bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі: KZ45VPY00102718
2026

БӨЛІМ: BUKETOV UNIVERSITY / UNIVER / СТУДЕНТ

Киберқауіпсіздік және ақпараттық жүйелерді қорғау: заманауи қатерлер мен қорғаныс әдістері

ЖАРИЯЛАНДЫ
28.05.2026

СІЛТЕМЕ
https://bilimger.kz/189004/

Тұрсынбай Мадияр Талғатұлы
Ғылыми жетекші: ***Қыдырәлі Дархан Досымбекұлы***
Математика және ақпараттық технологиялар факультеті
Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті, Қарағанды, Қазақстан

Аннотация

Бұл мақалада киберқауіпсіздік саласының заманауи жағдайы мен ақпараттық жүйелерді қорғаудың негізгі әдістері жан-жақты зерттелген. Мақалада кибершабуылдардың түрлері мен механизмдері, оның ішінде зиянды бағдарламалар, фишинг, қызмет көрсетуден бас тарту шабуылдары және әлеуметтік инженерия тәсілдері талданды. Ақпараттық жүйелерді қорғаудың техникалық және ұйымдастырушылық шаралары, шифрлау алгоритмдері, желіаралық қалқандар, кіруді анықтау жүйелері және нөлдік сенім архитектурасы егжей-тегжейлі қарастырылды. Зерттеу нәтижелері деректерді қорғаудың кешенді тәсілі ғана ұйымдарды заманауи киберқатерлерден сенімді қорғай алатынын дәлелдейді. Мақалада Қазақстандағы киберқауіпсіздік саласының даму деңгейі мен болашақ бағыттары да сараланған.

Кілт сөздер: киберқауіпсіздік, ақпараттық жүйелер, кибершабуыл, шифрлау, желіаралық қалқан, зиянды бағдарлама, фишинг, нөлдік сенім архитектурасы, деректерді қорғау, ақпараттық қауіпсіздік.

Кіріспе және өзектілік

Қазіргі заманда ақпараттық технологиялардың жедел дамуы экономика, денсаулық сақтау, білім беру, мемлекеттік басқару сияқты барлық салаларды түбегейлі өзгертті. Алайда бұл цифрлы трансформация жаңа тәуекелдерді де өмірге алып келді: ақпараттық жүйелерге кибершабуылдар жыл сайын күрделене түсуде, ал оның

экономикалық зияны да орасан зор. Халықаралық киберқауіпсіздік зерттеу орталықтарының деректері бойынша, 2023 жылы дүние жүзінде кибершабуылдардан болған шығын 8 триллион АҚШ долларынан асты.

Киберқауіпсіздік — ақпараттық жүйелерді, желілерді, бағдарламалар мен деректерді рұқсатсыз кіруден, зақымдаудан немесе шабуылдан қорғауға бағытталған іс-шаралар жиынтығы. Бұл — тек техникалық емес, сонымен бірге ұйымдастырушылық, заңдық және адамдық факторларды қамтитын кешенді тәртіп. Ақпараттық қауіпсіздіктің үш негізгі тірегі бар: деректердің құпиялылығы, тұтастығы және қол жетімділігі. Осы үш қасиеттің кез-келгеніне қатер төнсе, ол ақпараттық қауіпсіздік оқиғасы болып есептеледі.

Қазақстан Республикасында киберқауіпсіздікті қамтамасыз ету мемлекеттік деңгейде маңызды басымдыққа айналды. 2017 жылы қабылданған «Ақпараттандыру туралы» заң және 2023 жылға дейінгі «Цифрлы Қазақстан» мемлекеттік бағдарламасы ақпараттық инфрақұрылымды қорғауға ерекше назар аударады. Ұлттық ақпараттық қауіпсіздік үйлестіру орталығы еліміздің цифрлы кеңістігіндегі қатерлерді бақылап, тиісті шараларды үйлестіреді. Дегенмен, кибершабуылдардың саны мен күрделілігінің артуы бұл саладағы зерттеулердің өзектілігін күн санап арттырып отыр.

Ақпараттық жүйелерді қорғау мәселесі бірнеше себептен ерекше маңызды. Біріншіден, деректердің құны артты — жеке тұлғалардың, ұйымдардың және мемлекеттердің ақпараты бүгінде ең бағалы ресурстардың бірі болып табылады. Екіншіден, цифрлы тәуелділік өсті — заманауи экономика мен мемлекеттік басқару ақпараттық жүйелерсіз жұмыс істей алмайды. Үшіншіден, шабуылшылар да технологиялық жағынан жетіліп, жасанды интеллект пен автоматтандыру арқылы шабуылдарды жеделдетті. Осы жағдайда ақпараттық жүйелерді қорғау стратегиялары мен технологияларын жүйелі зерттеу аса қажетті болып отыр.

Осы мақалада киберқауіпсіздік саласының негізгі ұғымдары, шабуылдардың жіктелуі, қолданылатын қорғаныс технологиялары мен Қазақстандағы саланың даму бағыттары кешенді түрде қарастырылады. Зерттеу мақсаты — ақпараттық жүйелерді қорғаудың тиімді әдістерін жүйелеп, практикалық ұсынымдар жасау.

21Кибершабуылдардың түрлері мен механизмдері

1.1 ЗИЯНДЫ БАҒДАРЛАМАЛАР

Зиянды бағдарламалар — жүйеге зиян келтіру мақсатында жасалған бағдарламалық

қамтамасыз ету түрлері. Олардың ең кең тараған түрлеріне вирустар, трояндар, төлем талап ететін бағдарламалар, тыңшы бағдарламалар және желілік құрттар жатады. Вирустар заңды бағдарламаларға ендіріліп, орындалған кезде таралады; трояндар пайдалы бағдарлама ретінде жасырынып, пайдаланушыны алдайды. Желілік құрттар пайдаланушының әрекетінсіз-ақ желі арқылы автоматты таралуымен ерекшеленеді.

Төлем талап ететін бағдарламалар соңғы жылдары ерекше қауіпті қатерге айналды. Бұл бағдарламалар жәбірленушінің файлдарын шифрлап, оларды ашу үшін криптовалюта түрінде төлем талап етеді. 2021 жылы АҚШ-тағы Colonial Pipeline компаниясына жасалған шабуыл елдің отын тасымалдау инфрақұрылымын тоқтатып, 4,4 миллион доллар төлем алуға мәжбүр етті. Ірі ауруханалар, мемлекеттік мекемелер мен инфрақұрылымдық объектілер осындай шабуылдардың басты нысанасына айналып отыр.

1.2 ФИШИНГ ЖӘНЕ ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ

Фишинг — пайдаланушыны алдап, оның кіру деректерін, банктік ақпаратын немесе жеке мәліметтерін ұрлауға бағытталған шабуыл түрі. Шабуылшылар сенімді ұйымдардың — банктер, мемлекеттік органдар, электрондық пошта қызметтері — атынан жалған хабарламалар жіберіп, жасанды сайттарға бағыттайды. Нысандалған фишинг нақты тұлғаға арналып жасалады: алдаушы хаттар адресаттың аты-жөнін, лауазымын және ұйымдық деректерін пайдаланып, сенімді болып көрінеді.

Әлеуметтік инженерия адамдардың психологиялық осалдықтарын — сенімділік, қорқыныш, асығыстық — пайдалану арқылы жүйеге кіруді немесе ақпаратты алуды мақсат етеді. Ол техникалық шабуылдарға қарағанда анағұрлым қауіпті, өйткені ең күшті техникалық қорғаныс та адамдық факторды толығымен жоя алмайды. Зерттеулер бойынша, жалпы кибершабуылдардың 85 пайызында адамдық фактор шешуші рөл атқарады. Осыған байланысты қызметкерлерді тұрақты оқыту мен ақпараттық қауіпсіздік мәдениетін қалыптастыру маңызды болып табылады.

1.3 ҚЫЗМЕТ КӨРСЕТУДЕН БАС ТАРТУ ШАБУЫЛДАРЫ ЖӘНЕ ЖЕТІЛДІРІЛГЕН ТҰРАҚТЫ ҚАТЕРЛЕР

Қызмет көрсетуден бас тарту шабуылдары мақсаттық жүйені немесе желіні сұраулармен толтырып, заңды пайдаланушылардың қызметке қол жеткізуін мүмкін емес етуді мақсат етеді. Таратылған нұсқасы бірмезгілде жүздеген немесе мыңдаған жеке компьютерлерден шабуыл жасайды — бұл шабуылды анықтауды да, тойтаруды да қиындатады. 2016 жылы болған тарихи шабуыл интернет инфрақұрылымының маңызды бөлігін тоқтатып, Twitter, Netflix, Reddit сияқты алпауыт платформалардың жұмысын бірнеше сағатқа үзді.

Жетілдірілген тұрақты қатерлер — мемлекеттік органдармен байланысты немесе жоғары дәрежелі техникалық мүмкіндіктері бар ұйымдар жүргізетін ұзақ мерзімді, мақсатты кибершабуылдар. Олар мақсатты жүйеге ұзақ уақыт байқаусыз кіріп, құпия деректерді жинайды немесе инфрақұрылымды бақылауға алады. Мұндай шабуылдар кейде жылдар бойы анықталмай жүреді; олар мемлекеттік ақпаратты, зияткерлік меншікті немесе стратегиялық инфрақұрылымды нысана алады.

2. Ақпараттық жүйелерді қорғау технологиялары мен болашақ бағыттары

2.1 ШИФРЛАУ ЖӘНЕ КРИПТОГРАФИЯЛЫҚ ҚОРҒАНЫС

Шифрлау — деректерді рұқсатсыз оқудан қорғаудың негізгі криптографиялық әдісі. Симметриялық шифрлауда деректерді шифрлау мен шешу үшін бір кілт қолданылады; асимметриялық шифрлауда ашық және жабық кілт жұбы пайдаланылады. Заманауи деректерді қорғау стандарты 256-биттік кілтпен жұмыс істейді және оны бүгінгі ең қуатты компьютерлермен де бұзу мүмкін емес — тіпті теориялық есеппен ғаламның өмір сүру мерзімі де жетпейді. Ашық кілт инфрақұрылымы интернеттегі қауіпсіз байланыстың негізін қалайды, сандық сертификаттар мен электрондық қолтаңбаларды мүмкін етеді.

Алайда кванттық есептеу технологиясының дамуы классикалық криптографияға елеулі қатер төндіруде. Кванттық компьютерлер асимметриялық шифрлау алгоритмдерін теориялық тұрғыдан бұза алатын мүмкіндікке ие. Осыған байланысты АҚШ стандарттар және технологиялар ұлттық институты кванттық компьютерлерге төзімді жаңа криптографиялық стандарттарды 2024 жылы ресми бекітті. Қазақстан да ұлттық ақпараттық қауіпсіздік инфрақұрылымын осы жаңа стандарттарға бейімдеу бағытында жұмыстар жүргізуі тиіс.

2.2 ЖЕЛІНІ ҚОРҒАУ ТЕХНОЛОГИЯЛАРЫ МЕН НӨЛДІК СЕНІМ АРХИТЕКТУРАСЫ

Желіаралық қалқандар желі трафигін алдын ала белгіленген ережелер негізінде сүзіп, рұқсатсыз байланыстарды бөгейді. Дәстүрлі желіаралық қалқандар тек порт пен хаттама деңгейінде жұмыс істесе, заманауи терең пакет талдау технологиясы хаттамаларды ішінара оқып, зиянды мазмұнды анықтайды. Кіруді анықтау және алдын алу жүйелері желі трафигі мен жүйелік журналдарды үздіксіз талдап, күдікті іс-әрекеттерді нақты уақыт режимінде анықтайды. Осы жүйелердің тиімділігі сигнатураға

негізделген және аномалияны анықтау тәсілдерін бірге қолдануда жатыр.

Нөлдік сенім архитектурасы — «ешкімге, ешнәрсеге сенбе, бәрін тексер» қағидасына негізделген қауіпсіздік тәсілі. Дәстүрлі қорғаныс желінің ішіндегілерге сенімді деп қарайтын болса, нөлдік сенім моделі желіішіндегі немесе желіден тыс барлық пайдаланушыны, құрылғыны және байланысты тексеруді талап етеді. Бұл архитектура бірнеше деңгейлі аутентификацияны, ең аз артықшылық қағидасын және микросегментацияны бірге пайдаланады. Microsoft, Google сияқты технологиялық алпауыттар мен жетекші мемлекеттік органдар осы тәсілге біртіндеп көшуде.

2.3 ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕГІ ҚАУІПСІЗДІК ЖӘНЕ БОЛАШАҚ БАҒЫТТАРЫ

Жасанды интеллект киберқауіпсіздік саласына екі жақты ықпал етуде: бір жағынан шабуылшылар оны жаңа шабуыл векторлары үшін пайдаланса, екінші жағынан қорғаушылар қауіптерді анықтауды автоматтандыру үшін қолданады. Машиналық оқыту алгоритмдері желі трафигіндегі аномалияларды, зиянды бағдарламаларды және бұрын белгісіз шабуыл үлгілерін дәстүрлі сигнатура негізіндегі жүйелерге қарағанда әлдеқайда жылдам анықтайды. Мінез-құлықтық талдау технологиясы пайдаланушы немесе жүйе мінез-құлқының күнделікті үлгісінен ауытқуды байқап, тіркелгі бұзылғанын ерте хабарлайды.

Бұлтты есептеу ортасындағы қауіпсіздік — заманауи киберқауіпсіздіктің маңызды бағыты. Деректерді бұлтқа көшіру жаңа қорғаныс мәселелерін туғызады: ортақ жауапкершілік моделі, деректер орнының белгісіздігі, бірнеше бұлт қызметін бір уақытта пайдалану. Бұлт қызмет провайдерлері мен пайдаланушы арасындағы жауапкершілікті анық бөлу, деректерді бұлтқа жүктемес бұрын шифрлау, бұлттағы кіруді бақылау мен журналдауды күшейту — осы салада ұсынылатын негізгі шаралар.

Киберқауіпсіздік саласының болашақ дамуы бірнеше негізгі бағытпен байланысты. Біріншіден, кванттық криптография — кванттық механика заңдарына негізделген абсолютті қауіпсіз байланыс. Екіншіден, деректерді сыртқа шығармай есептеу технологиясы — деректерді шифрланған күйінде өңдеуге мүмкіндік беретін жаңа тәсіл. Үшіншіден, таратылған бас кітап технологиясы — деректердің тұтастығын тексеру мен іздеуге мүмкіндік береді. Төртіншіден, интернет заттарының қауіпсіздігі — ақылды үй, өнеркәсіптік басқару жүйелері мен медициналық құрылғылар сияқты желіге қосылған миллиардтаған құрылғыларды қорғау.

Қазақстанда киберқауіпсіздік маманы жетіспеушілігі — саланың дамуындағы басты кедергілердің бірі. Дүние жүзінде 3,4 миллион киберқауіпсіздік маманына деген сұраныс өтелмей тұрғанда, еліміз де осы мамандар тапшылығынан зардап шегуде. Жоғары оқу орындарында киберқауіпсіздік бағдарламаларын кеңейту, практикалық дағдыларға

бағытталған оқу зертханаларын ашу, халықаралық сертификаттауды қолдау — осы бағыттарда жүйелі жұмыс жүргізу еліміздің цифрлы болашағын қамтамасыз ету үшін аса маңызды.

Пайдаланылған әдебиеттер тізімі

1. *Андерсон Р. Қауіпсіздік инженериясы: сенімді таратылған жүйелерді жасау нұсқаулығы. — Вили баспасы, 2020. — 1232-бет.*
2. *Стэллингс У. Криптография және желілік қауіпсіздік: принциптер мен тәжірибе. — 8-басылым. — Пирсон баспасы, 2019. — 768-бет.*
3. *Кимерлинг Б. Жетілдірілген тұрақты қатерлер: мемлекет демеушілігіндегі кибершабуылдар. — Компьютерлік қауіпсіздік журналы, 29(4)-том, 2021. — 401–425-беттер.*
4. *Соломон М., Кляйн Г. Киберқауіпсіздікке кіріспе. — 3-басылым. — Джонс және Бартлетт баспасы, 2022. — 544-бет.*
5. *Чапл М., Стюарт Дж. Ақпараттық жүйе қауіпсіздігі кәсіби маманының оқу нұсқаулығы. — Вили баспасы, 2021. — 1056-бет.*
6. *Нист стандарттар бюросы. Нөлдік сенім архитектурасы туралы арнайы жарияланым. — АҚШ Ұлттық стандарттар және технологиялар институты, 2020.*
7. *Гарднер Р. Бұлттық есептеудегі қауіпсіздік: негіздер мен озық тәжірибелер. — Еуропалық киберқауіпсіздік журналы, 7(2)-том, 2023. — 88–105-беттер.*
8. *Вирен К., Лохуйс Дж. Жасанды интеллект және машиналық оқыту арқылы қауіп анықтау. — Халықаралық ақпараттық қауіпсіздік конференциясы материалдары, 2022. — 315–329-беттер.*
9. *Қазақстан Республикасы Үкіметі. Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету тұжырымдамасы 2023–2027 жж. — Астана, 2023.*
10. *Рахымбеков А., Сейіт Б. Қазақстандағы ақпараттық инфрақұрылымды кибершабуылдардан қорғау мәселелері. — Қарағанды университетінің хабаршысы, 3-шығарылым, 2022. — 95–108-беттер.*

ҚМ АА Куәлік нөмірі: **KZ45VPY00102718** — ҚР Мәдениет және Ақпарат министрлігі