіп. Бұл жағдайда шабуылдаушы шынайы болып көрінетін электрондық поштаны жібереді және жеке деректерді алуға тырысады.

DDoS (таратылған қызмет көрсетуден бас тарту) — бірнеше көздерден үлкен трафикті тудыру немесе Интернетке қосылған хост қызметтерін тоқтату арқылы кез келген онлайн қызметті уақытша қолжетімсіз ету әрекеті.

Keylogger — компьютер жүйесіндегі оқиғаларға тыңшылық жасай алатын шпиондық бағдарлама. Ол әрбір пернені басуды, кірген веб-сайттарды және жүйеде қол жетімді барлық ақпаратты жазуға қабілетті. Бұл жазылған журнал содан кейін көрсетілген тұлғаға жіберіледі.

Identity Theft (жеке деректерді ұрлау) - бұл сіздің жеке ақпаратыңыз ұрланып, кейін ол алаяқтық жасау үшін пайдаланылатын қылмыс.

Компьютерлік вирус — бұл өзін-өзі репликациялайтын бағдарлама, ол орындалған кезде оның көшірмелерін басқа компьютерлік файлға енгізу және оларды жұқтыру арқылы өзгертуге болады. Бұл вирус зиянды болуы мүмкін, өйткені ол даладағы өрт секілді тез таралады және жүйенің үлкен бөлігін қысқа мерзімде істен шығаруы мүмкін.

Rootkits - белгілі бір процестерді немесе бағдарламаларды антивирустық сканерлеу арқылы қалыпты анықтаудан жасыратын және жүйеңізге артықшылықты қолжетімділікті пайдалануды жалғастыратын зиянды бағдарламалық құрал. Бұл бағдарлама жүйеде әртүрлі файлдар мен процестерді орната алады. Ол анықталуы қиын бағдарлама, компьютер қосылған сайын ол іске қосылып отырады.

Spyware (шпиондық бағдарламалық құрал) – әдетте интернет қосылымынсыз Интернет арқылы жүйеден деректерді шпиондық түрде жинайтын бағдарламалық құрал. Шпиондық бағдарлама негізінен Интернеттен жүктеп алуға болатын тегін бағдарламаның жасырын құрамдас бөлігі болып табылады.

Кибершабуылдардың саны жылдан жылға қарай артып келеді. Біз тек негізгі түрлерін ғана келтіріп өттік. Негізінен, кибершабуылдардың барлығын хакерлік шабуылдар, киберқылмыстар және кибершпионаж сияқты үш топқа топтастыруға болады.

Хакерлік шабуылдар саяси, әлеуметтік немесе идеологиялық деңгейде әсер ету мақсатында компьютерлік жүйені бұзады немесе оған кіріп алады. Хакерлік шабуылдар негізінен DoS шабуылдары (қызмет көрсетуден бас тарту), DDoS шабуылдары (таратылған қызмет көрсетуден бас тарту), ақпаратты ұрлау, деректерді жария ету, веб-сайттарды зақымдау, типосквоттинг (URL мекенжайларын жазуда типографиялық қателерді пайдаланып URL мекенжайларын ұрлау) және басқа да көптеген әрекеттер арқылы жүзеге асырылатын цифрлық саботаж.

Киберқылмыс ақшалай сыйақы алу мақсатында цифрлық құралдар арқылы жүзеге асырылатын кез келген заңсыз әрекетті қамтиды. Мысалы, оған алаяқтық банктік операцияларды, ұрланған ақпаратты қара нарықта сатуды жатқызуға болады.

Кибершпионаж – жеке тұлғалардан, бәсекелестерден, жеке топтардан, үкіметтерден және қарсыластардан жеке, экономикалық, саяси немесе әскери пайда алу мақсатында Интернеттегі әдістерді пайдалана отырып, иесінің рұқсатынсыз (жеке, құпия немесе конфиденциалды) трояндық аттар, шпиондық бағдарламалар, зиянды бағдарламалар және жеке компьютерлер арқылы деректерді алу тәжірибесі.

Аталып өткен киберқауіптердің барлығы қысқа мерзімді және ұзақ мерзімді салдарларды тудыратын компаниялардың операциялық және қаржылық қызметіне айтарлықтай әсер етеді. Олар операциялық нәтижеге, қаржылық нәтижеге, сондай-ақ бизнестің тұрақтылық көрсеткіштеріне әсер етуі мүмкін.

Осылайша, кибершабуылдар өндірістік процестерге былайша ықпал етуі мүмкін:

- кибершабуылдар бизнес-процестерді үзіп тастауы ықтимал. DDoS, Ransomware сияқты кибершабуылдардың кейбір түрлері компаниялар қызметін уақытша немесе толығымен тоқтата алады, бұл бүкіл өндірістік процестің толық немесе ішінара тоқтатылуына, жеткізілімдердің кешігуіне және тапсырыстарды уақытында орындамауына әкеп соқтыруы мүмкін;

- кибершабуылдар компания деректерінің және оның зияткерлік меншіктерінің жоғалуына әкелуі мүмкін. Осылайша, жеке деректердің, соның ішінде клиенттер мен контрагенттер деректерінің жария болуына немесе жойылуына тап болған компаниялар оларды қалпына келтіруге жұмсалатын шығындардың артуына және нарықтағы бәсекелестік артықшылықтарын жоғалтуына ұшырауы мүмкін;

- кибершабуылдар компания қызметінің тиімділігін төмендетуі мүмкін, өйткені кибершабуылдардан кейін компаниялар IT-инфрақұрылымын қалпына келтіру үшін қосымша қаржылық ресурстарды жұмсайды. Бұл компанияның негізгі өндірістік қызметіне теріс әсер етуі мүмкін.

Сонымен бірге, кибершабуылдар компаниялардың қаржылық тиімділігін төмендетеді. Өйткені:

- бопсалаушыларға жасалған төлемдерге, жоғалған деректерді қалпына келтіруге, IT-инфрақұрылымын жаңғыртуға байланысты қаржылық шығындар өседі;

- киберқауіпсіздікті дамытуға кететін шығындар өседі. Осылайша, болашақ шабуылдардың алдын алу үшін компаниялар киберқауіпсіздікке, соның ішінде жаңа бағдарламалық қамтамасыз етуге, жабдықты сатып алуға және қыметкерлерді оқытуға жұмсалатын шығындарды ұлғайтуға мәжбүр болады деп есептеледі;

- тұтынушылардың сенімін жоғалтқаннан кейін сату көлемі және, сәйкесінше, табыс көлемі төмендеуі мүмкін;

- қаржылық тұрақтылық көрсеткіштері төмендейді, өйткені кибершабуылдардан кейін туындауы мүмкін шығындар, негізінен, қарыз қаражаттары есебінен қаржыландырылады. Бұл, сәйкесінше, компаниялардың қарыздық жүктемесін арттырып отырады.

Кибершабуылдар, негізінен, компаниялардың операциялық және қаржылық қызметіне қысқа мерзімді әсер етеді. Дегенмен, кибершабуылдардың ұзақ мерзімді салдары да бар, олар

компанияның алдағы жылдардағы қызметіне әсер етіп, компанияның қаржылық және операциялық көрсеткіштерін төмендетеді. Бұл салдарға мыналар жатады:

- компания беделінің төмендеуі, өйткені кейбір контрагенттер кибершабуылға ұшыраған компаниямен келісім-шарттарды бұзуы мүмкін (әсіресе жеке деректері жарияланған компаниялар бұған сезімтал болады);

- инвестициялық тартымдылықтың төмендеуі, ол инвестициялық тәуекелдің жоғарылауы түрінде көрінеді.

Егер компанияның жоғары тәуекел дәрежесі компанияның капиталды тарту мүмкіндігін төмендететін болса, тұтынушылардың төмендеуі нарықтағы үлестің қысқаруына әкелуі мүмкін. Осылайша, кибершабуылдар бірнеше деңгейде компаниялардың қызметіне және қаржылық көрсеткіштеріне әсер етуі мүмкін. Сондықтан, олардың салдарын барынша азайту үшін компаниялардың тәуекелдерді басқару стратегияларын, киберқауіпсіздік жүйелерін, сондай-ақ қызметкерлердің киберқауіпсіздік мәселесі бойынша біліктілігін жоғарылатып отыру қажет.

1.2 Компаниялардың инвестициялық саясаты және оның кибершабуылдарға осал болу факторлары

Инвестициялық саясат кез келген кәсіпорынның шаруашылық қызметін басқарудың маңызды элементтерінің бірі болып табылады. Инвестициялық саясат компанияның дамуында және оның тиімділігін арттыруда шешуші рөл атқарады.

Инвестициялардың теориялық мәселелерімен Ирвинг Фишер (Irving Fisher), Артур Сесил Пигу (Arthur Cecil Pigou), Альфред Маршалл (Alfred Marshall) және Джон Мейнард Кейнс (John Maynard Keynes) сияқты көрнекті экономистер айналысты. Сонымен қатар, бұл зерттеулерде тұңғыш рет инвестиция бойынша деректер айнымалы ретінде қолданылып, эмпирикалық талдау жүргізілді [19-22].

Сондай-ақ 1963 жылы жарияланған Дейл Йоргенсонның (Dale Jorgenson) инвестицияның неоклассикалық теориясы кеңінен танымал. Ол саяси өзгерістердің елдегі инвестицияға қалай әсер ететінін болжауға мүмкіндік береді [23].

Экономикалық әдебиеттерде инвестициялық белсенділікті зерттеу маңызды орын алады. Сол зерттеулерде инвестициялық қызмет мынадай негізгі ұғымдарға негізделеді: инвестиция, реципиент, инвестор, тиімділік критерийлері және т.б.

«Инвестициялар» терминінің негізгі анықтамаларын қорытындылайтын болсақ, оларды 1-кесте түрінде былайша келтіруге болады:

Кесте 1 - Ғылыми әдебиеттерде келтірілген «инвестиция» ұғымының анықтамасы

Анықтама	Әдебиет көзі
Инвестиция дегеніміз – қандай да бір оң пайда мөлшерін күтумен жасалған қаржы салымдары. Егер инвестиция дұрыс жасалса, кіріс инвестор қабылдайтын тәуекелге сәйкес болады	Fisher, D. E., & Jordan, R. J. (1995). <i>Security analysis and portfolio management</i> . Simon & Schuster.
Инвестиция – бұл сатып алуға тұрарлық зат, өйткені оның болашақта пайда табу мүмкіндігі бар	<i>The Compact Oxford English Dictionary</i>
Инвестиция - бұл пайда күтумен байланысты кәсіпорынға ақша немесе капитал салу, инвестициялау процесі	Princeton University Wordnet, wordnet.princeton.edu
Инвестициялар – бұл табыс алу немесе әлеуметтік нәтижеге қол жеткізу мақсатындағы қаржылық және материалдық ресурстарға, сондай-ақ меншік және зияткерлік меншік құқығына инвестициялау	Швандар В.А., Базилевич А.И. Управление инвестиционными проектами – М.: ЮНИТИ, 2017. – 444 с.
Инвестициялар – пайда табу немесе компанияны басқару мақсатында бағалы қағаздарды сатып алу арқылы капиталды инвестициялау	Инвестиции: учебник для вузов [Текст] / Л.И.Юзвович [и др.]; под редакцией Л.И.Юзвович, С.А.Дегтярева, Е.Г.Князевой. – Екатеринбург: Издательство Уральского университета, 2016. – 543 с.
Ескертпе: [19, 24-27] дереккөз негізінде автормен әзірленген.	

«Реципиент» термині инвестициялау объектісін анықтайды. Реципиент деп инвестицияны алушы болып табылатын заңды немесе жеке тұлға деп түсіндіріледі.

Кәсіпорынның инвестициялық қызметін келесі мынадай бағыттарға бөлуге болады:

- әрекеттің жаңа түрін меңгеру;
- қолданыстағы өндіріс көлемін ұлғайту;
- кәсіпорынның материалдық-техникалық базасын жаңарту.

Инвестициялық қызметтің жоғарыда аталған барлық бағыттары ықтимал тәуекелмен байланысты. Демек, инвестор инвестициялау туралы шешім қабылдауы үшін ол салынған қаражаттың өтелетініне, сонымен қатар ол қабылданған тәуекелге сәйкес келетін және балама инвестициялау жолдарынан жоғары пайда алатынына сенімді болуы керек.

Компанияның инвестициялық қызметін басқару үшін барлық инвестицияларды мынадай негізгі түрлерге бөлуге болады (2-кесте).

Инвестициялық белсенділіктің дамуына келесі факторлар әсер етуі мүмкін:

- экономикалық тұрақсыздық қаупі;
- экономикалық қызметке санкциялар мен шектеулер енгізу;
- саяси жағдайдың тұрақсыздығы;
- нарықтық конъюнктураның ауытқуы (ресурстардың әлемдік бағасы, валюта бағамы);
- климаттық факторлар;
- өндірістік тәуекел (апаттар, өндірістің тоқтап қалуы);
- компанияның қаржылық жағдайы туралы ақпараттың бұрмалануы (кибершабуылдар салдарынан деректердің ағып кетуі).

Соңғы фактор инвесторлардың компанияға деген сеніміне нұқсан келтіріп, оның инвестициялар үшін тартымдылығын кемітеді. Цифрландыру дәуірінде тұрақты киберқауіпсіздік жүйесі компаниялардың инвестициялық саясатына әсер етіп, оларды IT инфрақұрылымы мен киберқауіпсіздік жүйелеріне көбірек инвестициялау қажеттілігіне итермелейді.

Кибершабуылдар компаниялардың инвестициялық саясатына тікелей және жанама әсер етуі мүмкін. Тікелей әсердің салдары деректердің ағып кетуіне және операциялық ақауларға байланысты қаржылық шығындар арқылы көрінуі мүмкін.

Кесте 2 – Инвестициялардың жіктелуі

Сипаты	Инвестиция түрі	Сипаттамасы
Инвестициялау объектісі бойынша	Нақты	Активтерге инвестиция салу
	Портфельді	Қаржы активтеріне (акцияларға) инвестициялау
Инвестициялау кезеңі бойынша	Қысқа мерзімді	1 жылдан аспайтын мерзімге қаражатты инвестициялау
	Орта мерзімді	1-3 жыл мерзімге қаражат салу
	Ұзақ мерзімді	5 жылдан астам мерзімге қаражатты инвестициялау
Қатысу сипаты бойынша	Тікелей	Инвестор компанияны басқаруға қатысады
	Жанама	Инвестициялар инвестициялық және брокерлік компаниялар және басқа да қаржылық делдалдар арқылы жүзеге асырылады
Тәуекел деңгейі бойынша	Тәуекелсіз	капитал мен кірісті жоғалту қаупі жоқ
	Тәуекелі төмен	Капитал мен кірісті жоғалту қаупі орташадан төмен
	Тәуекелі орташа	Капитал мен табысты жоғалту тәуекелі орташа
	Тәуекелі жоғары	Капитал мен кірісті жоғалтудың тәуекел деңгейі орташадан жоғары
Меншік түрі бойынша	Жеке	Жеке және заңды тұлғалардың инвестициясы
	Мемлекеттік	Мемлекеттік бюджеттен бөлінетін инвестиция
	Аралас	Өртүрлі инвесторлардың инвестициялары (жеке және мемлекеттік)
	Шетел	Шетелдік жеке және заңды тұлғалардың инвестициясы
	Бірлескен	Бірнеше шетел мемлекеттерінің қатысуымен жасалатын инвестициялар
Территория бойынша	Ішкі	Отандық объектілерге бағытталған инвестициялар
	Сыртқы	Басқа елдердегі объектілерге бағытталған инвестициялар
Ескертпе: [26,27] дереккөз негізінде автормен әзірленген.		

Сәйкесінше, оны жою үшін компания қосымша инвестицияларды қажет етеді. Жанама әсер инвесторлардың компанияға деген сенімінің төмендеуі, капитал құнының артуы, кибершабуылдардың салдарына байланысты инвестициялық жобалардан бас тартуы түрінде көрінуі мүмкін.

Компаниялардың кибершабуылдарға осалдығына әсер етуі мүмкін факторларға мыналар жатады:

- компанияның киберқауіпсіздігіне инвестициялау деңгейінің төмен болуы;
- компанияның IT-инфрақұрылымы мен киберқауіпсіздік жүйесі әлсіз;
- қызметкерлердің киберқауіпсіздік саласындағы білімінің болмауы.

Сондай-ақ, компаниялардың кибершабуылдарға осалдығы компаниялардың көлеміне байланысты болуы мүмкін. Осылайша, ірі компаниялардың күрделі IT-инфрақұрылымы болуы мүмкін. Бұл киберқауіптер жағдайында тез шешім қабылдауды қиындатады. Ал, шағын компаниялардың киберқауіпсіздік жүйесін дамыту үшін қаржылық ресурстары көбінесе шектеулі болады.

Кибершабуылдар компанияның қаржылық тұрақтылығына да, инвестициялық тартымдылығына да әсер етуі мүмкін. Экономиканың цифрлық трансформациясы жағдайында киберқауіптер компанияның инвестициялық стратегиясын қалыптастыратын негізгі факторлардың біріне айналуға. Кибершабуылдардың салдары компанияның қаржылық және инвестициялық қызметінде әртүрлі проблемаларды тудыруы мүмкін, соның ішінде беделінің жоғалуы, компанияның шығындар құрылымының өзгеруі, компанияның инвестициялық басымдықтарының өзгеруі және т.б.

Кибершабуылдардың компаниялардың инвестициялық саясатына әсерін 3-кесте түрінде жүйелеуге болады. Онда кибершабуылдардың әсер ету факторлары, олардың ерекшеліктері мен салдары көрсетілген.

Кестеде берілген мәлімет компанияға кибершабуылдардың әсері инвесторлардың сенімінің төмендеуінен және киберқауіпсіздік шығындарының ұлғаюынан инвестиция тарту шарттарының нашарлауына және инвестициялық стратегиялардың өзгеруіне дейін көп қырлы екенін көрсетеді.

Кесте 3 - Кибершабуылдардың компаниялардың инвестициялық саясатына әсері

Әсер ету факторы	Сипаттамасы	Инвестициялық қызмет үшін салдары
Инвестициялық тартымдылықтың төмендеуі	Компанияның нарық құнының (нарықтық капитализациясының) төмендеуі	- тәуекелдің артуы; - инвестицияның қысқаруы; - инвесторлар тарапынан сенімнің төмендеуі.
Ұзақ мерзімді инвестициялардың төмендеуі	Кибершабуылдардың салдарын жою үшін қаржылық ресурстардың қайта бағытталуы	- бизнесті кеңейтуге арналған инвестициялардың қысқаруы; - жаңа өнімдерді немесе қызметтерді дамытуға бағытталған инвестициялардың қысқаруы
Киберқауіпсіздікке бағытталатын инвестициялардың артуы	Деректерді қорғауға, IT-инфрақұрылымын жаңғыртуға, қызметкерлерді оқытуға кететін шығындардың өсуі	- пайданың төмендеуі; - рентабельділіктің төмендеуі.
Қарыз капиталын тарту мүмкіндігінің шектелуі	Кибершабуылдардан кейін несие рейтингінің төмендеуі	- несиелер бойынша пайыздық мөлшерлемелердің өсуі; - қарыз капиталын тартудағы қиындықтар.
Стратегиялық серіктестікке әсері	Контрагенттер мен клиенттердің сенімін жоғалту	- бірлескен инвестициялық жобалардың баяулауы немесе тоқтап қалуы; - сыртқы инвестицияларды тартудың шектеулігі.
Сала үшін ұзақ мерзімді салдары	Көптеген кибершабуылдар инвесторлар үшін тартымдылықты төмендетуі мүмкін	- саланың технологиялық дамуының төмендеуі; - салаға инвестицияның қысқаруы.
Ескертпе: автормен әзірленген.		

Осылайша, киберқауіптерге жиі ұшырайтын компаниялар өз клиенттері мен контрагенттерінің сенімін сақтау үшін киберқауіпсіздік жүйесі мен IT-инфрақұрылымын дамытуға ерекше

көңіл бөлуге мәжбүр. Айта кету керек, кибершабуылдардан қорғау бойынша уақтылы шараларды қамтамасыз етудің кешенді тәсілі ғана олардың компаниялардың инвестициялық қызметіне тигізетін кері әсерін барынша азайта алады.

1.3 Киберқауіпсіздік тәуекелдерін басқару жүйесін құрудың негіздері

Цифрландырудың жылдам қарқыны компаниялардың операциялық тиімділігін түбегейлі өзгертті және нарықтық үрдістер мен тұтынушылардың қажеттіліктеріне сәйкес келетін инновациялық өнімдерді жасауға ықпал етті. Жаңа технологиялар өндірілетін өнімдер мен қызметтердің ауқымын кеңейтіп, цифрлық экожүйені инклюзивті және икемді етті. Дегенмен, компаниялардың бизнес-модельдеріндегі технологиялық инновациялардың тереңдеуімен компаниялардың экономикалық қауіпсіздігіне әсер ететін тәуекелдер де артып келеді.

Технологияларды қолдану деңгейінің артуы компаниялардың динамикалық жұмыс ортасына деген тәуелділігін мен киберқауіптерге ұшырау мүмкіндігін арттырып, тәуекелдерді басқару мен киберқауіпсіздікті қиындатып жіберді. Цифрландыру қолданбаларды, платформаларды және IT-инфрақұрылымын бір кеңістікке біріктірді. Компаниялар синхронды деректерді табуды, талдауды және сақтауды қолдау үшін заттар Интернетін, үлкен деректерді талдауды және бұлтты технологияларды қоса алғанда, цифрлық инновацияларды енгізуді белсенді түрде жалғастыруда. Дегенмен, онлайн транзакциялардың көлемі ұлғайған сайын қаржылық деректер мен цифрлық іздерді қорғау қажеттілігі артып отыр.

Кәсіпорындардың экономикалық қауіпсіздігі – бұл ақпаратты рұқсатсыз кіруден қорғау жүйесі. Дәстүрлі түрде ол корпоративтік мүдделерді, инфрақұрылымды, ақпараттық қауіпсіздікті және нарық қатысушыларын қорғауды қамтиды.

Цифрлық технологиялардың өсуі цифрлық ортада берілетін ақпаратты қорғауды күшейтуді талап етеді, бұл компаниялардың экономикалық қауіпсіздігінің негізгі факторына айналууда. Фишинг сияқты тәуекелді оқиғалардың жылдамдауы олардың компания кірістеріне әсер ету уақытын қысқартуда, сол себепті қауіпсіздік

жүйелерінде киберқылмыскерлердің әрекеттерін алдын алу кезінде жылдам реакция талап етіледі. Процестерді цифрландыру жағдайында экономикалық қауіпсіздіктің жоғары деңгейін қолдау үшін мынадай шаралар кешенін қолдану қажет:

- тұтынушыны идентификациялау үшін күрделі құпия сөздерді, кодтарды, биометриялық деректерді (мысалы, саусақ іздерін) қоса, көп факторлы аутентификацияны қолдану;
- рұқсатсыз кіруді болдырмау мақсатында тұтынушы мен транзакция туралы ақпаратты қорғау үшін деректерді шифрлау;
- күдікті әрекетті анықтауға және қауіптерге жылдам жауап беруге мүмкіндік беретін мониторинг және күдікті өзгерістерді анықтау әдістерін қолдану;
- мүмкін болатын тәуекелдер мен қауіптер туралы хабардарлықты арттыру үшін қызметкерлерді қауіпсіздік ережелеріне жүйелі түрде оқыту;
- осалдықтарды түзету және шабуылдарды болдырмау үшін бағдарламалық құралдарды үздіксіз жаңартып отыру;
- құпия деректерді қорғау, қаржы мен беделді жоғалтпау мақсатында ақпараттық қауіпсіздік саласындағы үздік серіктестермен ынтымақтастық жасау.

Жүйелердің тұрақты жаңартулары және қауіпсіздік аудиті компаниялардың экономикалық қауіпсіздігін нығайтудың негізгі шаралары болып табылады. Компаниялар өздерінің активтерін де, тұтынушыларының деректерін де қорғау үшін киберқауіпсіздіктің жаңа тенденцияларын меңгеріп, оларды дереу қолдануы керек.

Технологияның дамуымен және қоршаған ортаның жағымсыз факторларының әсерінің күшеюімен кез келген шаруашылық жүргізуші субъектінің қызметіне байланысты тәуекелдер ерекше мәнге ие болды. Экономикалық әдебиеттерде компания тәуекелі табысқа да, сәтсіздікке де әкелетін қауіп немесе белгісіздік жағдайында әрекет ету қажеттілігі ретінде қарастырылады. Тәуекелдерді басқару компаниялардың үздіксіз жұмыс істеуінің маңызды элементі болып саналады.

Тәуекелдің классикалық концепциясы ықтимал нәтижелердің олардың ықтималдықтарына көбейтілген сомасын қамтитын «күтілетін құн» түсінігіне негізделген. Тәуекел теориясының дамуына маңызды үлесін Фрэнк Найт (Frank Knight) қосқан. Ол өлшенетін тәуекелдер мен белгісіздікті бөліп ажыратты [28].

Сондай-ақ, Гарри Марковицтің (Harry Markowitz) еңбегін де атап өтуге болады. Ол портфельдік теория және тәуекел мен кіріс арасындағы тепе-теңдік ретінде тиімді шекара концепциясын тұжырымдап берді [29].

Цифрлық қауіпсіздік контекстінде Дональд Крессидің (Donald Cressy) «алаяқтық үшбұрышы» теориясы ерекше назар аударуда. Онда алаяқтық оны жүзеге асырудың мотиві, мүмкіндігі және схемасы болған кезде пайда болады деп тұжырымдалған [30]. Бұл зерттеулер психологиялық аспектілерді және қаржылық жоғалту ықтималдығын қоса алғанда, цифрлық тәуекелдерді талдаудың теориялық негізін құрайды.

Жалпы, компаниялардың цифрлық кеңістіктегі тәуекелдерін екі негізгі санатқа бөлуге болады: деректер қауіпсіздігі тәуекелі және киберқауіпсіздік тәуекелі. Бұл ұғымдар өзара байланысты, өйткені екі категория да компанияның ақпараттық активтерінің көпшілікке жария болуынан және рұқсатсыз кіруден қорғауға бағытталған.

Цифрлық кеңістік дегеніміз ақпарат, мазмұн және өзара әрекеттесу тарихы жинақталатын өзара байланысты құрылғылар, желілер және Интернетпен байланысқан виртуалды орта. Деректер қауіпсіздігі тұтынушылардың жеке деректерін, компаниялар операцияларының құпиялылығы мен тұтастығын қамтамасыз ету мақсатында авторизация және аутентификация деректерін қорғауды қамтиды.

Соңғы жылдары киберқауіпсіздік шаралары цифрландыру жағдайында ерекше өзекті болуда. Оларға тәуекелдерді басқару, цифрлық белсенділікті бақылау мен күрделі және тұрақты қауіптерге қарсы тұру жатады.

Қазіргі кездегі компаниялардың кемшілігі ол арнайы стратегияның болмауы болып отыр. Компаниялар, көбінесе, күтілетін қатерлерді есепке алмай, тек тәуекелдердің алдын алуға ғана тырысады. Сонымен бірге, өнімді әзірлеу, сату және корпоративтік мәдениет сияқты салалардағы стратегиялық тәуекелдерге ерекше назар аударылады. Сол себепті, басқарудағы кемшіліктерді анықтау үшін ішкі аудиттер жүйелі түрде жүргізілуі керек.

Бизнесті цифрландыру жаңа мүмкіндіктер ашқанмен, тәуекелдерді, оның ішінде экономикалық қауіпсіздік тәуекелін,

тиімді басқару қажеттілігін арттырып отыр. Тәуекелдерді басқару олардың пайда болу ықтималдығын азайтуға және ықтимал салдарын төмендетуге көмектеседі. Бұл процесс тәуекел факторларын анықтауды, талдауды және басқаруды қамтиды. Процесті тиімді ету үшін болашақ нәтижелерді бақылау мақсатында алдын-алу шаралары жүргізілуі шарт.

Компанияның тәуекелдерді басқару жүйесі операциялық немесе инвестициялық шешімдердегі жағымсыз салдарлардың ықтималдығын азайту үшін анықтау, бағалау және шаралар қабылдау процестерін білдіреді. Тәуекелге негізделген әдіс қауіптерді анықтауды, талдауды және олардың деңгейіне байланысты азайтуды қамтиды.

Тәуекелдерді басқару жүйесін қалыптастыру мынадай кезеңдерді қамтуы мүмкін:

1) Сәйкестендіру: тәуекелдердің сипаты мен көзін, сонымен қатар олардың компанияға қауіп төну себептерін анықтау.

2) Бағалау және талдау: тәуекелдердің туындау ықтималдығын және олардың ықтимал салдарын анықтау.

3) Жеңілдету: тәуекелдердің ықтималдығын азайту және олардың залалын барынша азайту бойынша шараларды әзірлеу және жүзеге асыру.

4) Мониторинг: басқару стратегияларының тиімділігін бағалау және жаңа тәуекелдерге жауап ретінде жүйені реттеу үшін қауіптерді қадағалау және оқиғаларды талдау.

5) Ынтымақтастық: жалпы тиімділікті арттыру үшін компания бойынша тәуекелдерді азайту стратегияларын үйлестіру.

6) Есеп беру: тәуекелдерді басқару нәтижелерін құжаттау және компанияның тәуекел профиліндегі өзгерістерді талдау.

Бұл жүйелі тәсіл компанияларға осалдықты азайтуға және сыртқы және ішкі қауіптерге төзімділікті арттыруға мүмкіндік береді.

Ғылыми әдебиеттерде компанияның тәуекелдерін басқарудың теориялық аспектілерін В.И.Авдийский, В.Н.Алферов, В.М.Безденежных, В.М.Синявский және т.б. зерттеген. Олар тәуекелді басқару циклді сипатқа ие екенін атап көрсетеді: процестің кезеңдері ұйымдық жағынан да, функционалдық жағынан да өзара байланысты [31-34].

Тәуекелдерді басқарудың әрбір кезеңін, атап айтқанда бағалау, ақпаратты жинау, мониторинг және талдау, заманауи технологиялар мен FinTech құралдарын қолдану арқылы жақсартуға болады.

В.М.Безденежных тәуекелдерді басқару жүйесі сәйкестендіру мен бағалаудан бастап, бақылау мен басқару әдістерін үнемі жаңартуға дейінгі кешенді реттеуді қамтамасыз ететін компанияның барлық басқару құрылымын қамтитынын атап өтті. Оған қоса, ол тәуекелге негізделген тәсілдің тиімділігі тәуекел иелерінің жауапкершілігіне байланысты болатынын көрсетті [33].

Сонымен қатар, тәуекелдерді басқару жүйесі ұйымдардың экономикалық қауіпсіздігін қамтамасыз етудің негізгі тетігі болып саналады. В.М.Безденежных күрделі әлеуметтік-экономикалық жүйеде қабылданатын шешімдердің шектеулі ұтымдылығын атап көрсетті. Сәйкесінше, бұл белгісіздік деңгейі жоғары стратегияларды қабылдау тәуекелін арттырып отырады. Бұл талдау, бағалау және басқару шешімдерінде субъективтілікті төмендету әдістерін кәсіби қолдануды қоса алғанда, тәуекелге негізделген тәсілді белсенді енгізу қажеттілігін күшейтеді [33].

Цифрландыру жағдайында кешенді тәсілдің және тәуекелдерді сенімді сәйкестендірудің болмауы компаниялардағы тәуекелдерді басқару жүйелерінің фрагменттелуіне әкеліп соқтыруы мүмкін, бұл олардың экономикалық қауіпсіздігіне қауіп төндіреді.

Цифрлық технологиялардың өсуімен компаниялар даму үрдісінің жеделдеуіне және нарықтың құбылмалылығына тап болады. Тәуекелдерді басқарудың дәстүрлі тәсілдері бұдан былай стратегиялар мен құралдарды қайта қарауды талап ететін заманауи талаптарға сай келмеуде. Жаңа тәуекелдің түрі – модель тәуекелі — бұлт деректерді бағалау және шешім қабылдау үшін пайдаланылатын бизнес үлгілеріндегі қателерден туындайтын жағымсыз салдарлардың ықтималдығы.

McKinsey сарапшылары модель тәуекелдерін басқару тәсілдерін қайта қарау қажеттігін атап көрсетуде. Компанияларға тұрақтылықты қамтамасыз ету үшін тиімді қысқа мерзімді шараларды және модельдерді жаңғыртудың ұзақ мерзімді стратегияларын әзірлеу ұсынылады. Бұл бизнестің үздіксіздігін

сақтап қана қоймайды, сонымен қатар тәуекелдерді басқару жүйелерін цифрлық шындыққа бейімдейді [35].

Заманауи компаниялар цифрлық трансформация қысымымен бетпе-бет келіп отырған кезеңге тап болуда, әсіресе цифрлық технологияларды енгізуді талап ететін операцияларды автоматтандыру саласында. Күшті басқару мен сенімді реттеуге негізделген дәстүрлі ұйымдар әдетте цифрлық трансформацияны сәтті басынан өткереді. Дегенмен, транзакциялар, сатылымдар және маркетингтік деректер ағыны ұлғайған сайын, қауіпсіздікті бұзу тәуекелі де артуда.

Компаниялардағы тәуекелдерді басқару үрдісі күрделі және ресурстарды көп қажет ететін тексерістерді қамтитын нормативтік талаптардың сақталуымен байланысты. Машиналық оқыту және жасанды интеллект технологиялары бұл процесті автоматтандыруға көмектеседі. Бизнес-аналитика тапсырмаларды орындау және адам интеллектін алмастыру үшін өзін-өзі оқытуды пайдалану арқылы компаниялардың қажеттіліктерін тиімді бағалап отырады. Мұндағы маңызды аспект тәуекелдерді бағалаудың жаңа қағидаттарын әзірлеу және стандарттарға сәйкес келу үшін сыртқы сарапшылар арқылы қызметкерлерді оқыту болып табылады.

Цифрландыру жағдайында тәуекелдерді көбінесе технологиямен байланыстырады, бірақ олардың мақсаттарға жетумен және бизнес-процестерге әсер етуімен байланысын нақтыламайды. Мысалы, Е.В. Янченко цифрлық тәуекелді «Ақпараттық коммуникациялық технологиялар мен автоматтандыру тудыратын барлық мүмкіндіктер» деп анықтайды. Ол сондай-ақ цифрлық технологиялардың тәуекелдерге әкелетінін айтады [36].

М.С.Марамыгин және басқалар цифрлық тәуекелдердің әртүрлі топтарын анықтайды, бірақ «цифрлық тәуекел» терминіне жалпы анықтама бермейді [37]. И.А.Аренков және басқалары жобаны бағалаудың цифрлық модельдеріне енгізу үшін тәуекелдерді, соның ішінде киберқауіптерді санаттауға және оларды сандық бағалау қажеттілігіне назар аударады [38].

Е.Н.Карпова және басқалар цифрландыру жаңа қауіптерге, әсіресе ақшаны жылыстатуға және терроризмді қаржыландыруға қарсы күрес саласындағы тәуекелдерге, әкелетінін атап көрсетеді

[39]. Зерттеушілердің көпшілігі цифрлық тәуекелге анықтама бермей, оның жіктелуіне ғана назар аударуда [40-43].

Көптеген экономист-ғалымдар «цифрлық тәуекел» термині киберқауіпсіздік, құпиялылық, нормативтік талаптарға сәйкестік, ақпараттық-коммуникациялық технологиялардың қолжетімділігі және тәуекелдерді басқару сияқты операциялардың, технологиялар мен қауіптердің өзгеруіне және олардың күрделілігінің артуына қатысты мәселелерді қамтитынын атап өтуде [39-43].

UpGuard киберқауіпсіздік сарапшылары «цифрлық тәуекелдің» түрлеріне назар аудара отырып, цифрлық трансформацияның болжауға болмайтын салдарымен байланысты екенін атап көрсетеді [44].

Proofpoint «цифрлық тәуекел» цифрлық құралдар мен технологияларды пайдаланудан туындайтын қауіптер мен осалдықтарды қамтитынын және бұл тәуекелді компания деңгейінде бағалау барысында цифрлық трансформацияның барлық ықтимал теріс салдары қамтылу қажеттігін атап өтуде [45].

McKinsey авторлары «цифрлық тәуекелді» тәуекелдерді басқару тиімділігін арттыратын барлық цифрлық мүмкіндіктерді қамтитын термин, соның ішінде процестерді автоматтандыру, шешім қабылдау және цифрлық бақылау мен ескерту деп анықтайды. Бұл Е.В. Янченконың берген анықтамасымен тұспа-тұс келеді [46]. Осылайша, барлық авторлар көбінесе «цифрлық тәуекелді» нақтылауды және толықтыруды қажет ететін «тәуекелмен» емес, «цифрландыру» ұғымымен байланыстырады.

Қорытындылай келе, қауіпсіздікті жақсарту және ықтимал қауіптерді, соның ішінде ақпараттық қауіптерді азайту үшін компаниялар тәуекелдерді басқарудың жаңа әдістерін қолдануы керек. Экономикалық қауіпсіздіктің дәстүрлі тәсілдері көбінесе технологиямен байланысты жаңа тәуекелдерді елемей, тек негізгі элементтерді қамтиды.

Алайда, жаңадан енгізіліп жатқан инновацияларды есепке алу және оларды цифрлық құралдарды пайдалана отырып біріктіру маңызды. Бұл, өз кезегінде, киберқауіпсіздікті жақсартып, тәуекелдерді төмендетуге мүмкіндік береді.

Теориялық талдау нәтижесінде мынадай тұжырым жасауға болады. Цифрлық технологияларды интеграциялаудың артықшылықтарына қарамастан, цифрлық осалдықтар мен қауіптер

пайдаланушылар мен компаниялар үшін күрделі мәселеге айналып отырғандығы анықталды. Қызметті цифрлық форматқа көшіру тәуекелдердің артуына, соның ішінде компанияның қаржылық тұрақтылығы мен операциялық тұрақтылығының төмендеу ықтималдығына, әкеледі. Сол себепті, соңғы жылдары ақпараттық қауіпсіздік компанияның экономикалық қауіпсіздігін қамтамасыз етудің негізгі элементіне айналып отыр.

Цифрландырумен байланысты тәуекелдерді тиімді басқару үшін «цифрлық тәуекел» түсінігі, цифрлық тәуекел түрлері мен оның бизнес-процестермен байланысын түсіндіретін теориялық негіздердің болу қажеттілігі күмән туғызбайды. Бұл цифрлық қауіпсіздікті қамтамасыз ету мәселесінің артуы жағдайында ерекше маңызды болып отыр.

ТАРАУ 2. КОМПАНИЯЛАРДЫҢ ҚАРЖЫЛЫҚ КӨРСЕТКІШТЕРІНЕ ЖӘНЕ ИНВЕСТИЦИЯЛЫҚ САЯСАТЫНА КИБЕРШАБУЫЛДАРДЫҢ ӘСЕРІН ТАЛДАУ

2.1 Компаниялардың қызметіне кибершабуылдардың әсерін талдаудың әдістемелік негіздері

Кибершабуылдардың қаржылық нәтижеге әсерін талдау үшін оқиғаларды талдау әдісі (Event Study) қолданылады. Оқиғаларды талдау әдісі компаниялардың қызметі туралы барлық қолда бар ақпарат пен ағымдағы оқиғалар компания акцияларының бағасында көрініс табады деген идеяға негізделген. Осылайша, оқиғаларды талдау әдісі белгілі бір оқиғалардың әсерінен компаниялардың акциялар құнының қозғалысын өлшеуге мүмкіндік береді. Бұл әдіс компаниялардың аномальды кірістілігін есептеуге негізделген. Бұл бөлімде оқиғаны талдау әдісінің ғылыми-теориялық және әдістемелік негіздері қарастырылып, сондай-ақ осы әдісті қолдану бойынша әдістемелік ұсыныстар беріледі.

Акциялар құнының қозғалысына әсер ететін оқиғалар мынадай болуы мүмкін: компаниялардың бірігуі, жаңа нарықтарға шығу, жаңа өнімді нарыққа шығару. Бұған қоса, компания акцияларының құнының өзгеруіне үкіметтің және мемлекеттік реттеуші органдардың мәлімдемелері, бәсекелес компаниялардың әрекеттері, тіпті пандемия мен кибершабуылдар да әсер етуі мүмкін. Осылайша, оқиғалар микродеңгейде, яғни компания әсер ете алатын, сонымен қатар компания әсер ете алмайтын, бірақ оның қызметі осы оқиғаларға тәуелді болатын макродеңгейде де болуы мүмкін [47].

Компаниялардың қызметіне әсер еткен маңызды оқиғаның бірі - Covid-19 жаһандық коронавирустық пандемия. Бұл оқиға көптеген компанияларға теріс әсер етті, дегенмен бұл оқиғадан үлкен пайда көрген компаниялар да болды. Жалпы, оқиғалар қысқа мерзімді де, ұзақ мерзімді де әсер етуі мүмкін екенін атап өткен жөн.

Соңғы ғылыми жарияланымдарды талдау айнымалылар арасындағы байланыстарды анықтау үшін экономистер негізінен

сауалнамаларды, сұхбаттарды, сонымен қатар уақыт қатарларын, панельдік деректерді, регрессиялық талдауды, корреляциялық талдауды және т.б. эконометриялық әдістерді пайдаланатынын көрсетті. Бұл әдістермен салыстырғанда, оқиғаларды талдау әдісі белгілі бір оқиғалардың компаниялар үшін қаржылық салдарын дәлірек анықтауға мүмкіндік береді. Сонымен бірге, оқиғаларды талдау әдісі компаниялар үшін объективті өзгерістерді көрсететін қаржылық нарық деректеріне негізделген. Ал, талдаудың басқа әдістері нақты менеджердің субъективті көзқарасының әсерінен бұрмалануы мүмкін.

Оқиғаларды талдаудың негізгі артықшылықтары мыналар:

1) Бұл талдау нақты оқиғаның компаниялардың негізгі қаржылық көрсеткіштеріне әсерін зерттеуге мүмкіндік береді [48]. Мысалы, осы әдісті қолдана отырып, сіз жаңа өнімнің нарыққа шығуы, ірі инвестициялар туралы ақпарат, компания басшысының ауысуы сияқты микро деңгейдегі оқиғалардың әсерін эмпирикалық түрде өлшей аласыз. Сонымен бірге, дивидендтерді төлеу, жаңа бәсекелестердің пайда болуы, заңнамадағы өзгерістер секілді макродеңгейдегі оқиғалардың да әсерін бағалай аласыз [49-52].

2) Екіншіден, акциялар құнының өзгеруін анықтай отырып, оқиғаларды талдау әдісі компанияның қызметін объективті бағалауға [53], сонымен қатар акциялардың құнына әртүрлі оқиғалардың әсерін өлшеуге мүмкіндік береді [54].

3) Үшіншіден, оқиғаларды талдау әдісі ұзын немесе қысқа терезелер арқылы ұзақ және қысқа мерзімде оқиғалардың әсерін бағалауға мүмкіндік беретін әмбебап әдіс болып табылады [55,56]. Осылайша, оқиғаларды талдау әдісі нақты оқиғалардың акциялар құнына және компанияның табыстылығына бірнеше күн немесе тіпті бірнеше жылдардағы әсерін зерттеуге мүмкіндік береді.

Монографияда оқиғаны талдау әдісінің негізгі кезеңдері анықталды. Бұл кезеңдерді зерттеушілер компаниялар қызметіне нақты оқиғалардың әсерін талдау үшін пайдалана алады. Сондай-ақ, монографияда кибершабуылдардың компаниялар қызметіне әсерін зерттеу кезінде оқиғаны талдау әдісін қолданудың практикалық мысалы келтірілген.

Оқиғаларды талдау әдісін қолдану кезінде кейбір шектеулердің болатынын ескеру керек:

1) Бұл әдіс негізінде жатқан болжамдар барлық жағдайда сәйкес келмеуі мүмкін. Осылайша, бұл әдіс капитал нарығы әрқашан да тиімді деп болжайды. Капитал нарығының тиімділігі акция құны әрқашан нарықтағы барлық ақпаратты өз бойына сіңіріп, анықталады дегенді білдіреді. Алайда, іс жүзінде бұл жағдай капитал нарығына әрқашан тән емес, және нақты өмірде капитал нарығы әрқашан да тиімді бола бермейді.

2) Қандай оқиға терезесі таңдалғаны зерттеу нәтижелеріне әсер етуі мүмкін. Негізі, оқиға терезесінің ұзақтығы зерттеушінің тәжірибесіне байланысты болады. Әдетте, осы зерттеу әдісін бірнеше рет қолданып, нақты жағдайда қандай оқиға терезесін қолдануға болатынын дәлірек анықтауға болады.

3) Компанияның қызметіне әсер етуді бағалау үшін қандай үлгі таңдалғаны да зерттеу нәтижелеріне әсер етуі мүмкін. Зерттеуші қандай көрсеткіштерді қолдануы ғалымның тәжірибесіне байланысты болады.

Оқиғаларды зерттеу әдісінің тарихи дамуы

Оқиғаларды талдау микро- және макродеңгейдегі оқиғалардың әсерінен компаниялардың акциялар құнының қозғалысын зерттейді. Оқиғаларды талдау әдісі қаржылық талдауда кеңінен қолданылады. Оқиғаларды зерттеу оқиға кезіндегі аномальді кірістілік мөлшерінің (дәлірек оқиға терезесі кезінде) осы оқиғаның компания акцияларының құнына, және сайып келгенде, акционерлердің әл-ауқатына айтарлықтай әсер ететіндігі туралы қорытынды жасау үшін негіз болатындығына негізделген. Осылайша, оқиғаларды зерттеу оқиғаның компания саясатына және компанияның топ-менеджменті қабылдайтын болашақ шешімдеріне әсерін дәлелдейді.

Сонымен қатар, оқиғаларды талдау капитал нарығының тиімділігін тексеруге мүмкіндік береді. Осылайша, белгілі бір оқиғадан кейін компания акцияларының аномальді кірістілігінің болуы және оның ұзақ уақыт сақталуы капитал нарығының тиімсіздігін көрсетеді [57,58].

Алғаш рет Fama et al. (1969) енгізген оқиғаны талдау әдісі нақты оқиғалардың салдарын зерттеудің тиімді әдісі болып саналады [53]. Бұл әдіс статистикалық талдау құралдарына негізделген және ең алдымен корпоративтік өзгерістердің қаржылық әсерін зерттеуге бағытталған. Бұл әдісті қолдана

отырып, зерттеушілер белгілі бір оқиғаның нәтижесінде туындаған «аномальді» кірістілікті анықтайды. Оқиғаларды талдау әдістемесі қазіргі уақытта бизнестің барлық дерлік салаларында қолданылады, мысалы, менеджмент, операциялық менеджмент, қаржылық менеджмент, маркетинг және т.б.

Оқиғаларды талдау әдістемесі шетелдік әдебиеттерде кеңінен қарастырылады, мысалы, Binder (1998), McWilliams & McWilliams (2011), Srinivasan & Bharadwaj (2004), Pynnönen (2005) [59-62].

Оқиғаларды зерттеудің негізгі мақсаты – аномальді кірістілікте көрінетін акциялар құнының қосымша қозғалысын анықтау. Бұл қосымша қозғалыс компанияның әлеуетті кірісіне әсер ететін күтпеген оқиғаның орын алуына байланысты болуы мүмкін. Оқиғаларды талдау белгілі бір оқиғаға ұшыраған компаниялардың аномальді кірістілігін зерттеуді, бұл көрсеткіштің статистикалық түрде нөлден айырмашылығын немесе жоқтығын анықтауды қамтиды.

Егер акциялардың орташа кірістілігі статистикалық тұрғыдан маңызды және оң болса, онда бұл оқиға компания үшін оң болып саналады, өйткені ол компанияның қызметіне оң әсер етеді, яғни акциялардың құнын арттырады және сәйкесінше акционерлердің әл-ауқатын арттырады.

Және керісінше, егер орташа аномальді кірістілік теріс және статистикалық маңызды болса, онда оқиға компания үшін теріс деп қабылданады. Бұл орын алған оқиға жағымсыз жаңалық болып есептеліп, компания мен оның қызметіне кері әсерін тигізеді, яғни акция бағасын және компания акционерлерінің әл-ауқатын төмендетеді.

Егер орташа кірістілік көрсеткішінің өзгеруі статистикалық тұрғыдан шамалы болса, бұл оқиға компанияның қызметіне және акционерлердің әл-ауқатына әсер етпегенін көрсетеді. Оқиға күтілсе және оның әсері акция бағасына енгізілген болса, оқиғаларға ешқандай реакция болмауы мүмкін деп саналады.

Оқиғаларды талдау әдісі белгілі бір компанияға әсер етуі мүмкін оқиғаларға, сондай-ақ бүкіл салаға, елге немесе жаһандық нарыққа әсер етуі мүмкін оқиғаларға қатысты қолданылуы мүмкін. Бас директордың ауысуы, қосымша дивидендтердің төленуі, компанияларға қарсы сот ісінің жүргізілуі, саяси өзгерістер, жаңа заңнамалар осындай оқиғаларға мысал бола алады.

Компания акцияларының аномальды кірістілігі қалай анықталады? Қандай оқиға терезесін таңдалуы керек? Зерттеу үшін бір күн жеткілікті ме, әлде бірнеше күнді қарастыру керек пе? Егер қордың қалыпты кірістілігін бағалау үшін нарық үлгісі таңдалса, осы үлгіні пайдаланып акция кірістілігі қалай анықталады? Акция құнының өзгеруін қандай теориялар түсіндіреді? Бұл сұрақтардың жауабын әр зерттеуші өз бетінше анықтап отырады. Дегенмен, барлық әдістемелер акцияның қозғалысы оқиға орын алмағандағы қозғалысымен салыстырғанда қалай өзгергенін анықтауға бағытталған. Оқиғаларды зерттеу әдістемесін көптеген зерттеушілер өз жұмыстарында қолданды. Олардың қатарында Binder (1985), McWilliams & Siegel (1997), Peterson (1989), MacKinlay (1997) және Corrado (2011) еңбектерін атап өтуге болады [54,63-66].

Оқиғаны талдағанда, алдымен зерттелетін оқиғаны анықтау керек. Оқиға белгілі бір фирмаға немесе бүкіл нарыққа әсер етуі мүмкін. Мысалы, дивидендтерді төлеу, компаниялардың қосылуы, бас директорды ауыстыру және акцияларды бөліп тастау компанияға тән оқиға ретінде қарастырылады. Ал заңнамадағы өзгерістер мен саяси өзгерістер бүкіл нарыққа әсер ететін оқиғалар ретінде қарастырылады.

Оқиғаны талдау әдісінде зерттелетін оқиға кездейсоқ сипатқа ие болу керек. Оқиғаларды зерттеу әдістемесі кездейсоқ оқиғалардың акциялар құнына әсерін зерттеу үшін пайдаланылады. Оқиғаларды зерттеу іріктелген әрбір фирма үшін нарық үлгісін бағалауды, содан кейін аномальды кірістілікті есептеуді қамтиды. Тиімді нарықтық гипотезасына сүйене отырып, бұл аномальды кірістілік қор нарығының күтілетін оқиғаның пайда болуына реакциясын көрсетуі мүмкін. Жалпы, оқиғаны зерттеу әдірісінің негізгі кезеңдерді 4-кестеде берілген.

Оқиғаның қаржылық салдарын анықтау үшін оқиғаны зерттеу әдісін жүргізу кезінде мынадай шарттар орындалуы керек:

- 1) Капитал нарығы тиімді болуы керек;
- 2) Оқиға күтпеген жерден орын алуы керек.

Бірінші шарт Fama (1991, p. 383) және Fama et al. (1969) еңбектерінде тұжырымдалған. Ол оқиғаның әсерін зерттеуге арналған іргелі теориялық болжам болып табылады. Нарықта жарияланған барлық жаңа ақпарат акцияның құнында көрініс

Кесте 4 — Оқиғаларды зерттеу әдісінің кезеңдері

Кезеңдер	Кезеңнің сипаттамасы	Ескертпе
1 кезең	Оқиғаны анықтау	Зерттелетін оқиға капитал нарығы үшін кездейсоқ болып, қаржылық салдары болуы керек
2 кезең	Бұл оқиғаға қаржылық реакцияның ғылыми-теориялық негіздемесін беру қажет	Теориялық негіздер оқиғаның нәтижесі туралы ғылыми түсінік береді
3 кезең	Оқиға әсер еткен компаниялардың іріктемесін анықтау. Оқиғалардың күндерін анықтау	
4 кезең	Оқиға терезесін анықтау	Қысқа мерзімді оқиға терезесін таңдау дұрыс, өйткені олардың зерттеу нәтижелерін бұрмалау ықтималдығы аз. 3,5 күндік оқиға терезелерін таңдаған дұрыс. Оқиғалар терезесін таңдаудың қысқаша негіздемесін келтіру керек.
5 кезең	Көрсетілген кезеңде басқа оқиғаларды бастан өткерген компанияларды алып тастау арқылы компаниялардың іріктемесіне талдау жүргізу	Бұл кезең басқа оқиғалардың қатарлас әсерін болдырмау үшін жүзеге асырылады
6 кезең	Белгілі бір оқиға терезесінде күн сайын жинақталған аномальды кірістілігінің есептеулерін орындау; есептелген аномальды кірістіліктің маңыздылығын зерттеу	Бұл кезеңде Binder (1998), McWilliams & Siegel (1997), Pynnonen (2005), Srinivasan & Bharadwaj (2004) сияқты зерттеулерде сипатталған стандартты әдістеме пайдаланылуы мүмкін
7 кезең	Акциялардың теріс жиынтық кірістілігінің пайызын анықтау	Биномдық Z сынақ статистикасын немесе Вилкоксон тестін (Wilcoxon test) пайдалануға болады.
Ескертпе: [59,60, 63] дереккөз негізінде әзірленген.		

табуы керек, бұл оқиғаның компанияның қаржылық нәтижелеріне әсерін зерттеудің бірден бір жолы [53,58].

Екінші шарт оқиғаның күтпеген жерден болуын талап етеді. Егер ақпарат көпшілікке жарияланғанға дейін ашылса, инсайдерлік ақпаратқа ие инвесторлар нарықтың басқа қатысушыларына қарағанда алдын ала әрекет ете алады. Бұл жағдай статистикалық сынақтардың мәнін шектейді және алынған нәтижелерді бұрмалайды.

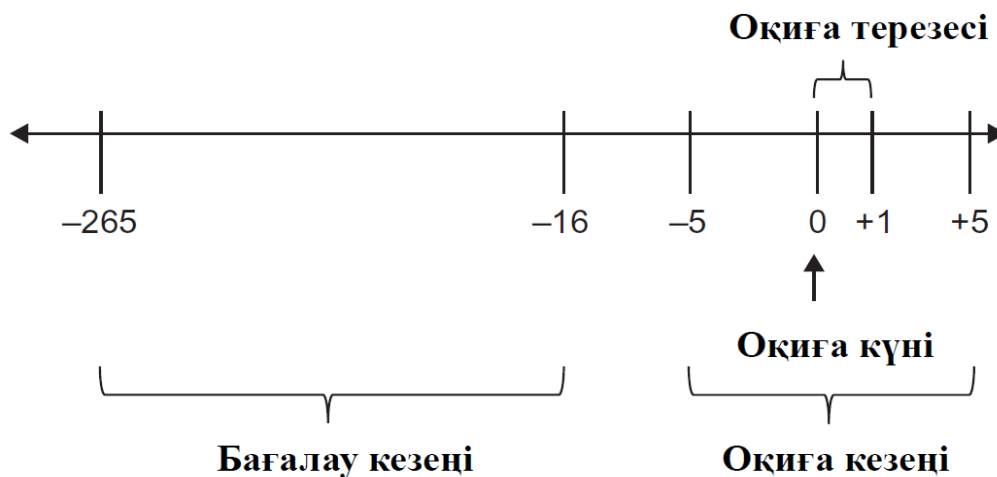
Оқиға күнін анықтау үшін зерттеуші компания көздерінен, жаңалықтардан, пресс-релиздерден, компания есептерінен және зерттеу дерекқорларынан жалпыға қолжетімді ақпаратты пайдалана алады. Оқиға күні нөлдік күн ретінде қабылданады және барлық кейінгі есептеулер осыған негізделеді.

Оқиға күнін анықтау қиын болса, онда оқиға мерзімін ұзақ етіп, яғни оқиғаға дейін 5 күн және оқиғадан кейін 5 күн (-5 және +5) етіп алуға болады. Осылайша, іс-шараның жалпы ұзақтығы 11 күн болып есептеледі.

Оқиға ұзақтығы мен оқиға терезесі бірдей болуы мүмкін. Кейде ақпарат көпшілікке жария болса және нарық тиімсіз болғанда оқиға кезеңі ұзағырақ болуы мүмкін. Оқиғаның ұзақ кезеңін анықтаудың негізгі себептерінің бірі ластаушы оқиғалардың, яғни басқа оқиғалардың өзара әсер етуі болып табылады. Оқиғаларды талдау кезінде мұндай ластаушы оқиғаларды іріктемеден алып тастау ұсынылады, өйткені олар зерттеу нәтижелерін бұрмалауы мүмкін және осы нақты оқиғаның акция кірістілігінің өзгеруіне әсер еткенін дәл көрсетуге мүмкіндік бермейді. Witte (2022) осындай ластаушы оқиғаларды анықтаудың әртүрлі әдістерінің артықшылықтары мен кемшіліктерін анықтап берді [67].

Ластаушы оқиғаларды іріктемеден алып тастағаннан кейін оқиға кезеңін таңдау керек, яғни оқиғаның басталу күні мен бағалау кезеңі (болжауға негіз болатын оқиғаға дейінгі күндер саны) анықталады. Көбінесе бағалау кезеңі ретінде 250 күн алынады. Бұл кезең көпшілікке жария болу немесе басқа да оқиғалардың әсерінен болуы мүмкін ластануды болдырмауға көмектеседі. Осылайша, оқиғаның әсерінсіз 250 күн ішінде акциялардың әрекеті зерттеледі.

1-сурет оқиға күнін, бағалау кезеңін және оқиға кезеңін көрсетіп отыр. Суретте оқиға күні 0 деп, оқиға кезеңі 10 күн $(-5,+5)$, оқиға терезесі 1 күн $(0,+1)$ деп алынды.



Сурет 1. Оқиғаларды зерттеу кескіні

Оқиға күні белгілі бір оқиға болған күнді білдіреді. Оқиғалар терезесі $(0,+1)$ – жаңалықтар акция құнына әсер ететін уақыт кезеңі. Оқиға кезеңі оқиғаға дейін және одан кейінгі 5 күн $(-5,+5)$, яғни бұл акция құнына әсер етуі мүмкін барлық басқа жаңалықтардың (ластаушы оқиғалардың) болуын талдайтын кезең. Бұл мысалдағы бағалау кезеңі 250 күнді құрайды және ол оқиғаның 265-күнінен 16-күніне дейін созылады. Бағалау кезеңі оқиға әсер етпегендегі кірістіліктің өзгеру заңдылығын анықтау мақсатында регрессия коэффициенттерін табу үшін қолданылады.

Бағалау кезеңін анықтау кезінде келесі модельдерді пайдалануға болады:

- 1) Орташа түзету моделі;
- 2) Нарықтық модель;
- 3) Нарықтық түзету моделі.

Орташа түзету моделі бағалау кезеңіндегі акцияның орташа кірістілігіне негізделген, яғни көрсетілген кезеңдегі орташа кірістілікке сүйене отырып, оқиға кезеңінде акциялардың кірістілігі болжанады.

Екінші үлгі, нарықтық модель, болжанатын нарықтық тәуекелге сәйкес акция кірістілігін түзетуді қамтиды. Осылайша,

нарықтық кірістілік есепке алынады және оқиғасыз кезеңдегі акция кірістілігімен салыстырылады. Бұл модельдің негізгі кемшілігі акция кірістілігі көрсеткішін анықтау болып табылады. Көптеген зерттеушілер Нью-Йорк қор биржасының нарықтық индекстерін пайдаланады. Сонымен бірге, зерттеуде салалық индекстер сияқты басқа көрсеткіштер де пайдаланыла алады. Дегенмен, нарықтық тепе-теңдік қор индекстерін пайдалану бағалау кезеңіндегі акциялардың орташа кірістілігін дәлірек бағалауды қамтамасыз етеді деп саналады.

Үшінші модель, нарықтық түзету моделі қор нарығы индексінің орташа кірістілігін негізге алады. Қор нарығы индексінің орташа кірістілігі бұл модельдегі акция кірістілігінің ең жақсы және дәл көрсеткіші деп саналады.

Бұл монографияда біз бағалау кезеңіндегі орташа кірістілігін есептеу үшін нарықтық модельді пайдаланамыз. Болжам жасау үшін регрессиялық талдауды (OLS – Ordinary Least Squares) пайдаланып, күтілетін тұрақты көрсеткіш (Intercept, α) пен көлбеу (slope, β) коэффициенттерін есептей аламыз. Әрбір компанияның күнделікті акцияларының кірістілігі күнделікті нарықтық кірістілікке регрессияға ұшырайды. Осылайша, егер іріктемеде компаниялар саны N болса, онда (α)-ның N және (β)-ның N саны есептелініп, кейін олар оқиға терезесі кезінде аномальды кірістілікті есептеу үшін қолданылады.

Жалпы алғанда, нарықтық модельді қолданған дұрыс, өйткені оның уақыттық қатарларды кластерлеуге байланысты туындауы мүмкін ауытқуларды азайту артықшылығы бар [64].

Аномальды кірістілік Brown and Warner (1985) ғалымдары ұсынған мына формула арқылы есептеледі [56]:

$$AR_{i,t} = R_{i,t} - \alpha_i - \beta_i * R_{m,t} \quad (1)$$

мұндағы, α_i – OLS регрессиясындағы i -ші компаниясы үшін тұрақты (intercept) шама,

β_i — OLS регрессиясындағы i -ші компаниясы үшін көлбеу (slope) шамасы,

$R_{i,t}$ - i -ші компаниясының акция кірістілігі,

$R_{m,t}$ — оқиға терезесінің t күніндегі нарық кірістілігі.

Егер біз 1-суреттегі мысал негізінде аномальды кірістілікті есептейтін болсақ, онда оқиға терезесі үшін іріктемедегі әрбір фирма үшін 11 аномальды кірістілік есептеледі (яғни 5 күн бұрын және кейін, сондай-ақ оқиғаның 0 күні). Осылайша, бірінші аномальды кірістілік фирманың β мәнін -5 күніндегі нарықтық индекс кірістілігіне көбейту арқылы есептеледі. Бұл бірінші фирма үшін тұрақты (intercept, α) мәніне қосылады. Тұрақты шаманың, β және нарықтық кірістіліктің көбейтіндісінің сомасы бірінші фирма үшін болжанған (немесе күтілетін) кірістілікті көрсетеді. Содан кейін бұл болжамды кірістілік бірінші фирманың акцияларының нақты кірістілігінен шегеріледі, ол бірінші фирманың -5 -ші күні аномальды кірістілігі бар-жоғын көрсетеді. Жоғарыда аталған процесс іріктемедегі әрбір компания үшін және оқиға терезесінің әрбір күні үшін орындалады.

Содан кейін жиынтық аномальды кірістіліктер есептеледі және кейіннен оның статистикалық маңыздылығы сыналады. Жиынтық аномальды кірістілік оқиға терезесінің барлық күндері үшін аномальды кірістіліктің қосындысынан тұрады және мына формуламен анықталады:

$$CAR_i = \sum_{t=0}^t AR_{i,t} \quad (2)$$

Оқиға терезесі зерттеушілердің зерттеу мақсатына байланысты анықталады. Егер екі күндік терезе қарастырылса, онда $-1, 0, +1$ күндердің CAR қосындысы алынады. Оқиға терезесінің алдында ақпараттың жария болуын тексеру қажет болса, $-5, -4, -3, -2, -1, 0, +1, +2, +3, +4, +5$ күндер үшін аномальды кірістілікті қосу керек. Содан кейін жиынтық аномальды кірістіліктің (CAR) статистикалық маңыздылығы анықталады. Peterson (1989) 1 күннен асатын кезеңдердегі аномальды кірістілікті түзетудің балама әдісін ұсынады. Ол келесі формула арқылы есептелетін стандартталған жиынтық аномальді кірістілікті (SCAR) пайдалануды ұйғарады [64]:

$$SCAR_i = \frac{CAR_i}{\sqrt{\text{Variance}(CAR)_i}} \quad (3)$$

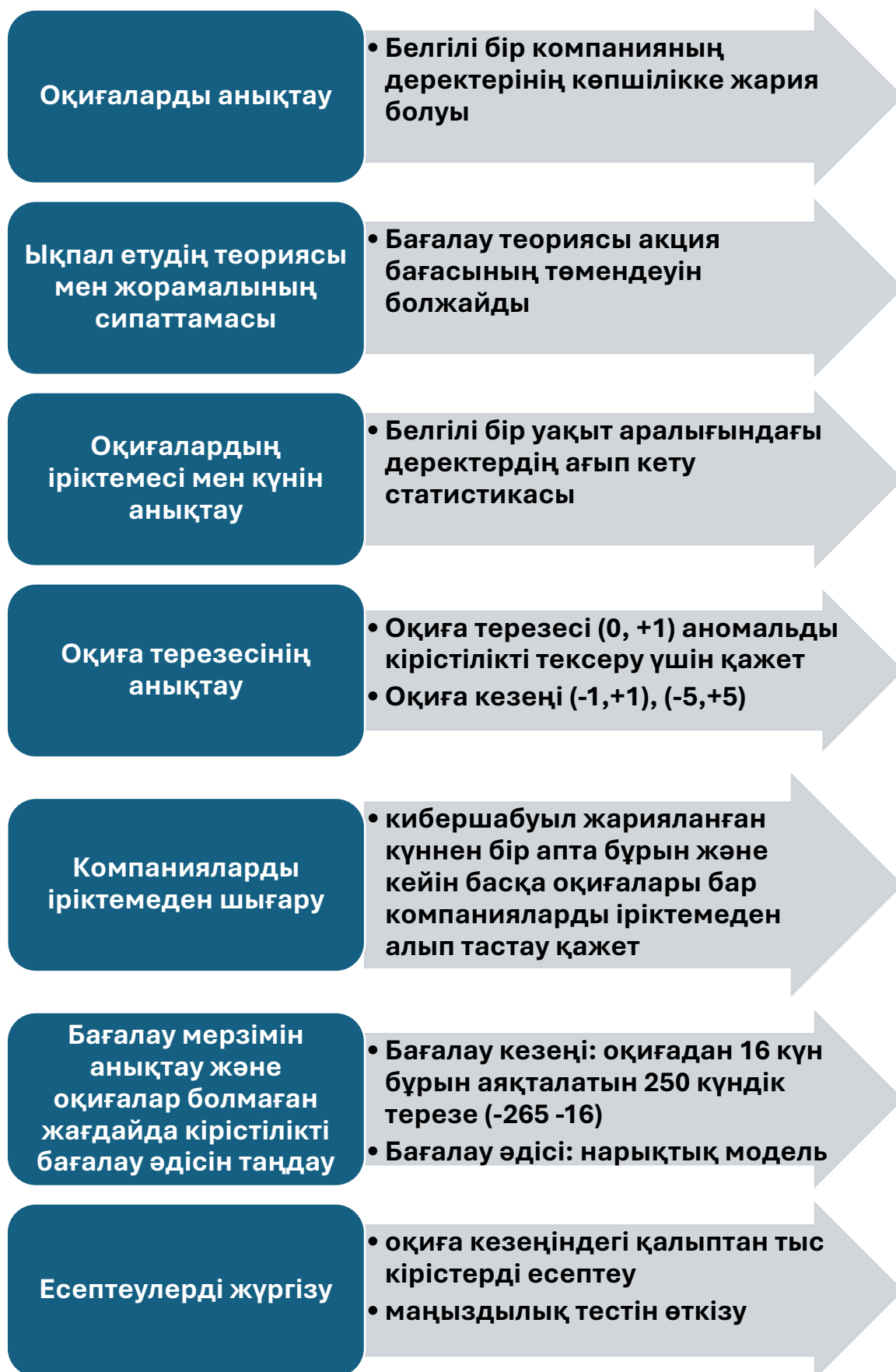
Егер мәліметтердің қалыпты таралуын болжасақ, оқиғаның әрбір күні үшін Z-статистикасын есептеу арқылы статистикалық маңыздылыққа тест жүргізуге болады. Сондай-ақ тестілеуден бұрын бір күндік аномальды кірістілікті стандарттауға болады. Стандартталған жиынтық аномальды кірістілікті есептеудің негізгі артықшылығы – талдаудың гетероскедатикалығын төмендетеді (бұл жағдайда аномальды кірістілік тәуелді айнымалы ретінде пайдаланылады) [64].

2-суретте оқиғаны талдауды жүргізу үлгісі көрсетілген, ол жеті кезеңнен тұрады. «Оқиғаны анықтау» мен «Оқиға терезесін таңдау» қадамдарын біріктіруге болады. Сонымен қатар, кейбір зерттеушілер компанияның сипаттамаларына негізделген SAR талдауын жүргізеді және мұны зерттеудің құрамдас бөліктерінің бірі ретінде қарастырады. Дегенмен, басқа ғалымдар мұны бөлек талдау деп санайды. Сондықтан, осы талдау схемасын пайдаланған кезде, әрбір зерттеуші қандай кезеңдерді жүзеге асыру керектігін және қайсысын біріктіруге немесе алып тастауға болатынын өзі шешеді.

Компанияны бағалау теориялары компанияның ағымдағы құны болжамды болашақ ақша ағындарының дисконтталған құны ретінде анықталады деген тұжырымға негізделеді. Кибершабуылдар кезінде деректердің бұзылуы қосымша қаражаттың жұмсалуына және сот шығындарына әкеледі, ол өз кезегінде, компанияның нарықтық құнын төмендетіп жібереді деп тұжырымдалады.

Сонымен қатар, деректердің көпшілікке жария болуынан кейін компанияның клиенттері болашақ транзакцияларға қатысты алаңдаушылық тудыруы мүмкін. Бұл компанияның клиенттерін жоғалтуына әсер етуі мүмкін, ал бұл қосымша шығындарға алып келетіні хақ. Осылайша, кибершабуылдарға нарықтың осындай реакциясын күте отырып, акция құнының теріс өзгеруін болжауға болады.

Келесі қадам оқиға терезесін таңдау болып табылады. Оқиғалар терезесі оқиғаны көпшілікке жариялау күні, яғни 0-күн және келесі күні (+1) деп қабылданады. Келесі күнді оқиға күні ретінде қабылдау жаңалықтардың сауда күнінің соңында хабарланатынына негізделген, сондықтан бұл жаңалықтың барлық салдары келесі сауда күнінде көрініс тауып отырады.



Сурет 2. Кибершабуыл мысалында оқиғаны талдау кезеңдері

Осылайша, екі күндік оқиға терезесі жаңалықтың компания акциясының құнына әсер етуі мүмкін кезеңді толығымен қамтиды. Егер біз аз зерттелген белгілі бір оқиғаның әсерін зерттейтін болсақ, онда оқиға кезеңін (оқиға терезесін) ұзарту ұсынылады.

Бұл зерттеушіге оқиға туралы ақпараттың жария болуын немесе нарықтың дәл осы сәтте тиімсіз болғанын анықтауға мүмкіндік береді. Оны оқиға басталар алдындағы акциялардың қозғалысынан-ақ көруге болады. Сондықтан, кейде оқиға терезесі ретінде екі апталық кезеңді алу ұсынылады.

Сол себепті, біз оқиғаға дейін және одан кейін 5 күнді, сондай-ақ іс-шара жарияланған күнді аламыз, сонымен ол жалпы 11 күн болады. Акция құнының реакциясына қатысты болжамның дұрыстығын анықтау үшін оқиғаның екі күндік терезесін алу қажет екенін тағы да ескеріңіз.

Келесі кезеңде әртүрлі оқиғалардың өзара әсерін жою үшін компанияларда белгілі бір кезеңдегі басқа жаңалықтардың бар-жоғын тексеру қажет. Егер компанияда дивидендтер төлеу туралы хабарландыру, компания басшылығының өзгеруі, басқа компаниямен қосылу, акциялардың бөлінуі, нарыққа жаңа өнімді шығару және т.б. сияқты маңызды оқиғалар орын алса, онда ол компанияны іріктемеден алып тастау қажет. Өйткені, бұндай компаниялар нақты оқиғаны, мысалы, біздің жағдайда компания қызметіне кибершабуылдарды, одан әрі қарай талдаудың дәлдігін бұзады.

Алтыншы кезең – бағалау кезеңін және бағалау моделін таңдау. Оқиға алдындағы бағалау кезеңін 250 күнге тең деп алу ұсынылады. Оқиға мен бағалау кезеңі арасында ешқандай сәйкестіктер орын алмауына сенім болу үшін бағалау кезеңі оқиғаның өзінен 16 күн бұрын аяқталуы ұсынылады. Бағалау үлгісін таңдаған кезде белгілі бір уақыт кезеңі үшін нарықтық кірістілікті есептеу кезінде тең салмақты нарықтық қор индексінен алынған кірістілікті пайдалануды ұсынамыз. Бір мезгілде, нарықтық бағалау моделін пайдалана отырып, оқиға болмаған жағдайда күтілетін кірістілік параметрлерін бағалау қажет. Осы мақсатта регрессиялық талдау қолданылады, мұнда іріктеудегі әрбір компания үшін регрессия константасы (intercept) және коэффициент (β) анықталады.

Келесі қадам аномальды кірістілікті есептеу және бұл көрсеткіштің статистикалық маңыздылығын тексеру болып табылады. Күтілетін кірістілік күнделікті нарықтық кірістілікті есептелген β коэффициентіне көбейту арқылы (1) формула бойынша есептеледі. Содан кейін есептелген α шегеріледі. Аномальды кірістілік оқиға болған күнгі нақты және күтілетін кірістілік арасындағы айырмашылық ретінде есептеледі. Осылайша, жинақталған аномальды кірістілік 0 және 1 күндердегі аномальды кірістіліктің қосындысын (CAR(0,1)) көрсетеді. CAR (-5,+5) -5-тен +5-ке дейінгі аномальды кірістіліктің қосындысын көрсетеді.

Оқиғаларды зерттеу әдістерінің сипаттамасы

Оқиғаларды талдау белгілі бір оқиғаны бастан өткерген компаниялар акцияларының кірістілігінің өзгеруін зерттейді. Оқиға уақыттың әртүрлі нүктелерінде орын алуы мүмкін немесе белгілі бір күнге топтастырылуы мүмкін (мысалы, белгілі бір күннен бастап заңнаманың өзгеруі). Оқиға уақыты $t = 0$ деп алсақ, онда t уақыт кезеңіндегі i акцияның кірістілігі R_{it} -ке тең болады:

$$R_{it} = K_{it} + e_{it} \quad (4)$$

мұндағы,

K_{it} – акцияның нормаға сай (күтілетін) кірістілігі;

e_{it} – аномальды (күтпеген, нормадан тыс) акция кірістілігі.

Бұл формуланы келесі формулаға түрлендіруге болады:

$$e_{it} = R_{it} - K_{it} \quad (5)$$

Осылайша, e_{it} белгілі бір оқиғада алынған кірістілік пен күтілетін (қалыпты) кірістіліктің (қалыпты уақытта алынатын) арасындағы айырмашылық болып табылады. Акцияның аномальды кірістілігі орын алған жағдайда оқиғаға байланысты акционердің әл-ауқаты өзгерді дегенді білдіреді. Негізінен, оқиғаларды талдау кезінде қарапайым акциялар құнының өзгеруін негізге алады. Тек кейбір жағдайларда ғана артықшылықты акциялар мен облигациялар құнының өзгеруін талдауға болады.

Күтілетін кірістілікті анықтау моделі аномальды кірістілікті есептеу алдында анықталуы керек. Күтілетін кірістілікті анықтаудың бірнеше әдістері бар, мысалы, тұрақты күтілетін кірістілік моделі, нарықтық модель, капитал құнын анықтау моделі. Жоғарыда аталған әдістерде күтілетін кірістілік әртүрлі болуы мүмкін, бұл есептелетін аномальды кірістілікке де әсер етуі мүмкін. Келесі бөлімдерде күтілетін кірістілікті анықтау үшін нарықтық модельді қолданылу мысалы келтіріледі.

Гипотезаларды тұжырымдау

Жиынтық аномальды кірістілік

Оқиғаларды зерттеуді жүргізген кезде оқиға терезесі кезеңінде кірістіліктің көлденең қимасы бойынша бөлінуі аномальді болып табылатыны, яғни күтілетін мәннен айырмашылығының бар болуы анықталады. Кірістіліктің нормадан тыс таралуын зерттегенде бірнеше әдіс қолданылады. Негізгі логика - нақты кірістілік күтілетінмен салыстырылады, болжамды мәннен нақты кірістіліктің ауытқуы бар ма, жоқ па анықталады. Мұндай ауытқулардың статистикалық жағынан маңыздылығы зерттеледі. Зерттеу гипотезасын тұжырымдағанда t уақытындағы орташа жиынтық аномальды кірістілік (CAR) 0 мәніне тең болуы тексеріледі.

Зерттелетін кезеңдегі кірістіліктің үлестіру медианасы мен дисперсиясы да анықталады. Орташа кірістілік көрсеткіштерін зерттеу белгілі бір оқиғаның компания акционерлерінің жалпы әлауқатына ықпал етуін анықтауға көмектеседі. Осылайша, N бағалы қағаздарының іріктемесі үшін t кезеңіндегі орташа нормадан тыс кірістілік келесі түрде есептеледі:

$$AR_t = \frac{1}{N} \sum_{i=1}^N e_{it} \quad (6)$$

Жиынтық уақыт қатары

Сонымен қоса, белгілі бір оқиғаның айналасында аномальды кірістілік бар-жоғы зерттеледі. Егер оқиға болжанатын болса, онда оған дейін-ақ нормадан тыс кірістілікті байқауға болады. Сондай-ақ, егер сіз белгілі бір оқиғадан кейін аномальды кірістілікті зерттесеңіз, нарықтың тиімділігі туралы қорытынды жасай аласыз. Өйткені нарықтағы барлық ақпарат акциялардың құнында көрініс табады.

Бірнеше күндік кезеңдегі көрсеткішті бағалау кезінде берілген кезеңдегі уақыт қатарларын жинақтау әдісі қолданылады. Осылайша, t_1 кезеңінен t_2 кезеңіне дейінгі әрбір бағалы қағаздың нормадан тыс орташа кірістілігінің көрсеткіші ретінде жиынтық орташа аномальды кірістілік (CAR) әдісі пайдаланылып, келесі жолмен есептелінеді:

$$CAR_{(t_1, t_2)} = \sum_{t=t_1}^{t_2} AR_t \quad (7)$$

Бұл әдістер нөлдік гипотезаны тексереді. Нөлдік гипотеза аномальды кірістілік нөлге тең деп анықтайды.

Сынақ статистикасының (t-тест) критикалық мәні 1%, 5%, 10% (0,01; 0,05; 0,1) шамаларынан асатын болса, нөлдік гипотеза қабылданбайды. t-тест мәні кездейсоқ шама деп қабылданады.

Теңдеуде көрсетілген жиынтық орташа аномальды кірістілік (CAR) үшін стандартты статистикалық сынақты орындауға болады. Стандартты ауытқуды анықтаудың бірнеше әдістері бар, мысалы Campbell et al. (1998) ұсынған әдіс [68]. Бұл монографияда балама тәсілді пайдалану ұсынылады, яғни CAR-ды келесі формула арқылы түбір астындағы стандартты ауытқуға бөлеміз:

$$\frac{CAR_{(t_1, t_2)}}{[\delta^2(t_1, t_2)]^{1/2}} \quad (8)$$

мұндағы,

$$\delta^2(t_1, t_2) = L\delta^2(AR_t) \quad (9)$$

мұндағы,

$\delta^2(AR_t)$ – бір кезеңдегі орташа аномальды кірістіліктің ауытқуы.

Соңғы теңдеу жиынтық орташа аномальды кірістілік (CAR) L мәнінен жоғары дисперсияға ие екенін көрсетеді. Ол сондай-ақ бір кезеңдегі орташа аномальды кірістіліктің уақыт қатарының тәуелсіздігін жорамалдайды.

Алынған нәтижені (5) формула бойынша статистикалық тестілеуден өткізу бір кезеңдегі орташа аномальды кірістіліктің

дисперсиясы дұрыс есептелген жағдайда ғана сенімді бола алады. Бір уақытта болып жатқан оқиғаларды зерттейтін болсақ, әр түрлі компаниялардың бір кезеңдегі аномальды кірістілігі бір-бірінен тәуелсіз деп саналады. Дегенмен, бұл болжам қате болуы мүмкін, өйткені бір оқиға бір уақытта бірнеше компанияның қызметіне әсер етуі мүмкін. Бұл олардың кірістілігі бір-бірімен байланысты болуы мүмкін дегенді білдіреді. Бұл жағдайда кірістіліктердің тәуелсіздігі туралы болжамды пайдалана отырып есептелген стандартты ауытқу көрсеткіші төмен болады, ал кірістіліктің статистикалық маңыздылығы жоғары деп бағаланады [69-71].

Статистикадағы бұл бұрмалануды жою үшін уақыт бойынша кірістіліктің өзгермелілігін ескеретін әдіс қолданылады. Ол үшін осы нақты оқиғадан зардап шеккен бірнеше компаниялардың кірістілігін біріктіретін «оқиғалар портфолиосын» жасау қажет. Әрі қарай, біз оқиғадан 180 күн бұрын және одан кейін болуы мүмкін осындай оқиғалар портфолиосының аномальды кірістілігінің уақыт қатарын аламыз. Бұл оқиға кезеңінде аномальды кірістіліктің статистикалық маңыздылығын дәлірек анықтауға мүмкіндік береді. Бұл жағдайда тәуелсіз мәндер негізінде аномальды кірістіліктің маңыздылығын есептеудің қажеті жоқ. Мұндай жағдайда кірістіліктің өзара тәуелділігі есепке алынады. Бұл оқиғаның кірістілікке әсерін бағалау кезінде алынған нәтижелердің дәлдігін айтарлықтай арттыратын болады.

Дегенмен, портфельді кірістілік әдісі де кейбір шектеулерге ие. Бұл әдістің негізгі кемшілігі оқиға кезеңі белгісіздігінің өте жоғары болуы. Ал бұл, кірістіліктің құбылмалылығын арттырып жібереді. Мысалы, оқиға компания үшін жаңа тәуекелдерді тудыруы мүмкін және белгілі бір кезеңдегі оның кірістілігінің үлкен ауытқуын тудыруы мүмкін. Алайда, біз есептеулер үшін оқиғаға дейін және одан кейінгі кірістілікті пайдаланған кезде (мысалы -180, +180 күн), есептелген мәндер оқиға кезеңіндегі нақты мәндерден әлдеқайда төмен болуы мүмкін. Мұның бәрі зерттеу нәтижелерін бұрмалауы мүмкін. Нәтижесінде, аномальды кірістілік асыра бағалануы мүмкін, өйткені оқиға кезеңінде өскен белгісіздік есепке алынбай есептелген төмендетілген стандартты ауытқу ескеріледі [56,57,69].

Бұл мәселені шешу үшін оқиға кезеңіндегі кірістілік өзгерісінің басқа кезеңдегі кірістілік өзгерісімен салыстыруға

болады. Осылайша, оқиға кезеңінде өзгеріс тым жоғары болды ма, жоқ па, сол бағаланады. Бұл оқиға кезеңінде өзгерістің қаншалықты артқанын өлшеуге және статистикалық маңыздылықты түзету кезінде оны есепке алуға мүмкіндік береді.

Оқиғаларды зерттеу кезінде тест сенімділігінің критерийлерін талдау қажет. Осылайша, статистикалық сынақтарды қолдану кезінде қателердің екі түрі орын алуы мүмкін:

- 1-типті қате нөлдік гипотеза ақиқат болса да қабылданбаған кезде орын алады. Мысалы, егер сынақ аномальды кірістілікті көрсетсе, біз нөлдік гипотезаны қабылдамаймыз. Ал, шын мәнісінде, кірістіліктің бұндай өзгерісі тек кездейсоқтыққа байланысты болды.

- 2-типті қате нөлдік гипотеза жалған болса да, қабылданған кезде пайда болады. Мысалы, шынайы аномальды кірістілік болғанмен, тест мұны көрсетпеді.

Сондықтан тест жоғары сапалы болуы үшін келесі екі негізгі қасиеттерді талдау қажет:

1. Орындалған сынақтың дұрыстығы. Егер 1-типті қатенің ықтималдығы сынақтың маңыздылық деңгейіне сәйкес келсе, сынақ статистика жағынан дұрыс деп саналады. Мысалы, егер маңыздылық деңгейін 5% таңдасақ, бұл 5% жағдайда нормадан тыс кірістілікті қате түрде көрсетуі мүмкін дегенді білдіреді. Бұл 1-типті қатенің ықтималдығы 5% дегенді білдіреді.

2. Сынақ қуаттылығы. Ол сынақтың қалыптан тыс нәтижелерді анықтау қабілетін көрсетеді. Бұл көрсеткіш 1 минус 2-ші типті қатенің ықтималдығы ретінде есептеледі. Мысалы, егер сынақ қуаты 80% болса, 80% жағдайда аномальды кірістілік дұрыс анықталады. Сондықтан қуат неғұрлым жоғары болса, ол нақты өзгерістерді соғұрлым жақсы анықтайды. Ал егер орындалған екі сынақ бірдей 1-типті қатені көрсетсе, қуаты жоғары сынақты таңдау керек.

Сынақтардың спецификациясы мен қуатын экономикалық түсіндіру өте күрделі процесс, өйткені оқиғаны зерттеудегі сынақтар бір уақытта екі аспектіні, аномальды кірістіліктің болуын және модельдің дұрыстығын қарастырады. Модельдің дұрыстығы CAPM (Capital Asset Pricing Model) немесе нарықтық үлгілерге сәйкес күтілетін кірістілікті болжайды. Модельдің дұрыстығын анықтау маңызды фактор болып табылады, өйткені күтілетін

кірістілік үлгісі дұрыс болмаса, онда сынақ нәтижелері де бұрмаланады.

Сонымен қатар, орташа аномальды кірістілікті бағалау кезінде акциялардың аномальды кірістілігінің үлестірілу дәрежесі қалыпты деген қосымша болжам жасау қажет. Сондай-ақ, акциялардың аномальды кірістілігі уақыт бойынша және бір-бірінен тәуелсіз болады деп болжау керек. Бұл болжамдар эмпирикалық түрде тексеріледі және шағын іріктемені пайдаланған кезде маңызды деп саналады.

Сынақ сипаттамасы мен қуатын талдау үшін модельдеу әдістері қолданылады. Бұл әдісті алғаш рет Brown and Warner (1980, 1985) ұсынды. Әдістің негізгі идеясы - кездейсоқ іріктемелер мен оқиғалардың кездейсоқ кезеңдеріне тестілеуді бірнеше қайталап жүргізу [56,57].

Егер әдіс дұрыс жұмыс істесе, кездейсоқ іріктемелерді талдау кезінде сынақ нормадан тыс нәтижелерді көрсетпейді. Бұл нөлдік гипотеза ақиқат болса да, сынақ оны қаншалықты дұрыс қабылдамайтынын бағалауға мүмкіндік береді.

Сынақ қуатын бағалау кезінде кейбір іріктемелерге аномальды кірістілікті әдейі қосып тексереді. Бұл сынақтың қуатын анықтауға мүмкіндік береді, яғни әдейі енгізілген аномальды кірістілікті тест анықтай алады ма, жоқ па тексеріледі.

Осылайша, осындай әрекеттер көмегімен оқиғаны зерттеу сынақтары дұрыс және сенімді түрде аномальды кірістілікті көрсете ме, жоқ па тексеріледі.

Оқиғаларды талдау сынақтарында қолданылатын статистикалық деректердің дұрыстығын тексеру үшін модельдеу әдістері қолданылады. Модельдеу тесттің дұрыс конфигурацияланғанын көрсетсе, оны толықтыру үшін аналитикалық әдістер қолданылады. Аномальды кірістіліктің әртүрлі деңгейлерінде сынақ қуатын аналитикалық есептеу деректердің таралуы туралы қосымша жорамалдарды қажет етсе де, Brown и Warner (1985, 13-бет) зерттеулері аналитикалық және модельдеу әдістері дұрыс конфигурацияланған сынақтар үшін ұқсас нәтижелер беретінін көрсетеді. Бұл процедуралар орындалған сынақтардың күшін тез және дұрыс айқандауға мүмкіндік береді [56].

Жоғарыда айтылғандардың барлығын 5-кесте түрінде қысқаша көрсетуге болады. Бұл кестеде сынақ спецификациясы (сынақ таңдалған үлгіге қаншалықты дәл сәйкес келетіні), қуат (тесттің алынған нәтижелердегі ауытқуларды анықтау мүмкіндігі), сынақ сезімталдығы сияқты оқиғаларды талдау сынақтарының негізгі қасиеттері көрсетілген.

Кесте 5 – Оқиғаларды талдау әдісінің негізгі сипаттамалары

Көрсеткіштер	Оқиға терезесінің ұзақтығы	
	ұзақ (12 айдан астам)	қысқа (12 айдан төмен)
Тест спецификациясы	нашар/орташа	орташа
Нормадан тыс кірістілік кезінде тесттің қуаты:		
- оқиға төңірегінде	төмен	жоғары
- оқиғаның айналасында емес	төмен	төмен
Тест сезімталдығы:		
Оқиғадан тәуелсіз күтілетін табыс	жоғары	төмен
Нормадан тыс кірістіліктің көлденең қимасы мен уақытқа тәуелділігі	орташа/ жоғары	төмен / орташа
Нормадан тыс кірістіліктің оқиғаға тәуелді дисперсиясы	жоғары	жоғары
Қуат сезімталдығы:		
Іріктеме мөлшері	жоғары	жоғары
Компанияның сипаттамалары (мысалы, көлемі, саласы, т.б.)	жоғары	жоғары
Ескертпе: [56] дереккөз негізінде әзірленді.		

Кестеге сүйене отырып, уақыт көкжиегі сынақтың сенімділігіне айтарлықтай әсер етеді деп қорытынды жасауға болады. Осылайша, қысқа бағалау көкжиегі бар сынақтар дәлірек болып саналады, ал ұзақ оқиғалар терезесі бар сынақтар қателерге әлдеқайда бейім. Сондай-ақ, қысқа бағалау көкжиегі бар

сынақтарда сынақтың күші айтарлықтай жоғары, өйткені аномальді нәтижелер оқиғаның белгілі бір кезеңінде шоғырланған. Ұзақ көкжиегі бар сынақтарда оның күші төмендейді. Сынақтың сезімталдығына қатысты айтсақ, қысқа горизонттық әдістер нормаға сай кірістілік үлгісіне немесе деректердің тәуелділігі туралы болжамдарға тәуелдігі төмен деп саналады. Ұзақ оқиғалар терезесі бар сынақтарда, керісінше, мұндай болжамдар сынақ дәлдігін арттырады.

Қорытындылай келе, қысқа көкжиектер үшін сынақтар дәлірек және қуаттырақ деп айта аламыз, ал ұзақ оқиғалар терезесі бар сынақтар модельді таңдауға және нәтижелерді түсіндіруге ерекше көзқарасты талап етеді, өйткені оларда қуат пен спецификация мәселелері төмен.

Дегенмен, кейбір жағдайларда қысқа және ұзақ көкжиектері бар сынақтар ұқсас нәтижелерді көрсетеді және бұл нәтижелерді модельдеу және талдау әдістері арқылы көрсетуге болады.

Екі сынақ үшін де ортақ мәселе - оқиғаға байланысты бағалы қағаздың аномальды кірістілігінің дисперсиясы ұлғайған кезде нөлдік гипотеза қабылданбайды. Ал бұл жалған тұжырым болуы мүмкін.

Екінші мәселе - іріктеме өлшемі. Көкжиектің ұзындығына қарамастан, іріктеме неғұрлым үлкен болса, сынақтың күші соғұрлым жоғары болады, яғни тесттің кірістіліктегі ауытқуларды анықтау қабілеті де жоғары болады деп есептеледі.

Келесі мәселе - компанияның сипаттамаларына тәуелділігі. Сынақ нәтижелері компанияның көлеміне, саласына және т.б. сипаттамаларына байланысты болады. Белгілі бір бағалы қағаздардың кірістілігіндегі айырмашылық неғұрлым көп болса, қажетті сигналды анықтау қиынырақ болады деп есептеледі, өйткені деректердегі «шудың» жоғарылауымен сынақтың күші төмендейді.

5-кестеде келтірілген деректерді жақсырақ түсіну үшін сынақ қуатының нақты сандық бағалауларын ескеру керек. Бұл бағалаулар 0,05 маңыздылық деңгейінде екі жақты тестілеуді пайдалана отырып, жоғарыда келтіріген (5) және (6) теңдеулердегі статистикалық көрсеткіштерге негізделген. Бұл статистика қысқа уақыт аралығында қолдануда тиімді болғандықтан, модельдеудің орнына қуатты есептеу үшін аналитикалық әдістер пайдаланылды.

Есептеу жүргізгенде бағалы қағаздардың кірістілігі уақыт бойынша да, бір-бірінен де тәуелсіз болады, сонымен қатар барлық бағалы қағаздардың стандартты ауытқуы бірдей болады деп болжанады. Сонымен қатар, кірістіліктің дисперсиясы мен аномальды кірістілік өзара тең деп қабылданады, бұл [Brown and Warner \(1980\)](#) тұжырымдаған «орташа түзетілген кірістілік» моделіне толығымен сәйкес келеді.

2.2 АҚШ компанияларының мысалында кибершабуылдардың қаржылық салдарын талдау

Соңғы жылдары кибершабуылдардың компаниялардың нарықтық құнына әсері белсенді түрде зерттелуде. Киберқауіпсіздіктің бұзылуы туралы ақпараттың жариялануы компаниялардың жиынтық аномальды кірістілігіне (CAR) теріс әсер етеді деп саналады. Осылайша, [Campbell et al. \(2003\)](#) құпия ақпараттың көпшілікке жария болуы CAR-ды айтарлықтай төмендететінін анықтады [4]. [Goel және Shawkey \(2009\)](#) кибершабуылдар компаниялардың нарықтық құнына зиян келтіретінін растады [72]. [Cavusoglu et al. \(2004\)](#) кибершабуылдар фирманың нарықтық құнының 2,1%-ға төмендеуіне әкелуі мүмкін екенін көрсетті. Сондағы, зерттеушілер теріс әсер ету дәрежесі оқиға түріне, сондай-ақ компанияның көлемі мен қызметі сияқты сипаттамаларына байланысты екенін атап өтті [9].

Веб-сайттарды белсенді түрде пайдаланатын және онлайн қызметтерді ұсынатын компаниялар киберқауіпсіздікті бұзудың зардаптарынан көбірек зардап шегеді деп саналады [7]. Дегенмен, бүгінде әрбір дерлік компания өзінің нарықтық үлесін кеңейту үшін Интернетті пайдаланады, мұны офлайн қызметтері шектелген COVID-19 пандемиясы кезінде айқын байқадық. Сондықтан, цифрландыру жағдайында киберқауіпсіздік онлайн ресурстарды пайдалануға байланысты бизнестің негізгі элементіне айналууда. Киберқылмыскерлер компаниялардың қаржылық және жеке ақпаратына қол жеткізу әдістерін жетілдіруді жалғастыруда. [Novav et al. \(2017\)](#) шабуылдың мақсаты, қолданылатын құралдар түрі және шабуылдаушылардың табиғаты сияқты факторлар компанияның нарықтық құнына айтарлықтай әсер ететінін атап өтті [13]. [Gordon et al. \(2003\)](#) киберқауіпсіздікті бұзу туралы

хабарламалар фирмалардың кірістеріне, пайдасы мен беделіне теріс әсер ететінін көрсетті [14].

Mukhopadhyaya et al. (2013) және Low (2017) кибершабуылдар компанияның кірісіне, нарықтық капитализациясына және материалдық емес активтерге, соның ішінде бренд имиджіне теріс әсер ететінін көрсетті [15,16]. Сонымен қатар, соңғы зерттеулер мұндай оқиғалар компаниялардың экономикалық саясатының өзгеруіне әкелетінін анықтады. Мысалы, фирмалар қолма-қол ақша қорларын көбейте бастады (Garg, 2020) және инвестиция мен өтемақыға деген көзқарастарды қайта қарастыруда (Kamiya, 2021) [17,18]. Осыған байланысты, кибершабуылдардың компаниялар қызметінің әртүрлі аспектілеріне қалай әсер ететінін егжей-тегжейлі зерттеу маңызды.

Кейбір зерттеушілер кибершабуылдар мен деректердің құпиялылығының желіге ағып кетуін бөлек қарастырады. Жеке деректердің желіге ағып кетуі, әдетте, киберқауіпсіздік оқиғаларының нәтижесі болып табылады және компания, оның тұтынушылары немесе жеткізушілері туралы ақпараттың жария болуын қамтиды. Зерттеулер деректердің бұзылуы компанияның жұмысына айтарлықтай теріс әсер ететінін көрсетеді. Осылайша, Gatzlaff & McCullough (2010) және Martin et al. (2017), Jeong et al. (2019) және Janakiraman et al. (2018) мұндай оқиғалар басқа компаниялар үшін бәсекелестік артықшылықтар тудырып, зардап шеккен фирмаларға зиян келтіретінін анықтады [73-76]. Бұл жеке ақпаратты сақтау және өңдеу проблемасын көтереді, өйткені бұл жағдай компания осалдығын арттыруы мүмкін. Сонымен қатар, Martin et al. (2017) кибершабуылдар туралы хабарламалар тұтынушылардың сатып алу және қызмет көрсету шешімдеріне теріс әсер ететінін көрсетті, бұл зардап шеккен компаниялардың кірісінің төмендеуіне әкелуі мүмкін [74]. Сондықтан деректер бұзылуының мүдделі тараптарға және фирманың ұзақ мерзімді тұрақтылығына қалай әсер ететінін тереңірек қарастыру маңызды.

Бұл жұмыс АҚШ бойынша соңғы он жылдағы деректер жиынтығын пайдалана отырып, кибершабуылдардың әртүрлі фирманың қызметіне қалай әсер ететінін зерттейді. Айта кету керек, АҚШ Мемлекеттік қауіпсіздікті бұзу туралы заңға (the State Security Breach Notification Laws) сәйкес компаниялар кибершабуылдар туралы ақпаратты көпшілікке жариялауға

міндетті болып келеді. АҚШ бұндай заңды енгізген тұңғыш ел болып саналады. Audit Analytics дерекқорына сәйкес, АҚШ-та 2021 жылдың алты айында ғана тіркелген киберқауіпсіздік оқиғалары (107), бұл 2020 жылғы барлық тіркелген киберқылмыс санынан (105) көп болғанын көрсетіп отыр. Айта кету керек, алдыңғы зерттеулердің көпшілігі 2000-шы жылдардың басында орын алған АҚШ фирмаларына жасалған кибершабуылдар оқиғаларын зерттеуге бағытталған еді [4-9]. Сол себепті, жаңартылған дерекқорды пайдалана отырып, өткен зерттеулердегі жасалған тұжырымдамаларды қайта қарап зерттеу өзекті болып келеді.

Бұл зерттеудің негізгі мақсаты кибершабуылдар компаниялардың нарықтық құнына қалай әсер ететінін зерттеу болып табылады. Өйткені компанияның нарықтағы құны оның қызмет етуінің негізгі көрсеткіші болып табылады. Ал компанияның нарықтық құнын және, сәйкесінше, акционерлердің әл-ауқатын, арттыру компания менеджерлерінің негізгі мақсаты болып табылатыны белгілі [77]. Кибершабуыл туралы хабарландыру нарықтық реакцияны өзгертуі керек және ол теріс болады деп болжанады. Өйткені киберқылмыс оқиғалары фирма үшін қосымша жасырын және айқын шығындарға әкелуі мүмкін. Нарықтың теріс реакциясы оқиға кезінде теріс жиынтық аномальды кірістілікті (CAR) көрсетеді. Бұл зерттеу әртүрлі салаларға тигізетін осындай әсерді зерттеуге тырысты. Бұл жұмыс тек белгілі-бір салалардың ғана компаниялары кибершабуылдардың нысанасы болып табылады ма, жоқ па осыны түсінуге көмектеседі. Сонымен қатар, ірі және шағын компанияларға киберқауіпсіздік оқиғалары қалай әсер ететіні де зерттеледі. Бұл мәселені зерттеу арқылы кибершабуылдар кезінде ірі компаниялардың орта және шағын компаниялармен салыстырғанда артықшылықтары бар ма, жоқ па деген сауалға жауап алуға болады.

Сонымен қатар, киберқылмыстың қай түрі көбірек зиян келтіретінін анықтау өте маңызды. Киберқылмыстың әрбір түрінің әсерін зерттеу олардың қайсысы компаниялар үшін қауіптірек екендігі туралы мәлімет беріп, менеджерлерге компанияның тиімді киберқауіпсіздік жүйесін құруға мүмкіндік береді. Бұған қоса киберқауіпсіздіктің бұзылуының әсерін сандық бағалау маңызды болып келеді. Ол үшін кибершабуылдан болатын орташа қаржылық

шығындар бағаланады. Сондағы елеулі қаржылық шығындар нарықтық құнның айтарлықтай төмендеуіне әсер ете ме, жоқ па осы сұраққа жауап алуға болады.

Аталған сұрақтарға жауап табу үшін, біріншіден, киберқауіпсіздіктің бұзылуына деген нарықтық реакциялар талданды. Кибершабуылдар фирманың нарықтық құнының төмендеуіне, компания беделінің қалпына келуіне байланысты қосымша шығындарға, және кибершабуылдан кейін туындайтын қомақты қаржылық шығындар сияқты теріс салдарға әкеледі деп саналады. Зерттеу барысында мұндай салдардың бар болуы тексеріледі, және теріс жиынтық аномальды кірістілік бар немесе жоқ болуы анықталады. Бұл мынадай гипотезаны тұжырымдап, оны статистикалық сынақтан өткізуге әкеледі:

H1: Киберқауіпсіздіктің бұзылуы туралы хабарландыру жиынтық аномальды кірістілікті арттырады

Нөлдік гипотезадан (H_0) бас тарту нарық қатысушыларының деректердің бұзылуы туралы хабарландыруға реакциясы бар екенін білдіреді.

Сонымен қатар, кибершабуылдардың қандай фирмаларға әсер етуі мүмкін екендігі мынадай гипотезаны тұжырымдау арқылы анықталады:

H2: Кибершабуылдың болғаны туралы хабарландырудың жиынтық аномальды кірістілікке ықпалы компанияның саласына байланысты болады

Нөлдік гипотезаны (H_0) қабылдамау компаниялардағы киберқауіпсіздіктің бұзылуына деген реакция сала түріне байланысты әр түрлі екенін көрсетеді.

Сонымен қатар, фирма көлемінің жиынтық аномальды кірістілікке ықпалын зерттеу үшін компания өлшемі (шағын, орташа, ірі) пайдаланылады. Осы мақсатта келесі гипотеза қарастырылады:

Н3: Кибершабуылдың болғаны туралы хабарландыру жиынтық аномальды кірістілікке ықпалы компания көлеміне байланысты болады

Нөлдік гипотезаны (H_0) қабылдамау компания көлеміне сәйкес кибершабуылға деген реакция әр түрлі болатынын білдіреді.

Киберқауіпсіздіктің бұзылуы туралы хабарландырудың әсерін қарастырудың тағы бір жолы - киберқылмыс түрі мен жиынтық аномальды кірістілік арасындағы байланысты табу. Campbell et al. (2003), Cavusoglu et al. (2004), Gatzlaff & McCullough (2010) кибершабуылдар түріне байланысты компанияның нарықтық құнына әсері де әртүрлі болатынын анықтады [4,9,73]. Әртүрлі кибершабуылдың фирманың қызметіне қалай әсер ететінін тағы да қайта тексеру үшін мынадай гипотезаны тексеруді жөн көрдік:

Н4: Кибершабуыл түріне байланысты теріс жиынтық аномальды кірістіліктер арасында айырмашылық болады

Нөлдік гипотезаны (H_0) қабылдамау кибершабуылдың түріне байланысты компанияның нарықтық құнындағы өзгерістер әртүрлі болатынын көрсетеді.

Көптеген зерттеулерге қарамастан, кибершабуылдардың акционерлер әл-ауқатына, компания сатылымдар көлемінің өсуіне және фирманың қаржылық және инвестициялық саясатына қалай әсер ететіні туралы жүйелі дәлелдер жоқ. Киберинциденттер фирманың өнімділігіне теріс әсер етіп, ROA, ROE көрсеткіштерін, сондай-ақ сату көлемі мен қаржылық тұрақтылықты төмендетеді деп болжануда [10]. Фирмалар шабуылдан кейін киберқауіпсіздік жүйесіне көбірек инвестиция салады деп саналады. Бұл зерттеу кибершабуылдың фирманың операциялық көрсеткіштеріне, инвестициялық және қаржылық шешімдеріне ықпалы бар-жоғын анықтауға тырысады.

Ол үшін мынадай гипотеза тексеріледі:

Н5: Кибершабуылдар шабуылдан кейінгі кезеңдегі фирманың операциялық көрсеткіштеріне, инвестициялық және қаржылық қызметіне әсер етеді

Нөлдік гипотезаны (H_0) қабылдамау шабуылға ұшыраған фирмалар операциялық, қаржылық және инвестициялық саясатта өзгерістерге ұшырайтынын білдіреді.

Деректер мен әдістеме

Бұл жұмыста кибершабуылдар туралы хабарландырулардың фирманың нарықтық көрсеткіштеріне әсерін талдау үшін оқиғаларды зерттеу әдістемесі пайдаланылады. Оқиғаларды зерттеу қауіпсіздікті бұзу оқиғаларынан туындаған жиынтық аномальды кірістілікті зерттеуге көмектеседі. Акция құнының ауытқуы болған жағдайда, оқиғаның акция құнының ауытқуына айтарлықтай әсер еткенін McWilliams & Siegel (1997), MacKinlay (1997) түсіндіріп берді [54,65].

McWilliams & Siegel (1997) және MacKinlay (1997) ұсынған нарықтық үлгі (Market Model) киберқауіпсіздік инциденттерінен туындаған жиынтық аномальды кірістілікті зерттеу үшін пайдаланылады. Стандартты оқиғаларды зерттеу әдісіне сәйкес, кірістілік пен күтілетін кірістілік арасындағы айырмашылық регрессиялық талдауды орындау арқылы анықталады. Бұндай есептеу үшін қолданылатын стандартты формула мынадай:

$$R_{it} = \alpha_i + \beta_i * R_{mt} + \varepsilon_{it} \quad (10)$$

мұндағы, R – кірістілік

i – компания,

t – оқиға күні,

R_{mt} – нарық индексі,

α , β - нарықтық үлгі көрсеткіштері

ε - қалдық құн.

Нарық үлгісі үшін оқиға терезесін және бағалау кезеңін анықтау қажет. Әдетте, бағалау кезеңі оқиға терезесіне дейін 120 сауда күнге тең деп алынады. Оқиға терезесін оқиғадан 1,3,5,10 күн бұрын және оқиғадан кейін 1,3,5,10 күн ретінде орнатуға болады. Бұл монографияда жалпы 3, 7, 11 күндік оқиға терезелері, кибершабуыл оқиғасынан бір күн бұрын және кейін, үш күн бұрын және кейін, бес күн бұрын және кейін қолданылады. [-1,+1], [-3,+3], [-5,+5] оқиғалар терезелерін таңдаудың себебі, бұзушылық орын алып, кейін ол көпшілікке жария болған күндер арасында қандай да

бір аралық болуы мүмкін. Нарықтық күн қысқа оқиға терезесіндегі 1 немесе 3 сауда күнде барлық ақпаратты қабылдамауы мүмкін. Сондықтан оқиға терезелерінің нәтижелері арасындағы айырмашылықтарды көру және оларды салыстыру өте маңызды. Ұзақ 21 күндік оқиға терезесі басқа оқиғалармен шатасып, басқаша әсер етуі мүмкін. Сондықтан оқиғаны зерттеген кезде бағалау терезелерін 119 күндік (-120,-2), 117 күндік (-120,-4), 115 күндік (-120,-6) деп, ал оқиға терезелері ретінде, тиісінше, 3 сауда күнін (-1,+1), 7 сауда күнін (-3,+3), 11 сауда күнін (-5,+5) орнату дұрыс болады.

Содан кейін, нақты кірістілік регрессия арқылы есептелген күтілетін кірістілікпен салыстырылады. Оның моделі мынадай:

$$AR_{ik} = R_{ik} - (\alpha_i + \beta_i * R_{mk}) \quad (11)$$

мұндағы, AR – нормадан тыс кірістілік

i – компания,

k – оқиға терезесі

R – k кезеңіндегі i-компаниясының нақты кірістілігі

R_{mk} – k кезеңіндегі нарық индексі

α, β - нарық үлгісінің көрсеткіштері

Содан кейін, 11 күндік оқиға терезесі үшін аномальды кірістіліктерді қосу арқылы жиынтық аномальды кірістілік (CAR) есептеледі. Ол үшін келесі формула қолданылады:

$$CAR_i = \sum_{k=-5}^{k=5} AR_{ik} \quad (12)$$

Жиынтық аномальды кірістілікке әсер ететін факторларды және кибершабуыл туралы ақпараттың фирма өлшемі, түрі, кибершабуыл түрі, қаржылық шығындарға сәйкес қалай өзгеретінін зерттеу үшін сызықтық регрессиялық талдау (OLS) жүргізіледі. Эмпирикалық модельді келесі теңдеу түрінде беруге болады:

$$CAR_i = \beta_0 + \beta_1 * \text{Фирма мөлшері} + \beta_2 * \text{Сала түрі} + \beta_3 * \text{Шабуыл түрі} + \beta_4 * \text{Қайталанатын шабуыл} + \beta_5 * \text{Бірнеше рет жасалған шабуыл} + \beta_6 * ROA + \beta_7 * \ln(\text{Кіріс}) + \varepsilon_{it} \quad (13)$$

Тәуелді айнымалы жиынтық аномальды кірістілік болады. Регрессиялық модель тәуелсіз айнымалылардың төрт түрін қамтиды. Біріншіден, компания өлшемі, сала түрі сияқты компанияны сипаттайтын айнымалылар пайдаланылады. Фирма көлемі жалпы активтер бойынша шағын, орта, ірі және өте ірі компаниялар болып анықталды.

Содан кейін сала түріне сәйкес *Фирма түрі* = {Өндіріс, көлік, көтерме сауда, бөлшек сауда, қаржы, қызметтер} жалған айнымалылар (dummy variables) жиынтығын жасау қарастырылды. Іріктемедегі компанияларды жіктеу үшін SIC кодының классификациясы қолданылды [78].

Оқиға сипаттамаларын басқару үшін «оқиға түрі» деген айнымалы қосылды. Cavusoglu et al. (2004), Chen et al. (2011), Das et al. (2012), Gordon et al. (2011), Hovav & D'Arcy (2003) кибершабуылдардың ең қауіптілері несие карталары туралы мәліметтердің жария болуы, ақпарат жүйесін бұзу, жеке ақпараттың жария болуы, бағдарламалық жасақтаманың зақымдануы деп көрсетуде [7,9,79-81].

Audit Analytics дерекқорынан жүктеп алынған деректер жиыны инциденттердің кеңейтілген түрлерінен тұрады, соның ішінде бағдарламалық қамтамасыз ету арқылы бопсалау және кибербұзушылықтың жеке түрі ретінде рұқсатсыз жүйеге кіру түрлері де берілген. Кибершабуылдың қай түрі фирма жұмысына теріс әсер ететінін анықтау үшін оқиға түрлерін бөліп алу маңызды. Біздің үлгіде *Инцидент* = {Фишинг, Зиянды бағдарлама, Қате конфигурация, Бопсалау, Рұқсатсыз жүйеге ену және түрі көрсетілмеген} деген жалған айнымалылар жинағы жасалды.

Сонымен қатар, жыл ішінде және бүкіл кезең ішінде қайталанатын шабуылдар туралы ақпаратты пайдалануды жөн көрдік. Осы мақсатта біз фирмаларды екі топқа бөліп, қайталанатын шабуылдар және бірнеше рет қайталанатын шабуылдар деп жалған айнымалыларды жасадық. Регрессияда осы екі айнымалыларды пайдалану қайталанатын шабуылдардың CAR-ға әсер ететінін немесе әсер етпейтінін тексеруге көмектеседі.

Әрі қарай, активтердің кірістілігі (ROA) және кірістіліктің логарифмі ($\ln$ (Кірістілік)) сияқты фирманың өнімділігін анықтайтын ерекше сипаттамалар қолданылған.

Содан кейін кибершабуылдардың экономикалық әсерін зерттеу үшін кибершабуылдардан туындайтын орташа қаржылық шығындар анықталды. Mukhopadhyay (2013) бұл айнымалыны келесідей анықтауға болады деп есептейді [15]:

$$\text{Қаржы шығыны}_{\text{орташа}} = \text{CAR}_{\text{орташа}} * \text{Нарық капитализациясы}_{\text{орташа}} \quad (14)$$

Содан кейін, тәуелсіз айнымалылар арасындағы корреляция мен мультиколлинеарлық әсер тексерілді.

Деректерді жинау және үлгіні сипаттау

Кибершабуылдың болғаны туралы мәліметті жариялау күні «оқиға» күні ретінде қабылданып, бұл компаниялардың нарықтық құнына оның әсерін зерттеу үшін пайдаланылатын болады. Кибершабуылдардың акционерлердің әл-ауқатына теріс әсерін анықтаған алдыңғы зерттеулерді тексеру үшін 2011-2020 жылдар аралығындағы АҚШ фирмаларының жаңа деректер жинағы пайдаланылды. АҚШ компаниялары үшін 2011 жылдың қаңтары мен 2020 жылдың желтоқсаны аралығындағы киберқауіпсіздік оқиғаларының саны Audit Analytics дерекқорынан алынды. Кибершабуылдардың бастапқы іріктемесі 674 оқиғаны қамтыды. Оқиға күні көрсетілмеген 2 оқиға және компания саласы көрсетілмеген 6 оқиға іріктемеден алып тасталған соң, іріктеме 666 оқиғадан құралды. 6-кестеде 2011-2020 жылдар аралығындағы кибершабуылдардың саны көрсетілген:

Кесте 6 - 2011-2020 жылдардағы кибершабуылдар саны

Жыл	Кибершабуыл саны	Үлесі
2011	24	3.59
2012	29	4.35
2013	39	5.86
2014	55	8.26
2015	41	6.16
2016	49	7.36
2017	82	12.31
2018	109	16.37
2019	133	19.97
2020	105	15.77
Барлығы	666	100
Ескертпе: Audit Analytics дерекқоры негізінде автормен әзірленді		

Салалар бойынша 666 кибершабуылдың үлестірілуі 7-кестеде берілген.

Кесте 7 - Салалар бойынша кибершабуылдардың үлестірілуі

Сала түрі	Оқиғалар саны	Үлесі
Тау-кен, газ және мұнай кен орындары	2	0.3
Құрылыс	2	0.3
Өндіріс	160	24.03
Көлік, байланыс	93	13.96
Көтерме сауда	17	2.55
Бөлшек сауда	95	14.26
Қаржы	102	15.32
Қызмет көрсету салалары	195	29.28
Барлығы	666	100
Ескертпе: Audit Analytics дерекқоры негізінде автормен әзірленді		

Фирманы сипаттайтын cuspіp нөмірлері көрсетілмегендіктен, 31 оқиға іріктемеден алып тасталды. Қалған 635 киберинцидент қайталанатын кибершабуылдардың болған-болмағаны бойынша зерттелді. Жылына 125 фирмада кибершабуыл қайталанса, 510 фирма жылына бір рет қана кибершабуылға тап болды. Сонымен қатар, 2011-2020 жылдар аралығында 313 фирма бір ғана шабуылды бастан өткерді, ал жалпы 322 фирма осы кезеңде бірнеше шабуылды бастан өткергені белгілі болды (8-кесте). Сонымен, біздің іріктеме бір ғана киберинцидент болған 427 фирмадан тұратын болады деп шешілді.

Кесте 8 - 2011-2020 жылдар аралығында қайталанған кибершабуылдар саны

2011-2020 жылдар аралығындағы қайталанған кибершабуылдар саны	Шабуылдардың жалпы саны	Фирмалар саны
1	313	313
2	138	69
3	75	25
4	36	9
5	30	6
6	-	-

8-кестенің жалғасы

7	7	1
8	16	2
9	-	-
10	20	2
Барлығы	635	427
Ескертпе: Audit Analytics дерекқоры негізінде автормен әзірленді		

Содан кейін қайталанатын 208 оқиға іріктемеден алып тасталды. Сонымен, деректер жинағы 427 кибершабуылдан құралды. Одан кейін, жалпы активтері туралы дерегі жоқ 24 компания іріктемеден алып тасталды. Өйткені, жалпы активтер фирманың жалпы активтерінің логарифмін пайдалана отырып, фирма көлемін анықтау үшін пайдаланылатын болған соң, бұл көрсеткіш маңызды болып келеді. 9-кестеде талдау үшін пайдаланылатын іріктеменің іріктелу процесі көрсетілген.

Кесте 9 - Деректер жинағы мен кибершабуыл оқиғалары үшін қолданылған фильтрлер

№	Қолданылған фильтрлер	Оқиғалар саны		
		бастапқы	алып тасталғаны	қалғаны
1	Audit Analytics дерекқорынан жиналған бақылаулар саны	674	-	674
2	Алып тасталғаны:			
	оқиға күні, siccode, cusip нөмірлері сияқты оқиға сипаттамалары туралы жазбалары жоқ фирмалар	674	39	635
	қайталанатын оқиғалар	635	208	427
	жетіспейтін мәндері бар фирмалар	427	24	403
	киберқауіпсіздік оқиғаларының қорытынды іріктемесі	403		403
Ескертпе: Audit Analytics дерекқоры негізінде автормен әзірленді				

Сонымен қатар, Wharton Research Data Services (WRDS) дерекқоры, атап айтқанда Зерттеу және бағалы қағаздар бағалары

орталығы (CRSP- Center for Research and Securities Prices) деректер жинағы күнделікті АҚШ фирмалары бойынша акциялары туралы деректері (яғни жабылу бағасы, жинақталған түзетілген баға коэффициенті, акциялар саны, нарықтық табысқа прокси ретіндегі үлестірулерді қоса алғанда құнмен өлшенген кірістілік) пайдаланылды. Бұл бастапқы деректер жиынтығы 18 046 296 бақылаудан тұрды, оның 8 674 525-і акционерлік емес компанияларға қатысты болғандықтан іріктемеден алынып тасталды.

Сонымен қатар, қарапайым акциялары NYSE, NASDAQ және AMEX сияқты үш негізгі қор биржаларында саудаланбайтын фирмаларға қатысты 99 196 бақылау жойылды. Қалған 9 272 575 бақылаудың қайталануы тексерілді, қайталанатын оқиғалар анықталмады. Екі деректер жиынын біріктіргеннен кейін 8 413 404 бақылау жойылды, соңғы іріктеме 859 171 бақылаулар санынан құралды. 10-кестеде сынама алу процесі жинақталған.

Кесте 10 - Деректер жинағы және қолданылған филтрлер

№	Қолданылған филтрлер	Оқиғалар саны		
		бастапқы	шегерілгені	қалғаны
1	WRDS дерекқорынан жиналған бақылаулар	18,046,296	-	18,046,296
2	Шегерілгені: акционерлік компаниялар емес	18,046,296	8,674,525	9,371,771
	акциялары биржада сатылмайтын компаниялар	9,371,771	99,196	9,272,575
	қайталанатын оқиғалары бар компаниялар	9,272,575	-	9,272,575
3	Audit Analytics бойынша оқиғалар саны (2000-2020)	403	-	403
4	Екі деректер жиынын біріктіру	9,272,575	8,413,404	859,171
5	Алып тасталғаны:			
	Оқиғалар терезесі 11 күннен аз және бағалау мерзімі 115 күннен аз болатын бақылаулар	859,171	94,185	764,986

10-кестенің жалғасы

6	Бақылаулардың қорытынды іріктемесі	764,986		764,986
	оқиғалардың қорытынды іріктемесі	337		337
Ескертпе: Audit Analytics дерекқоры негізінде автормен әзірленді				

Нарықтың реакциясын көру және оларды салыстыру үшін 1, 3 және 5 күндік оқиғалар терезелерін қолдану туралы шешім қабылданды, өйткені киберқауіпсіздік оқиғаларын анықтап, оны жариялауда кейбір кешігулер болады. Сондықтан кибершабуылдардың басталу күндері бұзушылықтарды анықтау және жариялау күндерімен бірдей бола бермейді.

Одан кейін оқиға терезелерінің 11 күннен аз уақытты қамтитын бастапқы 76 797 бақылау және бағалау терезелерінің 115 күнінен аз 17 388 бақылау іріктемеден алып тасталды. Таңдалған оқиғаларды зерттеу әдістемесінің талаптарына сәйкес келетін қалған бақылаулардың жалпы саны 764 986, ал кибершабуылдар оқиғаларын бақылау саны 337-ге тең болды.

2.3 Event study әдісі арқылы кибершабуылдардың компания құнына әсерін талдау

Бұл бөлімде 2011-2020 жылдарға арналған кибершабуылдар оқиғаларын зерттеу нәтижелері берілген. Нарық реакциясын зерттеу үшін 1-,3-,5 күндік оқиға терезелері және 119-,117-,115 күндік бағалау терезелері алынды. 11-кестеде әртүрлі оқиғалар терезелері үшін CAR-дың сипаттамалық статистикасы берілген. Талдау оқиға күніндегі CAR орташа мәні барлық үш терезе үшін -0,70%, -0,94% және -0,84% мәндерге тең болып, теріс болғандығын көрсетеді.

Сондай-ақ, CAR көрсеткішінің үлестірілуі сол жаққа қарай көлбеу келетінін көруге болады, бұл CAR мәндерінің көбірек теріс болатынның дәлелі. Осылайша, CAR (-5,+5) мәні көлбеулігі орташа, яғни -0,88 мәніне ие. Ал қысқа оқиғалар терезелері үшін CAR (-1,+1) көлбеулігі -1,83 және CAR (-3,+3) үшін -1,69 болып отыр, бұл айтарлықтай жоғары шама, бірақ нормадан аспаған деп саналады. Сонымен қатар, іріктеменің эксцесі (kurtosis) CAR(-1,+1) үшін 27,71 және жоғары мәнге ие, ал CAR (-3,+3) үшін 15,59 және

CAR (-5,+5) үшін 11,17 болып келеді. Бұл CAR үлестіріміндегі мәндерінің көбісі орташа шамасына жақын екенін көрсетеді. Бұнымен қатар, CAR үлестірімі нормадан ауытқиды, оның кейбір экстремалды мәндері бар екенін байқауға болады деп қорытындылауға болады (Қосымша А).

Кесте 11 - CAR-дың сипаттамалық статистикасы

Көрсеткіштер	CAR (-1, +1)	CAR (-3, +3)	CAR (-5, +5)
Орташасы	-0.0070102	-0.0093855	-0.0084125
Стандартты ауытқу	0.0458051	0.0653101	0.0794416
Min	-0.4112283	-0.4342175	-0.5136665
Max	0.276567	0.2667364	0.3209026
Дисперсиясы	0.0020981	0.0042654	0.006311
Қиғаштығы	-1.830237	-1.689383	-0.8761859
Эксцессы (Kurtosis)	27.71093	15.58599	11.16658
Бақылаулар саны	337	337	337
CAR оң мәні бар фирмалардың саны	144	146	152
CAR теріс мәні бар фирмалардың саны	193	191	185
Ескертпе: автормен STATA бағдарламасында есептелген.			

Сонымен қатар, кестеде көрсетілгендей, 1 күндік терезеде 193 фирма теріс және 144 фирма оң CAR болды, ал 5 күндік терезеде теріс CAR фирмалар саны 185 және оң 152 болды. Сонымен қатар, 3 күндік терезедегі теріс CAR көрсеткіші -0,70%-дан -0,94%-ға дейін өсетіні байқалады, содан кейін 5 күндік терезеде ол қайтадан -0,84%-ға дейін аздап төмендейді. Осыған сүйеніп, кибершабуыл оқиғалары қысқа уақыт ішінде нарыққа айтарлықтай әсер етеді деп қорытындылауға болады.

Теріс CAR мәнінің маңыздылығын тексеру үшін біз үш оқиға терезесі үшін бір жақты t-тестін орындадық (критикалық t мәні - 1,96 деп алынды). Тест нәтижесі 12-кестеде көрсетілген.

Зерттеу CAR (-1,+1), CAR (-3,+3) орташа мәндері 99% маңыздылық деңгейінде статистикалық түрде маңызды екенін көрсетеді. CAR (-5,+5) орташа мәні де статистикалық маңызды, бірақ 95% сенімділік деңгейінде.

Осылайша, жүргізген гипотеза сынағы Cavusoglu et al. (2004) жасаған тұжырымдарға қосымша толықтырулар енгізуге мүмкіндік

береді [9]. Біздің талдауымыз бойынша кибершабуылдар фирманың нарықтық құнына теріс әсер етеді, және бұл әсер ұзақ мерзімді кезеңде әлсірейді деген қорытынды жасауға болады. Ұзақ уақыт әсерін зерттеу үшін болашақта 21 күндік оқиға терезесін таңдап қосымша зерттеу ұсынылады.

Кесте 12 - CAR бойынша t-тестінің нәтижелері

Көрсеткіштер	CAR (-1, +1)	CAR (-3, +3)	CAR (-5, +5)
Бақылаулар саны	337	337	337
Орташасы	-.0070102***	-.0093855***	-.0084125**
Стандартты қате	.0024952	.0035577	.0043275
Стандартты ауытқу	.0458051	.0653101	.0794416
[95% Сенімділік интервалы]	-.0119183	-.0163836	-.0169248
	-.0021021	-.0023874	.0000998
t	-2.8095	-2.6381	-1.9440
еркіндік дәрежелері	336	336	336
Pr(T < t)	0.0026	0.0044	0.0264
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.			

Фирманың және киберқауіпсіздіктің нақты сипаттамаларының орташа CAR-ға әсері

Компания түрлері бойынша нарық реакциясын зерттеу үшін біз t-тест пен ANOVA-тесттерін орындадық, мұндағы тәуелді айнымалы ретінде CAR, ал тәуелсіз айнымалы ретінде фирма түрі алынды. 13-кестеде фирма түрі 1, 3, 5 күндік оқиға терезесінде CAR-ға әсер ететін гипотеза тестінің нәтижесі берілген. Осы нәтижелерге сәйкес, қаржы, көлік және коммуникация саласындағы фирмалар барлық үш оқиға терезесінде елеулі теріс CAR-ға ие болды. Көлік және байланыс компаниялары үшін 5 күндік терезеде ең жоғары теріс CAR (-2,76%) байқалады. Бұл нәтиженің маңыздылығы 1% деңгейінде. Бөлшек сауда фирмалары CAR (-1,+1) және CAR (-3,+3) терезелері бойынша, тиісінше, 5% деңгейінде елеулі теріс мәнге ие (-1,23% және -1,67%). Сонымен қатар, құрылыс фирмаларының CAR көрсеткіші үш күндік терезеде 10% маңыздылық деңгейінде айтарлықтай теріс болғаны

байқалды (-2,82%). Дегенмен, бұл нәтиже сенімді емес, өйткені біздің үлгідегі құрылыс фирмаларының саны тым аз.

Кесте 13 - Компания түрлері арасында CAR көрсеткіштерін салыстыру (t-тест нәтижелері)

	Байқау лар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәні				
Өндіріс	88	-.0066015 (0.1365)	-.0062863 (0.2472)	.0015081 (0.5558)
Көлік және байланыс	51	-.0090739* (0.0595)	-.0155868* (0.0596)	-.0276463*** (0.0052)
Көтерме сауда	14	.0067564 (0.7028)	.0042973 (0.6094)	-.0027943 (0.4121)
Бөлшек сауда	44	-.0122539** (0.0194)	-.0167325** (0.0305)	-.0107113 (0.2566)
Қаржы	48	-.0084587* (0.0633)	-.0124012** (0.0376)	-.0109097* (0.0802)
Қызмет көрсету	89	-.005046 (0.1506)	-.0064684 (0.1204)	-.0057795 (0.1661)
Тау-кен, мұнай және газ	1	.022003 (N/A)	.0885888 (N/A)	.0375121 (N/A)
Құрылыс	2	-.0205207 (0.1178)	-.0281797* (0.0666)	-.0234096 (0.1159)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмашылықтарды тексеру				
F-test (ANOVA)		0.39 (0.9102)	0.64 (0.7213)	0.71 (0.6613)
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.				

Фирмалардың белгілі бір түрі үшін CAR елеулі теріс мәнге ие болуына қарамастан, айырмашылықтар сынағы (ANOVA-тест) Р-мәнінің 0,05-тен жоғары екенін анықтайды (тиісінше 0,9102, 0,7213 және 0,6613). Сондықтан біз нөлдік гипотезаны жоққа шығара

алмаймыз және CAR мәні фирмалардың әртүрлі типтері арасында айтарлықтай ерекшеленбейді деп айта аламыз.

14-кесте мен В-Қосымшасында әртүрлі көлемдегі фирмалардың CAR мәндерін салыстыру үшін t-тест нәтижелері берілген.

Кесте 14 - Әртүрлі фирма көлемі арасындағы CAR мәндерін салыстыру (t-тест нәтижелері)

	Байқаулар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәні				
Шағын	85	-.0141368** (0.0287)	-.0230848** (0.0159)	-.0234269** (0.0315)
Орташа	83	.0006368 (0.5522)	.0029421 (0.6677)	.0108433 (0.9239)
Ірі	84	-.0092558*** (0.0041)	-.0132984*** (0.0023)	-.0137703** (0.0412)
Өте ірі	85	-.0051315* (0.0532)	-.0038568 (0.1980)	-.006906* (0.0698)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмашылықтарды тексеру				
F-test (ANOVA)		1.58 (0.1940)	2.57* (0.0541)	2.82** (0.0390)
Bonferroni test (Орта және шағын фирмалар арасындағы айырмашылықтар)			.026027* (0.058)	.03427** (0.031)
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.				

Сынақ нәтижесі орташа компаниялардан басқа барлық дерлік фирмалардың әртүрлі деңгейде теріс CAR көрсеткіштері бар екенін көрсетеді. Осылайша, 5% маңыздылық деңгейінде ең жоғары теріс

CAR шағын фирмалар үшін байқалады, сәйкесінше 1-, 3-, 5 күндік оқиғалар терезелері үшін бұл көрсеткіш -1,41%, -2,31% және -2,34% мәндеріне ие. 10% маңыздылық деңгейіндегі ең төменгі теріс көрсеткіші CAR (-1,+1) және CAR (-5,+5) үшін ең ірі фирмаларда орын алды (сәйкесінше, 0,51% және 0,69%). Ірі фирмалардың CAR мәні 1% маңыздылық деңгейінде -0,93% және -1,33%, және 1-,3-,5 күндік терезелер үшін 5% маңыздылық деңгейінде -1,38% мәнге ие. Орташа компаниялар оң мәнді CAR көрсеткіштеріне ие, сәйкесінше 0,64%, 0,29% және 1,08%. Дегенмен, олардың статистикалық маңыздылығы жоқ.

Айырмашылықтар сынағы әртүрлі өлшемді фирмалар арасында нарықтық реакцияда кейбір айырмашылықтар бар екенін көрсетеді, өйткені Р-мәні CAR (-3,+3) үшін 0,06 және CAR (-5,+5) үшін 0,03 болып келеді. Осылайша, біз нөлдік гипотезаны жоққа шығара аламыз және фирма мөлшері CAR-ға ықпал етуі мүмкін деп қорытынды жасай аламыз. Фирмалар арасындағы айырмашылықты анықтау үшін қосымша Bonferroni тесті жүргізілді.

Bonferroni тесті орта және шағын фирмалар арасындағы айырмашылықты көрсетеді. Осылайша, шағын фирмалардың орташа CAR көрсеткіші 3 күндік терезеде 10% маңыздылық деңгейінде -2,6% және 5 күндік терезеде 5% маңыздылық деңгейінде -3,43% теріс болды.

15-кесте мен В-Қосымшасы шабуылдың түрлеріне қарай нарықтың реакциясындағы ерекшелігін анықтауға арналған t-тестінің нәтижесін көрсетеді.

Кесте 15 - Кибершабуылдың түрлері бойынша CAR салыстыру (t-тест нәтижелері)

	Байқаулар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәні				
Зиянды бағдарлама	66	.0015475 (0.6359)	.0029846 (0.6777)	.0091654 (0.8078)
Зиянды бағдарлама/фишинг	1	-.0236324 (N/A)	-.0955965 (N/A)	-.0738811 (N/A)
Қате конфигурация	15	-.0048971 (0.3524)	.0049877 (0.6073)	-.0070993 (0.3934)

15-кестенің жалғасы

Түрі көрсетілмеген	115	-.00538* (0.0617)	-.0076282* (0.0586)	-.010851** (0.0371)
Фишинг	63	-.0101885** (0.0342)	-.0196888** (0.0269)	-.010651 (0.1653)
Бопсалайтын бағдарлама	25	-.0126298 (0.2733)	-.0162184 (0.2428)	-.0233398 (0.1622)
Рұқсатсыз жүйеге кіру	52	-.0152148*** (0.0003)	-.0156924** (0.0191)	-.014561* (0.0578)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмашылықта рды тексеру				
F-test (ANOVA)		0.82 (0.5517)	1.21 (0.2994)	0.88 (0.5127)
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.				

Сынақ «Рұқсатсыз жүйеге кіру» түрі бойынша 1-, 3-, 5-күндік терезелер үшін 1% маңыздылық деңгейінде -1,52%, 5% маңыздылық деңгейінде -1,57% және 10% маңыздылық деңгейінде -1,46% ең жоғары теріс және статистикалық маңызды CAR-ға ие екенін көрсетті. Сонымен қатар, «Түрі көрсетілмеген» кибершабуылдарда да айтарлықтай теріс орташа CAR бар екенін көруге болады. Осылайша, CAR (-1,+1) үшін 10% маңыздылық деңгейде -0,54%, CAR (-3,+3) үшін 10% маңыздылық деңгейде -0,76%, және CAR (-5,+5) үшін 5% маңыздылық деңгейінде -1,09% мәндеріне ие. «Зиянды бағдарламалық құралдың» оң, бірақ статистикалық маңызы жоқ CAR көрсеткіші бар. Ал, «Фишингтің» CAR (-1,+1) және CAR (-3,+3) көрсеткіштері 5% маңыздылық деңгейінде -1,02% және -1,97% мәндеріне ие. «Зиянды бағдарламалық қамтамасыз ету» мен «Фишинг» секілді кибершабуылдардың тек бір ғана оқиғасы болғандықтан, бұл нәтижелерді сенімді нәтиже деп айтуға болмайды. Дегенмен, олардың CAR теріс мәндері басқа кибершабуыл түрлерімен салыстырғанда өте жоғары болып отыр (-2,36%, -9,56% және -7,39%).

P-мәні 0,05-тен артық болғандықтан (0,55, 0,30 және 0,51), ANOVA-тесті кибершабуылдар түрлері бойынша CAR арасында ешқандай айырмашылық болмайтынын дәлелдейді. Осылайша, біз нөлдік гипотезаны жоққа шығара алмаймыз және әртүрлі бұзушылықтарға нарықтық реакция айтарлықтай ерекшеленбейді деп тұжырым жасай аламыз.

16-кесте мен В-Қосымшасында ақпарат жоғалтудың әр түрлерін бастан кешірген фирмалардың CAR көрсеткіштері келтірілген.

Кесте 16 - Әртүрлі ақпаратты жоғалту арасындағы CAR мәндерін салыстыру (t-тест нәтижелері)

	Бақылаулар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәне				
Қаржылық ақпарат	105	-.0125318*** (0.0039)	-.0158735*** (0.0030)	-.0140109** (0.0487)
Түрі көрсетілмеген ақпарат	15	.0128775 (0.7081)	.0080284 (0.5817)	-.0176679 (0.2339)
Басқа да ақпарат	53	-.0117663* (0.0958)	-.007227 (0.2488)	-.0042458 (0.3789)
Жеке деректер	164	-.0037571** (0.0461)	-.0075218** (0.0355)	-.0053281 (0.1519)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмалышықтарды тексеру				
F-test (ANOVA)		1.93 (0.1240)	0.76 (0.5154)	0.37 (0.7743)
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.				

Сынақ қаржылық ақпараттың жоғалуы нарыққа айтарлықтай әсер ететінін көрсетеді. Осылайша, орташа CAR (-1,+1) 1% маңыздылық деңгейінде -1,25%, орташа CAR (-3,+3) 1% маңыздылық деңгейінде -1,59%, ал CAR (-5,+5) 5% маңыздылық деңгейінде -1,4% екенін көруге болады. Жеке ақпараттың жоғалуы

CAR-ға 5% маңыздылық деңгейінде теріс әсер етеді, сәйкесінше 1 күндік және 3 күндік оқиға терезелерінде CAR мәндері -0,38% және -0,75% құрайды. Ақпараттың басқа түрлерін жоғалту да теріс, бірақ CAR (-3,+3) және CAR (-5,+5) бұл көрсеткіштердің статистикалық маңыздылығы жоқ. Ал, түрі көрсетілмеген ақпарат жоғалтуларының CAR мәндері оң, бірақ CAR (-1,+1) және CAR (-3,+3) бойынша статистикалық маңыздылығы жоқ. Түрі көрсетілмеген ақпарат жоғалтуларының іріктемесі мардымсыз болғандықтан, соңғы нәтижелерді статистикалық жағынан мағынасыз деп қабылдауымыз керек.

ANOVA-тестінің орындалуы әртүрлі ақпарат жоғалтулары арасында нарықтық реакцияда айтарлықтай айырмашылық жоқ екенін көрсетті, өйткені Р-мәні үш терезе үшін де 0,05-тен жоғары, және сәйкесінше, 0,12, 0,52, 0,77 мәндеріне ие. Сондықтан біз нөлдік гипотезаны жоққа шығара алмаймыз және әртүрлі ақпарат жоғалтулары CAR-ға әртүрлі әсер етпейді деп айта аламыз.

17-кесте мен В-Қосымшасында бір жыл ішінде бір реттік және қайталанатын кибершабуылдарды бастан кешірген фирмалар арасындағы CAR салыстырылады. t-тест киберқылмыскерлердің назарын көбірек аударатын фирмаларға деген нарықтың реакциясы басқа фирмалармен салыстырылып зерттеледі.

Сынақ екі топ арасында айтарлықтай айырмашылықтар жоқ екенін көрсетті, өйткені Р-мәні 0,95, ол 0,05-тен жоғары болып отыр. Дегенмен, жылына бір рет шабуылға ұшырайтын фирмалар 1-,3-,5 күндік терезелер үшін 1% маңыздылық деңгейінде CAR көрсеткішінің орташа мәні -0,66%, 1% маңыздылық деңгейінде -1,09% және 5% маңыздылық деңгейінде -0,85% болып отыр. Бұндай жағдай кибершабуыл оқиғалары қайталанатын фирмаларда ондай шабуылдарға төтеп беру тәжірибесі бар екенімен түсіндіруге болады. Сонымен қатар, бұл фирмалар киберқауіпсіздік жүйесін жақсартып отырады деп пайымдауға болады. Бұл, сәйкесінше, осындай фирмаларға деген нарық қатысушылары тарапынан сенімділікті арттырып отырады.

18-кесте мен В-Қосымшасында бірнеше және бір реттік шабуылдарды бастан өткерген фирмалар арасында CAR орташа мәнінің айырмашылығы бар-жоғы тексерілген t-тест нәтижелері берілген.

Кесте 17 - Бір жылда қайталанатын және қайталанбайтын кибершабуылдар арасындағы CAR мәндерін салыстыру

	Бақыл аулар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәні				
Бір жыл ішіндегі жалғыз кибершабуыл	313	-.0066049*** (0.0063)	-.0108994*** (0.0019)	-.0084873** (0.0319)
Бір жыл ішінде қайталанатын шабуыл	24	-.0122959* (0.0522)	.0103588 (0.8267)	-.0074371 (0.2810)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмалышықтарды тексеру				
F-test (ANOVA)		0.34 (0.5583)	2.37 (0.1245)	0.00 (0.9503)
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.				

Кесте 18 - 2011-2020 жылдардағы бір және бірнеше кибершабуылдар бойынша CAR көрсеткіштерін салыстыру

	Бақылау лар саны	CAR (-1,+1)	CAR (-3,+3)	CAR (-5,+5)
CAR орташа мәні				
Жалғыз шабуыл	248	-.006151** (0.0249)	-.0107706*** (0.0088)	-.0093899** (0.0416)
Бірнеше шабуыл	89	-.0094045*** (0.0065)	-.0055259 (0.1317)	-.0056889 (0.1932)
Барлығы	337	-.0070102*** (0.0026)	-.0093855*** (0.0044)	-.0084125** (0.0264)
Айырмалышықтарды тексеру				
F-test (ANOVA)		0.33 (0.5662)	0.42 (0.5166)	0.14 (0.7067)

Ескертпелер:

- 1) * 10% деңгейінде маңызды
- 2) ** 5% деңгейінде маңызды
- 3) *** 1% деңгейінде маңызды
- 4) автормен STATA бағдарламасында есептелген.

Сынақ Р-мәні 0,7067 екенін көрсетеді, бұл біз нөлдік гипотезаны жоққа шығара алмайтынымызды көрсетіп отыр. Осылайша, бір және бірнеше кибершабуылды өткерген фирмалар арасында орташа CAR бойынша айтарлықтай айырмашылық жоқ деп пайымдауға болады. Дегенмен, бірнеше рет кибершабуыл өткерген фирмаға нарықтық реакция 1 күндік оқиға терезесінде анағұрлым теріс екенін көруге болады, ал бір рет бұзылған фирмалардың CAR көрсеткіші барлық үш терезе үшін статистикалық маңызды теріс мәнге ие.

Жоғарыда айтылғандай, кибершабуылдарды үнемі бастан кешіретін фирмалар шабуылдарға дайын болуы мүмкін, және ондай шабуылдарға жылдам және тиімді төтеп бере алуы мүмкін деп атап өтуге болады. Нарық үшін бұндай әрекеттер жақсы сигнал болғандықтан, нарық реакциясы да сәйкес болып келеді. Нәтижесінде, тиімді киберқауіпсіздік жүйесі инвесторларды компанияның тұрақтылығына деген сенімін арттырады.

Айнымалылар арасындағы корреляциялық байланысты талдау

Регрессиялық талдаудың алдында барлық айнымалылар арасындағы корреляциялық байланысты анықтау үшін талдау жүргізіледі. Талдау нәтижелері 19-кестеде көрсетілген. CAR және ROA көрсеткіштері арасында күшті оң сызықтық байланыс бар екенін байқауға болады, бұл жоғары ROA көрсеткіштері бар компанияларда, төмен ROA бар компаниялармен салыстырғанда, оң CAR болатынын көрсетеді. Сонымен қатар, CAR мен жоғалған деректертердің жалпы саны арасындағы корреляция коэффициенті -0,1985, бұл 5% деңгейінде статистикалық маңызды. Бұл дегеніміз, үлкен көлемдегі деректердің жоғалуы CAR көрсеткішінің төмендеуіне әкелетінін көрсетеді. Сонымен қатар, корреляциялық талдау CAR мен шабуыл түрі арасындағы сызықтық байланысты анықтады (5% маңыздылық деңгейінде).

Кесте 19 - Айнымалылар арасындағы корреляция байланысы

	CAR	Фирма мөлшері	Фирма саласы	Шабуыл түрі	Дерек түрі	ROA	Қайтала натын шабуыл	Жылына бірнеше рет болған шабуыл	Кіріс	Жоғалға н дерек саны	Шабуыл ұзақтығы	Кеш ашылуы	Кеш жариял ануы
CAR	1.0000												
Фирма мөлшері	0.0426 (0.4358)	1.0000											
Фирма саласы	0.0054 (0.9213)	-0.0042 (0.9388)	1.0000										
Шабуыл түрі	- 0.1170** (0.0317)	- 0.1300** (0.0170)	0.0201 (0.7131)	1.0000									
Дерек түрі	0.0685 (0.2097)	0.0713 (0.1919)	- 0.0982* (0.0719)	0.1875** *	1.0000								
ROA	0.2321** *	0.2238** *	0.1270* *	-0.0523 (0.3381)	0.0257 (0.6385)	1.0000							
Қайталана тын шабуыл	-0.0320 (0.5583)	0.0716 (0.1897)	-0.0014 (0.9803)	0.0009 (0.9864)	0.0642 (0.2402)	0.0071 (0.8961)	1.0000						
Жылына бірнеше рет болған шабуыл	-0.0314 (0.5662)	0.1882** *	0.0978* (0.0731)	-0.1275** (0.0192)	0.0464 (0.3956)	0.0961* (0.0782)	0.4622** *	1.0000					
Кіріс	0.0516 (0.3448)	0.8143** *	-0.0278 (0.6108)	- 0.1961** *	-0.0184 (0.7369)	0.3958** *	0.0678 (0.2143)	0.2649** *	1.0000				
Жоғалған дерек саны	- 0.1983** (0.0202)	0.1145 (0.1829)	0.1340 (0.1184)	-0.1460* (0.0888)	0.0635 (0.4613)	0.1245 (0.1472)	-0.0946 (0.2715)	0.1013 (0.2391)	0.1317 (0.1249)	1.0000			
Шабуыл ұзақтығы	-0.0269 (0.7542)	0.1125 (0.1890)	-0.0315 (0.7137)	- 0.3214** *	-0.0499 (0.5613)	0.0215 (0.8022)	0.0326 (0.7042)	-0.0180 (0.8337)	0.0200 (0.8160)	0.0364 (0.7918)	1.0000		
				(0.0001)									

19- кестенің жалғасы

Кеш ашылуы	-0.0280 (0.7678)	0.1761** (0.0609)	-0.0735 (0.4371)	- 0.3956** * (0.0000)	-0.0948 (0.3156)	0.0625 (0.5087)	0.0574 (0.5438)	0.0390 (0.6801)	0.1214 (0.1982)	0.0826 (0.5724)	0.9380*** (0.0000)	1.0000	
Кеш жариялан уы	0.0071 (0.9229)	0.0844 (0.2520)	-0.0259 (0.7259)	-0.1207 (0.1007)	0.0173 (0.8144)	0.0427 (0.5627)	-0.0176 (0.8117)	-0.0752 (0.3077)	0.0192 (0.7948)	-0.1283 (0.2725)	0.8945*** (0.0000)	0.9619*** (0.0000)	1.0000

Ескертпелер:

- 1) * 10% деңгейінде маңызды
- 2) ** 5% деңгейінде маңызды
- 3) *** 1% деңгейінде маңызды
- 4) автормен STATA бағдарламасында есептелген.

Сонымен қатар, корреляциялық талдау қайталанатын шабуылдар мен фирма көлемі, ROA және кіріс арасындағы маңызды оң сызықтық байланысты көрсетіп берді. Корреляция коэффициенттері сәйкесінше 0,1882, 0,0961 және 0,2649 болып табылады. Бұл дегеніміз, үлкен кірісі бар ірі, табысты фирмалар циклдік қайталанатын кибершабуылдардың нысанасы болуы мүмкін екенін көрсетеді. Сондай-ақ, қайталанатын шабуылдар мен фирма түрі арасында да сызықтық байланыс бар [82].

Бұл нақты фирма түрі кибершабуылдардың нысанасы болуының дәлелі. Сонымен қатар, бірнеше шабуылдар мен шабуыл түрлерінің арасындағы байланыс шабуылдардың нақты түрінің қайталану үрдісі бар екенін көрсетеді.

Айта кету керек, шабуыл түрі деректердің жоғалу санын, ұзақтығын, кеш ашылуын және көпшілікке жарияланудың кешігуін айқындайды. Соңғы үш айнымалылардың айтарлықтай күшті өзара байланысы бар, өйткені олардың ақпарат негізі бір болады.

CAR көрсеткішіне регрессиялық талдау жасау

Қарапайым кіші квадраттар (OLS) регрессиялары CAR орташа мәнінің теріс болуына қандай факторлар әсер ететінін анықтауға мүмкіндік береді. Бұл жұмыста фирма мөлшері, фирма түрі, ұрланған ақпарат түрі, кибершабуылдар түрі, бір жыл ішінде қайталанатын шабуылдар, онжылдықта бірнеше қайталанатын шабуылдар, активтердің кірістілігі (ROA) және кірістің логарифмі, жоғалған деректер саны, шабуыл ұзақтығы, шабуылдың кеш ашылуы, шабуылдың кеш жариялануы секілді айнымалылардың CAR(-1,+1) орташа мәніне ықпалы зерттелді. 20-кестеде регрессия талдауының нәтижелері берілген.

ROA және Кірістер фирма өнімділігін сипаттаушы айнымалылар ретінде пайдаланылды. Қайталанатын шабуылдар және жылына бірнеше рет қайталанатын шабуылдар «жалған айнымалылар» (dummy variables) деп қабылданды, яғни кибершабуылдар қайталанса, оның мәнін бірге тең деп, ал кері жағдайда нөлге тең деп қабылдаймыз.

Регрессияда (1) ең ірі фирмаларға қарағанда шағын фирмалар CAR көрсеткішіне 10% маңыздылық деңгейінде елеуді ықпал етіп, -2,24%-ға төмендететінін көруге болады.

Кесте 20 - OLS регрессиялары

Тәуелсіз айнымалылар	CAR (-1,+1)					
	(1)	(2)	(3)	(4)	(5)	(6)
Фирма мөлшері						
-шағын	-.0224109* (0.095)	-.0137501 (0.346)	-.0302107 (0.222)	-.0292697 (0.276)	-.0205293 (0.291)	-.0172435 (0.579)
-орташа	-.0041696 (0.681)	.0058964 (0.610)	-.0136546 (0.478)	-.0037608 (0.866)	-.0073647 (0.625)	-.0155849 (0.536)
-ірі	-.0118362 (0.141)	-.0029025 (0.731)	- .0299058* * (0.047)	-.0265128* (0.090)	-.0221395* (0.066)	-.0249929 (0.219)
Фирма саласы						
- көлік және байланыс	-.0086959 (0.286)	.003599 (0.703)	-.0237054 (0.116)	-.0295763** (0.050)	-.0207879* (0.084)	.0022437 (0.901)
- көтерме сауда	.0154902 (0.246)	.0008729 (0.954)	.0277922 (0.207)	.0080544 (0.743)	.0269602 (0.173)	.0208835 (0.407)
- бөлшек сауда	-.0061444 (0.494)	.0082069 (0.389)	-.0077172 (0.600)	-.017069 (0.379)	-.0080543 (0.524)	.0378311 (0.103)
- қаржылық фирмалар	-.0059558 (0.503)	-.0016364 (0.878)	.0054239 (0.749)	.0012398 (0.944)	.0028519 (0.824)	-.0240959 (0.345)
- қызмет көрсету саласы	-.0044135 (0.523)	.003812 (0.655)	.0065199 (0.584)	.0117631 (0.320)	.003136 (0.735)	-.0091616 (0.531)
- тау-кен, мұнай және газ	.0643414 (0.156)		.0717957 (0.165)	.0773448 (0.130)	.0651697 (0.174)	
- құрылыс	-.0132923 (0.679)	-.0012706 (0.968)	-.0382893 (0.463)	-.0067576 (0.888)	-.0229778 (0.492)	-.0261251 (0.457)
Кибершабуыл түрі						
Зиянды бағдарлама/ фишинг	-.0478857 (0.288)	-.0552065* (0.081)	-.0444152 (0.380)		-.0483222 (0.304)	
Қате конфигурация	-.0141337 (0.278)	-.022683 (0.147)	-.0258678 (0.297)	-.0128572 (0.676)	-.0027261 (0.896)	
Түрі көрсетілмеген	-.0120896 (0.092)	-.0120994 (0.129)	-.0057861 (0.659)	-.0027526 (0.870)	-.0074728 (0.492)	-.0287886* (0.093)
Фишинг	-.0189631** (0.024)	-.0152866 (0.121)	-.021067 (0.158)	-.0063932 (0.700)	-.0192474 (0.101)	-.0118159 (0.537)
Бопсалайтын бағдарлама	-.023008** (0.045)	-.006097 (0.789)	-.0033531 (0.859)	-.0032964 (0.869)	-.0086657 (0.566)	.0127584 (0.652)
Рұқсатсыз жүйеге кіру	- .0228738*** (0.009)	- .0191226** (0.042)	-.0209978 (0.148)	-.0209157 (0.208)	-.02637** (0.026)	-.0281078* (0.060)

20-кестенің жалғасы

Ақпарат түрі						
Қаржылық	-.0127289** (0.040)	- .0150466** (0.012)	-.0068775 (0.562)	-.0050862 (0.680)	-.0147548 (0.110)	-.016904 (0.280)
Түрі көрсетілмеген	.0314874** (0.017)		.0401149* (0.071)	.0815204** * (0.002)	.0278061 (0.143)	
Басқа да ақпарат	-.0073519 (0.324)	.0209929 (0.421)	-.0106077 (0.533)	-.0232652 (0.172)	-.0094739 (0.423)	
Бір жыл ішінде қайталанатын шабуыл	-.0031755 (0.771)	-.0117402 (0.315)	.0194547 (0.368)	.0133497 (0.563)	.022158 (0.180)	.0389444* (0.095)
Бүкіл кезең ішінде болған бірнеше шабуылдар	-.0045556 (0.499)	-.0124724* (0.079)	-.0213786 (0.102)	- .0350284** * (0.009)	-.0209221** (0.032)	-.049187*** (0.005)
Кірістің натурал логарифмі	-.0040539 (0.124)	.0001112 (0.971)	-.0053887 (0.288)	-.0015131 (0.787)	-.003081 (0.417)	-.0042617 (0.502)
ROA	.0728947*** (0.000)	.0403289 (0.281)	.1094454* (0.072)	.1515666** (0.031)	.0847125* (0.076)	-.0147139 (0.855)
Жоғалған деректер санының натурал логарифмі		- 019995*** (0.005)				-.0019237 (0.315)
Шабуылдың ұзақтығы			4.27e-06 (0.874)			
Шабуылды кеш анықтау				5.53e-06 (0.828)		-3.18e-06 (0.931)
Шабуылды кеш жариялау					5.54e-07 (0.967)	
Тұрақты шама	.1124365* (0.078)	.0302402 (0.687)	.1452737 (0.230)	.0537439 (0.689)	.0950955 (0.301)	.1491804 (0.371)
Бақылаулар саны	337	137	138	114	186	49
F-Statistic	2.16*** (0.0018)	1.46 (0.1028)	1.26 (0.2125)	1.86** (0.0208)	1.37 (0.1269)	1.60 (0.1226)
R ²	0.1372	0.2198	0.2105	0.3218	0.1701	0.5340
Adj. R ²	0.0737	0.0692	0.0428	0.1484	0.0463	0.2011
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.						

Сонымен қатар, «фишинг», «бопсалайтын бағдарламалар» және «рұқсатсыз жүйеге кіру» сияқты кибершабуылдардың коэффициенттері теріс және статистикалық маңызды болып отыр. Осылайша, фишинг бағдарлама шабуылына қарағанда орташа CAR көрсеткішін 1,90%-ға төмендететінін көрсетіп отыр (5% маңыздылық деңгейінде). Сонымен қатар, зиянды бағдарламамен салыстырғанда төлемдік бағдарламалық қамтамасыз ету CAR орташа мәнін 2,3%-ға төмендетеді (5% маңыздылық деңгейінде).

Рұқсатсыз жүйеге кіру зиянды бағдарламаға қарағанда CAR көрсеткішін 2,29%-ға төмендетуі мүмкін (1% маңыздылық деңгейінде). Бұдан басқа, жеке ақпаратты жоғалтумен салыстырғанда, қаржылық ақпараттың жоғалуы CAR-ды 1,27% төмендетуі мүмкін (5% маңыздылық деңгейіне). ROA CAR мәніне оң әсер ететінін байқаймыз. ROA-ны 1 мөлшерлемеге ұлғайту орташа CAR-ды 7,29%-ға жоғарылатады (1% деңгейінде). Бұл дегеніміз, орташа ROA көрсеткіші жоғары фирмаларға кибершабуылдар теріс әсер тигізбейтінін көрсетеді. Регрессиялық модельдің аталған байланыстарды түсіндіру күші тұрғысынан, түзетілген R^2 (adjusted R^2) айтарлықтай жоғары емес, яғни біздің таңдаған тәуелсіз айнымалылармыз CAR көрсеткішінің өзгермелілігін тек 7,37% ғана түсіндіре алатынын көрсетеді. Дегенмен, P-мәні 0,0018 болғандықтан F-статистикасы 1% деңгейінде маңызды болып отыр, сондықтан да біздің түзген регрессиямыз (1) статистикалық жағынан мағыналы деп айта аламыз.

Регрессия (2) қосымша түсіндірме айнымалы ретінде «Жоғалған деректер саны» қосылып талданды. Нәтижесінде, іріктеме кішірейіп, 137 бақылаудан құралды. Жүргізілген F-тесттің маңыздылық деңгейі төмен болып, регрессия моделі статистика жағынан мәні жоқ екенін көрсетті. Коэффициенттердің P-мәнінде шамалы өзгерістер бар. Жоғалған деректер саны 1% маңыздылық деңгейінде t-тесттен өтті. Осылайша, орташа есеппен жоғалтқан деректер санының 1%-ға ұлғаюы CAR мәнін 0,20%-ға төмендетіп отырады деген қорытынды жасауға болады, егер барлық басқа жағдайларды ескермейтін болсақ (*ceteris paribus*).

Содан кейін шабуылдың ұзақтығы, компанияның кибершабуылды анықтау реакциясы және көпшілікке хабарлаудың кешігуі нарық реакциясына қалай әсер ететіні зерттелді.

Корреляциялық талдауға сәйкес, олардың өзара күшті сызықтық байланысы бар, сондықтан олардың қайсысы кибершабуылды түсіндіру күші бар екенін анықтау үшін оларды регрессиялық модельде бөлек пайдалану қарастырылды.

Регрессия (3) CAR мен кибершабуыл ұзақтығы арасындағы байланысты тексеру үшін талданды. Мұндағы бақылаулар саны – 138. Р-мәні (0,2025) 0,05-тен жоғары болғандықтан, регрессия моделі F-тестінің сынағынан өтпеді. Сондықтан бұл регрессия моделінің статистикалық мәні жоқ деп айта аламыз. Айнымалы ретінде кибершабуыл ұзақтығының түсіндіру күші де жоқ, өйткені Р мәні 0,05-тен үлкен болып отыр.

Регрессия (4) кибершабуыл ұзақтығы айнымалысы шабуылды кеш анықтау айнымалысымен ауыстырылып, фирманың киберқауіпсіздік жүйесінің әлсіздігі CAR-ға ықпал ететінін анықтады. Р-мәні 0,1-ден жоғары болғандықтан кибершабуыл ұзақтығы айнымалысы маңызды емес болса да, регрессия 5% мәнділік деңгейінде F-тестіден өтті, яғни регрессия (4) статистикалық мәнге ие деп қорытынды жасай аламыз. Регрессиялық модельдегі барлық айнымалылар CAR өзгергіштігінің шамамен 14,84% түсіндіре алады.

Регрессия (5) кибершабуылды кеш анықтау айнымалының орнына қосымша түсіндірме айнымалыны қойып қайта талданды. Бұл талдаудың мақсаты – кибершабуылды кеш жариялау акционерлердің әл-ауқатына қалай ықпал ететінін айқындау. 20-кестедегі талдау нәтижелері регрессия моделінің статистикалық мәні жоқ екенін көрсетті, өйткені F-тестінің Р-мәні 0,1269 және ол 0,05-тен жоғары болып отыр.

3,4,5-регрессияларында бақылаулар саны өте аз, өйткені кибершабуылдарды бастан өткерген фирмалардың барлығы бұзушылықтың басталу күні, анықталған күні туралы ақпаратты жариялай бермейді. Олар бұл ақпаратты барынша жасыруға тырысады. Осылайша, бізде кибершабуыл ұзақтығы айнымалысын есептеу үшін оқиғаның басталу және аяқталу күндері көрсетілген тек 138 бақылау бар. Сонымен қатар, хабарландыру күні мен басталу күндері арасындағы айырмашылықтарды пайдалана отырып, шабуылды кеш жариялау айнымалысын қосқанда үлгіде тек 114 фирма қалады. Сонымен, шабуылды кеш анықтау үлгісі үшін бізде қолжетімді ақпараты бар тек 186 фирма бар болып отыр.

Осы үш айнымалының негізгі статистикасы 21-кестеде берілген. Зерттеу шабуылдың орташа ұзақтығы 31 күн болатынын көрсетіп отыр. Басталу күнінен бастап көпшілікке хабарландыруға дейінгі күндердің медианалық саны 92 күнді құрайды. Сонымен қоса, кибершабуылдарды анықтаудың орташа күні 30 құрайтынын көруге болады.

Кесте 21 - Қосымша айнымалылардың сипаттамалық статистикасы

	Шабуыл ұзақтығы	Шабуылдың кеш анықталуы	Шабуылдың кеш жариялануы
Орташа	87.76812	101.5526	159.9409
Медиана	30.5	30	91.5
Стандартты ауытқу	185.2806	216.1358	270.7347
Min	0	0	1
Max	1327	1327	2427
Дисперсия	34328.91	46714.69	73297.29
Қиғаштығы (Skewness)	4.400683	3.734604	4.92504
Эксцесс (Kurtosis)	25.37525	17.9848	34.10317
Бақылаулар саны	138	114	186
Ескертпе: автормен STATA бағдарламасында есептелген.			

Регрессия (6) 2-регрессияны кибершабуылды кеш анықтау айнымалысымен біріктіріп талданды. Іріктеме көлемі 49 бақылауға дейін қысқарды, өйткені барлық фирмалар жоғалған деректер санының мәнін, және шабуылдың басталу мен анықталу күндері туралы мәліметтерін көрсетпеген. Іріктеме шағын болды және статистикалық мағынасы да болмады, өйткені F-статистикасының Р-мәні 0,1226, яғни 0,05-тен жоғары екенін байқауға болады.

Жалпы алғанда, түзетілген R^2 (**Adj. R^2**) мөлшерлемелері аз екенін және біздің регрессияларымызда жеткілікті түсіндіру күші жоқ екенін байқауға болады. Дегенмен, F-статистикасының мәні үлкен және статистикалық жағынан маңызды болып табылады, атап айтқанда 1-регрессияда 1% және 4-регрессияда 5% деңгейінде, F-статистикасының Р-мәні, сәйкесінше 0,0018 және 0,0208 мәндерге тең.

Соңғы регрессияда ең жоғары түзетілген R^2 (Adj. R^2) көрсеткішті байқауға болады, оның мәні 20,11%. Алайда, бақылаулар саны тым аз (49 бұзушылық) және F-статистикасының мәні де төмен және статистикалық жағынан мардымсыз (P -мәні=0,1226) болғандықтан, 6-регрессияның нәтижесі статистикалық жағынан мағынасы жоқ деп саналады.

Кибершабуылдың анықталуы мен оның ұзақтығы компанияның әрдайым жаңартуды қажет ететін киберқауіпсіздік жүйесіне байланысты екенін атап өткен жөн. Сондықтан орнықты киберқауіпсіздік жүйесін құру және оны әрдайым жаңартып отыру қосымша қаржылық шығындарды талап етеді. Компаниялар кибершабуылдарға деген реакциясы қандай болады? Компаниялар аталған шығындарды арттырады ма, жоқ па? Біз бұл сұрақтарға жауап беру үшін шабуылға дейін үш жыл бұрын және үш жылдан кейін қосымша деректер жинау арқылы зерттедік. Содан кейін біз осы екі қосымша іріктемелерді талдап, ғылыми-зерттеулерге жұмсалатын шығындарында айырмашылықтар бар-жоғын тексеру үшін t-тест жүргіздік.

2.4 Компаниялардың инвестициялық стратегиясына кибер қауіп-қатерлерінің әсері

Кейбір зерттеушілер кибершабуылдардан кейін компаниялар киберқауіпсіздік жүйесіне инвестициясын көбейтеді деп есептейді. Жұмыста кибершабуылдан кейін компания қаржылық және инвестициялық саясатын өзгертіп, киберқауіпсіздікті күшейту мақсатында қомақты қаражатты инвестициялауға жұмсайтын бола ма, жоқ па, соны зерттейтін боламыз. Ол үшін біз шабуылдардан үш жыл бұрын және одан кейінгі фирмалардың ғылыми-зерттеу шығындары арасындағы айырмашылықтарды салыстыратын боламыз. Ол үшін “Difference-in-Differences” тесті қолданылатын болады.

“Difference-in-Differences” тесті кибершабуылға ұшыраған және ұшырамаған фирмалардың екі тобын құруды және кибершабуылдарға дейін және кейін бақылауларды пайдалануды ұйғарады. Зерттеу үшін кибершабуылдарға дейін және одан кейінгі үш жыл ішінде олардың фирма қызметіне қалай әсер ететінін талдау жүргізіледі. Сондықтан 2019 жылғы киберқауіпсіздіктің

бұзылуы бастапқы іріктемеден алынып тасталды. Әрі қарай, бейімділік баллы әрбір шабуылға ұшыраған фирма үшін ұқсас бақылау фирмасын анықтау үшін пайдаланылды. Осы мақсатта сәйкестендіру үшін кибершабуылдың алдындағы жыл пайдаланылды. Содан кейін бейімділік көрсеткішін анықтау үшін акция кірістілігіне, акция құбылмалылығына, фирма көлеміне және левереджге шабуылдың логиттік регрессиясы (logit regression) орындалды. Сонымен қатар, бейімділік көрсеткіші саланың (екі таңбалы SIC коды) және жылға тіркелген әсердің көмегімен есептелді. Одан кейін шабуылға ұшыраған және ұшырамаған фирмалар 0,1 калибрімен бейімділік баллына қарай сәйкестендірілді [83].

Шабуылға ұшыраған және бақыланатын фирмалардың топтарын құрғаннан кейін келесі “Difference-in-Differences” регрессиясы қолданылды:

$$Y_{it} = \alpha + \beta_1 * post_{it} * Treatment_{it} + \beta_n * Control\ variables + v_{it} + \varepsilon_{it} \quad (15)$$

мұндағы, i – фирма,

t – уақыт,

Y – тәуелді айнымалы,

α, β – регрессия моделінің көрсеткіштері

$post_{it}$ – шабуылдан кейінгі кезеңнің индикаторы (шабуыл кезеңінен кейін ол бірге тең, болмаса нөлге тең),

$Treatment_{it}$ – киберқауіпсіздік инцидентінің көрсеткіші (бұзушылықты бастан өткерген фирмалар үшін ол бірге тең, ал шабуыл болмаған фирмалар үшін нөлге тең),

$Control\ variables$ – фирманы сипаттайтын айнымалылар,

v – салалық және жылдық тіркелген әсер,

ε – қалдық.

Кезең ішінде ықпалдың таралуын зерттеу үшін шабуылдан кейінгі кезеңнің көрсеткіші үш бөлек жылға (t_1, t_2, t_3) бөлінді. Регрессияға фирма өлшемі (кіші және үлкен), фирма түрі (қаржылық және қаржылық емес) сияқты фирмаға тән бақылау айнымалыларын қосу шабуылдан кейінгі фирма сипаттамаларының жыл сайынғы өзгерістерін көрсете алады. Сонымен қатар, Tobin's Q, қарыздың меншікті капиталға қатынасы, акциялардың

құбылмалылығы, ROA бақылау айнымалылары ретінде регрессияларға кіргізілген.

22-кестеде кибершабуылдарды басынан өткерген 195 фирма мен 195 бақылау фирмаларының іріктемесі үшін сипаттамалық статистика көрсетілген. Сәйкес келетін фирмалар оқиға орын алған фирмаларға ұқсас сипаттамаларға ие болу керек. *t*-тест нәтижелеріне сәйкес, егер олардың арасында айтарлықтай айырмашылықтар болмаса, оларды «Difference-in-differences» сынақтарында пайдалануға әбден мүмкін.

Кесте 22 - Сәйкес келетін фирмалар үшін сипаттама статистикасы

Айнымалы	Оқиға орын алған фирмалар	Бақылау фирмалары	Айырмашылық тесті
	орташа	орташа	<i>t</i> -тестінің <i>p</i> -мәні
Акция кірістілігі	0.070	0.088	0.838
Акциялардың құбылмалылығы	0.846	0.837	0.873
Қарыздың меншікті капиталға қатынасы	-2.733	-24.787	0.378
Фирма мөлшері	8.802	8.715	0.682
Бақылаулар саны	195	195	
Ескертпе: автормен STATA бағдарламасында есептелген.			

23-кестеде «Difference-in-differences» тестінің нәтижелері берілген. Оқиға орын алған фирмалар мен бақылау фирмалары арасындағы кибершабуылдардан кейін орын алған өзгерістер салыстырылды.

Регрессия нәтижелері кибершабуылдарды бастан өткерген фирмалардағы ROA, сатылым көлемі және ұзақ мерзімді қарыздар шабуыл жасамаған фирмалармен салыстырғанда, тиісінше, 0,20, 2,992 және 0,001-ге өскенін көрсетеді. Сонымен қатар, кибершабуылдардан кейін фирмалардың ROE көрсеткіші 51,02-ге және ғылыми-зерттеу шығындары 0,013-ке төмендеген. Дегенмен, бұл айырмашылықтар маңызды емес, өйткені «Difference-in-differences» тестіндегі *p*-мәндері 0,05-тен асып отыр.

Кесте 23 - Айырмашылықтарды бағалау («Difference-in-differences» тестінің нәтижелері)

	(1)	(2)	(3)	(4)	(5)
Тәуелсіз айнымалылар	ROA	ROE	Сатылымның өсімі	ҒЗШ/активтер	ҰМҚ/активтер
Кибершабуылдар	-0.017 (0.281)	51.10 (0.130)	-0.597 (0.710)	0.037*** (0.002)	-0.002 (0.883)
Шабуылдан кейінгі кезең	-0.007 (0.657)	51.02 (0.135)	-0.139 (0.933)	-0.002 (0.899)	0.027** (0.025)
Кибершабуылдар *	0.020 (0.372)	-51.02 (0.285)	2.992 (0.195)	-0.013 (0.457)	0.001 (0.965)
Шабуылдан кейінгі көрсеткіш					
Тұрақты шама	0.025** (0.024)	-51.09** (0.034)	0.953 (0.408)	0.034*** (0.000)	0.235*** (0.000)
Бақылаулар саны	2091	2068	1840	1176	2283
adj. R^2	-0.001	0.000	0.000	0.009	0.003
Ескертпелер: 1) жақшада көрсетілген Р-мәндері стандартты қателерге негізделген * $p < 0,10$, ** $p < 0,05$, *** $p < 0,01$ 2) ҒЗШ – ғылыми-зерттеу шығындары 3) ҰМҚ – ұзақ мерзімді қарыздар 4) автормен STATA бағдарламасында есептелген.					

Айырмашылықтарды бағалау құралы жыл сайынғы өзгерістерді зерттеу үшін үш жылға (t_1 , t_2 , t_3) бөлінді. 24-кестеде осы зерттеу нәтижесінде алынған регрессиялардың көрсеткіштері беріледі.

Регрессиялар (1,2) кибершабуылдарды бастан өткерген фирмалар үшін ROA және ROE нашар болатыны туралы дәйекті дәлелдер көрсетпейді. Бұл фирманың тиімділік көрсеткіштері фирма түрі мен көлеміне байланысты өзгеруі мүмкіндігімен түсіндіріледі [10].

Дегенмен, кибершабуылдың ҒЗШ/активтерге, сатылым көлемінің өсіміне және ҰМҚ/активтерге айтарлықтай оң әсері анықталды. Орташа алғанда, ҒЗШ/активтер көрсеткіші шабуылдан кейінгі бірінші жылы 10% маңыздылық деңгейінде 1,3%-ға өскені анықталды. Сол себепті, фирмалар өздерінің киберқауіпсіздік жүйесін жақсарту үшін, әсіресе шабуылдан кейінгі кезеңнің

бірінші жылында ғылыми-зерттеу және тәжірибелік-конструкторлық шығындарды көбейтеді деп айтуға болады.

Кесте 24 - Тиімділік коэффициенттерінің OLS регрессиялары

	(1)	(2)	(3)	(4)	(5)
Тәуелсіз айнмалылар	ROA	ROE	Сатыл ымның өсімі	ҒЗШ/ активтер	ҰМҚ/ активтер
t ₁	0.016	16.56	0.146	0.013*	0.008
	(0.217)	(0.697)	(0.944)	(0.056)	(0.624)
t ₂	0.009	15.04	6.816***	0.004	0.022
	(0.472)	(0.725)	(0.001)	(0.531)	(0.167)
t ₃	0.015	17.23	0.890	0.007	0.042***
	(0.256)	(0.690)	(0.680)	(0.279)	(0.008)
Акция құбылмалылығы	-0.040***	-165.0***	1.571	-0.0001	0.057***
	(0.000)	(0.000)	(0.207)	(0.984)	(0.000)
Қарыздың меншікті капиталға қатынасы	-0.0001	-0.163	0.003	-0.0002	0.0001
	(0.574)	(0.756)	(0.904)	(0.413)	(0.499)
Tobin Q	-0.057***	2.311	-0.257	0.014***	-0.006***
	(0.000)	(0.516)	(0.573)	(0.000)	(0.002)
Фирма мөлшері	0.015**	10.69	-1.314	-0.012***	0.005
	(0.039)	(0.655)	(0.265)	(0.002)	(0.608)
Қаржылық фирмалар	-0.040***	-12.01	-0.938	-0.040***	-0.041***
	(0.000)	(0.742)	(0.653)	(0.000)	(0.002)
ROA				-0.250***	-0.010
				(0.000)	(0.699)
Тұрақты шама	0.167***	114.0***	0.594	0.025***	0.214***
	(0.000)	(0.000)	(0.713)	(0.000)	(0.000)
Бақылаулар саны	2066	2066	1818	1158	2066
<i>F-statistic</i>	379.14***	5.85***	1.70*	551.08***	8.43***
	(0.000)	(0.000)	(0.094)	(0.000)	(0.000)
adj. <i>R</i> ²	0.594	0.019	0.003	0.811	0.031
Ескертпелер: 1) * 10% деңгейінде маңызды 2) ** 5% деңгейінде маңызды 3) *** 1% деңгейінде маңызды 4) автормен STATA бағдарламасында есептелген.					

Сонымен қатар, біз шабуылдан кейінгі екінші жылы сатудың айтарлықтай өсіп жатқанын көреміз (шамамен 681,6%). Бұны, біздің іріктеме фирмалардың әртүрлі сала мен өлшемдерінен тұратынымен түсіндіруге болады. Kamiya (2018) кибершабуылдардың нысанасы тиімділігі жоғары және ерекше фирмалар екенін анықтаған [10].

Сонымен қатар, шабуыл кезінде ерекше фирмалардың тауарына деген сұраныс кейінге қалдырылуы мүмкін, сәйкесінше, бұл келесі кезеңдердегі сатылымға ықпал етіп отырады. Сондықтан кибершабуылдар тауарларды сату көлемін айтарлықтай нашарлатпайды және фирмалар тез қалпына келіп, сатылымдарын арттыра алады деп болжауға болады.

Сондай-ақ, үшінші жылы ұзақ мерзімді қарыз коэффициенті 4,2%-ға айтарлықтай өскенін және фирмалар өздерінің левередждерін арттыру арқылы шабуылға байланысты қаржылық проблемаларды жеңуге тырысатынын атап өтуге болады.

Регрессиялық модельдердің түсіндіру күшіне келетін болсақ, регрессиялар (1) және (4) жоғары түзетілген R^2 (adjusted R^2) көрсеткіштеріне ие болып отыр (сәйкесінше, 59,4% және 81,1%). Оған қоса, регрессиялардың (2,3,5) түзетілген R^2 (adjusted R^2) көрсеткіші жеткілікті деңгейде үлкен емес, бұл тәуелсіз айнымалылар тәуелді айнымалының өзгеруін шамалы ғана түсіндіретінін көрсетеді. Дегенмен, F-статистикасы тиісінше 1%, 10% және 1% статистикалық маңызы бар, бұл регрессиялардың статистикалық мәні де бар екенін дәлелдейді (24-кесте).

Жалпы, 24-кесте фирмалардың кибершабуылдардан кейін F3Ж шығындарын ұлғайтуға бейім екенін көрсетеді, бұл олардың киберқауіпсіздікке төзімділік жүйесін жақсартуға тырысатынын көрсетеді. Сонымен қатар, шабуылдардан кейінгі ұзақ мерзімді қарыздардың артуы кибершабуылды өткерген фирмалардың бұрынғы кезеңге қарағанда жоғары тәуекелге баратынын көрсетеді.

ТАРАУ 3. КИБЕР ҚАУІП-ҚАТЕРЛЕР ЖАҒДАЙЫНДА КОМПАНИЯЛАРДЫҢ ҚАРЖЫЛЫҚ ТҰРАҚТЫЛЫҒЫН ҚАМТАМАСЫЗ ЕТУ ТЕТІКТЕРІ

3.1 Қаржылық менеджменттің элементі ретінде киберқауіпсіздік тәуекелдерін бағалау әдістерін жетілдіру

Киберқауіптерге байланысты тәуекелдер цифрландыру кезеңінде компания қызметінің ажырамас бөлігі болып табылады. Сондықтан компаниялар қолданатын тәуекелдерді бағалау әдістері цифрлық ортадағы жаңа жұмыс жағдайларына бейімделуі керек. Цифрлық тәуекелдерді азайту бойынша әдістемелік ұсыныстарды әзірлеу кезінде компаниялардың дәстүрлі тәуекелдерін модельдеудің теориялық негіздерін ескеру қажет. Тәуекелдерді модельдеу – бұл компанияның бизнес-процестерінің тәуекел элементтерін көрсететін болжау әдістерінің жиынтығы. Бұл модель оқиғаның ықтималдығын сандық бағалауға, компания басшылығының операциялық, қаржылық және стратегиялық шешімдерін қабылдауға көмектесетін оқиғаның математикалық болжамдауға мүмкіндік береді.

Осы тұрғыда цифрлық тәуекелдерді бағалаудың негізгі әдісі ретінде «деректер конвертінің талдауы» (DEA - Data Envelopment Analysis) болып табылады. Бұл әдіс цифрлық тәуекелдердің екі жақтылығын ескереді. Екі жақтылық бір оқиға бірнеше қауіп тудыруы мүмкін дегенді білдіреді. Сондай-ақ, бұл әдіс бірнеше кіріс және шығыс айнымалыларын пайдалануға негізделгенін атап өткен жөн. Кіріс айнымалылары компанияның шығындарын қамтиды, ал шығыс айнымалылары компанияның жұмыс нәтижелері болып табылады. DEA әдісі объектілердің ресурстары мен нәтижелерін ескере отырып, олардың тиімділігін өлшеуге мүмкіндік береді.

Тәуекелдерді бағалау әдістерін ескере отырып, компанияның цифрлық тәуекелдерінің бұрын анықталған жіктелуі бизнес-процестердің цифрлық трансформациясын жүзеге асыратын ұйымдардың тәуекелдер деңгейін және тиімділігін анықтайтын қаржылық көрсеткіштерді жүйелеуге көмектеседі. DEA әдісін қолдану тиімділікті кешенді бағалауға (сандық көрсеткіштер

арқылы) және тәуекелді азайту аймақтарын анықтауға мүмкіндік береді, бұны Li et al. (2017) зерттеулері дәлелдеп отыр [84].

DEA классикалық нұсқасында кіріс деректері ресурстар, ал шығыс деректері өндіріс көлемі болып табылады. Бұл олардың арасындағы тура пропорционалдылықты көрсетеді. Бұл әдісті цифрлық тәуекелдерді төмендетуде қолдану оларды азайту жолдарын анықтауға мүмкіндік береді. Модельдік тәуекелдер үлгілерді әзірлеу, енгізу немесе пайдалану кезіндегі қателіктерге байланысты ықтимал шығындарды қамтиды. Модельдік тәуекелдерді басқару қате немесе сәйкес емес модельдермен байланысты тәуекелдерді бақылауға бағытталған.

Операциялық ортаны талдау үлгісін пайдалану компаниялардағы қауіпсіздік деңгейін бақылау үшін пайдалы болуы мүмкін. Заманауи жағдайдағы негізгі мәселелердің бірі – цифрлық тәуекелдермен күресте ерекше маңызды болып табылатын тұрақты киберқауіпсіздік жүйелерін құру. Осылайша, кейбір сарапшылар киберқауіпсіздік әлемдегі ең ірі компаниялар үшін басты қауіп екенін атап өтуде [84].

Қызмет ету ортасын талдау арқылы компаниялар басқалармен салыстырғанда киберқауіпсіздік шараларының тиімділігін бағалай алады. Киберқауіпсіздікке қатысты маңызды көрсеткіштерге анықталған және шешілген инциденттер саны, белсенді шаралар арқылы алдын алған шабуылдардың пайызы, мониторингтің жалған позитивті және жалған негативті нәтижелер саны, фишингтік шабуылдардың жиілігі, сондай-ақ кибершабуылдарды анықтаудың, оған төтеп беру мен жоюдың орташа уақыты қамтиды.

Есептеулерді жүргізу үшін үлгінің кіріс және шығыс көрсеткіштерін анықтау қажет. Қазақстандық компанияларда киберқорғаныс жүйелерінің жеткіліксіз дамуын ескере отырып, модель қарапайым және түсінікті болуы керек. Сонымен бірге ол кәсіпорынның экономикалық қауіпсіздік деңгейін арттыруға бағытталған басқару шешімдерін қабылдау үшін жеткілікті ақпаратпен қамтамасыз ету керек.

Ағымдағы киберқауіпсіздік шараларының тиімділігін бағалау үшін 3-суретте келтірілген операциялық ортаны талдау моделінің көрсеткіштерін пайдалану ұсынылады.



:

Сурет 3 - Компанияның киберқауіпсіздік шараларының тиімділігін бағалауға арналған кіріс және шығыс көрсеткіштері

Бұл көрсеткіштерді таңдау инвестицияланған қаражатқа және персонал санына қатысты тойтарылған кибершабуылдардың санын бағалау қажеттілігіне байланысты. Нәтиже – компанияларды бәсекелестерімен салыстыратын «киберқауіпсіздік тиімділігінің көрсеткіштерінің» болып табылады. Көрсеткіш жоғарғы басшылық

үшін ашық болып, цифрлық тәуекелдерді басқару және ақпараттық қауіпсіздікпен тығыз байланысты экономикалық қауіпсіздік деңгейін бағалау үшін қосымша көрсеткіш ретінде пайдаланылуы мүмкін.

Цифрлық тәуекелдер цифрландыру жағдайында компанияның капиталына немесе қаржылық нәтижелеріне теріс әсер етуі мүмкін оқиғалардың ықтималдығын білдіреді. Бұл тәуекелдер, егер олар өлшенетін, бақыланатын және компанияға қолайсыз жағдайларға тиімді әрекет етуге мүмкіндік беретін шектерде болса, негізделген деп саналады.

Цифрлық тәуекелдерді басқару үшін компаниялар жетекші сарапшылар қолданатын тәсілдерді қолданғаны жөн. Мысалы, тәуекелдердің келесі түрлерін бөлуге болады: операциялық, бедел, стратегиялық, нарықтық, транзакциялық және комплаенс тәуекелі. Осы тәуекелдерді зерттеу және бақылау компанияларға олардың ағымдағы тұрақтылығын бағалауға және ықтимал проблемаларды болжауға мүмкіндік береді. Цифрлық технологияларды белсенді пайдалану жағдайында әсіресе өзекті болып табылатын операциялық тәуекелдердің жаңа нысандарына ерекше назар аударылады. Мысалы, кейбір сарапшылар корпоративтік ортаға цифрлық валютаны және басқа да технологиялық инновацияларды енгізуге байланысты қосымша тәуекелдерді атап көрсетеді.

Кез келген компания өнімі немесе қызметі өзара әрекеттесетін және бірін-бірі нығайта алатын тәуекелдердің бірнеше түрлерімен байланысты. Мысалы, стратегиялық тәуекелдер компания беделіне, ал операциялық тәуекелдер қаржылық тәуекелдерге әсер етуі мүмкін. Бұл, әсіресе жеделдетілген цифрландыру және жоғары бәсекелестік жағдайында тәуекелдерді басқаруға кешенді көзқарасты талап етеді.

Халықаралық тәжірибелер киберқауіпсіздік, деректерді басқару, бұлттық технологияларды пайдалану, электрондық коммерция және әлеуметтік желілер сияқты көрсеткіштерге негізделген цифрлық тәуекелдерді талдау модульдерін пайдалануды қамтиды. Негізгі тәуекелдер анықталғаннан кейін компаниялар төзімділікті жақсарту үшін оларды төмендету стратегияларын әзірлейді және шешімдерді құжаттайды.

Сондағы, тәсілдер бизнестің ауқымына байланысты өзгеруі мүмкін: ірі корпорациялар мен жүйелік маңызды компаниялар

шағын және орта кәсіпорындарға қарағанда тәуекелдерді басқарудың күрделі әдістерін пайдаланады.

Осылайша, тиімді цифрлық тәуекелдерді басқару компаниялардың тұрақтылығы мен бәсекеге қабілеттілігінің негізгі факторына айналады. Қазіргі заманғы бағалау әдістері қауіптерді төмендетуге ғана емес, сонымен қатар цифрлық трансформация жағдайында бизнестің жалпы экономикалық қауіпсіздігін нығайтуға мүмкіндік береді.

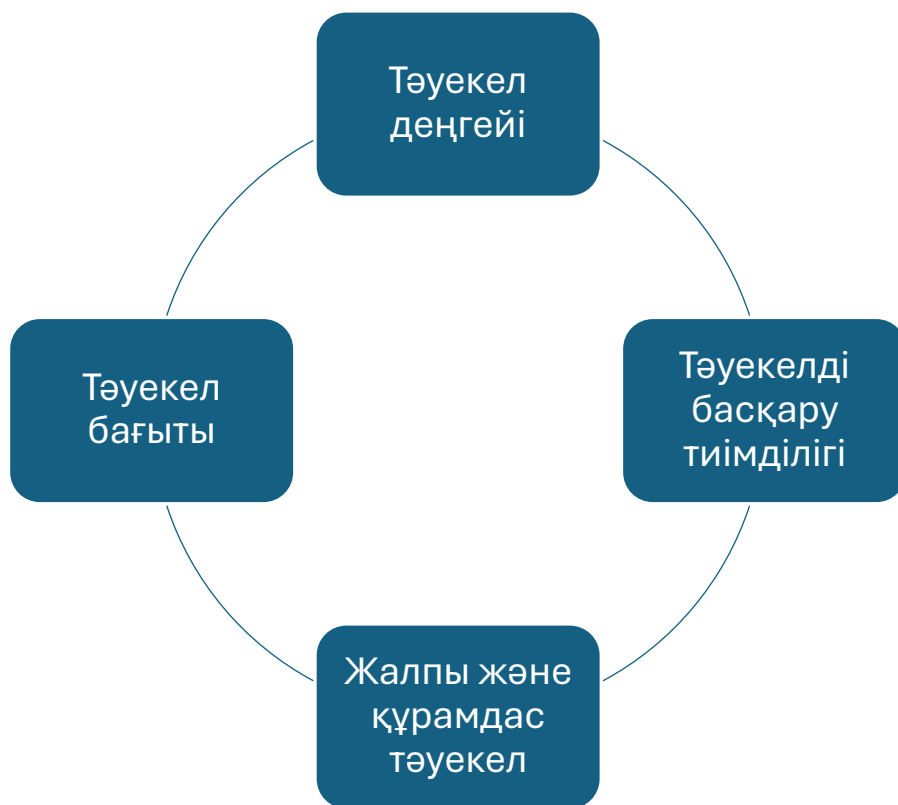
Ірі компаниялар үшін тәуекелдерді бағалау жүйесіндегі негізгі аспектілер мыналар болып табылады:

1. Тәуекел деңгейі. Бар тәуекелдің көлемі немесе дәрежесі анықталады. Сондағы, сандық бағалау әрқашан ақшалай түрде бола бермейді, әсіресе транзакциялық немесе комплаенс-тәуекелдері үшін.

2. Тәуекелдерді басқарудың тиімділігі. Басқару сапасы әлсіз, қолайлы немесе күшті деп бағаланады. Процесс тәуекелдерді анықтауға, өлшеуге, мониторинг пен бақылауға бағытталған, болашаққа бағдарланған және белсенді болуы керек. Тиімді менеджмент ішкі бақылау бөлімдеріне баса назар аудара отырып, барлық бөлімдердің үйлестірілген жұмысын қамтиды.

3. Жалпы және құрамдас тәуекел. Жалпы тәуекел – бұл компаниядағы тәуекелдерді басқару сапасын ескергендегі олардың жалпы деңгейі. Ол төмен, орташа және жоғары болып жіктеледі. Құрамдас тәуекел – бұл стратегиялық және беделдік сияқты жеке тәуекелдердің динамикасын сипаттайды. Ол төмен, орташа немесе жоғары деп бағаланады.

4. Тәуекелдің бағыты. Белгілі бір кезеңдегі жиынтық немесе құрамдас тәуекелдер деңгейіндегі өзгерістерді анықтайды (мысалы, 12 ай). Тренд жоғары, тұрақты немесе төмен болуы мүмкін. Күрделі операциялары бар жүйелік маңызды компаниялар үшін олардың жоғары тәуекелді аймақтарын және олардың аймақтық қатысуының әртүрлілігін ескеретін тәсілдер маңызды (4-сурет).



Сурет 4 - Тәуекелді бағалаудың негізгі аспектілері

Тәуекелдерді бағалау және есепке алу жүйесі төрт негізгі деңгейді қамтиды:

- Ұйымды басқару. Бұл деңгей үш қорғаныс желісін қамтитын есеп беру құрылымын қамтиды және тәуекелдердің таралуы мен көздерін анықтайды. Тәуекелдерді бақылау және есеп беру деңгейі де белгіленеді, ол тәуекел комитеттері арқылы жүзеге асырылады және ұйымның саясаты шеңберінде ресімделеді. Менеджмент пен бөлімдер арасында жауапкершілікті бөлу үшін тәуекел таксономиясын қамтиды.

- Процестер мен әдістеме. Бұл деңгейде тәуекелдерді басқарудың жалпы тәсілі және онымен бірге жүретін процестер анықталады. Олар әдетте шектеулерге назар аударады және оқиғаларды басқару, тәуекелді бағалау және бақылау, тәуекелге тәбет, мониторинг және есеп беру процестері сияқты әдістер арқылы тәуекелді басқарады.

- Тәуекелдерді басқару процестері. Бұл деңгейде тәуекелдердің нақты түрлері басқарылады. Әдетте стресс-тестілеу механизмдері және сценарийлік талдау қолданылады. Олар

ықтимал өзгерістерге бейімделуге, ықтимал тәуекелдер мен олардың салдарын азайтуға мүмкіндік береді.

- Мінез-құлықты басқару. Бұл деңгейде корпоративтік киберқауіпсіздік мәдениеті қалыптасады. Ол киберқауіптерді басқару стандарттарын құруды және қызметкерлерді оқытуды қамтиды (5-сурет).



Сурет 5 - Кибертәуекелді бағалау және есепке алу жүйесі

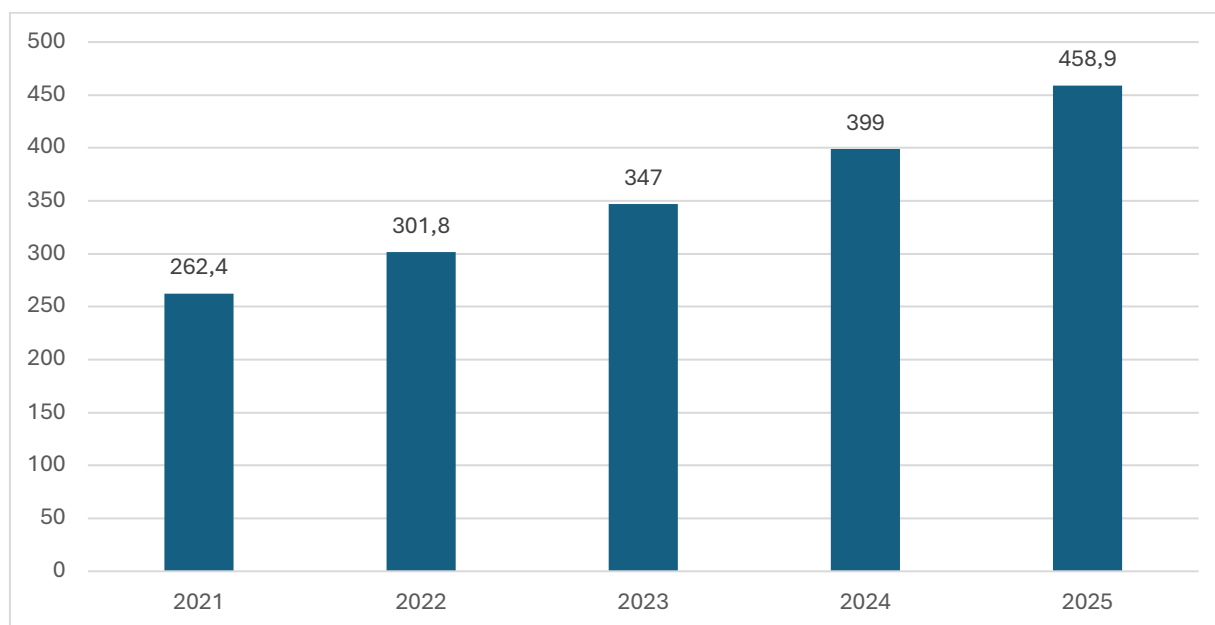
Осы элементтердің барлығын қамтитын киберқауіптерді кешенді бағалау мен есепке алуды енгізу компанияларға ықтимал кибершабуылдарға дайын болуға, олардың салдарын барынша азайтуға және экономиканың цифрлық трансформациясы жағдайында компанияның жалпы тұрақтылығын арттыруға мүмкіндік береді.

3.2 Компаниялардағы киберқауіпсіздік стратегиясын оңтайландыру жолдары

Цифрландырудың жедел дамуы компанияларды бұлтты онлайн қызметтерін белсенді түрде енгізуге, бар өнімдерін қайта қарап, жаңаларын әзірлеуге мәжбүр етеді. Дегенмен, мұндай қызметтер компаниялардың киберқауіпсіздігінде осалдықтарды тауып, төлем бағдарламалық құралдары арқылы қылмыс жасайтын киберқылмыскерлердің нысанасына айналуға.

Сондықтан киберқауіпсіздік соңғы кездері бизнес үшін бірінші кезектегі мәселеге айналуға. Осылайша, KPMG мәліметтері бойынша, 2021 жылы сауалнамаға қатысқан компаниялардың 500 бас директорларының 18%-ы қазіргі уақыттағы компанияның өсуіне негізгі кедергі ретінде киберқауіптерді атады [85].

Қазіргі кезде цифрлық бизнес үлгілері белсенді түрде қабылдануда. Осылайша, бас директорлардың 52%-ы өз компанияларының киберқауіпсіздігін нығайтуға назар аударуды жоспарлап отыр. Бұл, өз кезегінде, киберқауіпсіздік шығындарының өсуіне алып келуі мүмкін. 2025 жылға қарай бұл шығындар 458,9 миллиард долларға жетеді деп болжамдануда (6-сурет) [85].



Ескертпе: [84] дереккөз негізінде автормен әзірленген.

Сурет 6 - Әлемдегі киберқауіпсіздікке жұмсалған шығындар, миллиард АҚШ доллармен

Суретте көрсетілген 2025 жылғы деректер болжамдық шама. Әлемде киберқауіпсіздікке жұмсалатын жаһандық шығындар 2025 жылы 2024 жылмен салыстырғанда 15 пайызға өсіп, 458,9 миллиард АҚШ долларын құрайды деп күтілуде. Жалпы алғанда, бес жыл ішінде киберқауіпсіздікке жұмсалатын шығындар шамамен 1 769,1 миллиард долларды құрайтын болады [85].

Киберқауіпсіздікті қаржыландыруды ұлғайту киберқауіптерді азайту жолындағы маңызды қадам екені анық. Алайда, қазіргі кездегі маңызды аспект қатарында кибершабуылдарға қарсы тұруға бағытталған қаражатты ұтымды пайдалану болып табылады. Бұл дегеніміз, кибершабуылдардан келетін зиянды азайтуға басты назар аудару керек.

Бұл мақсатқа жету үшін қолжетімді технологияларды түсінуге негізделген инвестициялық саясатты әзірлеу кезінде нақты стратегия қолдану қажет. Мысалы, Gartner 2024 жылы бұлттық қауіпсіздікке жұмсалатын шығындар 41,2%-ға өседі, ал деректерді қорғауға, қол жетімділігін басқаруға жұмсалатын шығындар да осылайша өседі деп болжануда. Дегенмен, IoT қауіпсіздігі және авиациялық қауіпсіздік сияқты нарықтардың маңызды бөліктері әлі де бағаланбай қалуда.

Киберқауіпсіздік нарығы 2024 жылдың бірінші жартыжылдығында 9 миллиард доллардан асқан венчурлық инвестициялардың арқасында стартаптар мен инновациялық технологияларды дамытуды ынталандыратын болады. Тәуекелдерді төмендету үшін компаниялар жаңа шешімдермен және серіктестермен жұмыс істеп көру керек.

Дегенмен, шығындарды тиімді бөлудің негізгі элементі киберқауіпсіздік мамандары болып келеді. Ақпараттық қауіпсіздік бойынша директорды тағайындау бизнес мақсаттарын техникалық тәуекелдермен сәйкестендіруге және қажетті салаларға қаржыландыруды оңтайлы бағыттауға мүмкіндік береді. Бұл рөлдің маңыздылығына қарамастан, көптеген компаниялар оны маңызды деп санамайды, және компания құрылымында мұндай позицияның болуы кемде кем.

Киберқауіпсіздік басқарудың ең жоғарғы деңгейінде стратегиялық басымдыққа айналмайынша, бұл саладағы шешімдер тиімділігі жоғары болмайды.

Киберқауіпсіздік шығындарының мөлшерін шектеу мүмкін емес. Осылайша, кибершабуылға дейін компаниялар бюджет шегінде жұмыс істесе, кибер шабуыл орын алғанда компанияның жүйесін қалпына келтіру үшін барлық қолда бар ресурстарды жұмсауға дайын болады. Өйткені жоғары бағаға қарамастан, ешбір компания өз деректерін қорғаудан бас тартпайды.

Киберқауіпсіздік шығындары киберқылмыстық әрекетке байланысты өсіп жатыр деп есептеледі. Шығындары болжана алмайтын бопсалаушы вирустар секілді кибершабуылдардың өсуі жағдайында компаниялар, әсіресе ірі компаниялар, қорғанысқа қомақты қаражат жұмсауға дайын.

Осылайша, технологиялық алпауыттар киберқауіпсіздік шараларын белсенді түрде күшейтуде. Осылайша, Microsoft алдағы бес жылда инвестиция көлемін 20 миллиард долларға дейін ұлғайтуды жоспарлап отыр, бұл бұрынғы көрсеткіштерден төрт есе жоғары. Google жеткізілім тізбегінің қауіпсіздігі мен ашық бастапқы код қауіпсіздігін нығайту үшін 10 миллиард доллар инвестициялауға ниетті.

Мұндай бастамалар бизнестің негізгі бағыты ретінде киберқауіпсіздіктің маңыздылығын көрсетеді. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету үшін мынадай өзекті сұрақ туындап отыр: шектеулі ресурстармен сенімді қорғауды қалай қамтамасыз ету керек? Бұл сұраққа жауап компанияның ерекшелігіне байланысты ерекше тәсілді қажет етеді. Дегенмен, жалпы алғанда киберқорғаныстың сенімділігі мынадай маңызды аспектілерге байланысты болады деп қорытынды жасауға болады:

1. Бағдарламалық қамтамасыз ету. Антивирустар, желіаралық қалқандар және сақтық көшірме жүйелері сияқты қауіпсіздік құралдары бюджеттің шамамен 30%-ын құрауы керек. Оңтайландыру компания көлеміне сәйкес келетін технологияларды таңдауды қамтиды. Мысалы, күрделі кәсіпорын шешімдері шағын бизнес үшін артық, ал қарапайым жүйелер ірі компаниялар үшін жеткіліксіз болады.

2. Кадрлар. Бюджеттің шамамен 30 пайызы киберқауіпсіздік мамандарына бөлінуі керек. Компаниялар қызметкерлердің жұмыс жүктемесін азайту үшін автоматтандыруды пайдалана алады, бұл командаларға маңызды тапсырмаларға назар аударуға мүмкіндік береді. Балама аутсорсинг

қызметін пайдалануға да болады. Мысалы, қауіпсіздік талдаушылары, инженерлер және ақпараттық қауіпсіздік директоры сияқты рөлдерді сырттан шақырылған мамандар да атқара алады.

3. Аутсорсинг және инфрақұрылым. Осалдықты бағалау, жүйеге кіруді тексеру және бақылау сияқты қызметтер көбінесе аутсорсингке беріледі. Бұлттық қауіпсіздікке, сондай-ақ жергілікті жүйелерді жаңғыртуға жұмсалатын шығындар маңызды бағыт қатарында болып қала береді.

4. Оқыту. Персоналды оқытуға инвестиция салу өте маңызды. Қызметкерлер мен басшылықты оқыту тәуекелдерді азайтуға көмектеседі және олардың қызмет тиімділігін жүйелі түрде тексеру жалпы қорғаныс деңгейін күшейтеді.

5. Нормативтік талаптарға сәйкестік. Бұл шығындарға аудит және есеп беру шығындары, сот шығындары, тұтынушылардың өтемақылары және беделін басқару шығындары кіреді.

Кибер инциденттерден тиімді қорғауды қамтамасыз ету үшін бюджетті құру кезінде барлық қарастырылған шығыс баптарын дұрыс бөлу маңызды. Шығындар мен киберқауіптерді азайтуды теңестіру үшін компания киберқауіпсіздікке салынған инвестицияның табыстылығын бағалауы керек.

Киберқауіпсіздік шығындарының тиімділігін арттыру үшін серверлер, артықшылықты есепті жазбалар және тұтынушы деректері сияқты негізгі ресурстарды қорғауға назар аудару керек. Мысалы, қаржылық компанияларда бұл құпия транзакцияларға рұқсаты бар банктік жүйелер мен шоттарды қамтуы мүмкін. Бұл тәуекелдерді азайтуға және тұтынушылардың сенімін сақтауға көмектеседі.

Сонымен қатар, ағымдағы шығындарды бағалап, оларды басым салаларға қайта бөлу қажет:

- жаңа серіктестерді қорғауды қамтамасыз ету үшін API (Application Programming Interface) қауіпсіздігін қамтамасыз ету қажет;

- фишингтік қауіптерді азайту үшін көп факторлы және құпия сөзсіз аутентификацияны пайдалану керек;

- қашықтан қол жеткізуді қамтамасыз ету үшін Zero Trust Network Access (ZTNA) пайдалану керек;

- қауіптерді анықтау және қауіпсіздік топтарын қолдау үшін XDR (Extended Detection and Response) платформаларын пайдалану керек;

- бұлттық жүйелер SaaS (Software as a service) үшін қауіпсіздік жағдайын басқару (SPM – Security Posture Management);

- құпиялылық ережелерін сақтау үшін келісімді басқару шешімдерін пайдалану қажет;

- қауіпсіз аналитика және модельді оқыту үшін AI (жасанды интеллект) бар синтетикалық деректерді пайдалану қажет.

Сонымен қатар, тұтынушылармен өзара әрекеттесетін және кіріске әсер ететін жүйелерді қорғауға инвестициялау ұсынылады.

Операцияларды автоматтандыру процестерді оңтайландыруға және шығындарды азайтуға көмектеседі. Мына құралдарды пайдалануға болады:

- шабуылдарды автоматты түрде болдырмау үшін SOAR (Security Orchestration, Automation and Response);

- қауіпсіздікті басқару үшін Microsoft Secure Score және соған ұқсас бұлттық платформалардың қызметтерін.

Процесті автоматтандыру қолмен басқаруға тәуелділікті азайтады және жұмыс тиімділігін арттырады.

Сондай-ақ тиімділігі төмен құралдарды алып тастау ұсынылады. Мысалы:

- жергілікті қауіпсіздік құрылғыларының орнына бұлттық шешімдерге ауысуға болады;

- жүйеге кірудің шамадан артық сынақтары сияқты тиімсіз қызметтерді азайтуға болады;

- тиімділігі төмен технологияларды жойып, оларды заманауи шешімдермен ауыстыруға болады.

Осылайша, компаниялар ресурстарды үнемдеу, тәуекелді азайту және өнімділікті арттыру тұрғысынан дәлелденетін тиімділігі бар құралдарға назар аударуы керек.

Киберқауіпсіздік бюджетін басқарудың тағы бір маңызды аспектісі бюджеттік жоспарды орындау және бақылау болып табылады. Киберқауіпсіздік шығындарын бақылау және бастамалардың тиімділігін бағалау үшін қажет шаралар мыналар:

- әрбір бастаманың шығыны мен пайдасын талдау;

- мақсаттармен байланысты негізгі тиімділік көрсеткіштерін (KPI – Key Performance Indicators) анықтау және қадағалау;

- шаралардың инциденттер көрсеткіштеріне, мысалы, кибербұзушылықтарды тоқтату уақытына, ықпалын бағалау;

- қауіпсіздік туралы қызметкерлер мен тұтынушылардың пікірлерін жинау;

- қаржылық табысты бағалау үшін таза келтірілген құн (NPV – Net Present Value) талдауы сияқты әдістерді қолдану.

Алынған мәліметтерге сүйене отырып, жыл бойына бюджетті түзетіп отыру қажет.

Жаһандық киберқауіптерді ескере отырып, компанияларға киберқауіпсіздік стратегияларын күшейту ұсынылады. Атап айтқанда:

- қауіпсіздік үшін бюджет буферін жасау және кибер тұрақтылықты дамыту;

- киберсақтандыруды енгізу;

- тестілеуге, кибершабуылдарға жауап беруге және қызметкерлерді кибершабуылға жауап беруге үйретуге инвестициялау арқылы киберқауіпсіздікті үздіксіз процесс ретінде қарастыру.

Осылайша, шығындарды тәуекелдермен, жоба басымдықтарымен және құралдармен сәйкестендіру арқылы киберқауіпсіздік стратегияны оңтайландыру компаниялардың кибершабуылдарға төзімділігін және киберқауіпсіздік шығындарының тиімділігін арттыруға көмектеседі.

ҚОРЫТЫНДЫ

Монография қарқынды цифрландыру және киберқауіпсіздік қаупінің өсуі жағдайында өзекті болып табылатын кибершабуылдардың компаниялар тиімділігіне әсерін зерттейді. Кибершабуылдар компаниялардың нарықтық құнына айтарлықтай кері әсер ететіні анықталды. Киберқауіпсіздік оқиғалары барысында жиынтық аномальды кірістіліктің (CAR) талдауы бұл әсерлердің компания сипаттамаларына өте тәуелді екенін көрсетіп берді.

Зиянның мөлшерін анықтайтын негізгі фактор компанияның көлемі болып табылатыны анықталды. Әсіресе шағын компаниялар акцияларының құны кибершабуылдардан кейін айтарлықтай төмендеп отырады. Бұл, кішігірім фирмалар үлкен компаниялармен салыстырғанда қауіпсіздік технологиясына аз инвестиция салатынына байланысты болады. Нәтижесінде, шағын компанияларға болашақ тәуекелдерді азайту үшін сенімді киберқауіпсіздік жүйелерін әзірлеуге және енгізуге жұмсалатын шығындарды ұлғайту ұсынылады.

Дегенмен, зерттеу нәтижесінде кибершабуылдарға нарықтың реакциясы компания түріне немесе шабуылдың өзіне байланысты болатынына сенімді дәлелдер табылмады. «Difference-in-Differences» айырмашылықтар сынағының нәтижелері кибершабуылға ұшырамаған фирмалармен салыстырғанда шабуылдарға дейін және одан кейінгі компаниялардың жұмысында айтарлықтай айырмашылықтарды көрсетпеді. Осыған қарамастан, кибершабуылдардан кейінгі жылдардағы компания көрсеткіштерінің динамикасындағы өзгерістерді талдау бірнеше қызықты тенденцияларды анықтады. Атап айтқанда, шабуылдан кейінгі бірінші жылы компаниялар ғылыми-зерттеу және тәжірибелік-конструкторлық жұмыстарға (ҒЗТКЖ) шығындарын көбейтеді. Бұл компаниялардың киберқауіпсіздік ұстанымдарын нығайтуға және болашақ қауіптерден қорғауды жақсартуға ұмтылатынын көрсетуі мүмкін.

Кибершабуылдан кейінгі екінші жылы сатылым көлемі өседі. Себебі кибершабуылға ұшыраған компаниялар жиі ерекше тауарлар мен қызметтерді өндіреді, сонымен қатар олар бәсекелестік деңгейі төмен салаларда қызмет етеді. Кибершабуыл

салдарынан сатылымның уақытша төмендеуінен кейін, олар өз өнімдеріне деген сұраныстың қайта артуына тап болады.

Сонымен қатар, кибершабуылдан кейінгі үшінші жылы компаниялар әдетте оқиғалардың қаржылық салдарын жеңуге мүмкіндік беретін левереджді (несиелерді) арттырады. Бұл олардың дағдарысты еңсеру және жаңа нақты жағдайда қаржылық тұрақтылығын нығайту стратегиясының бір бөлігі болуы мүмкін.

Осы нәтижелерге қарамастан, зерттеудің бірнеше шектеулері бар. Біріншіден, Audit Analytics, Privacy Rights Clearinghouse, ProQuest, ABIInforms сияқты киберинциденттер туралы ақпаратты жинауға арналған әртүрлі дерекқорлар бар. Әрқайсысы кибершабуылдардың әртүрлі санын қамтиды және әртүрлі ақпарат түрлерін қамтиды. Сондықтан зерттеу нәтижелері таңдалған деректер қорына байланысты болуы мүмкін. Ал бұл, өз кезегінде, қол жеткізілетін нәтижелерге әсер етуі мүмкін. Болашақта кибершабуылдар мен компанияның өнімділігі арасындағы байланысты жақсырақ түсіну үшін киберқылмыс деректерінің сенімді және біркелкі көздерін пайдалану ұсынылады.

Жалпы, зерттеу кибершабуылдардың компаниялардың қаржылық және инвестициялық қызметіне, оның ішінде олардың нарықтық құнына, шығындарына, инвестицияларына және стратегиялық шешімдеріне айтарлықтай әсер ететінін растайды. Монографияда берілген ұсыныстар киберқауіпсіздік жүйесін жетілдіруге, компанияларға кибершабуылдарға төзімділігін арттыруға және олардан болатын қаржылық шығындарды азайтуға мүмкіндік беретін қаржылық стратегияларды оңтайландыруға бағытталған.

Шетел тәжірибесіне сүйене отырып, Қазақстан жағдайында кибершабуылдардың компанияларға ықпалын зерттеу үшін, ең алдымен, арнайы заңнамалық актілердің қабылданғаны абзал екенін атап өтуге болады. Бұл заң бойынша барлық акционерлік қоғамдар орын алған кибершабуылдар туралы мәліметтерді арнайы мекемелерге жіберу міндетті деп тану керек, және оқиға туралы хабарламаны көпшілікке жариялау қажет болатыны белгіленуі керек. Осындай деректер базасы болған жағдайда ғана монографияда көрсетілген әдістеме негізінде талдау жүргізіліп, қазақстандық компаниялардың кибершабуылдарға деген төзімділігі сыналуды мүмкін.

ПАЙДАЛАНҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Murphy, H. and Bond, S. (2019). Capital One data breach sparks cloud security fears. *Financial Times*. [Online]. 30 July. [Accessed 10 July 2023]. Available from: <https://www.ft.com/content/5b3046ca-b2d4-11e9-bec9-fdcab53d6959>
2. Warrell, H. (2019). Malicious software attacks ‘spiralling out of control’, report warns. *Financial Times*. [Online]. 29 March. [Accessed 10 July 2023]. Available from: <https://www.ft.com/content/f3cc4243-5942-46d0-8d26-ee757c8f225f>
3. Hiscox. (2020). Hiscox cyber readiness report 2020. [Online]. [Accessed 10 July 2023]. Available from: https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF.
4. Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*. **11**(3), pp.431-448.
5. Garg, A., Curtis, J. and Halper, H. (2003a). The financial impact of IT security breaches: what do investors think? *Information Systems Security*. **12**(1), pp.22-33.
6. Garg, A., Curtis, J. and Halper, H. (2003b). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security*. **11**(2), pp.74-83.
7. Hovav, A. and D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*. **6**(2), pp.97-121.
8. Hovav, A. and D'Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*. **13**(3), pp.32-40.
9. Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*. **9**(1), pp.70-104.
10. Kamiya, S. (2018). *What is the Impact of Successful Cyberattacks on Target Firms? NBER Working Paper Series*.

Cambridge: National Bureau of Economic Research. Article no: 24409 [no pagination]

11.Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, 47(7), 87-92.

12.Hovav, A. and D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*. 6(2), pp.97-121.

13.Hovav, A., Han, J. and Kim, J. (2017). Market Reaction to Security Breach Announcements: Evidence from South Korea. *The Data Base for Advances in Information Systems*. 48(1), pp.11–52.

14.Gordon, L. A., Loeb, M. P. and Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*. 22(6), pp.461–485.

15.Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*. 56, pp.11–26.

16.Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud & Security*. 2017(4), pp.18–20.

17.Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719-749.

18.Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*. 49(2), pp.503–519.

19.Fisher, D. E., & Jordan, R. J. (1995). *Security analysis and portfolio management*. Simon & Schuster.

20.Pigou, A. C. (2013). *Theory of unemployment*. Routledge.

21.Marshall, A. (2013). *Principles of economics*. Springer.

22.Keynes, J. M. (1937). The general theory of employment. *The quarterly journal of economics*, 51(2), 209-223.

23.Jorgenson, D. W. (1963). Capital theory and investment behavior. *The American economic review*, 53(2), 247-259.

24.Dictionary, O. E. (1989). *Oxford english dictionary*. Simpson, Ja & Weiner, Esc, 3.

25.Rudnicka, E. K., Witkowski, W., & Kaliński, M. (2015). Towards the methodology for extending princeton wordnet. *Cognitive Studies| Études cognitives*, (15).

26.Швандар В.А., Базилевич А.И. Управление инвестиционными проектами – М.: ЮНИТИ, 2017. – 444 с.

27.Инвестиции: учебник для вузов [Текст] / Л.И.Юзвович [и др.]; под редакцией Л.И.Юзвович, С.А.Дегтярева, Е.Г.Князевой. – Екатеринбург: Издательство Уральского университета, 2016. – 543 с.

28.Knight, F. H. (1921). Risk, uncertainty and profit. *Hart, Schaffner and Marx*.

29.Markowitz, H. M. (2010). Portfolio theory: as I still see it. *Annu. Rev. Financ. Econ.*, 2(1), 1-23.

30.Nadhirin, N., & Husnurrosyidah, H. (2018). The Study of Fraud in Financial Institutions (Analysis of the Theory of Fraud Triangle in Perspective of Islamic Sharia). *Iqtishadia: Jurnal Kajian Ekonomi Dan Bisnis Islam STAIN Kudus*, 11(1), 195-220.

31.Авдийский, В. И. (2012). Национальная экономическая безопасность в условиях глобализации. *Международное публичное и частное право*, (2), 9-10.

32.Алферов, В. Н. (2011). Антикризисные механизмы финансовой стабилизации и развития организации. *Стратегические решения и риск-менеджмент*, (6), 78-83.

33.Безденежных, В. М. (2014). Стандарт обеспечения экономической безопасности хозяйствующего субъекта. *Экономика. налоги. право*, (4), 79-84.

34.Синявский, Н. Г. (2004). *Оценка бизнеса*. Финансы и статистика (ФС).

35.McKinsey. (2021). Новые модели работы: как сделать организацию эффективнее. (28 июля 2021 г.). Текст: электронный. – URL: <https://www.mckinsey.com/ru/our-insights/new-models-of-work-how-to-make-the-organization-more-efficient>.

36.Янченко, Е.В. Риски организации в условиях цифровизации экономики / Е.В. Янченко // Креативная экономика. – 2022. – No 6. Том 16. – С. 2239-2256. – ISSN 1994-6929.

37.Марамыгин, М. С., Чернова, Г. В., & Решетникова, Л. Г. (2019). Цифровая трансформация российского рынка финансовых услуг: тенденции и особенности. *Управленец*, 10(3), 70-82.

38.Аренков, И. А., Салихова, Я. Ю., & Сайфутдинов, А. А. (2021). Цифровая трансформация: направления исследований и цифровые риски. *Креативная экономика*, 15(7), 2757-2776.

39.Карпова, Е. Н., Чумаченко, Е. А., & Коновалов, А. А. (2022). Новые риски отмывания денег и финансирования терроризма в условиях цифровизации экономики. *Управленческий учет*, (3-2), 271-278.

40.Киуюцевская, А.М. Финтех: современные тенденции и вызовы для денежно-кредитной политики / А.М.Киуюцевская // Вопросы экономикию – 2019.- № 4. – СЮ137-151.- ISSN 0042-8736.

41.Маркова, О.М. Реализация операционного риска коммерческого банка в цифровой среде / О.М.Маркова // Финансовые рынки и банки. – 2020. - № 2. – С.63-68. – ISSN 2658-3917.

42.Орлова, Л.Н. Анализ существующих систем управления рисками в финансовых и нефинансовых организациях / Л.Н.Орлова, В.О.Одинцов, К.А.Санникова // Креативная экономика. – 2022. - № 4. Том 16. – С.1341-1358. – ISSN 1994-6929.

43.Токарев, К.К. Цифровизация банковского сектора экономики / К.К.Токарев, Т.П.Носова // Modern Science. – 2021. - № 4-1. – С.172-176. – ISSN 2414-9918.

44.What is Digital Risk? Definition and Protection Tactics. UpGuard: website. - [Online]. [Accessed 10 July 2024]. Available from <https://www.upguard.com/blog/digital-risk>

45.What is Digital Risk? Proofpoint: website. – Sunnyvaly. – [Online]. [Accessed 10 July 2024]. Available from: <https://www.proofpoint.com/us/threat-reference/digital-risk>.

46.Янченко, Е.В. Риски организации в условиях цифровизации экономики / Е.В. Янченко // Креативная экономика. – 2022. – No 6. Том 16. – С. 2239-2256. – ISSN 1994-6929.

47.Sorescu, A., Warren, N. L., & Ertekin, L. (2017). Event study methodology in the marketing literature: an overview. *Journal of the Academy of Marketing Science*, 45, 186-207.

48.Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of financial economics*, 8(3), 205-258.

49. Lubatkin, M., & Shrieves, R. E. (1986). Towards reconciliation of market performance measures to strategic management research. *Academy of Management Review*, 11(3), 497-512.
50. de Mortanges, C. P., & Rad, A. T. (1998). Marketing strategy and market value:: An event-study analysis. *European Management Journal*, 16(3), 365-371.
51. Delattre, E. (2007). Event study methodology in marketing. *Recherche et Applications en Marketing (English Edition)*, 22(2), 57-75.
52. Sorescu, A. (2017). Data-driven business model innovation. *Journal of Product Innovation Management*, 34(5), 691-696.
53. Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The adjustment of stock prices to new information. *International economic review*, 10(1), 1-21.
54. McWilliams, A. and Siegel, D. (1997). Event Studies in Management Research: Theoretical and Empirical Issues. *Academy of Management Journal*. 40(3), pp.626–657.
55. Cowan, A. R. (1992). Nonparametric event study tests. *Review of Quantitative Finance and accounting*, 2, 343-358.
56. Brown, S. J., & Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of financial economics*, 14(1), 3-31.
57. Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of financial economics*, 8(3), 205-258.
58. Fama, E. F. (1991). Efficient capital markets: II. *The journal of finance*, 46(5), 1575-1617.
59. Binder, J. (1998). The event study methodology since 1969. *Review of quantitative Finance and Accounting*, 11, 111-137.
60. McWilliams, T. P., & McWilliams, V. B. (2011). Another look at theoretical and empirical issues in event study methodology. *Journal of Applied Business Research (JABR)*, 16(3), 1.
61. Srinivasan, R., & Bharadwaj, S. (2004). Event studies in marketing strategy research. *Assessing marketing strategy performance*, 2004, 9-28.
62. Pynnönen, S. (2005). On regression based event study. *Acta Wasaensia*, 143(2), 327-354.
63. Binder, J. J. (1985). On the use of the multivariate regression model in event studies. *Journal of Accounting Research*, 370-383.

64. Peterson, P. P. (1989). Event studies: A review of issues and methodology. *Quarterly journal of business and economics*, 36-66.
65. MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of economic literature*. **35**(1), pp.13–39
66. Corrado, C. J. (2011). Event studies: A methodology review. *Accounting & Finance*, 51(1), 207-234.
67. Witte, J. A. (2022). *Investor reactions to political board appointments: an analysis of director specific attributes* (Doctoral dissertation).
68. Campbell, J. Y., Lo, A. W., MacKinlay, A. C., & Whitelaw, R. F. (1998). The econometrics of financial markets. *Macroeconomic Dynamics*, 2(4), 559-562.
69. Collins, D. W., & Dent, W. T. (1984). A comparison of alternative testing methodologies used in capital market research. *Journal of accounting research*, 48-84.
70. Bernard, V. L. (1987). Cross-sectional dependence and problems in inference in market-based accounting research. *Journal of Accounting Research*, 1-48.
71. Liu, D., Wang, C., Zhang, H., Yao, S., & Li, Z. (2023). Financial market imperfections and sensitivity of cash holdings to R&D investment: Evidence from chinese listed firms. *Research in International Business and Finance*, 66, 102025.
72. Goel, S, and Shawky, H.A. (2009). Estimating the market impact of security breach announcements on firm values. *Information and Management*. **46**(7), pp.404-410.
73. Gatzlaff, K. M. and McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*. **13**(1), pp.61-83.
74. Martin, K. D., Borah, A. and Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of marketing*. **81**(1), pp.36–58.
75. Jeong, C. Y., Lee, S.-Y. T. and Lim, J.-H. (2019). Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information and Management*. **56**(5), pp.681–95.
76. Janakiraman, R., Lim, J. H. and Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of marketing*. **82**(2), pp.85–105.

77. Martin, K. D. and Murphy, P. E. (2017). The Role of Data Privacy in Marketing. *Journal of the Academy of Marketing Science*. **45**(2), pp.135–155.

78. SIC-NAICS. (2021). SIC Code and NAICS Code Business List. [Online]. [Accessed 10 July 2021]. Available from: <http://siccode.com>

79. Chen, X., Bose, I., Leung, A. C. M. and Guo, C. (2011). Assessing the Severity of Phishing Attacks: A Hybrid Data Mining Approach. *Decision support systems*. **50**(4), pp.662–672.

80. Das, S., Mukhopadhyay, A. and Anand, M. (2012). Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. *Journal of Information Privacy and Security*. **8**(4), pp.27–55.

81. Gordon, L. A., Loeb, M. P. and Zhou, L. (2011). The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security*. **19**(1), pp.33–56.

82. Issayeva G.K., Zhussipova, E.E., Aitymbetova, A.N., Kuralbayeva, A.S., Abdykulova, D.B. (2023). The Impact of Cybersecurity Breaches on Firms' Market Value: the Case of the USA. *Economics: the strategy and practice*. **18**(4), pp.200-219.

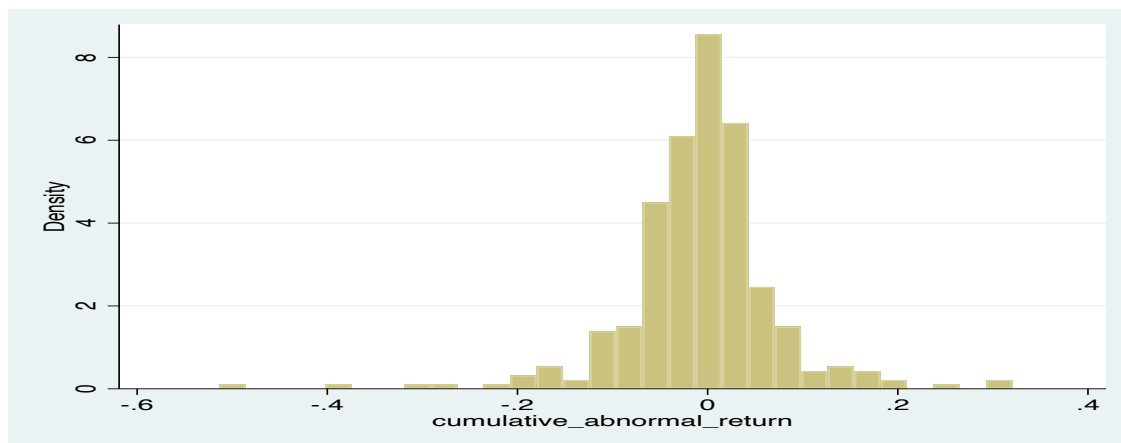
83. Caliendo, M., & Kopeinig, S. (2008). Some practical guidance for the implementation of propensity score matching. *Journal of economic surveys*, **22**(1), 31-72.

84. Li, X., Tripe, D. W., & Malone, C. B. (2017). Measuring bank risk: An exploration of z-score. *Available at SSRN 2823946*.

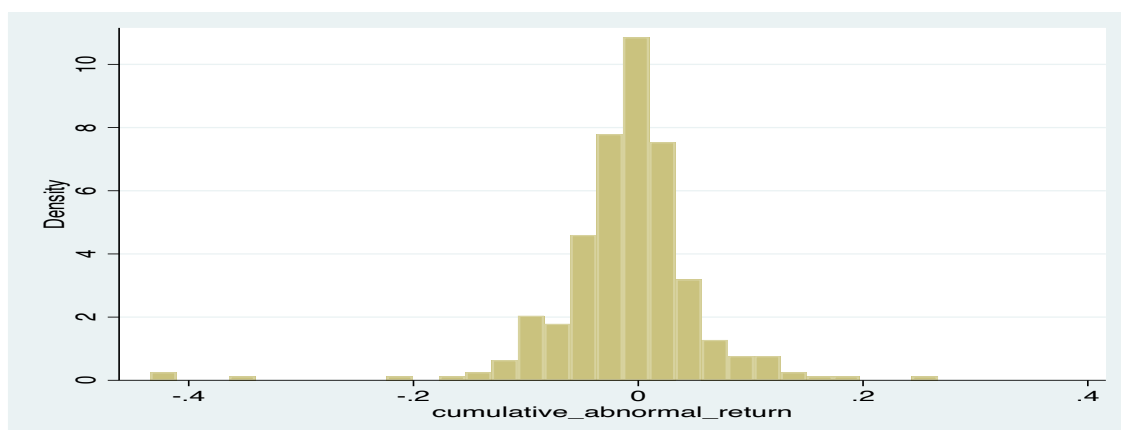
85. KPMG. (2022). Обеспечение безопасности новой бизнес-реальности: как бороться с киберпреступностью? Текст: электронный. — URL: <https://kpmg.com/kz/ru/home/insights/2021/11/cybersecurity.html>

Қосымша А

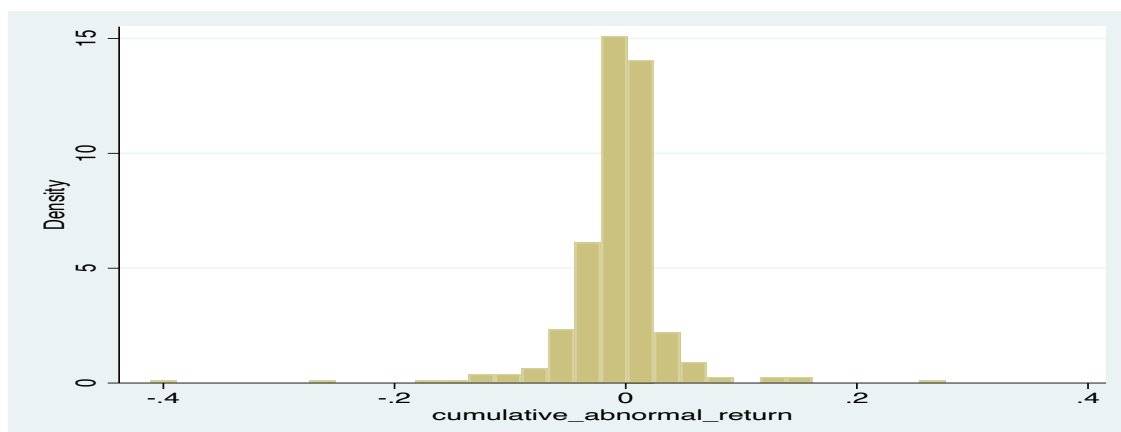
CAR орташа мәнінің үлестірілуі



5-күндік терезе



3-күндік терезе



1-күндік терезе

Сурет – 1, 3, 5-күндік терезелер үшін CAR орташа мәнінің
үлестірілуі

Қосымша В

t-тестінің нәтижелері

Кесте 1 - Өртүрлі көлемдегі фирмалардың CAR көрсеткішінің сипаттамалық статистикасы

	Шағын	Орташа	Ірі	Өте ірі
Айнымалы	CAR	CAR	CAR	CAR
Бақылаулар саны	85	83	84	85
Орташа	-.0141368**	.0006368	-.0092558***	-.0051315*
Стандартты қате	.0073355	.0048352	.0034123	.0031439
Стандартты ауытқу	.0676296	.044051	.0312741	.0289854
[95% сенімділік интервалы]	-.0287242	-.008982	-.0160427	-.0113835
	.0004505	.0102556	-.0024689	.0011205
t	-1.9272	0.1317	-2.7125	-1.6322
Еркіндік дәрежесі	84	82	83	84
Pr(T < t)	0.0287	0.5522	0.0041	0.0532
Ескертпе: автормен STATA бағдарламасында есептелген.				

Кесте 2 - Өртүрлі кибершабуылдың CAR көрсеткішінің сипаттамалық статистикасы

	Зиянды бағдарлама	Зиянды бағдарлама Фишинг	Қате конфигурация	Түрі көрсетілмеген	Фишинг	Бопсалайтын бағдарлама	Рұқсатсыз жүйеге кіру
Айнымалы	CAR	CAR	CAR	CAR	CAR	CAR	CAR
Бақылаулар саны	66	1	15	115	63	25	52
Орташа	.0015475	-.0236324	-.0048971	-.00538*	-.0101885**	-.0126298	-.0152148***
Стандартты қате	.0044322	-	.012665	.0034664	.0054929	.0206526	.0041327
Стандартты ауытқу	.0360074	-	.0490515	.0371733	.0435987	.1032629	.0298012
[95% сенімділік интервалы]	-.0073042	-	-.0320609	-.012247	-.0211687	-.0552546	-.0235115
	.0103992	-	.0222667	.001487	.0007917	.029995	-.0069181
t	0.3492	-	-0.3867	-1.5520	-1.8548	-0.6115	-3.6816
Еркіндік дәрежесі	65	0	14	114	63	24	51
Pr(T < t)	0.6359	-	0.3524	0.0617	0.0342	0.2733	0.0003
Ескертпе: автормен STATA бағдарламасында есептелген.							

Кесте 3 – Түрлі жария болған деректердің CAR көрсеткішінің сипаттамалық статистикасы

	Қаржылық	Түрі көрсетілмеген	Басқа да деректер	Жеке деректер
Айнымалы	CAR	CAR	CAR	CAR
Бақылаулар саны	105	15	53	164
Орташа	-.0125318***	.0128775	-.0117663*	-.0037571**
Стандартты қате	.004615	.0229671	.0088928	.0022187
Стандартты ауытқу	.0472901	.0889511	.0647407	.0284131
[95% сенімділік интервалы]	-.0216836	-.036382	-.0296111	-.0081381
	-.0033799	.062137	.0060784	.000624
t	-2.7154	0.5607	-1.3231	-1.6934
Еркіндік дәрежесі	104	14	52	163
Pr(T < t)	0.0039	0.7081	0.0958	0.0461
Ескертпе: автормен STATA бағдарламасында есептелген.				

Кесте 4 – Бір жылда қайталанатын және бір рет болатын кибершабуылдың CAR көрсеткішінің сипаттамалық статистикасы

	Жылына бірнеше рет кибершабуылға ұшыраған фирмалар	Жылына бір рет кибершабуылға ұшыраған фирмалар
Айнымалы	CAR	CAR
Бақылаулар саны	24	313
Орташа	-.0122959*	-.0066049***
Стандартты қате	.0072727	.0026292
Стандартты ауытқу	.0356288	.0465146
[95% сенімділік интервалы]	-.0273406	-.0117781
	.0027488	-.0014318
t	-1.6907	-2.5122
Еркіндік дәрежесі	23	312
Pr(T < t)	0.0522	0.0063
Ескертпе: автормен STATA бағдарламасында есептелген.		

Кесте 5 – Бірнеше және бір кибершабуылды өткерген фирмалардың CAR көрсеткішінің сипаттамалық статистикасы

	Кезең ішінде бірнеше кибершабуылға ұшыраған фирмалар	Кезең ішінде бір ғана кибершабуылға ұшыраған фирмалар
Айнымалы	CAR	CAR
Бақылаулар саны	89	248
Орташа	-.0094045***	-.006151**
Стандартты қате	.0037077	.0031208
Стандартты ауытқу	.0349784	.0491467
[95% сенімділік интервалы]	-.0167728	-.0122978
	-.0020362	-4.17e-06
t	-2.5365	-1.9710
Еркіндік дәрежесі	88	247
Pr(T < t)	0.0065	0.0249
Ескертпе: автормен STATA бағдарламасында есептелген.		

Исаева Гульмира Куздеуалиевна

**КИБЕР ҚАУІП-ҚАТЕРЛЕР ЖАҒДАЙЫНДА
КОМПАНИЯЛАРДЫҢ ҚАРЖЫ ЖӘНЕ
ИНВЕСТИЦИЯЛЫҚ САЯСАТЫН ЖЕТІЛДІРУ**

МОНОГРАФИЯ

Басуға 21.02.2025 ж. қол қойылды.

Көлемі 7,00 баспа табақ.

Таралымы 500 дана. Тапсырыс № 5

«Типография "GOLDYES"»

Шымкент қаласы, Иляев көш., н/с

Тел. +7 (707) 465 00 44

tipografia_goldyes@mail.ru

ISBN 978-601-7787-99-8

