ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті» коммерциялық емес АҚ
Ақпараттық технологиялар институты
Ақпараттық жүйелер және киберқауіпсіздік кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
PhD
_____ А.К. Мукашева
«____» _____ 2021 ж.

МАГИСТЕРЛІК ДИССЕРТАЦИЯ

Тақырыбы: «Көліктік ақпараттық жүйеде кибершабуылды танудың моделі мен алгоритмін жасау»

Мамандығы: 7М06102 – «Ақпараттық жүйелер»

Орындаған: Зтелеу Ш.С. Тобы: МИСнк-19-2
Ғылыми жетекші: PhD, аға оқытушы Мукашева А.К.

Кеңесшілер:
Программалық қамтама бөлімі: PhD, аға оқытушы_____А.К. Мукашева
«____» _____ 2021 ж.

Норма бақылаушы: аға оқытушы_____ Б.А. Тулегенова
«____» _____ 2021 ж.

Сын-пікір беруші: профессор_____ Б.К. Жузбаевна
«____» _____ 2021 ж.

Алматы 2021ж

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті» коммерциялық емес АҚ

Ақпараттық технологиялар институты

Ақпараттық жүйелер және киберқауіпсіздік кафедрасы

Мамандығы 7М06102 – «Ақпараттық жүйелер»

Диссертациялық жұмысты орындауға берілген
ТАПСЫРМА

Білім алушы Зтелеу Шыңғыс Серікұлы

Жұмыстың тақырыбы: Көліктік ақпараттық жүйеде кибершабуылды танудың моделі мен алгоритмін жасау.

2020 жылғы «27» қазан №217 университет бұйрығымен бекітілген.

Аяқталған жұмысты тапсыру мерзімі: «10» маусым 2021 ж.

Жоба бойынша бастапқы деректер (зерттеудің (жобалаудың) нәтижелерінің талап етілетін параметірлері және объектінің бастапқы деректері):

Диссертациялық жұмыста қарастырылатын сұрақтар тізімі немесе диссертация жұмысының қысқаша мазмұны:
а) талдау бөлімі;
б) жобалау бөлімі;
в) жобаны жүзеге асыру бөлімі;

Графикалық материялдардың тізімі (қажетті сызбаларды көрсете отырып): 2 кесте, 57 иллюстрация келтірілген.

Негізгі ұсынылатын әдебиеттер:
1. J.Rubina, Parveen. Neural networks in cyber security.-2017
2. Муханова А.А. Классификация угроз и уязвимостейинформационной безопасности в корпоративных системах - 2013
3. Талалаев А.А., Тищенко И.П., Фраленко В.П., Емельянова Ю.Г.- Нейсетевая технология обнаружения сетевых атак на информационные ресурсы - 2011

4. Павлов В.В. Локальная сеть как инструмент информационной безопасности // Информация-Коммуникация-Общество - 2017

Диссертациялық жұмыс бөлімдеріне қатысты белгіленген кеңес берушілер

Бөлімдер	Кеңесшілер	Мерзімі	Қолы
Программалық қамтама	Мукашева А.К	11.06.2021	
Норма бақылау	Тулегенова Б.А.	11.06.2021	

Диссертацияны дайындау кестесі

Бөлімдердің атауы, әзірленетін мәселелер тізімі	Ғылыми жетекшіге ұсыну мерзімі	Ескерту
Жұмыстың талдау бөлімі		
Жұмыстың жобалау бөлімі		
Жобаны жүзеге асыру бөлімі		

Тапсырманың берілген күні «__» _____ 20__ ж.

Кафедра меңгерушісі _____ А.К. Мукашева

Жұмыстың ғылыми жетекшісі _____ А.К. Мукашева

Тапсырманы орындауға алған білім алушы _____ Ш.С. Зтелеу

Аңдатпа

Диссертациялық жұмыста көліктік саладағы ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды анықтауға жүйелерін әзірлеу жұмыстары талдау нәтижесінде олардың осы жүйелерді дамытудың негізгі жолдарының бірі жасанды нейрондық желілер теориясының заманауи шешімдеріне негізделген желілік трафикті талдау әдістерін енгізу болып табылады.

Диссертациялық жұмысты орындау нәтижесінде мынадай міндеттер шешілді:

- Ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды танудың нейрондық желілік құралдарының мүмкіндіктеріне талдау жасалды;
- Нейрондық желі модельдері және желілік кибершабуылдарды тану әдістері жасалды;
- Желілік кибершабуылдарды танудың алгоритмі жасалды.

Аннотация

Диссертационная работа посвящена выявлению кибератак на сетевые ресурсы информационных систем в транспортной сфере одним из основных путей развития этих систем является внедрение методов анализа сетевого трафика, основанных на современных решениях теории искусственных нейронных сетей.

В результате выполнения диссертационной работы были решены следующие задачи:

- Проведен анализ возможностей нейронных сетевых средств распознавания кибератак на сетевые ресурсы информационных систем;
- Разработаны модели нейронных сетей и методы распознавания сетевых кибератак;
- Разработан алгоритм распознавания сетевых кибератак.

ANNOTATION

Dissertation work on the development of systems for detecting cyber attacks on network resources of Information Systems in the transport industry as a result of their analysis, one of the main ways to develop these systems is to introduce methods for analyzing network traffic based on modern solutions of the theory of artificial neural networks.

As a result of the dissertation work, the following tasks were solved::

- Analysis of the capabilities of neural network tools for recognizing cyber attacks on network resources of Information Systems;
- Neural network models and methods for recognizing network cyber attacks have been developed;
- An algorithm for recognizing network cyber attacks has been developed.

Әдістемелер мен қысқартулар

АЖ	Ақпараттық Жүйе
IOT	Internet Of Things
ANN	Artificial neural network
SMB	Server Message Block
DDOS	Distributed Denial of Service
KDD	Knowledge Discovery in Databases
COF	Connectivity-Based Outlier Factor
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
INFLO	Influenced Outlierness
FTP	File Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
LOCI	Local Correlation Integral
CPU	Central Processing Unit
IO	Information Operation
FLDS	Fast Local Density Score
ЛВС	Лока́лды есептеуіш желі
LOF	Local Outlier Factor
НСМ	Нейрожелілік модель

Мазмұны

КІРІСПЕ 6
1 АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӨЗЕКТІЛІГІ..... 7
1.1 Ақпараттық қауіпсіздік ұғымы 7
1.2 Көлік саласындағы киберқауіпсіздік 13
1.3 Қазақстанның көлік саласындағы киберқауіпсіздік проблемалары 16
2 ЖЕЛІЛІК КИБЕРШАБУЫЛДАРҒА ҚАРСЫ ТҰРУ ПРОЦЕСІН ТАЛДАУ... 18
2.1 Желілік қауіптерді талдау 18
2.2 Кибершабуылдарға қарсы нейрондық желінің тиімділігін қамтамасыз етудің тұжырымдамалық моделі 20
3 КИБЕРШАБУЫЛДАРДЫ ТАНУ НЕЙРОНДЫҚ ЖЕЛІ МОДЕЛЬДЕРІН ЖӘНЕ АЛГОРИТМДЕРІН ЖАСАУ..... 24
3.1 Сараптамалық білімді қолдана отырып, желілік кибершабуылдарға қарсы тұрудың нейрондық желілік моделі 24
3.2 FLDS аномалиясын анықтау алгоритмін жасау..... 31
ҚОРЫТЫНДЫ..... 39
ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ 40

Кіріспе

Қазіргі уақытта адамзат қоғамының барлық салаларында компьютерлік желілерді кеңінен қолдану нәтижесінде ақпараттық кеңістіктің қауіпсіздігін қамтамасыз ету күрделене түсуде. Сондықтан компьютерлік желілерге шабуылдарды анықтау міндеті, әрі ең өзекті мәселелердің бірі болып табылады. Көптеген қорғалған жүйелерде осалдықтар бар: бағдарламалық жасақтамаларда, операциялық жүйеде, веб-сайттарда, желілерде және байланыс құралдарында және т. б. Тіпті қазіргі уақыттаға көлектер және сол сияқты машиналардың өзі де интернет заттары арқылы жұмыс жасайды, және сол себепті оларды қорғау да маңызды мәселе болып табылады.

Компьютерлік жүйелерді қорғау саласындағы ең қиын міндеттердің бірі-қандай да ақпараттық жүйелерге шабуылдардың алдын алу. Қазіргі уақытта ақпараттық жүйелерге шабуылдардың толық қорғауға кепілдік берудің ешқандай жолы жоқ және оның басты себебі - компьютерлік жүйелердің дамуы, интернетті пайдаланушылар санының көбеюі және де киберқылмыскерлер қолданатын әдістердің үнемі жетілдірілуі. Сондықтан осы типтегі кибершабуылдарды диагностикалау мен алдын-алудың алгоритмдері мен әдістері өзекті.

Жұмыстың мақсаты – желілік трафикті және ақпараттық ортаның жай-күйі туралы деректерді талдау негізінде желілік шабуылдарды анықтау алгоритмдері мен әдістерін зерттеу; шабуылдарды анықтаудың адаптивті алгоритмін құруға қойылатын талаптарды әзірлеу болып табылады.

Энергетика, өнеркәсіп, байланыс және көлік, ірі мегаполистердің инфрақұрылымдық объектілерінде және т.б. сындарлы компьютерлік жүйелердің жаһандық дамуы киберқауіптердің, сондай-ақ техникалық компоненттер мен бағдарламалық қамтамасыз етудің осалдықтарының тұрақты мониторингін талап етеді. Киберқорғаныстың қолданыстағы әдістерінің жетілмегендігі, сондай-ақ кибершабуылдардың өзгеретін сипаты қауіпті жағдайға әкелуі мүмкін.

Кибершабуылдардан болатын зиянды болдырмаудың ең тиімді құралы-оларды уақтылы анықтау. Қабылданған қауіпсіздік шараларының нақты уақыт режимінде жұмыс істеуі, компьютерлік жүйенің жай-күйін ескеруі, шабуылдардың үнемі өзгеріп отыратын схемаларына жедел әрекет етуі. Бұл мәселені шешудің бір жолы-адаптивті алгоритмдерді қолдану.

Көлік саласына цифрлық технологиялардың кеңінен енгізілуіне байланысты ақпараттық қауіпсіздік проблемасы көлік қауіпсіздігін қамтамасыз етудің басым міндеттерінің біріне айналды. Ақпараттық көлік жүйелерін қорғау-кез келген дамыған ел үшін маңызды міндет.

Ақпараттық қауіпсіздік проблемасы трансшекаралық сипатқа ие, бірақ бұл ел ішінде қолданылатын ережелер кешенін әзірлеуді жоққа шығармайды. Сонымен қатар, шетелдік тәжірибені зерттеу осы саладағы ұлттық тәсілдерді қалыптастыру үшін өте пайдалы болуы мүмкін.

1 Ақпараттық қауіпсіздікті қамтамасыз ету өзектілігі

1.1 Ақпараттық қауіпсіздік ұғымы

"Ақпараттық қауіпсіздік" термині компьютерлік технологиялар мен компьютерлердің дамуымен пайда болды. Төменде ақпараттық қауіпсіздіктің екі анықтамасы берілген.

Ақпараттық қауіпсіздік – қоғамның ақпараттық ортасын азаматтардың, ұйымдардың, мемлекеттердің мүдделері үшін қалыптастыруды, пайдалануды және дамытуды қамтамасыз ететін қорғалу жағдайы.

Ақпараттық қауіпсіздік – ақпараттың өзіне, оның иелеріне немесе инфрақұрылымына залал келтіруі мүмкін кез келген кездейсоқ немесе зиянды әсерлерден ақпараттың және оны қолдайтын инфрақұрылымның қорғалуы.

Ақпараттық қауіпсіздік тұжырымдамасы үш негізгі ережеге негізделген:

– ақпараттың құпиялылығы (ағыл. confidentiality) - ақпаратқа қол жеткізуді оған құқығы бар субъектілер ғана жүзеге асыратын ақпараттың жай-күйі;
– ақпараттың тұтастығы (ағыл. integrity) - ақпаратты рұқсатсыз өзгертудің алдын алу;
– ақпараттың қолжетімділігі (ағыл. availability) - қолжетімділік құқығын алған пайдаланушылардан ақпаратты уақытша немесе тұрақты жасыруды болдырмау.

Ақпараттық қауіпсіздік, қолданылатын бағдарламалық жасақтаманың қауіпсіздігін, аппараттық және техникалық құралдардың қауіпсіздігін, байланыс арналарының қауіпсіздігін және басқаларын қамтиды.

Ақпараттық қауіпсіздікті қамтамасыз ету - іс-шаралар тізбесін қамтиды және ақпараттық қауіпсіздікті қамтамасыз ету жүйесін қалыптастырады. Ақпараттық қатынастардың субъектілері өздерінің ақпараттық қауіпсіздігін қамтамасыз етуге мүдделі, атап айтқанда:

- қажетті ақпарат пен автоматтандырылған сервистерге уақытылы қол жеткізу;
- ақпараттың дұрыстығы;
- ақпараттың құпиялылығы және оның тұтастығы;
- дезинформациядан қорғау (жалған ақпарат енгізу);
- ақпаратты заңсыз көбейтуден қорғау;
- ақпаратты өңдеу және беру процестерін үздіксіз бақылау және басқару мүмкіндігі.

Ақпараттық қатынастар субъектілеріне зиян тек жергілікті және жаһандық желілерден ғана емес, сонымен қатар тасымалдаушылардан белгілі бір ақпарат арқылы да келтірілуі мүмкін. Сондықтан ақпарат, кез келген ақпарат тасығыштар, ақпарат тасығыштар және оны өңдеу (беру) процестері ақпараттық қатынастардың қауіпсіздігін қамтамасыз ету мақсатында қорғалуға жататын объектілер ретінде қаралуға тиіс.

Ақпараттық қауіпсіздік қатерлері

Ақпараттық қауіпсіздікке тікелей немесе жанама зиян келтіруі мүмкін ақпаратқа, оның тасымалдаушыларына немесе өңдеу процестеріне әсер ететін ықтимал оқиға, құбылыс немесе процесс қауіп деп аталады.

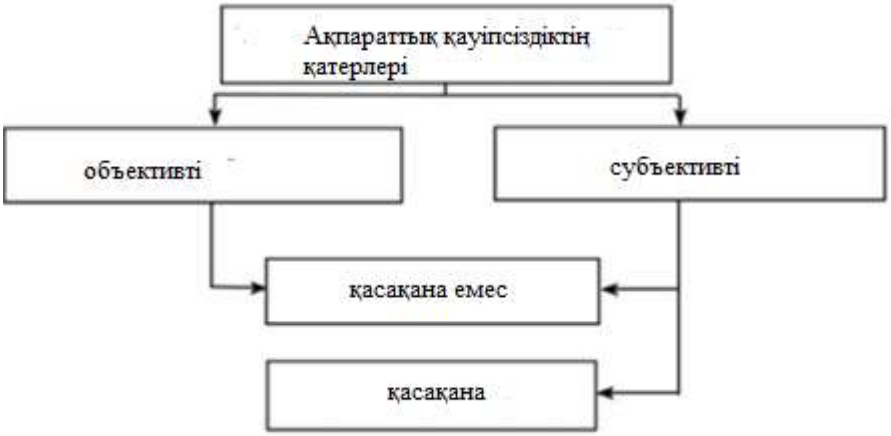
Ақпараттық қауіпсіздік қатерін іске асыру әрекеті шабуыл деп аталады, ал мұндай әрекетті жасаған субъект шабуылдаушы деп аталады.

Ақпарат қауіптерінің көздері мыналар болуы мүмкін:

- Жабдықтың (техникалық құралдардың) істен шығуы мен ақаулары;
- қаскүнемдер мен бұзушылардың қасақана әрекеттері;
- АЖ компоненттерін жобалау және әзірлеу кезіндегі қателер (аппараттық құралдар, ақпаратты өңдеу технологиялары, бағдарламалар және т. б.);
- операциялық қателер (пайдаланушылар, операторлар және басқа субъектілер);
- табиғи апаттар мен авариялар (су тасқыны, дауыл, жер сілкінісі, өрт және т.б.).

Көбінесе қауіп ақпараттық жүйелерді (АЖ) қорғауда осалдықтардың болуының салдары болып табылады, бірақ олардың кейбірін қандай да бір қателер мен есептеулер салдары деп санауға болмайды, олар қазіргі АЖ-ның табиғатына байланысты (мысалы, электр энергиясын өшіру немесе оның параметрлерінің диапазоннан тыс шығу қаупі).

Ықтимал қауіптерді екі субкласса бөлуге болады: объективті (табиғи) және субъективті (жасанды).



1.1-сурет – Ақпараттық қауіпсіздік қатерлерін жіктеу

Объективті - бұл АЖ-ға және оның элементтеріне объективті физикалық құбылыстар мен табиғи стихиялық процестердің әсерінен туындаған қауіптер.

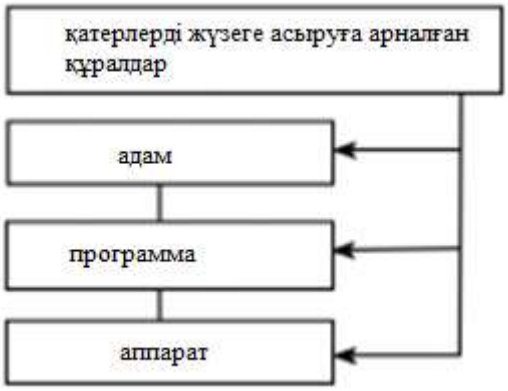
Субъективті - АЖ-ның адам қатысуымен болған қауіптері болып табылады. Олардың іс-әрекеттерінің мақсатына қарай оларды екі подкласса бөлуге болады: қасақана және байқаусызда.

Кездейсоқ - бұл идеологиялық көзқарастармен, кек алудан, шабуылдаушылардың пайдакүнемдік мақсаттарымен және т. б. байланысты қауіптер.

Кездейсоқ қауіптер жұмыста және ақпаратпен және бағдарламалық жасақтамамен, оның элементтерінің дизайнымен және т. б. қателіктерден туындайды.

Субъективті қауіптердің ішінде тіркелмеген бағдарламаларды заңсыз пайдалану, компьютерді вирустармен жұқтыру, қол жеткізуді басқару атрибуттарын (парольдер, шифрлау кілттері, жеке куәліктер, рұқсаттамалар және т.б.) ашу, беру немесе жоғалту ерекше орын алады. Сондай-ақ, жүйеде жұмыс істеу кезінде ұйымдастырушылық шектеулерді (белгіленген ережелерді) елемеу, қауіпсіздік құралдарын айналып өту, қауіпсіздік қызметкерлерінің қауіпсіздік құралдарын біліксіз пайдалану, орнату немесе заңсыз өшіру және т. б. орын алады.

Қауіпті жүзеге асыру үшін қолданылатын негізгі әсер ету құралдарының түріне сәйкес жүйеге ену мен ақпараттың ағып кетуінің барлық мүмкін арналарын үш топқа бөлуге болады. Мұндай өткізу құралдары мыналар болып табылады: субъект (тұлға), бағдарлама, аппараттық құралдар.



1.2-сурет – АЖ-ға шабуылдардың ену арналарын негізгі әсер ету түрі бойынша жіктеу

TCP / IP желілері қауіпсіздік жүйесі болмаған жағдайда, егер жергілікті желі ғаламдық желіге қосылған болса, жергілікті желінің ішінен де, сыртынан да көптеген шабуылдарға ұшырауы мүмкін. Кейбір шабуылдар пассивті болып табылады және желіде айналатын ақпаратты бақылауға дейін азаяды, ал басқалары белсенді, ақпараттың немесе желінің тұтастығын бұзуға немесе бұзуға бағытталған. TCP / IP желісіндегі шабуылдардың ең көп таралған түрлері:

- DDoS шабуылдары (қызмет көрсетуден бас тарту) ;
- деректердің зақымдануы - желілік құрттар;
- компьютерлік вирустар;
- трояндық жылқы бағдарламалары;

- спам - агрессивті жарнамалық жіберулер;
- фишинг және т.б.

Ақпараттық қауіпсіздік мәселелерінің түрлері

Бүгін, мүмкін, біз ғаламдық желіден ОЖ-ға енетін вирустарға тап болмайтын бірде-бір интернет пайдаланушысын таба алмайсыз. Сенімсіз сайттарға кіргенде немесе кез-келген ақпаратты жүктеген кезде, компьютерге бақытсыз "құрттың" түсу ықтималдығы жоғары, бұл кейіннен компьютердің аппараттық және техникалық құралдарының немесе жалпы жергілікті желінің болжанбайтын мінез-құлқына әкеледі.

Компьютерлік вирус - бұл орындалатын файлдарда, жүйелік диск аймағында, драйверлерде, құжаттарда және т.б. орналасқан бағдарламаларға өз көшірмелерін жаза (енгізе) алатын бағдарлама түрі. Сондай-ақ, ол вирус жұққан бағдарлама іске қосылған пайдаланушының деректерін зақымдауы немесе толығымен жоюы мүмкін.

Вирустарды бөлу әдеттегідей:

- әсер ету объектілері бойынша (файлдық вирустар, жүктеу вирустары, сценарий вирустары, желілік құрттар);
- зардап шеккен ОЖ және платформалар (DOS, Microsoft Windows, Unix, GNU / Linux, Java және т. б.);
- вирус қолданатын технологиялар бойынша (полиморфты вирустар, жасырын вирустар);
- вирус жазылған тіл бойынша;

Бағдарламаға вирустық көшірмені енгізу процесі (дискінің жүйелік аймағы және т.б.) инфекция деп аталады, ал вирус жұқтырған бағдарлама немесе басқа объект (вирус бар) вирус жұқтырған деп аталады.

Вирус жұқтырған бағдарлама жұмыс істей бастағанда, оның ішіндегі вирус алдымен бақылауға алынады. Вирус басқа бағдарламаларды немесе басқа нысандарды табады және "жұқтырады" және кез-келген байқаусызда әрекет етуі мүмкін. Содан кейін вирус басқаруды ол орналасқан бағдарламаға жібереді және ол әдеттегідей жұмыс істейді. Осылайша, сырттай, жұқтырған бағдарламаның жұмысы дезинфекцияланбаған жұмыс сияқты көрінеді. Алайда, вирус жұққан бағдарламаның әрбір іске қосылуымен пайдаланушының операциялық жүйесінде вирус бар бағдарламалар көбейіп келеді, бұл компьютердің істен шығуына әкеледі.

Желілік құрттар

Желілік құрттар әдетте зиянды бағдарламалар деп аталады, олардың негізгі мақсаты - әртүрлі желілік құрылғыларға тарату болып табылады. Файлдық немесе пакеттік құрттар деп аталатын көптеген желілік құрттар бар. Олар желілік пакеттер түрінде таратылады, тікелей компьютердің жадына еніп, сол жерде өз кодын іске қосады. Мұндай желілік құрттар операциялық жүйенің бағдарламалық жасақтамасында осалдықтарды пайдаланады.

Қауіпті файл түрлері:

- asx, bas, bat, cmd, com, crt, exe, inf, ins, js, msc, msi, pif, reg, scf, scr, vbs

Желілік құрт қалай жұмыс істейді.

1. Желілік құрт компьютерге енеді. Ол үшін әртүрлі компьютерлік және мобильді желілерді пайдаланады: электрондық пошта, IRC және файл алмасу (P2P, peer-to-peer, peer-to-peer, орталықтандырылмаған немесе peer-to-peer желілерінен) желілер, LAN, мобильді құрылғылар арасындағы деректер алмасу желілері және т. б. Көптеген желілік құрттар файлдар ретінде жасырылады: электрондық поштаға тіркеме, ICQ және IRC хабарламаларында веб немесе FTP ресурсында вирус жұққан файлға сілтеме және т. б.

2. Құрттың көшірмесі жасалып, іске қосылады.

3. Құрттың көшірмесі келесі құрылғыға көшуге тырысады: интернеттегі компьютерлер, жергілікті желілер және т. б.

Әдеттегі компьютерлік вирустар

Әдеттегі компьютерлік вирустар - бұл өз көшірмелерін жергілікті компьютердің ресурстарына таратады бағдарламалар:

- пайдаланушының кез-келген әрекетінде кодты келесі іске қосу;
- басқа компьютерлік ресурстарда одан әрі іске асыру.

Олар басқа компьютерлерге кіру үшін желілік қызметтерді пайдаланбайды. Вирустың көшірмесі қашықтағы компьютерлерге вирус жұқтырған объект басқа компьютерде іске қосылған жағдайда ғана жетеді, мысалы:

- қолжетімді дискілерді зақымдаған кезде вирус жалпы желілік ресурста орналасқан файлдарға енеді;
- вирус өзін алынбалы құралға немесе ондағы вирус жұққан файлдарға көшірді;
- пайдаланушы вирус жұқтырған файлмен электрондық хат жіберді.

Трояндар

Трояндық ат - шабуылдаушы ақпарат жинау, оны жою немесе өзгерту, компьютер жұмысын бұзу немесе оның ресурстарын қолайсыз мақсаттарда пайдалануы үшін қолданатын зиянды бағдарлама.

Трояндық ат вирустар сияқты өзін-өзі таратуға қабілетті емес; оны қолданушы қолмен немесе автоматты түрде бағдарлама немесе жәбірленушінің компьютерінде жұмыс істейтін операциялық жүйенің бөлігі іске қосады.

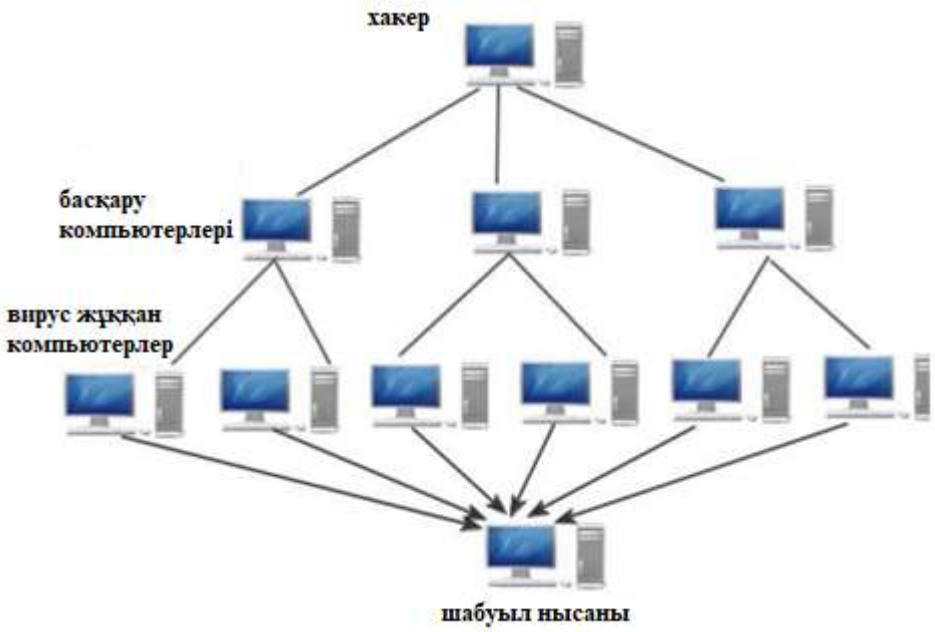
Бағдарлама файлы оны кез-келген басқа бағдарлама, басқа типтегі файл ретінде жасыратын немесе жай ғана іске қосылатын тартымды атау, белгіше және т.б. беретін қызмет атауы деп аталады. Трояндық ат қандай да бір дәрежеде жасырылған тапсырманы немесе деректер файлын еліктей алады. Трояндық ат вирустың модулі бола алады және өзінің көшірмелерін тарата алады.

Троянның мақсаты файлдарды жүктеу және жүктеп алу мүмкіндігі; жалған сайттарға, чаттарға немесе басқа тіркеу сайттарына апаратын жалған сілтемелерді көшіру; пайдаланушының араласуы; құнды немесе құпия деректерді ұрлау; вирустық шабуыл кезінде файлдарды шифрлау; вирустар сияқты басқа зиянды бағдарламаларды тарату.

Шабуылдар мен қарсы шабуылдар

Желілік шабуылдар шабуылға ұшыраған желілік ресурстарды пайдаланушыларға қызмет көрсетуден бас тартуға әкеледі. Желілік ресурсты түрлі зиянды бағдарламалармен өшіруге немесе зиянкес шабуылдаушы компьютерге көптеген сұраныстар жіберген кезде шамадан тыс жүктеуге болады. Бұл проблема қызмет көрсетуден бас тарту немесе DOS (Denial of Service) шабуылы деп аталады. Dos шабуылдарының жұмыс принципі 1.3 суретте көрсетілген.

Қарсы шаралар алдын алу шараларын қабылдаудан тұрады. Мысалы, жүйе шабуылдаушыға кіріс деректер пакеттерінің мекен-жайларын тексеру және күдікті мекен-жайлары бар пакеттерді тастау арқылы қызметке кіруге тыйым салады.



1.3- сурет – DoS шабуылдарының жұмыс істеу принципі.

Спам және фишинг

Спам (ағылш. Spam - "спам") - бұл алушылардың келісімінсіз жарнамалық хабарламалардың жаппай таратылуы. "Спам" термині 1993 жылдан басталады. Спам жіберушінің (спамердің) мақсаттары мен міндеттеріне байланысты коммерциялық ақпаратты немесе өзге де ақпаратты қамтуы мүмкін.

Әдетте спамерлер келесі схеманы қолданады: SMTP қосылымы хостқа орнатылады, оған поштаны кез-келген хостқа жіберуге рұқсат етіледі (Ашық пошта релесі). Оған көптеген адресаттармен және әдетте жіберушінің жалған мекен-жайымен хат жіберіледі. Хост-жәбірленуші алынған хабарламаны барлық алушыларға жібереді. Нәтижесінде спам жіберуге кететін

шығындарды алушылар мен қайта жіберу торабы көтереді. Интернет-провайдерлер спамға теріс әсер етеді, өйткені бұл олардың жүйелеріне айтарлықтай жүктеме және пайдаланушылар үшін қолайсыздықтар тудырады. Көптеген интернет-провайдерлер спам жіберетін деп саналатын ашық қайталаушылардан пошта қабылдауды өшіреді. Электрондық пошта жүйесі бір хабарламаны бір уақытта көптеген мекен-жайларға жіберу бір электрондық поштаны жіберумен бірдей болатындай етіп жасалған. Алушы осы пайдасыз хатты алуға жұмсаған уақыты үшін төлейді. Мұндай жаппай хабарламалар пошта серверлерін айтарлықтай жүктей алады, бұл маңызды поштаны алудың кешігуіне әкелуі мүмкін.

Фишинг (ағылш. phishing, fishing - балық аулау, fishing and password - пароль) - пайдаланушының сәйкестендіру деректерін алу мақсаты болып табылатын интернет-алаяқтықтың түрі. Бұған парольдерді, несие карталарының нөмірлерін, банктік шоттарды және басқа да құпия ақпаратты ұрлау кіреді.

Фишингтік шабуылдар барған сайын күрделі және әлеуметтік жобаланған болып келеді. Бірақ кез-келген жағдайда олар клиентті қорқытуға тырысады, оның жеке мәліметтерін беру үшін маңызды себеп ойлап табады. Әдетте, хабарламаларда қауіптер бар, мысалы, егер алушы хабарламада көрсетілген талаптарды орындамаса, есептік жазбаны бұғаттайды.

Мұндай шабуылдармен күресу үшін, ең алдымен, күмәнді хаттарға жауап бермеу керек, спам үшін поштаны тексеретін және мұндай хаттарды тікелей пошта серверінде жоятын арнайы сүзгі бағдарламаларын пайдаланған жөн.

1.2 Көлік саласындағы киберқауіпсіздік

Қосылған құрылғылар туралы ойласақ, көпшілігіміз компьютерлерді, телефондарды және планшеттерді – мүмкін ақылды теледидарлар мен үйдегі гаджеттерді қарастырамыз. Бірақ, біз көлік саласы туралы ойламаймыз. Алайда, егер біз жаңа модельді көлік жүргізетін болсақ, ол көптеген ішкі микрочиптер мен сыртқы сенсорларға сүйенеді, ал олар жай ғана жолдан шығады. Ақылды немесе автономды көліктерден бастап жаңа буынның GPS құрылғыларына дейін көлік индустриясы трансформациялық көлік технологиялары мен заттар интернеті (IoT) арқылы айтарлықтай өзгерістерге ұшырайды. Көлік секторы адамдар мен тауарлардың қозғалысын қолдайды және осы қозғалыстарды қамтамасыз ететін көлік құралдарының, инфрақұрылымдардың және операциялардың жиынтығын қамтиды. Көлік жүйесіне авиация, жолдар мен көпірлер, ішкі су жолдары, порттар, теміржол және транзит кіреді.

Көлік саласы кез-келген мемлекеттің экономикасы үшін өте маңызды және бұл жүйенің дұрыс жұмыс істемеуі айтарлықтай әлеуметтік-экономикалық салдарға әкелуі мүмкін. Цифрлық технологиялар көлік инфрақұрылымының функционалдығы мен тиімділігін жақсартқанымен,

кибер жүйелердің алдында да жоғары тәуекелге ие. Бұл дегеніміз, тұтастай алғанда, көлік секторы киберқауіпсіздік тәжірибесін жетілдіруді қажет етеді. Сенімді киберқауіпсіздік көлік жүйелерінің қауіпсіз және үздіксіз жұмыс істеуі және тасымалданатын адамдар мен тауарлардың қауіпсіздігі үшін қажет.

Ақпараттық технологиялармен өзара байланыстылық көлік инфрақұрылымының тиімділігі мен функционалдығын арттыруға мүмкіндік берді. Алайда, олар сонымен бірге желіде болуға байланысты қауіптің жоғарылауына әкелді. Қазіргі уақытта электрондық деректер активтердің және олармен байланысты инфрақұрылымның орналасқан жерін және жай-күйін бақылауға мүмкіндік береді. Сонымен қатар, ол ауа-райының қауіп-қатері, трафик және порттар мен шекаралардың жабылуы сияқты қоршаған орта факторларын бақылай және есеп бере алады. Өзара байланысты ақпараттық жүйелер құндылық тізбегінде неғұрлым көп жүрсе, компания соғұрлым осал болады. Авиакомпаниялар мен әуежай инфрақұрылымы, теміржол инфрақұрылымының иелері мен операторлары, логистикалық компаниялар және автомобиль өнеркәсібі - барлығы физикалық желілерді үзіп, жаппай бұзылуларға әкелуі мүмкін кибершабуылдарға бейім.

Кез-келген басқа сектордағыдай, үлкен сандық түрлендіру үлкен тәуекелді білдіреді. Көлік саласында физикалық және сандық желілерді басқаратын, көбінесе кең географиялық аудандарды қамтитын желілік көлік жүйелері арқылы берілетін мәліметтердің кең спектрі бар. Көптеген басқару жүйелері мен интернет құрылғылары желіге қосылған сайын, физикалық активтердің бұзылу ықтималдығын арттыратын осалдықтар пайда болады. Қауіптерді анықтау қауіп-қатер ландшафтын кеңейте отырып, көлік секторын құрайтын кең электронды және физикалық желілермен күрделене түседі. Көлік саласына әсер ететін оқиғалардың көптеген түрлері бар. Ең жиі кездесетін оқиғалар – зиянды деректердің ағуы. Зиянды деректерді бұзу барлық оқиғалардың 27,1 пайызын құрайды, бұл эпизод үшін орташа есеппен 330 000 доллар жоғалтуға әкеледі. Құпиялылыққа байланысты оқиғалар рұқсат етілмеген байланыс немесе ақпаратты ашу үшін 1,52 миллион доллар және рұқсат етілмеген деректерді жинау үшін 1,61 миллион доллар орташа шығындармен кибер оқиғалардың 22,9 пайызын құрайды. Киберинциденттердің барлық түрлерінің ішінен деректерді байқаусызда ашу ең жойқын болып табылады, зардап шеккен компанияларға әр оқиға үшін орташа есеппен 3,17 миллион доллар кетеді. Деректерді абайсызда ашу, әдетте, компаниялардың мемлекеттік жария ету ережелерін сақтамауынан болады, содан кейін айыппұлдарға, сөгістерге және беделін жоғалтуға әкеледі.

2015 жылы әлемдегі екінші ірі авиакомпания және АҚШ-тың мемлекеттік сапарлары үшін ірі мердігер United Airlines-ті Қытайдан келген мемлекет қаржыландыратын топ бұзды. Бұл жолы несие карталары басты назарда болмады. Рейстің барлық жолаушылары, оның ішінде олардың шығу тегі мен бағыттары туралы ақпарат бар ұшу манифесттері ұрланған, яғни

хакерлер тобы миллиондаған халықтың қозғалысы туралы мәліметтерді алды, ал олардың кейбіреулері жоғары дәрежелі жетекшілер болуы мүмкін.

Авиакомпаниялар, әрине, жалғыз мақсат емес. Сандық нарықтағы нарыққа шығу уақыты өндірушілерге, бөлшек сауда орындарына және клиенттерге тауарларды тез жеткізуге көбірек қысым жасайды, бұл дегеніміз, операциялық технологиялардың көлік секторы жеткізілімді тездететін желілік құрылғыларға көбірек тәуелді, сондықтан киберқауіптерге көбірек бейім.

Киберқылмыскерлер контейнерлік компаниялар мен контейнерлік порт операторларының технологияларын теріс пайдалануда. Операциялық технологиялар желілік жүйелерін бұзу арқылы қылмыскерлер жүк жүйелеріне контейнерлерді қайта бағыттау арқылы қол жеткізе алды, ал одан да жаманы, оларды желіден шығарып жіберді. Маңызды көлік инфрақұрылымын бұзудың ең сәтті әдісі – бұл Операциялық технология желісіне, атап айтқанда дәстүрлі оқшауланған операциялық технология орталарына қосылған IoT құрылғылары мен жүйелеріне бағытталған. Тұтынушылық деректерді жеткізілімге байланыстыру тауарлардың жеткізілуін бақылауға көмектеседі. Алайда, қазір бұл деректер бір тұтынушыға қауіп төндіреді.

Навигациялық және жүк жүйелерін спутниктік және интернет байланыстарына қосу кибер тәуекелдердің тез өсуіне әкеледі. 2013 жылы Остин университетінің студенті, 80 миллион долларлық яхта бортындағы экспериментке қатысып, кеменің навигациялық жүйесін сәтті алдап, оны жолдан шығарды. 2017 жылы АҚШ-тың ішкі қауіпсіздік департаменті өзінің авиациялық байланыс жүйесін қолдана отырып, 757 тұраққа қойылған коммерциялық ұшақты қашықтықтан бұза алатындығын көрсетті.

Кеңейтілген тұрақты қауіптер көлік саласы үшін айқын және нақты қауіп болып табылады. Мысалы, бұзылған билеттерді сату және жоспарлау жүйелері көлік тораптарын бірнеше сағат немесе күнге жабуы мүмкін. Авиакомпанияның қауіпсіздік сарапшылары күрделі кибершабуылдармен күресу үшін тасымалдаушылар кибер-өлтірулер тізбегі туралы көбірек ақпарат бөлісуі керек, бірақ бұл қазіргі уақытта мемлекеттік және жеке секторлар арасындағы ынтымақтастықты қажет етеді.

Кемелер немесе ұшақтар сияқты көлік өндірушілері үшін тыңшылық тағы бір басты мақсат болып табылады. Өндірушілерге бағытталған зиянды бағдарламалардың 47% - зы зияткерлік меншік пен коммерциялық құпияны ұрлауға арналған. Ұлттық өндіріс ғылымдары орталығының мәліметі бойынша, кибершабуыл нәтижесінде өндірушілердің 21% - зы зияткерлік меншігін жоғалтты, ал қылмыскерлер сүзген корпоративті деректердің 90% - дан астамы "құпия" немесе "меншікті" болып саналады.

Көлік секторына төнетін қауіп көп және күрделі. Кибер тәуекелдердің өсуіне қарамастан, көптеген Операциялық технологиялар операторлары әлі күнге дейін өз жүйелерін қорғау бойынша барабар шаралар қабылдаған жоқ. Шындық мынада, көптеген ұйымдар өздерінің коммуникациялары үшін Secure Shell немесе Transport Layer Security трафигін шифрлауды қолданбаған. Сонымен қатар, көптеген компаниялар өз қызметкерлері үшін рөлдік

бақылауды пайдаланбайды және жеткізушілер мен серіктестерге жоғары деңгейлі жүйеге қол жетімділік беру арқылы өз тәуекелдерін көбейтеді.

1.3 Қазақстанның көлік саласындағы киберқауіпсіздік проблемалары

Компьютерлердің дамуымен қазіргі әлем өзгерді. Енді бәрі компьютердің көмегімен немесе оның ең аз қатысуымен басқарылады. Компьютерлер биржаның жұмысына, электр станцияларының жұмысына, пойыздар мен ұшақтардың қозғалысына, автомобиль қозғалтқышының жұмысына жауап береді. Компьютерлер барлық жерде, олар бізге адам қателіктерінен арылуға көмектесті, өйткені компьютер ешқашан қателеспейді. Компьютер бәрін алдын-ала бағдарламаланған бағдарлама бойынша жасайды. Егер бағдарлама дұрыс болса, онда компьютер дұрыс әрекет етеді. Егер бағдарлама жақсы әзірленген болса, онда компьютер адамға, мысалы, атом станциясын басқаруға қарағанда әлдеқайда сенімді болады, себебі онда бір уақытта көптеген параметрлерді бақылау қажет.

Неліктен әлем жаһандық компьютерлендірумен қауіпсіз бола алмады? Бұл сұрақтың жауабы қарапайым: компьютерлер неғұрлым көп басқарылса, соғұрлым сол компьютерлерді хакерлік басқара алатын адамдар күшті болады.

Бүгінгі көшбасшылардың проблемасы - олар компьютерлік шабуылдардың не екенін нашар түсінеді. Ұзақ уақыт бойы "компьютерлік шабуыл" термині тар мамандарға ғана белгілі болды, вирустардан қорғау олардың міндеті болды. Кенеттен, соңғы онжылдықтарда компьютерлік сауаттылық ел басшыларына қажет болды. Неліктен? Бұл қарапайым-әуесқой студенттердің бағдарламаларынан вирустар елдердің геосаяси қарама-қайшылығында нақты қаруға айналды. Енді кибершабуылдарды түсіну әлемдегі кез-келген менеджер үшін міндетті білім болып табылады.

Көлік жүйесі киберқылмыскерлер тұрғысынан экономиканың ең осал секторларының бірі болып табылады. Ол жеткілікті қорғалған ба? Мұндай жүйелерге шабуыл жасау қаупі бар ма? Бұған мысалдар бар. 2016 жылы хакерлер Вьетнамның 22 әуежайына шабуыл жасады. Әуежайдағы дауыс зорайтқыштар кенеттен вьетнамдықтарға әдепсіздіктерді айқайлай бастады. Ақпараттық жүйелер Вьетнам халқы туралы қорлайтын бейнелер шығарды. Жолаушылардың жеке деректерінің гигабайтты құжаттары ұрланған. Бірақ басты нәтиже бұл емес еді. Вьетнамның көлік желісі кенеттен өзінің инвестициялық тартымдылығын жоғалтты. Инвесторлар бұдан былай мұндай шабуылдар қайталанбайды, болашақта ешкім жолаушылардың жеке деректерін ұрлап, жарияламайды деп сенбеді.

Біздің еліміздің ірі әуежайына шабуыл жасауды елестетіп көрейік. Шабуыл тек әуежайы бұзылған елге ғана әсер етпейді, бүкіл өңірдің көлік торабының беделі соққыға жығылады. Теміржол көлігі де ерекшелік емес. Жоғары жылдамдықпен қозғалатын қазіргі заманғы пойыздар да

компьютерлерге толы. 300-400 км/сағ жылдамдықпен адам жүздеген параметрлерді басқара алмайтыны анық, ал компьютер оны жасай алады. Егер вирус мұндай жүйеге араласса, онда ауыр зардаптар болатыны анық. Бірақ бұл жерде мүлдем басқа қауіпті атап өтуге болады. Қазіргі заманғы жүрдек пойыздар, дәлірек айтсақ, осы пойыздардағы қозғалтқыштар GSM модемдерімен жабдықталғанын аз адамдар біледі. Не үшін? Олардан диагностикалық ақпаратты біздің елімізде жоқ пойыз өндірушілерінің штаб-пәтеріне ресми түрде жібереді. Бірақ бұл модемдердегі деректер шифрланған түрде беріледі. Бұл қауіпсіздік мақсатында жасалатыны анық. Бірақ бұл қауіпсіз бе? Бұл деректерде тағы не болуы мүмкін? Арна бір бағытты немесе екі бағытты ма? Басқарушы командалар сырттан берілуі мүмкін бе? Бұл үлкен сұрақ.

АҚШ өзінің доктринасында кибершабуылға нақты әскери соққыны теңестіретіні бекер емес. Неге бұлай? Құқығы келтіруі мүмкін қарымта соққы. Бұл тек бір нәрсені білдіреді – кибершабуылдар тиімді және қауіпті құрал.

Көптеген эксперттер ең қымбат қорғаныс әдістерін қолдана отырып, кибершабуылдар мен киберқылмыстардың жаңа әдістерінен қорғануға болады деп санайды. Алайда, бұл жалған. Шабуылдаушылар шабуылдардың жаңа принциптерін жиі есекеріп отырады. Жаудың үнемі өзгеріп отыратын әдістеріне дайын болу үшін әрдайым дайын болу керек, икемді болу керек, парадигманы ұдайы өзгертіп керек.

Кибершабуылдарға қарсы күресте үйлестіру өте маңызды міндет. Осы саладағы жағдайды қарастыра отырып, біздегі көлік саласында үйлестіру жоқ деп сеніммен айтуға болады.

Осы сәтте мен көліктік киберқауіпсіздік саласындағы үйлестіру орталығын құру міндетін қозғағым келеді. Орталықтың міндеті көлік инфрақұрылымын кибершабуылдардан қорғау бойынша күш-жігерді шоғырландыру болуға тиіс. Орталық басқаруындағы негізгі функционалдық бөлімшелері бар коммерциялық емес бірлестік нысанында іске асырылуы мүмкін.

Орталықтың міндеттері қандай болуы керек? Олар келесідей қарастырылады:

Біріншіден, шығындарды орталықтандыру және бюджеттердің қайталануын болдырмау есебінен аса маңызды көлік инфрақұрылымдарының иелерін кибершабуылдардан қорғауға арналған шоғырландырылған шығындарды азайту қажет. Бүгінгі таңда біз осы саладағы ойыншылар арасындағы шоғырландырылған қатынастарды анық көре алмаймыз.

Қаражат не үшін қажет?

Бұл орталықтың екінші міндеті - инциденттерді зерттеу бойынша мамандандырылған зертхананы қамтитын көліктегі киберқауіпсіздік саласындағы бірыңғай құзыреттілік орталығын құру. Бұл жалпы қауіпсіздік деңгейін арттырады және ақпарат алмасуға мүмкіндік береді.

Орталық сонымен қатар сертификаттау зертханаларын дамытуға ықпал етуі керек. Бұл зертханада, ондағы мамандар бағдарламалық қамтамасыз етумен танысады және оны сынайды.

Сындарлы инфрақұрылым үшін автоматтандырылған жүйелердің кез келген жеткізілімі мамандандырылған сертификаттау зертханаларында жабдықты сынақтан өткізгеннен кейін ғана жүзеге асырылуы тиіс. Верификация үшін ашық бастапқы кодты алу аса маңызды объектілерді берудің негізгі критерийі болады. Мұндай зертханалар киберқылмыскерлердің өмірін едәуір қиындатады. Енді бәрі мұқият тексеріледі. Сондай-ақ, ірі компаниялардың біздің елге жеткізілімдерден ақша табуға деген ықыласы бірден пайда болады. Біз басқалардың еркіне тәуелді болмаймыз.

2 Желілік кибершабуылдарға қарсы тұру процесін талдау

2.1 Желілік қауіптерді талдау

Қазіргі уақытта көптеген көліктік саладағы ұйымдар өз жұмысында ақпараттық қауіпсіздік проблемаларына, атап айтқанда ақпараттық қауіптерге тап болады.

Компьютерлік жүйелерге зиян келтіретін процестер немесе оқиғалар ақпараттық қауіпсіздікке қауіп төндіреді. Бұл қауіптердің ішкі және сыртқы көздері бар.

Ақпараттық қауіптер болуы мүмкін:

- хакерлер мен зиянды бағдарламалардың әсері;
- әдейі ішкі диверсанттар, инсайдерлер;
- компания қызметкерлері тарапынан немқұрайлылық;
-өрттер, авариялар сияқты форс-мажорлық жағдайлар энергия жүйелері және т. б.

Компанияның ақпараттық жүйелеріне шабуыл жасаудың негізгі мақсаттарын атап өтейік:

- құнды ресурстарды игеру, мысалы, қаржылық ресурстарды ұрлау немесе есептеу құралдарына қол жеткізуді бақылау компанияның ішкі желісінің ресурстарына;
- қызметті шектеу мақсатында жосықсыз бәсекелестерге тапсырыс беру компаниялар, мысалы, ақпараттық жүйенің ақаулығы, корпоративтік клиенттермен және серіктестермен байланысты үзу.

Қауіпсіздікке төнетін қауіптердің екі түрі бар: табиғи және жасанды. Қауіпті табиғи құбылыстарға адамға тәуелді емес табиғи құбылыстар жатады, мысалы: дауыл, өрт және басқа да дүлей апаттар. Жасанды адамның қатысуына байланысты және қасақана және байқаусызда.

Абайсызда орын алған қауіп-қатерлер абайсызда және қызметкерлердің компанияның ішкі талаптарын сақтамауынан туындайды, бұл оларды жауапкершіліктен босатпайды.

Қасақана қауіптер арнайы жасалады. Оларға компанияның сыртында да, ішінде де шабуылдаушылардың (хакерлердің) шабуылдары кіреді. Сәтті шабуыл зиянкестерге құпия ақпаратты және компанияның жеке деректерін (ақша, бағалы қағаздар және т.б.) иеленуге көмектеседі.

Қашықтағы шабуылды анықтау оңай емес. Қиындық-мұндай шабуылдарды уақтылы анықтамау. Нәтижесінде хакерлердің сәтті шабуыл жасау мүмкіндігі артады.

Жергілікті желінің қауіпсіздігі брандмауэр қауіпсіздігінен ерекшеленеді, өйткені бұзушылықтар бірінші тіркелген пайдаланушылар болып табылады, өйткені негізінен жергілікті желінің деректер арналары бақыланатын аймақта орналасқан.

Желілік шабуылдар әртүрлі қауіп көздерінен туындайды. Мұндай көздерге мыналар жатады:

- қажетсіз мазмұн;
- рұқсатсыз кіру;
- ақпараттың тарауы;
- деректердің жоғалуы;
- алаяқтық;
- кибер соғыс және кибертерроризм.

Ең танымал көздердің бірі-қалаусыз мазмұн. Орынсыз мазмұн ақпаратты жою мен ұрлауға негізделген ықтимал зиянды бағдарламалар мен спамдарды қамтиды. Сондай-ақ, оларды пайдаланатын адамның жасына сәйкес келмейтін әртүрлі жағымсыз сайттар.

Рұқсат етілмеген бағдарламаларды пайдалану компанияның кез-келген маңызды ақпаратына қол жеткізу құқығын бұзуға әкеледі. Мұндай түрдегі ағып кетулер әртүрлі тәсілдермен жүзеге асырылуы мүмкін, мысалы, сайттарға шабуылдар, желі арқылы деректерді ұстап алу, пакеттік сниффер арқылы.

Деректердің жоғалуы-әртүрлі факторлардың әсерінен ақпараттың жоғалуы немесе жоғалуы. Бұл жағдайда ақпарат кездейсоқ немесе қасақана әрекеттер нәтижесінде жойылуы немесе бүлінуі мүмкін. Сіз олармен жұмыс істеу кезінде, сондай-ақ ақпаратты компьютерде, серверде немесе RAID массивтерінде сақтау кезінде деректерді жоғалтуыңыз мүмкін. Деректердің жоғалуы ақпараттың тұтастығын бұзу (бағдарламалық жасақтаманың бұзылуы) және аппараттық құралдың бұзылуы нәтижесінде пайда болуы мүмкін. Ақпараттың тұтастығын бұзу дегеніміз-қалпына келтіру процедураларын орындамай ақпаратты оқу / көшіру мүмкін болмайтын деректердің бүлінуін білдіреді. Егер тұтастық бұзылса, деректердің барлығын және бір бөлігін жоғалту қаупі, сондай-ақ бүкіл компьютерлік жүйелерге қауіп төнеді.

Құпия ақпараттың ағып кетуін екі үлкен топқа бөлуге болады: зиянды ұрлау (инсайдерлік тәуекелдерді қоса) және қызметкерлердің немқұрайлылығы немесе бақылауынан ағып кету. Тәжірибе көрсеткендей, құпия ақпараттың ағып кету жағдайларының басым көпшілігі

қызметкерлердің деректермен жұмыс жасау кезіндегі қателіктерінің нәтижесі болып табылады. Бұл инсайдерлік қауіп пен өнеркәсіптік тыңшылықты елемеуге болады дегенді білдірмейді, өйткені мұндай оқиғалардың үлесі өте аз. Егер ақпараттың ағып кетуінің нақты арналары туралы айтатын болсақ, онда соңғы бірнеше жылдағы ең өзекті деп атауға болады.

2.2 Кибершабуылдарға қарсы нейрондық желінің тиімділігін қамтамасыз етудің тұжырымдамалық моделі

Осы диссертациялық жұмыстың бірінші бөлімінде жүргізілген зерттеулердің нәтижелері ақпараттық жүйелердің желілік ресурстарына шабуылдарға қарсы тұру жүйесін дамытудағы маңызды бағыт және оларда кибершабуылдарды танудың нейрондық желісін енгізу болып табылады. Ол үшін операциямен бақыланатын ақпараттық жүйелердің жұмыс істеу параметрлерін талдау негізінде кибершабуылдарды нейрондық желіні танудың ғылыми мәселесін шешу қажет.

Тұжырымдалған мәселенің ерекшелігі - шабуылға қарсы тұрудың заманауи жүйелеріндегі іске асыру жағдайларына бейімделген нейрондық желі модельдері мен әдістерінің сипаттамаларын теориялық негіздеу қажеттілігі. Мұндай жағдайларға рұқсат етілген даму мерзімі, Еңбек ресурстарын тарту мүмкіндігі, нейрондық желілік модельдерді оқытуға қажетті шабуыл үлгілері мен қалыпты мінез-құлық үлгілерінің мәліметтер базасына қол жетімділік, ақпараттық жүйелердің функционалдық параметрлерін бақылау жүйесінің ерекшеліктері және шабуылдардан қорғау жүйелері тұтынатын есептеу ресурстарының рұқсат етілген көлемі жатады.

Тұжырымдалған мәселені шешудің бастапқы нүктесі ақпараттық жүйенің желілік ресурстарына кибершабуылдарды нейрондық желіні танудың тиімділігін қамтамасыз етудің тұжырымдамалық моделін жасау болды. Диссертацияның күтілетін практикалық нәтижесі бағдарламалық-аппараттық кешен құруды қарастыратындығына байланысты ақпараттық жүйенің желілік ресурстарына кибершабуылдарды нейрондық желіде тану процесінің тиімділігін анықтау үшін ақпараттық қауіпсіздік, компьютерлік және бағдарламалық инженерия саласындағы терминологияны қолдану қарастырылған.

Сондай-ақ, осы диссертациялық зерттеудің міндеті тұрғысынан тұжырымдамалық модель, ең алдымен, қазіргі заманғы ақпараттық жүйелердің қауіпсіздік деңгейін арттыру қажеттілігіне байланысты ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды тану процесіне тән себеп-салдарлық байланыстарды ресімдеуге арналған. Сонымен қатар, тұжырымдамалық модель мыналарды ескереді:

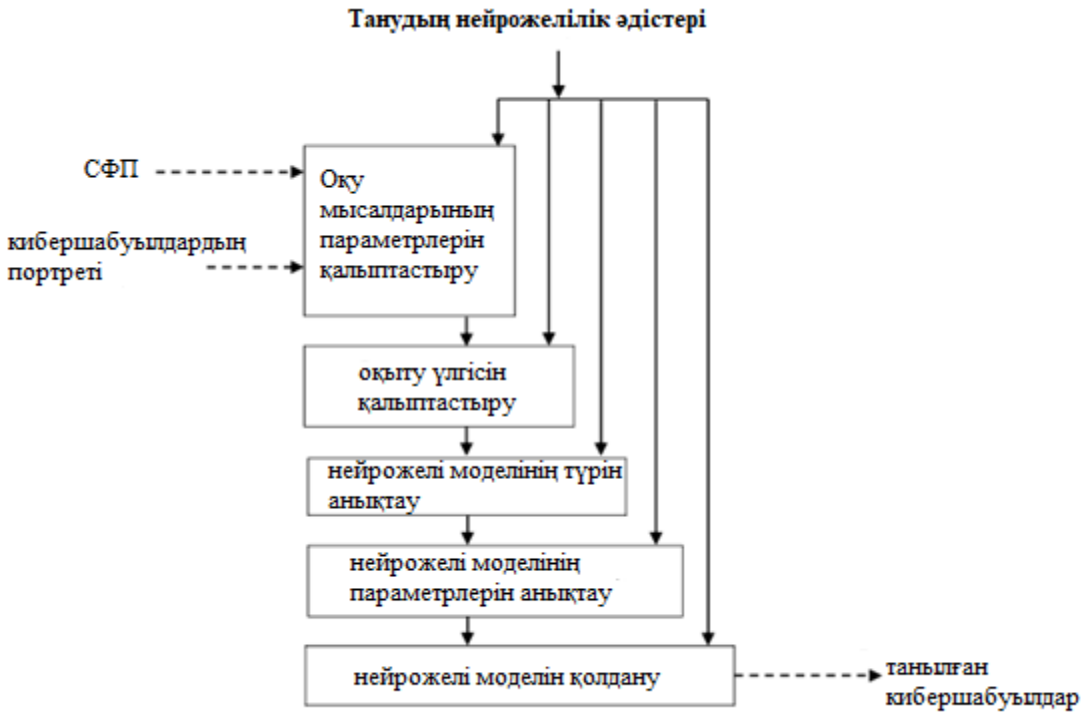
- Ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды танудың нейрондық желілерінің жұмыс істеу шарттары шабуылдардан қорғау жүйелерінің жекелеген бөліктері мен ақпараттық жүйелер компоненттерінің өзара әрекеттесу сипатымен анықталады.

- Кибершабуылдарды тану үшін нейрондық желі модельдерін тиімді пайдалануды енгізу қажеттілігі негізделген және оның жұмысын жақсартудың негізгі бағыттары анықталған.

- Нейрондық желі құралын басқару және оның өзгермелі айнымалыларын анықтау мүмкіндігі.

Нейрондық желі модельдерін қолданудың жалпы қабылданған технологиясын ескере отырып, тұжырымдамалық модель құрудың келесі кезеңінде кибершабуылдарды нейрондық желіні тану процесі оқу мысалдарының параметрлерін қалыптастыруды, оқу үлгісін қалыптастыруды, нейрондық желі модельдерінің түрі мен параметрлерін анықтауды және нейрондық желі модельдерін тануды қамтуы керек екендігі анықталды.

Бұл тұжырымды қолдану 2.1 суретте көрсетілген ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды нейрондық желіні танудың декомпозиция диаграммасын құруға мүмкіндік берді.



2.1-сурет – Кибершабуылдарды нейрондық желіні танудың декомпозиция схемасы

Бұл диаграмманың құрамдас бөліктерінің мақсаты келесідей:

- Оқу мысалдарының параметрлерін қалыптастыру-кибершабуылдардың әр түрі үшін кіріс және шығыс параметрлерінің жиынтығын және оларды кодтау әдісін анықтау.

- Оқыту үлгісін қалыптастыру - кибершабуыл стандарттарына сәйкес келетін оқыту мысалдарының осындай жиынтығын анықтау. Мысалдардың

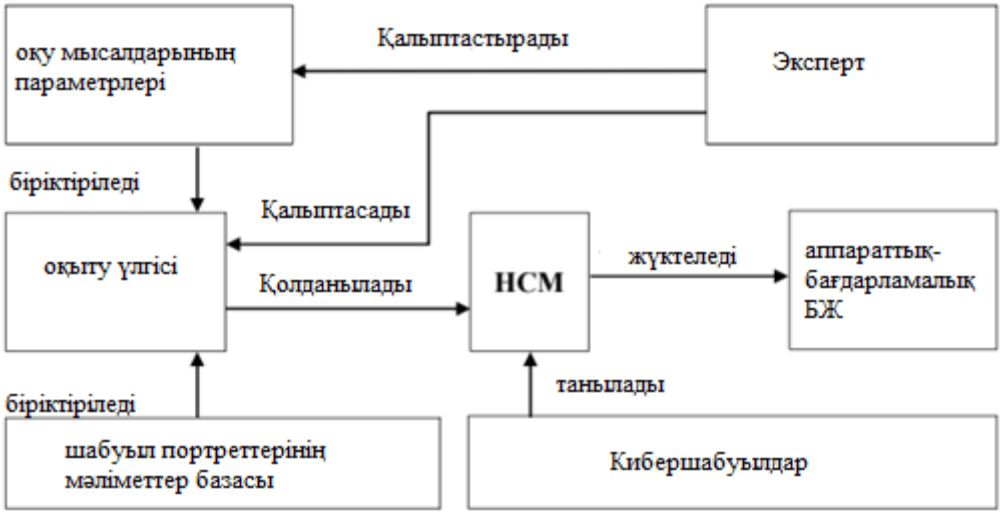
саны, сапасы және номенклатурасы нейрондық желі модельдерін оқыту үшін жеткілікті болуы керек.

- Нейрондық желі модельдерінің түрі мен параметрлерін анықтау - белгілі бір ақпараттық жүйенің желілік ресурстарына кибершабуылдарды тану мәселесінің шарттарын толығымен қанағаттандыратын параметрлері бар нейрондық желі модельдерінің белгілі-бір түрін қолдануға арналған анықтама.

- Нейрондық желі моделін қолдану – ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды танудан тұрады. Нейрондық желі моделін қолдану ақпараттық жүйеге қосымша жүктеме әкелетінін атап өткен жөн, бұл есептеу ресурстарының сарқылуына әкелуі мүмкін.

Тұжырымдамалық модельді құрудың келесі қадамы 2.2 суретте көрсетілген кибершабуылдарды танудың нейрондық желілік жүйесінің құрамдас бөліктерінің сызбасын жасау болды.

Схема ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды тануға арналған нейрондық желілік жүйелерді іске асырудың ерекшеліктерін және ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды танудың белгілі нейрондық желілік құралдарының кемшіліктеріне қатысты нәтижелерді ескереді.



2.2-сурет – Кибершабуылдарды танудың нейрондық желілік компоненттерінің өзара әрекеттесу схемасы

Осылайша, әзірлеу процесінде ескерілді:

- Ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды тануға арналған нейрондық желілік модельдер үшін оқыту мысалдарының параметрлерін қалыптастыру әдістерінің жетілмегендігі.

- Кибершабуылдардың портреттерінің мәліметтер базасына қол жетімділігі шектеулі болған жағдайда нейрондық желі модельдері үшін оқу үлгісін қалыптастырудың ұзақ кезеңі.

- Кибершабуылшылардың қолданыстағы мәліметтер базасына қол жеткізудегі қиындықтар.

- Нейрондық желілердің ақпараттық жүйенің аппараттық және бағдарламалық жасақтамасына қосымша жүктеме жұмысына байланысты.

Сондықтан схема сараптамалық деректерді қолдана отырып, оқыту мысалдары мен оқу үлгісінің параметрлерін қалыптастыру мүмкіндігін қарастырады.

2.1 және 2.2 суреттерде келтірілген деректерді талдау кибершабуылдарды нейрондық желіні танудың тиімділігі ақпараттық жүйелердің желілік ресурстарына көрсетілген бірқатар факторларға әсер етеді деп 2.3 суретте болжайды.

2.3-сурет – Тану тиімділігіне әсер ететін факторлар

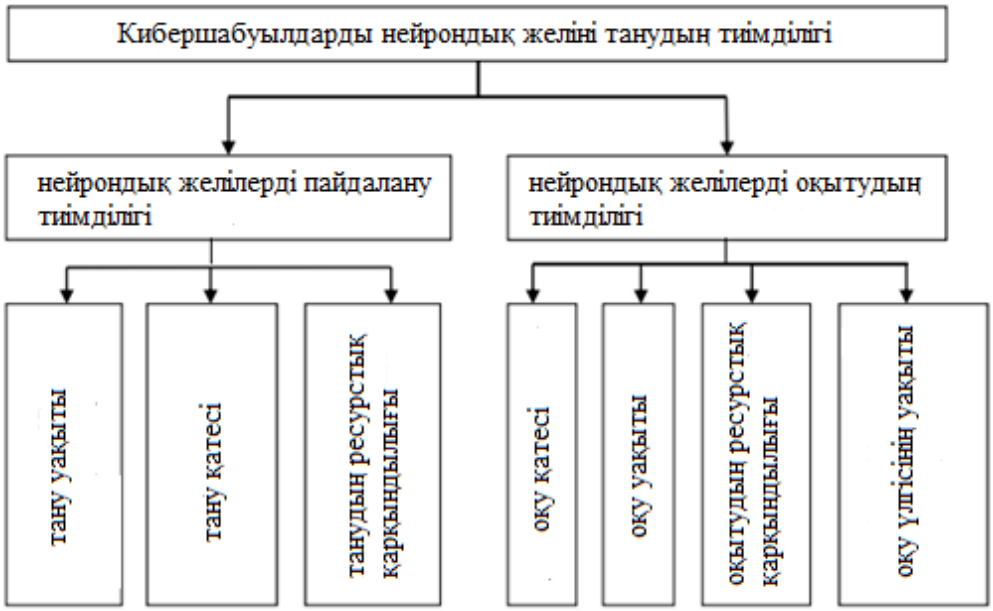
Сонымен қатар, нейрондық желіні танудың тиімділігін нейрондық желі құралдарын қолдану процесінің тиімділігі тұрғысынан да, нейрондық желі моделін оқыту процесінің тиімділігі тұрғысынан да бағалаған жөн деп айтуға болады. Сонымен бірге тиімділік көрсеткіштері аталған процестердің ұзақтығын, ресурс сыйымдылығын және дәлдігін көрсетуі керек. Осылайша, 2.4-суретте көрсетілген ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды нейрондық желіні танудың тиімділігін бағалау көрсеткіштері негізделген.

Нәтижесінде аналитикалық түрде ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды нейрондық желіні тану процесінің

тиімділігін қамтамасыз етудің тұжырымдамалық моделін өрнектерді қолдана отырып көрсетуге болатындығы анықталды:

$$E_{\Sigma} = f(E_{\text{НСП}}, E_{\text{ОВ}}), \quad (2.1)$$
$$E_{\text{НСП}} = f(e_1, e_2, e_3), \quad (2.2)$$
$$E_{\text{ОВ}} = f(e_4, e_5), \quad (2.3)$$

мұндағы E_{Σ} - процестің интегралды тиімділігі, $E_{\text{НСП}}$ - нейрондық желісі құралдарын құру және пайдалану тиімділігі, $E_{\text{ОВ}}$ - оқыту үлгісін құру тиімділігі, e_1 - нейрондық желі модельдерінің тиімді түрлерін анықтау, e_2 - нейрондық желі модельдерінің параметрлерін анықтау, e_3 - нейрондық желі құралдарын пайдаланудың ресурс сыйымдылығы, e_4 - оқыту мысалдарының параметрлерін анықтау, e_5 - оқыту үлгісін қалыптастыру.



2.4-сурет – Нейрондық желілерді тану тиімділігін бағалау көрсеткіштері

Әзірленген тұжырымдамалық модельді талдау кибершабуылдарды тиімді нейрондық желіні тану үшін әдістемелік базаны оларға негізделген нейрондық желі құралдарын қолдану процестерінің бірқатар принциптері мен модельдерімен толықтыру қажет деп айтуға мүмкіндік береді. Болашақта нейрондық желі модельдерін және желілік кибершабуылдарды тану әдістерін жасау үшін әдістемелік базаның алынған элементтерін қолдану қажет.

3 КИБЕРШАБУЫЛДАРДЫ ТАНУ НЕЙРОНДЫҚ ЖЕЛІ МОДЕЛЬДЕРІН ЖӘНЕ АЛГОРИТМДЕРІН ЖАСАУ

3.1 Сараптамалық білімді қолдана отырып, желілік кибершабуылдарға қарсы тұрудың нейрондық желілік моделі

Оқу үлгісін қалыптастыру үшін сараптамалық білімді пайдаланудың ұсынылған принципіне сүйене отырып, бірінші жақындау кезінде желілік трафик параметрлерін өндірістік ережелерде қолданылатын кибершабуылдардың сәйкестендіру параметрлері ретінде пайдалануға болатындығы анықталды. Осы болжамға байланысты алдыңғы өрнектер келесідей болады:

$$If\ x_1 = X_1 \wedge \ldots \wedge x_K = X_K \rightarrow Y_l, l = ..1\ L, \quad (3.1)$$

$$If\ x_1 \in \left[X_1^{min}, X_1^{max}\right]_l \wedge \ldots \wedge x_k \in \left[X_K^{min}, X_K^{max}\right]_l \rightarrow Y_l, l = 1..L, \quad (3.2)$$

мұндағы $x_1, .. x_K$ - нейрондық желі модельдерінің кіріс параметрлерінің мәндері, K - желілік трафик параметрлерінің саны, $\left[X_1^{min}, X_1^{max}\right], \ldots, \left[X_K^{min}, X_K^{max}\right]$ - берілген $x_1, .. x_K$ ауқымдары, l - өндірістік ереженің нөмірі, L - өндірістік ережелер саны.

Талдау нәтижелері PNN және MPNN сияқты нейрондық желі модельдерінің өндірістік ережелерін қолдана отырып оқытуға толық бейімделгенін көрсетеді. Сонымен бірге, талдау PNN және MPNN-нің теріс ерекшеліктері шығыс сигналының ақпараттылығы төмен екенін көрсетеді. Нейрондық желілердің осы модельдерінде шығыс сигналының мәні қандай оқиғаның болуы мүмкін екенін көрсетеді - кибершабуыл немесе қадыпты күй. Бұл ақпараттық қауіпсіздік жүйелерінде кибершабуыл/қалыпты күй ықтималдығының белгіленген шекті мәндерін немесе осы ықтималдықтар арасындағы айырмашылықтың шекті мәнін пайдалануға мүмкіндік бермейді. Осылайша, тану блогы MPNN желісі негізінде жұмыс істейтін ақпараттық қауіпсіздік жүйелерінде келесі түрдегі қорғаныс ережелерін орындау мүмкін емес:

$$If\ \Theta_{Ka} > \Delta_{Ka} \rightarrow Z, \quad (3.3)$$

$$If\ \Theta_{Nm} < \Delta_{Nm} \rightarrow Z, \quad (3.4)$$

$$If\ (\Theta_{Ka} - \Theta_{Nm}) > \Delta_{\Delta} \rightarrow Z, \quad (3.5)$$

$$If\ \Omega_i > \Delta_i \rightarrow Z, \quad (3.6)$$

мұндағы Θ_{Ka}, Θ_{Nm} - кибершабуылдардың ықтималдығы, Θ_{Nm} - қалыпты жағдайдың ықтималдығы, Z - қорғау шаралары, Ω_i - і типті кибершабуылдың ықтималдығы, Δ_{Ka} Δ_{Nm} Δ_{Δ} Δ_i - шекті мәндер.

Сонымен қатар, нейрондық желі моделінің шығыс сигналының жеткіліксіз ақпараттылығы ақпаратты қорғау жүйесіне желілік трафик параметрлерінің әртүрлі комбинацияларына икемді жауап беруге мүмкіндік бермейді, сонымен қатар ықтималдығы ең ықтимал күйден өзгеше болатын қауіпсіздік күйлерінің параметрлерін тіркеуге мүмкіндік бермейді. Мұндай параметрлерді тіркеу мүмкіндігі кибершабуылдардың белгілі түрлерін тану ережелерін нақтылауға және кибершабуылдардың белгісіз түрлерін тану ережелерін қалыптастыруға арналған мәліметтер базасын құруға мүмкіндік береді.

Осы кемшіліктерді жою үшін ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды тануға арналған MPNN желісінің шығыс ақпараты толықтырылуы мыналармен керек екендігі анықталды:

Кибершабуылдардың белгілі түрлерін жүзеге асыру ықтималдығы.

Кибершабуылдың ең ықтимал түрінің ықтималдығы.

Кибершабуылдың ықтималдығы.

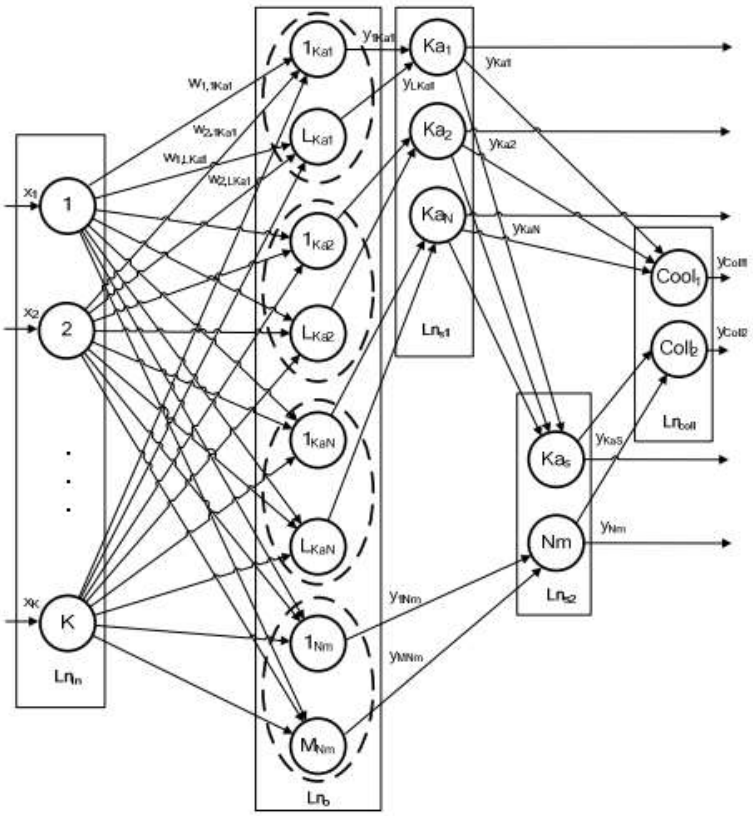
Қалыпты жағдайдың ықтималдығы.

Ендігі кезекте, PNN және MPNN моделдері тиісті шығыс қосылыстарымен, сондай-ақ кибершабуылдардың белгілі түрлерінің ықтималдығын есептеуге арналған нейрондардың қосымша қабатымен толықтырылуы керек.

Өзгертілген PNN құрылымы 3.1 суретте (3.1)-де көрсетілген түрдің өндірістік ережелеріне негізделген ақпараттық жүйенің желілік ресурстарының күйін тануға арналған, ал MPNN құрылымы (3.2) түрінің өндірістік ережелерін қолдануға бейімделгені 3.2 суретте көрсетілген.

Құрылымдық өзгертілген PNN 5 нейрондық қабаттан тұрады. Бұл - кіріс қабаты (Ln_{in}), кескін қабаты (Ln_o), бірінші жиынтық қабаты (Ln_{s1}), екінші жиынтық қабаты (Ln_{s2}) және салыстыру қабаты (Ln_{coll}).

Классикалық PNN желісі сияқты, кіріс қабатының нейрондары деректерді сыртқы ортадан кескін қабатының нейрондарына жібереді. Кескін қабаты нейрондық желі тануы керек барлық сыныптар үшін оқу мысалдарының параметрлерін есте сақтауға арналған. Тиісінше, кескін қабатындағы нейрондардың саны нейрондық желі есте сақтайтын оқу мысалдарының санына тең. 3.1 суретте кескін қабатының нейрондары шартты түрде кибершабуылдардың белгілі түрлеріне және ақпараттық жүйенің желілік ресурсының қалыпты жағдайына сәйкес келетін топтарға бөлінеді. Мысалы, 1_{KaN}…L_{KaN} көрсетілген нейрондар кибершабуылдардың N-ші түрінің жаттығу мысалдарына сәйкес келеді, ал 1_{Nm}…M_{Nm} белгіленген нейрондар қалыпты жағдайдың оқу мысалдарына сәйкес келеді. Жалпы, кибершабуылдардың әр түрі үшін және қалыпты жағдай үшін оқу мысалдарының саны әртүрлі болуы мүмкін.



3.1- сурет – Өзгертілген PNN құрылымы

Жинақтаудың бірінші қабатының міндеті - нейрондық желіге белгілі кибершабуылдардың әр түрін жүзеге асыру ықтималдығын есептеу. Сондықтан бұл қабаттың нейрондары Ka_1, Ka_2, … Ka_N, кибершабуылдардың белгілі түрлерімен байланысты және олардың саны кибершабуылдардың көрсетілген түрлерінің санына тең (N). Жинақтаудың екінші қабаты кибершабуылдардың барлық түрлерінің жалпы ықтималдығын және ақпараттық жүйенің желілік ресурсының қалыпты жағдайының ықтималдығын анықтауға арналған. Бұл қабатта екі нейрон бар. Ka_s нейроны кибершабуылдардың жалпы ықтималдығын есептеу үшін, ал Nm нейроны қалыпты жағдайдың ықтималдығын есептеу үшін қолданылады. Салыстыру қабатының міндеті - ең ықтимал кибершабуылдың түрін, сондай-ақ қауіпсіздіктің ең ықтимал жағдайының түрін анықтау. Кибершабуылдың ең ықтимал түрін $Coll_1$ нейроны анықтайды, ал қауіпсіздіктің ең ықтимал күйін (кибершабуыл немесе қалыпты жағдай) $Coll_2$ нейроны анықтайды.

Ln_{in} және Ln_o қабаттары арасындағы байланыс құрылымы толығымен байланысқан. Бұл жағдайда кіріс қабатының әр нейроны кескін қабатының әр нейронымен тікелей байланысады. Бұл байланыстардың салмақтық коэффициенттері оқыту мысалдарының компоненттеріне тең:

$$w_{1,l} = X_1, w_{2,l} = X_2, \dots w_{K,l} = X_K, \tag{3.7}$$

мұндағы l - (3.1) түрдің өнім ережесінің нөміріне сәйкес келетін кескін қабатының нейрон нөмірі, K - кіріс параметрлерінің саны, X_1, X_2, X_K - L-ші өнім түрінің компоненттері.

Мысалы, 3.1 суретте бірінші кіріс нейроны мен $1_{Ka1}\ldots L_{Ka1}$, $1_{Ka2}\ldots L_{Ka2}$ қабатының нейрондары арасындағы байланыстың салмақ коэффициенттері көрсетілген. PNN желісіндегі барлық басқа байланыстардың салмақ коэффициенттері 1-ге тең екенін ескеру керек. Кескін қабатының нейрондарында Гаусс функциясы активтендіру функциясы ретінде қолданылады. Кескін қабатының нейрондарынан ерікті l - ші шығу сигналы келесідей есептеледі:

$$y_l = \sum_{k=1}^{K} \exp(-\left(w_{k_1,l} - x_k\right)^2 / 2\sigma^2), \tag{3.8}$$

мұндағы $w_{k_1,l}$ - кіріс қабатының k - ші нейроны мен кескін қабатының l - ші нейроны арасындағы байланыстың салмақтық коэффициенті, x - k кіріс сигналының мәні, K - кіріс параметрлерінің саны, σ - Гаусс функциясының радиусы.

Гаусс функциясының радиусы σ∈ [3,0 ..., 7,0]. Кескін қабаты мен жиынтықтың бірінші қабаты арасындағы байланыс құрылымының ерекшелігі бар. Тек осы нейрон байланысқан кибершабуыл түрінің параметрлеріне сәйкес келетін кескін қабатының нейрондары ғана жиынтықтаудың бірінші қабатының нейронымен байланысады. Мысалы, 3.1 суретте көрсетілгендей, $1_{Ka1}\ldots L_{Ka1}$ нейрондары тек Ka_1 нейронымен байланысады. Жинақтау қабаттарының нейрондарында сызықтық активтендіру функциясы қолданылады. Бірінші қабаттың ерікті n-ші нейронына арналған шығыс сигналы келесідей есептеледі:

$$y_{Ka_n} = \frac{\sum_{l=1}^{L_{Ka_1}} y_{l_{Ka_1}}}{L_{Ka_1}}, \tag{3.9}$$

мұндағы L_{Ka_1} - жиынтықтаудың бірінші қабатының n-ші нейронымен байланысқан кескін қабатының нейрондарының саны, $y_{l_{Ka_1}}$ - жиынтықтаудың бірінші қабатының n-ші нейронымен байланысқан кескін қабатының l-ші нейронының шығысы.

$y_{Ka_1}, \ldots y_{Ka_n}$ шығыс сигналдарының шамалары $Ka_1, \ldots Ka_N$ кибершабуылдарының әр белгілі түрін жүзеге асыру ықтималдығын көрсетеді. Бұл сигналдар PNN желісінің шығыс ақпаратының бір бөлігін құрайды. Сонымен қатар, олар $Cool_1$ салыстыру қабатының нейронына және екінші қабаттың Ka_s нейронына қосылады. Бұл нейронның шығуы келесідей есептеледі:

$$y_{Ka_s} = \frac{\sum_{n=1}^{N} y_{Ka_n}}{N}, \tag{3.10}$$

мұндағы N - кибершабуылдардың белгілі түрлерінің саны.

y_{Ka_s} шамасы , кибершабуылдардың барлық түрлерін іске асырудың жалпы ықтималдығын көрсетеді, сонымен қатар PNN желісінің шығыс ақпаратының бөлігі болып табылады. Сонымен қатар, y_{Ka_s} одан әрі өңдеу үшін $Cool_2$ салыстыру қабатының нейронына жіберіледі.

Жинақтаудың екінші қабатының Nm нейронының шығыс сигналы ақпараттық жүйенің желілік ресурсының қалыпты күйінің ықтималдығын бағалау болып табылады. Бұл нейрон қалыпты жағдайдың жаттығу мысалдарымен байланысты кескін қабатының нейрондарымен ғана байланысты. Nm нейронының шығыс сигналының мәні келесідей есептеледі:

$$y_{Nm} = \frac{\sum_{m=1}^{M_{Nm}} y_{Nm_m}}{M_{Nm}}, \tag{3.11}$$

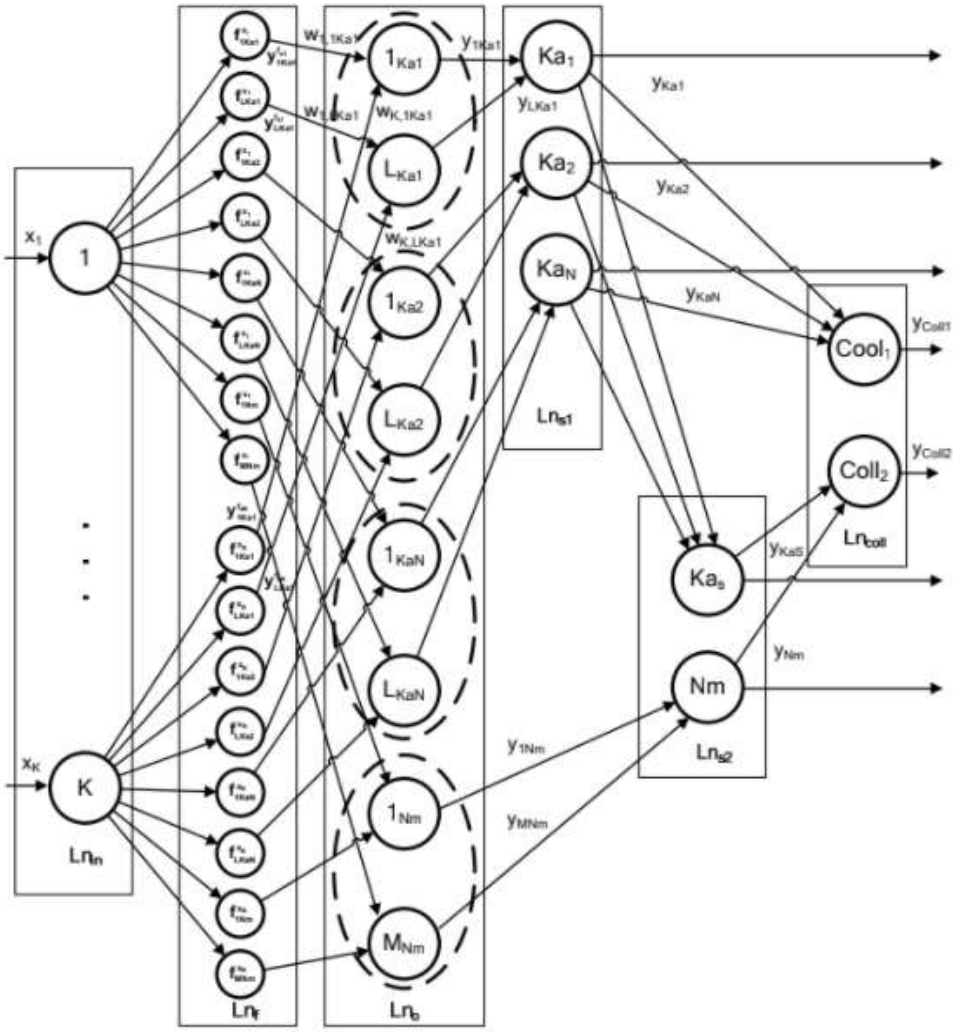
мұндағы M_{Nm} - қалыпты жағдайдың оқу мысалдарына сәйкес келетін кескін қабатының нейрондарының саны, y_{Nm_m} - қалыпты күйдің m-мысалына сәйкес келетін кескін қабатының m-ші нейронының шығысы.

y_{Ka_s} сияқты y_{Nm} сигналы желінің шығыс ақпаратының бөлігі $Cool_2$ нейронына жіберіледі. $Cool_1$ және $Cool_2$ нейрондарында кибершабуылдың ең ықтимал түрі анықталады және қауіпсіздіктің неғұрлым ықтимал жағдайы анықталады – кибершабуыл іске асырылады/қалыпты жағдай. 3.1 суретте тиісті шығыс сигналдары y_{Coll1} және y_{Coll2} деп белгіленген.

Өзгертілген MPNN желісі мен өзгертілген PNN желісінің басты айырмашылығы - сүзу қабатының болуы (3.2 суретте – Ln_f деп көрсетілген), нейрондар (3.2) түрдің өндірістік ережесіне сәйкес кіріс сигналының құрамдас бөліктерінің мәндерін сүзуге арналған. Бұл жағдайда кейбір $f_l^{x_k}$ нейронының міндеті – x_kкіріс параметрін l өндіріс тану ережесіне сәйкес сүзу. Сигналды сүзу түрді белсендіру функциясын қолдану арқылы жүзеге асырылады:

$$\exists x_k \in \left[X_k^{max}, X_k^{min}\right]_l \rightarrow y_l^{f_{x_k}} = x_k, \exists x_k \notin \left[X_k^{max}, X_k^{min}\right]_l \rightarrow y_l^{f_{x_k}} = 0, \tag{3.12}$$

мұндағы x_k – k кіріс параметрінің мәні, $y_l^{f_{x_k}}$ - нейронның $y_l^{f_{x_k}}$шығыс сигналы.



3.2- сурет – Өзгертілген MPNN құрылымы

Сүзу қабатының нейрондары мен кескін қабатының нейрондары арасындағы салмақ коэффициенттері келесідей есептеледі:

$$w_{f_l^{x_k},l} = \frac{X_k^{max} - X_k^{min}}{2}, \tag{3.13}$$

мұндағы l - (3.2) түрдің өнім ережесінің нөміріне сәйкес келетін кескін қабатының нейрон нөмірі, $f_l^{x_k}$ – бұл x_k кіріс нейронынан кескін қабатының l–ші нейронына сигналды сүзетін нейрон, k - кіріс параметрлерінің саны, X_k^{max}, X_k^{min} - l-ші өнім ережесінің компоненттері.

3.2 FLDS аномалиясын анықтау алгоритмін жасау

Аномалияны анықтау - машиналық оқыту мен деректерді іздеудің маңызды мәселелерінің бірі. Аномалияны анықтау - бұл күтілетін мінез-құлыққа сәйкес келмейтін мәліметтерден үлгіні табу мәселесі.

Аномалиялардың бірнеше түрлері бар, мысалы, нүктелік ауытқулар, контекстік ауытқулар, ұжымдық ауытқулар. Бұл тарауда әртүрлі қосымшаларда қолдануға болатын нүктелік ауытқуларды анықтауға баса назар аударылады. Нүктелерден тұратын мәліметтер жиынтығы үшін, егер ол көптеген басқа нүктелерден өзгеше болса, нүкте аномалия деп аталады. Аномалияларды анықтау үшін жіктеу әдістері, жақын көршілердің әдістері, кластерлеу әдістері, статистикалық әдістер, қашықтыққа негізделген әдістер (өлшемдер) және т. б. көптеген әдістер жасалды.

Математикалық тұрғыдан алғанда, аномалияны анықтау мәселесін қолданудың барлық салаларында қалыпты мінез-құлықты модельдеу, аномалды оқиғаларды анықтау керек. Бұл аномалияны анықтауға негізделген екі қарапайым болжамға әкеледі:

1. деректер жиынтығында ауытқулар өте сирек кездеседі;
2. аномалиялардың сипаттамалары қалыпты мәліметтерден айтарлықтай ерекшеленеді.

Жіктеуге негізделген аномалияны анықтаудың екі категориясы бар: аномалияны анықтаудың көп класты және одақтық әдістері. Көп кластық жіктеу әдістерінде оқыту деректерінде барлық қалыпты сыныптардың белгіленген нүктелері болады деп болжанады. Оқытушымен оқыту алгоритмін қолданатын әдіс (supervised learning) белгіленген мәліметтерді қолдана отырып оқытылады. Классификатор әр қалыпты класс пен сыныптың қалған бөлігін ажырата алады. Бақылау нүктесі, егер ол қандай да бір қалыпты класқа жатпаса, аномалды болып табылады. Аномалияны анықтаудың одақтық әдістерінде тек бір қалыпты класс бар деп болжанады. Классификатор қалыпты сыныптың шекарасын анықтауға мүмкіндік беретін модельді зерттейді. Егер бақылау нүктесі қалыпты сыныптан тыс болса, онда ол аномалия болып саналады. Көптеген әдістер жасалғанына қарамастан, олардың басты кемшілігі нақты өмірде қолдануға оңай болмайтын қарапайым сыныптар үшін дәл белгілердің болуына негізделген. Жақын көршілерге негізделген ауытқуларды анықтау әдістері үшін келесі болжам қолданылады: қалыпты нүктелер тығыз аймақтарға жатады, ал ауытқулар сирек аймақтарға жатады. Осы әдістердің ішіндегі ең танымалы - LOF алгоритмі. Бұл әдістің негізгі мақсаты - әр объектіге ауытқу дәрежесін беру. Бұл дәреже объектінің жергілікті аномалия факторы (local outlier factor – LOF) деп аталады. Бұл жергілікті, LOF мәні объектінің қоршаған ортамен салыстырғанда қаншалықты оқшауланғанына байланысты. Жергілікті аномалия ұғымы өте маңызды, өйткені көптеген қосымшаларда мәліметтер жиынтығының әртүрлі бөліктері әртүрлі сипаттамаларды көрсете алады және объектінің оған жақын орналасқан басқа объектілерге негізделген аномалия болуы мүмкін екендігі туралы шешім қабылдаған дұрыс. LOF алгоритмінде деректер объектісі мен оның айналасы арасындағы тығыздық айырмашылығы - жергілікті аномалия факторы ретінде белгілі екпін дәрежесі. Интуитивті түрде, аномалиялар - бұл жердің құны жоғары деректер объектілері, ал LOF мәні төмен деректер объектілері қоршаған ортаға қатысты қалыпты болуы мүмкін. Жоғары

тығыздықтың болуы төмен тығыздықтағы нүктелерге жақындықтың белгісі болып табылады, сондықтан аномалия болу мүмкіндігі жоғары.

LOF мәні - нүктенің ең жақын көршілерінің орташа жергілікті тығыздығының k қатынасы және деректер нүктесінің жергілікті тығыздығы. Берілген x нүктесі үшін x көршілері деп аталатын нүктелер келесідей анықталады:

$$N(x, mp) = \{y \in X \mid d(x, y) \leq d(x, x_{mp})\}, \tag{3.14}$$

мұндағы X - бастапқы мәліметтер жиынтығы, x_{mp} - бұл x-тің mp-шы ең жақын көршісі, mp - шекті параметр. Осылайша, $N(x, mp)$ кем дегенде mp нүктелері бар. X тығыздығы келесі формула бойынша есептеледі:

$$density(x, mp) = \left(\frac{\sum y \epsilon N(x, mp)^{d(x,y)}}{|N(x, mp)|}\right)^{-1}. \tag{3.15}$$

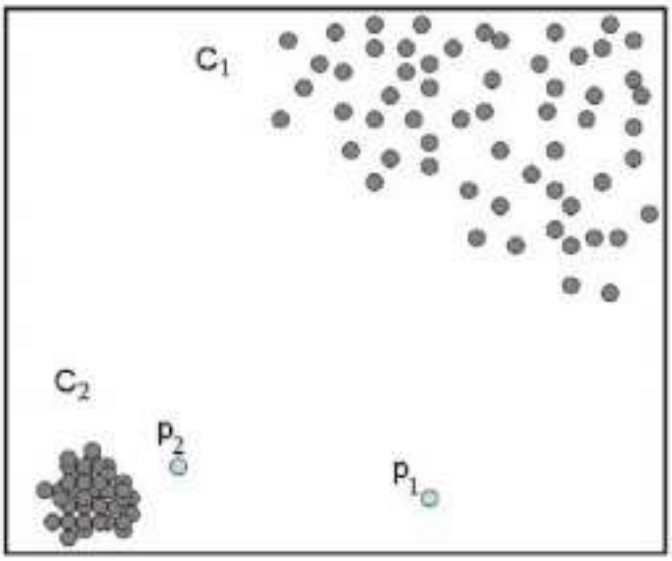
X тығыздығы мен x көршілерінің орташа тығыздығы арасындағы қатынас формула бойынша анықталады:

$$ard(x, mp) = \frac{density(x, mp)}{\left(\frac{\sum y \in N(x, mp)^{density(y,mp)}}{|N(x, mp)|}\right)}. \tag{3.16}$$

X нүктесінің жергілікті тығыздығының мәні келесідей анықталады:

$$LOF(x, mp) = ard(x, mp)^{-1}. \tag{3.17}$$

LOF тәсілінің мәнін көрсету үшін 3.3 суретте көрсетілген қарапайым екі өлшемді мәліметтер жиынтығын қарастыру ұсынылады. C1 кластерінде C2 кластеріне қарағанда әлдеқайда көп элементтер бар, ал C2 кластерінің тығыздығы C1 кластерінің тығыздығынан едәуір жоғары. Жергілікті аномалия ұғымы тұрғысынан p1 және p2 нысандарын аномалия ретінде белгілеу қажет. C1 кластерінің тығыздығы төмен болғандықтан, C1 кластерінің ішіндегі әрбір x элементі үшін x элементі мен оның жақын көршісі арасындағы қашықтық p2 элементі мен C2 кластерінің жақын көршісі арасындағы қашықтықтан үлкен екендігі анық, сондықтан p2 элементі аномалия болып саналмайды. Сондықтан қашықтықты есептеуге негізделген жақын көршілердің қарапайым әдісін қолдану осы сценарийлердегі ауытқуларды анықтауға мүмкіндік бермейді. Алайда, p1 элементін тек жақын көршіге дейінгі қашықтықты қолдана отырып, аномалия ретінде анықтауға болады. Екінші жағынан, LOF алгоритмі нүктелердің айналасындағы тығыздықты ескере отырып, екі аномалияны (p1 және p2) анықтай алады.



3.3-сурет – LOF алгоритмінің мысалы

LOF-ті іске асырудың көптеген нұсқалары бар, мысалы, қосылуға негізделген аутификатор факторы (Connectivity-Based Outlier Factor, COF), локальды асып түсу ықтималдығы (Local Outlier Probability, LOOP), әсер етілген нәтиже (Influenced Outlierness, INFLO), жергілікті корреляциялық интеграл, (Local Correlation Integral, LOCI) және т.б. Олардың басты кемшілігі - $O(n)^2$ орындалуының есептеу күрделілігі, мұнда үлкен О әрпі есептеу күрделілігінің белгісі болып табылады. Есептеу күрделілігі - алгоритмді орындау үшін қажет есептеу ресурстарының *n* енгізу көлеміне тәуелділігі.

Кластерлеу алгоритмдеріне негізделген ауытқуларды анықтау әдістері үшін идея деректерді кластерлерге топтастыру болып табылады. Егер нүктелер ешқандай кластерлерге жатпаса, онда олар аномалия болып саналады.

Кейбір кластерлеу әдістері DBSCAN, KNN және т. б. сол сияқты ауытқуларды анықтай алады. Шын мәнінде, кластерлеудің мақсаты кластерлерді табу болып табылады, сондықтан ауытқулар тек кластерлеу процесінің өнімі болып табылады, демек мұқият оңтайландырылмаған. Бұл тәсілдің тағы бір ерекшелігі – кластерлеу әдістерінің күрделілігі – $O(n)^2$.

Аномалияны анықтаудың статистикалық әдістері келесі болжамға негізделген: қалыпты деректер нүктелері стохастикалық модельдің жоғары ықтималдық аймақтарында кездеседі, ал ауытқулар стохастикалық модельдің төмен ықтималдық аймақтарында пайда болады. Аномалияны анықтаудың белгілі бір түрлері үшін кейбір әдістер жасалды. Жалпы алғанда, статистикалық әдістер статистикалық модельді (Гаусс үлестірімі, параметрлік статистикалық үлестірімнің тіркесімі және т.б.) берілген мәліметтерге бейімдейді, содан кейін осы модельдің көрінбейтін данасы тиесілі ме, жоқ па, соны анықтау үшін статистикалық болжамды тексереді. Бұл әдістердің негізгі

шектеуі - қалыпты деректер нүктелері белгілі бір үлестірімге бағынады деген болжам жасау қажеттілігі. Егер деректердің өлшемі жоғары болса, онда бұл болжам дұрыс емес, нәтижесінде ауытқуларды анықтау дәлдігі төмендейді.

Қашықтыққа негізделген аномалияларды анықтау әдістерінде, Егер деректер жиынында D_{min} шекті мәнінен аз болатын нүктелер жеткіліксіз болса (олардың саны берілген мәнінен аз pct%), нүкте аномалия болып саналады.

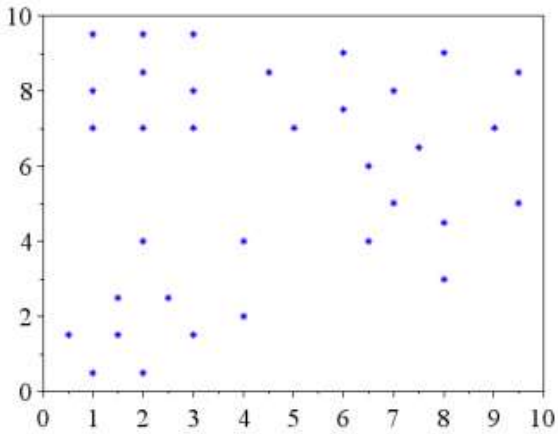
Оқытусыз оқумен аномалияны анықтау әдістері (unsupervised) - оларда оқытудың қажеті жоқ артықшылығы бар. Сондай-ақ, оларда белгісіз нысандарды табу мүмкіндігі бар, бұл оқыту әдістерімен шешілмейді. Сондықтан, бұл әдістер хакерлік шабуылдарды анықтау сияқты салада қолдануға жарамды, өйткені хакерлер өздерінің мінез-құлқын үнемі өзгерте алады.

Бұл алгоритмдердің жалпы сипаттамасы $O(n)^2$ ретін есептеу күрделілігі болып табылады. Сондықтан есептеу күрделілігі төмен алгоритмдерді құру өзекті болып табылады.

Осы диссертацияда ұсынылған бейімделу әдісі жергілікті тығыздықты бағалау алгоритміне негізделген (Local Density Score - LDS). Оны дамыту үшін *K*-жақын көршілердің графигі қолданылады. Граф *K*-ең жақын көршілердің графигі, егер ол келесі шарттарды қанағаттандырса ғана:

1. граф салмағы бар бағдарланбаған график болып табылады және әр шыңда осы шыңнан шығатын қабырғалары k_{nn}-ден аспайды;
2. жиек x_i және x_j шыңдарының бір жұбы арасында жасалады, содан кейін тек x_i x_jнүктесінің *K*-жақын көршілерінің жиынтығына жатады және керісінше.

K-жақын көршілердің графигінің қалыптасуын нақты түсіндіру үшін төмендегі суреттерде бастапқы мәліметтер жиынтығының мысалдары (3.4 сурет) және k_{nn}= 4 үшін қалыптасқан график келтірілген, мұндағы k_{nn} - жақын көршілердің саны (3.5 сурет).



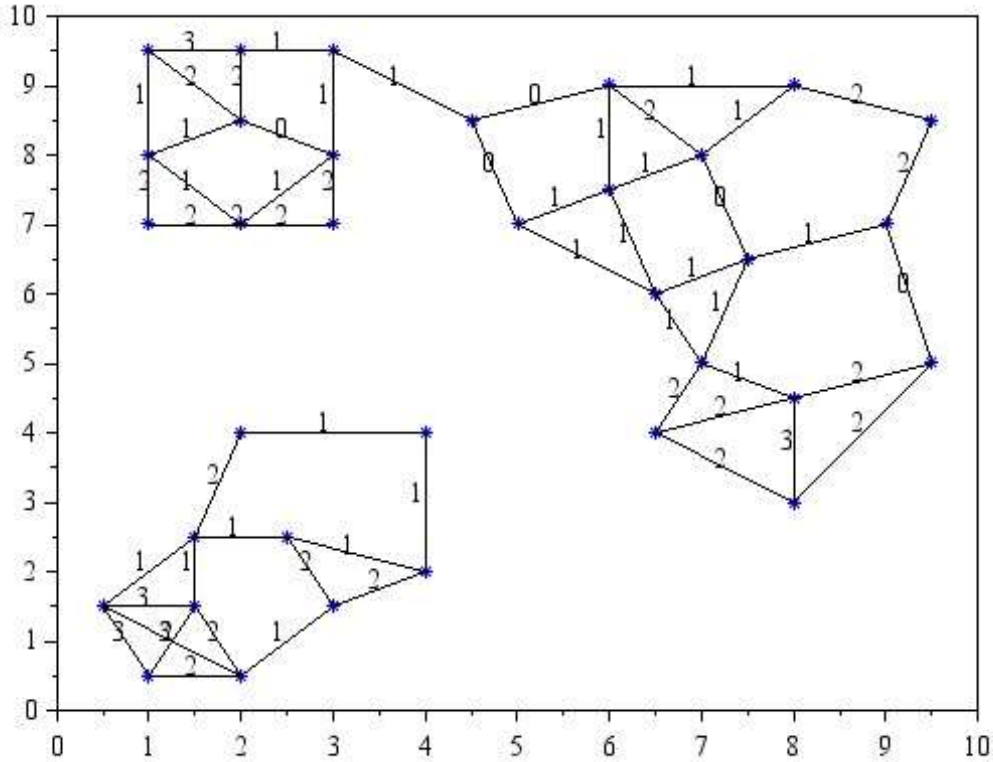
3.4-сурет – *K* графигін құрудың мысалы - жақын көршілер. Бастапқы деректер жиынтығы.

LDS алгоритмін жасамас бұрын қажетті анықтамаларды берейік.

Анықтама 1. x_i - нің кез-келген шыңы үшін x_i - ді қоспағанда, x_i-ге жақын *K* - көршілердің жиынтығы $NN(x_i)$ арқылы көрсетіледі.

Анықтама 2. Жиектің ұзындығы немесе кез-келген жұп шыңдар арасындағы салмақтың мәні (x_i, x_j) графикте $\omega(x_i, x_j)$ деп белгіленеді және *K* - жақын көршілердің $NN(x_i)$ және $NN(x_j)$ екі жиынының жалпы нүктелерінің саны ретінде анықталады:

$$\omega(x_i; x_j) = |NN(x_i) \cap NN(x_j)|.$$



3.5- сурет – *K* графигін құрудың мысалы - жақын көршілер. $k_{nn}=4$ кезінде құрылған график

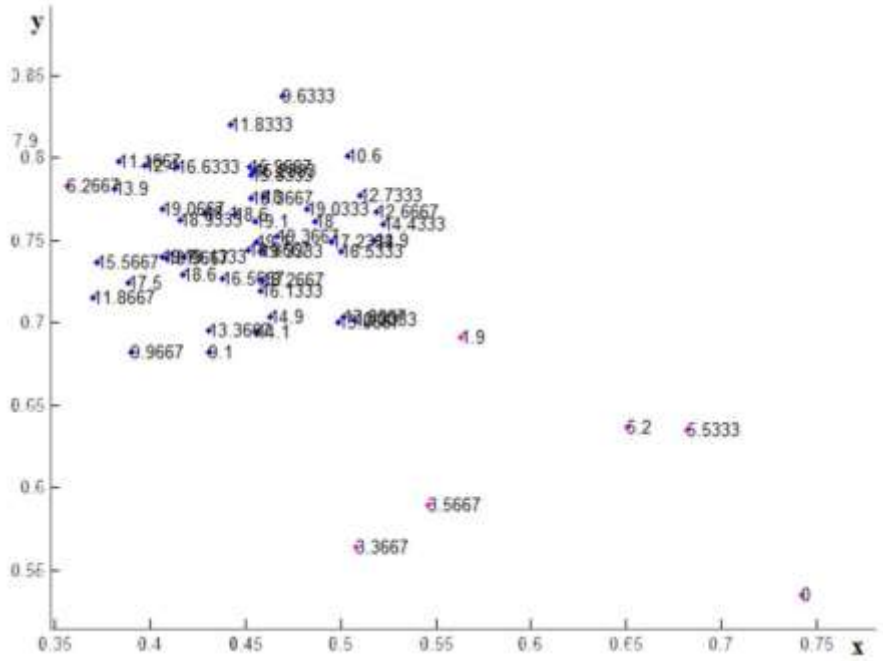
Бұл анықтама салмақты есептеу үшін маңызды ақпарат береді: бұл аймақтар арасындағы жергілікті тығыздық есептеулерге әсер етпейді (Эвклид қашықтық формуласы сияқты қарапайым формула арқылы салмақтынемесе қашықтықты есептеуден өзгеше). Сонымен қатар, LDS алгоритмін әртүрлі тапсырмаларда формуламен қолдануға болады, тарату тығыздығы мен бастапқы деректердің пішініне назар аудармай, бұл басқа алгоритмдерге, мысалы, *k*-орташа, FastDBSCAN және т. б. шектеу болып табылады.

Анықтама 3. Графиктегі кез келген *x* шыңының жергілікті тығыздығы $Score(x)$ ретінде белгіленеді және мынадай формула бойынша айқындалады:

$$Score(x) = \frac{\sum_{q \epsilon NN(x)} \omega(x,q)}{K_{nn}}.$$	(3.18)

X шыңының жергілікті тығыздығы *x* шыңының көршілерімен байланыс деңгейіне байланысты анықталады. Қосылу деңгейі неғұрлым жоғары болса, *x* айналасындағы аймақтың тығыздығы соғұрлым жоғары болады. $Score(x)$ мәні [0; k_{nn}-1], аралығында және бұл өте маңызды, ол жоғары тығыздық аймағында және керісінше.

LDS алгоритмі бетті тану, ішінара оқыту алгоритмі (semisupervised) үшін белгісі бар ең жақсы үміткерді таңдау және т.б. сияқты мәселені шешу үшін ғана ұсынылған болатын, ал ауытқуларды анықтау үшін қолдану мүлдем жоқ. Сондықтан LDS алгоритмін аномалияны анықтау міндетіне қолдану ұсынылды. Бұл жағдайда бастапқы деректердегі әрбір жазба жақын көршілердің *K* бағанындағы шың болып саналады. Аномалия - бұл басқа нүктелерден алыс орналасқан координаттары бар нүкте. Аномалиялардың мысалдары 3.6 суретте көрсетілген.



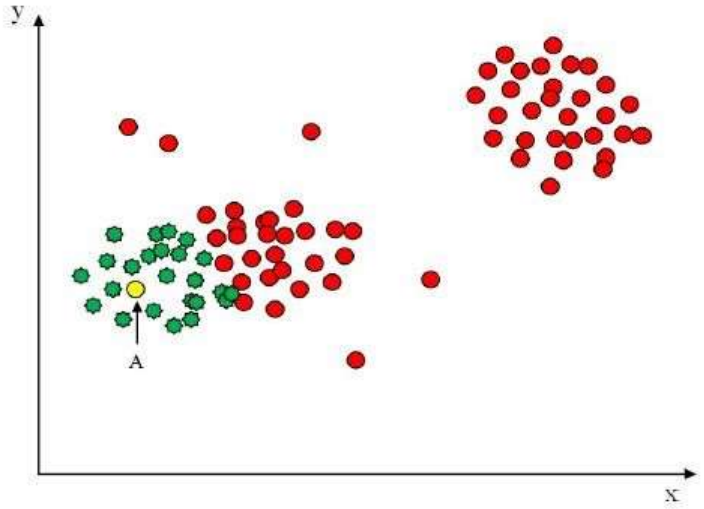
3.6- сурет – LDS алгоритмі арқылы алынған нүктелердің жергілікті тығыздығы. Көк-қалыпты нүктелер, күлгін-ауытқулар

Алгоритмдердің сапасын жақсарту бірнеше өлшемдерге негізделуі мүмкін, олардың екеуі жылдамдық пен дәлдік маңызды. Осы тармақта бірінші критерий қолданылады, ал екіншісі тараудың келесі тармағында қарастырылады.

LDS алгоритмін және LOF сияқты басқа ұқсас алгоритмдерді есептеу уақытының 99% - ы барлық бастапқы деректер үшін ең жақын көршілерді табуға жұмсалатыны іс жүзінде көрсетілген, сондықтан есептеу күрделілік

$O(n^2)$ретінде анықталады. KD-tree немесе X-tree арнайы құрылымдарын пайдалану сияқты *K*-жақын көршілерді іздеуді тездетудің бірнеше тәсілдері ұсынылған, бірақ олар барлық бастапқы деректерге қолданылады, бұл олардың жұмысына теріс әсер етеді. Осы себепті берілген кеңістікті ішкі кеңістікке бөлу арқылы *K*-жақын көршілерді іздеуді оңтайландыру идеясы ұсынылады.

3.7-суретте көрсетілгендей, кез-келген А нүктесі үшін қызыл түсті нүктелер А нүктесінен алыс және А нүктесінің көптеген *K*-жақын көршілеріне үміткер бола алмайтыны анық, ал А нүктесінің айналасындағы жасыл нүктелер ғана А нүктесінің жақын көршілерінің *K* жиынына түсу ықтималдығы жоғары (k_{nn}=5 болсын), сондықтан жасыл нүктелері бар аймақты пайдалану жеткілікті.



3.7- сурет – А нүктесінің 5 көршісі бар А нүктесінің айналасындағы жергілікті аймақтың суреті

Кеңістікті бөлу идеясына сәйкес алгоритм оңтайландырылды. Кеңістікті бөлу үшін *K*-орташа алгоритм таңдалады, өйткені оның түсіну қарапайымдылығы, бағдарламалаудың қарапайымдылығы және есептеу күрделілігі ($O(k \times n)$, k – кластерлер саны, n – бастапқы деректер жазбаларының саны сияқты көптеген артықшылықтары бар. LDS және *K*-алгоритмдерінің тіркесімі $O(n^{1.5})$ есептеу қиындығы төмен гибридті FLDS (FastLDS) алгоритміне әкеледі.

FLDS алгоритмі үш параметрді қолданады: *k*-алгоритм кластерлерінің саны *K*-орташа, k_{nn} - жақын көршілердің саны, ε - аномалия болып табылатын кандидатты таңдау шегі. Параметр эксперименталды түрде таңдалады. *k* параметрі $\lfloor \sqrt{n} - \varepsilon, \sqrt{n} + \varepsilon \rfloor$ интервалында таңдалады, нақты аймаққа байланысты, мысалы, 8000 k жазбаларынын CHAMELEON дерекқоры үшін [68, 49] сегментте таңдауға болады. k_{nn} параметрі $\lfloor n/k \rfloor$ мәнінен аспайтын етіп таңдалады, ал ε параметрін сарапшы таңдайды. Ұсынылған алгоритмнің

негізгі идеясы - алдымен берілген *x* жиынтығы *k* кластерлеріне сәйкес келетін $(X_1, X_2, X_3, \dots, X_k)$, ішкі жиындарындағы *k*-орташа алгоритмді қолдана отырып бөлінеді. Осыдан кейін LDS алгоритмі әр $X_i\ (i = 1{:}k)$ ішкі жиынында көптеген жергілікті *E* ауытқуларын алу үшін қолданылады. *E* жиынтығы - жаһандық ауытқуларға үміткерлер жиынтығы. Берілген *X* жиынындағы *E* жиынындағы әрбір жергілікті аномалия үшін *Score* мәні формула бойынша қайта есептеледі және ғаламдық аномалияны таңдау үшін ε параметрін қолданатын LDS шамалары алынады.

FLDS алгоритмі (*Fast Local Density Score*)

Кіру: $X = \{x_1, x_2, \dots, x_n\}$ бастапқы деректер жиынтығы, *k* - кластерлер саны, k_{nn} - жақын көршілердің саны, ε - шегі; *Шығу:* *G* - көптеген жаһандық ауытқулар.

Процесс:

1-қадам: Min–max тәсілімен орталықтарды инициализациялау немесе бастапқы деректерден кездейсоқ таңдау.

2-қадам: *X*-ті *k* ішкі жиындарға бөлу үшін *K* орталықтары бар *k*-орта әдісін енгізу.

3-қадам: Жергілікті *E* аномалиясын алу үшін алынған әрбір ішкі жиынға LDS алгоритмін қолдану.

4-қадам: 3-қадамда барлық жергілікті ауытқуларды қайта есептеу арқылы әр жергілікті аномалияның *Score* шамаларын алу.

5-қадам: *Score* мәні ε-дан аз жазбалардың жиынтығы болып табылатын *G* ғаламдық аномалиялардың жиынтығын алу.

Қорытынды

Диссертациялық жұмыста көліктік және басқа да сол сияқты салаларда қолданылатын ақпараттық жүйедегі кибершабуылдардың түрлерін тез тануға қабілетті тиімді нейрондық желі модельін және алгоритмін, кибершабуылдарды тану әдістері мен құралдарын әзірлеудің өзекті ғылыми-тұжырымдамалық міндеті шешілді.

Жүргізілген зерттеулер келесі қорытындыларды тұжырымдауға мүмкіндік береді:

- Жалпы мақсаттағы ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды тану жүйелерін әзірлеу мен пайдалануға арналған ғылыми-тұжырымдамалық жұмыстарды талдау нәтижесінде олардың осы жүйелерді дамытудың негізгі жолдарының бірі жасанды нейрондық желілер теориясының заманауи шешімдеріне негізделген желілік трафикті талдау әдістерін енгізу болып табылады.

- желілік кибершабуылдарды нейрондық желіні тану үшін оқу үлгісін құру әдісі жасалды.

- әзірленген нейрондық желі модельдері мен алгоритмдерін қолдану арқылы ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды нейрондық желіні тану әдісі жасалды.

Пайдаланылған әдебиеттер тізімі

1 J.Rubina, Parveen. Neural networks in cyber security. - 2017

2 Ahmad M. S., Ramachandran V. Cafe latte with a free topping of cracked wep retrieving wep keys from road warriors // Proc. Conf. ToorCon. - 2007

3 Aburomman A. A., Reaz M. B. I. A novel SVM-kNN-PSO ensemble method for intrusion detection system // Applied Soft Computing - 2016.

4 Aaron B., Tamir D. E., Rishe N. D., Kandel A. Dynamic incremental fuzzy Cmeans clustering // Proceedings of The The Sixth International Conference on Pervasive Patterns and Applications - 2014

5 Bakhshi T., Ghita B. On internet traffic classification: A two-phased machine learning approach // Journal of Computer Networks and Communications - 2016

6 Муханова А.А. Классификация угроз и уязвимостейинформационной безопасности в корпоративных системах - 2013.

7 Halenar Igor, Juhasova Bohuslava, Juhas Martin, Nesticky Martin - Application of Neural Networks in Computer Security - 2013

8 Талалаев А.А., Тищенко И.П., Фраленко В.П., Емельянова Ю.Г. - Нейросетевая технология обнаружения сетевых атак на информационные ресурсы - 2011

9 E.Kesavulu Reddy - Neural Networks for Intrusion Detection and Its Applications - 2013

10 Information Supplement: Penetration Testing Guidance. PCI Security Standards Council - 2015

11 SANS Institute - Application of Neural Networks to Intrusion Detection - 2015

12 Сканер уязвимостей OpenVas // Электронная версия на сайте: https://www.kali.org/penetration-testing/openvas-vulnerability-scanning.

13 Корнев П.А., Пылькин А.Н., Свиридов А.Ю. - Применение инструментария искусственного интеллекта в системах обнаружения вторжений в вычислительные сети - 2014

14 «KaliLinux- любимец хакеров» на сайтеhttps://prostolinux.ru/kali-linux.

15 Bagirov A. M., Ugon J., Webb D. Fast modified global k-means algorithm for incremental cluster construction // Pattern recognition - 2011

16 Боршевников А.В. - Сетевые атаки. Виды. Способы борьбы - 2011

17 Fritzke B. - A Growing Neural Gas Network Learns Topologies - 2017

18 Павлов В.В. Локальная сеть как инструмент информационной безопасности // Информация–Коммуникация–Общество - 2017

19 . Information Supplement: Penetration Testing Guidance. PCI Security Standards Council - 2015.

20 Муравьёв А.С., Белоусов А.А. - Модифицированный алгоритм растущего нейронного газа, применительно к задаче классификации - 2014

21 Jim Holmström - Growing Neural Gas Experiments with GNG, GNG with Utility and Supervised GNG - 2012