МРНТИ 62.21.29 **DOI 10.48501/3007-6986.2025.90.49.001**

Мукашева Г.Е., Бейсебаева Ж.Е.
«Alikhan Bokeikhan University» білім беру мекемес
Қазақстан, Семей
E-mail: gulzira_7777@mail.ru

ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНА ОТЫРЫП АҚПАРАТТЫ ҚОРҒАУ

Аннотация

Мақалада жасанды интеллект (AI) технологияларын қолдана отырып, ақпаратты қорғаудың заманауи әдістері мен тәсілдері қарастырылады. Ақпараттық қауіпсіздік саласында машиналық оқытуды, нейрондық желілерді және зияткерлік алгоритмдерді қолданудың негізгі бағыттары қарастырылады. Жасанды интеллекттің артықшылықтары атап өтіледі, оны қолданудың шектеулері мен қиындықтары анықталады. АИ базасында практикалық қорғау жүйелерінің мысалдары келтіріледі, сондай-ақ осы саланың даму перспективалары болжанады.

Кілттік сөздер: ақпараттық қауіпсіздік, жасанды интеллект, киберқауіптер, Машиналық оқыту, Big Data, киберқауіпсіздік.

Мукашева Г.Е., Бейсебаева Ж.Е.
УО «Alikhan Bokeikhan University»
Казахстан, Семей
E-mail: gulzira_7777@mail.ru

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация

В статье исследуются современные методы и подходы к защите информации с использованием технологий искусственного интеллекта (ИИ). Рассматриваются основные направления применения машинного обучения, нейронных сетей и интеллектуальных алгоритмов в области информационной безопасности. Подчеркиваются преимущества ИИ, выявляются ограничения и вызовы его применения. Приводятся примеры практических систем защиты на базе ИИ, а также прогнозируются перспективы развития данной области.

Ключевые слова: информационная безопасность, искусственный интеллект, киберугрозы, машинное обучение, Big Data, киберзащита.

Mukasheva G.E., Бейсебаева Ж.Е.
«Alikhan Bokeikhan University»
Kazakhstan, Semey
E-mail: gulzira_7777@mail.ru

INFORMATION PROTECTION USING ARTIFICIAL INTELLIGENCE

Annotation

The article examines modern methods and approaches to information protection using artificial intelligence (AI) technologies. The main directions of application of machine learning, neural networks and intelligent algorithms in the field of information security are considered. The advantages of AI are emphasized; the limitations and challenges of its application are revealed. Examples of practical AI-based protection systems are given, and the prospects for the development of this area are predicted.

Keywords: information security, artificial intelligence, cyber threats, machine learning, Big Data, cyber defense.

Кіріспе

Қазіргі ақпараттық қоғам деректер көлемінің өсуімен, олардың маңыздылығы мен осалдығымен сипатталады. Жаһандық цифрландыру жағдайында ақпараттық қауіпсіздік мәселелері бірінші орынға шығады, өйткені деректердің ағып кетуі немесе бұрмалануы елеулі экономикалық, саяси және әлеуметтік салдарға әкелуі мүмкін. Криптографияға, қол жеткізуді басқару жүйелеріне және антивирустық шешімдерге негізделген ақпаратты қорғаудың дәстүрлі әдістері Күрделі киберқауіптер жағдайында жеткіліксіз болады. Бұл жағдайда жасанды интеллект (AI) технологияларын қолдану ерекше рөл атқарады, олар оқуға, деректердің үлкен массивтерін талдауға және шабуылдардың жаңа түрлеріне бейімделуге қабілетті [1].

Ақпараттық қауіпсіздік-қоғам мен мемлекеттің тұрақты жұмыс істеуінің маңызды шарттарының бірі. Деректер көлемінің ұлғаюы, интернет-технологиялардың белсенді дамуы және киберқылмыстың таралуы ақпаратты қорғаудың жаңа шешімдерін іздеуді қажет етеді.

Классикалық қорғаныс құралдары-брандмауэрлер, антивирустық жүйелер, криптографиялық Алгоритмдер - өзекті болып қала береді, бірақ олар қазіргі шабуылдарға қарсы тиімді бола бермейді. Зиянкестер дәстүрлі қорғаныс механизмдерін айналып өте алатын әлеуметтік инженерия әдістерін, көп деңгейлі шабуыл сценарийлерін, шифрлаушылар мен боттарды пайдаланады.

Жасанды интеллект киберқауіпсіздік үшін жаңа мүмкіндіктер ашады. Ол пайдаланушылардың мінез-құлқын талдауға, жасырын заңдылықтарды анықтауға және белгісіздік жағдайында шешім қабылдауға қабілетті, бұл оны киберқауіптерге қарсы тұрудың күшті құралы етеді .

Негізгі бөлім

Бірінші бағыт қауіп-қатерді талдауға және алдын алуға байланысты. Машиналық оқыту алгоритмдеріне негізделген интрузияны анықтау жүйелері желілік трафиктегі ауытқуларды және пайдаланушылардың әдеттегі мінез-құлқына тән емес әрекеттерді анықтай алады. Классикалық қолтаңба шешімдерінен айырмашылығы, мұндай жүйелер қауіп-қатер туралы мәліметтер базасының жаңартулары әлі жасалмаған шабуылдардың жаңа түрлеріне қарсы тұра алады .

Екінші бағыт - биометриялық аутентификация. Жасанды интеллект бетті тану, саусақ ізі және ирис жүйелерінде белсенді қолданылады. Сонымен қатар, адамның жеке ерекшеліктері талданған кезде мінез-құлық биометриясының әдістері дамиды: теру ритағы, тышқанның қозғалысы немесе жүру ерекшеліктері. Бұл аутентификация жүйелерінің сенімділігін айтарлықтай арттырады және ұрлық немесе құпия сөздің ағып кету қаупін азайтады.

Үшінші бағыт-оқиғаларға жауап беруді автоматтандыру. Қазіргі заманғы қауіпсіздік мониторингі орталықтары (SOC) оқиғалар ағындарын сүзуге, жалған позитивтерді жоюға және ең маңызды қауіптерді көрсетуге көмектесетін ақылды жүйелерді қолданады. Сонымен қатар, кейбір AI негізіндегі шешімдер автоматты түрде қорғаныс әрекеттерін жасай алады: күдікті қосылыстарды блоктау, жұқтырған құрылғыларды оқшаулау немесе жүйені қалпына келтіру процесін бастау [2].

Төртінші бағыт дербес деректерді қорғаумен байланысты. Дифференциалды құпиялылық және Федеративті оқыту әдістері пайдаланушылардың деректеріне тікелей қол жеткізбестен жасанды интеллект модельдерін құруға және үйретуге мүмкіндік береді. Бұл әсіресе ақпаратты қорғау және құпиялылық саласындағы заңнаманы қатаңдату жағдайында маңызды. Сонымен қатар, AI шифрлау сенімділігін арттыру және кілттерді басқару жүйелерін оңтайландыру үшін қолданылады.

Бесінші бағыт-әлеуметтік шабуылдарға қарсы тұру. Зиянкестер пайдаланушыларды адастыру үшін фишингті, жалған сайттарды немесе deepfake мазмұнын жасау технологиясын

жиі пайдаланады. Жасанды интеллект алгоритмдері мәтіндік мазмұнды, метадеректерді және жіберушілердің мінез-құлқын талдау арқылы фишингтік хаттарды анықтай алады. Сондай - ақ жалған аудио және бейне мазмұнын анықтау әдістері белсенді түрде әзірленуде.

Ақпараттық қауіпсіздіктің заманауи қауіптерін шартты түрде бірнеше санатқа бөлуге болады:

1. Кибершабуылдар-вирустар, Трояндар, фишинг, DDoS шабуылдары, эксплуатациялар.

2. Әлеуметтік инженерия - құпия ақпаратқа қол жеткізу үшін адамдарды манипуляциялау.

3. Ішкі қауіптер - ұйым қызметкерлерінің қасақана немесе кездейсоқ деректердің бұзылуы.

4. Инфрақұрылымға қауіп-қатер-бұлтты қызметтердің бұзылуы, IoT құрылғыларының бұзылуы, өнеркәсіптік жүйелерге шабуылдар.

Бұл қауіптердің үнемі күрделенуі қорғаудың интеллектуалды және динамикалық әдістерін енгізуді қажет етеді.

Жасанды интеллект (AI) - бұл адамның танымдық функцияларын модельдеуге бағытталған технологиялардың жиынтығы. Ақпаратты қорғау саласында алгоритмдерге деректерді талдау негізінде жұмыс сапасын жақсартуға мүмкіндік беретін Машиналық оқыту (ML) ең сұранысқа ие болып табылады [3].

Негізгі әдістер:

- мұғаліммен оқыту-қауіптерді жіктеу үшін қолданылады (мысалы, зиянды және қауіпсіз файлдарды анықтау);
- мұғалімсіз оқыту - пайдаланушылардың мінез-құлқындағы ауытқуларды анықтау үшін қолданылады;
- терең оқыту (терең оқыту) - желілік трафик сияқты құрылымдалмаған деректердің үлкен көлемін талдау үшін қолданылады.

Ақпараттық жүйелердегі аномалия - бұл қалыптыдан өзгеше мінез-құлық. AI қолдану кибершабуылдың хабаршысы болуы мүмкін күдікті әрекеттерді тіркеуге мүмкіндік береді:

- бірнеше авторизация әрекеттері;
- файлдарды жаппай көшіру;
- желілік трафиктің күрт өсуі.

AI ақпараттың алып массивтерін (логика, желілік трафик, бақылау деректері) талдау үшін қолданылады. Бұл қолмен анықтау мүмкін емес үлгілерді анықтауға мүмкіндік береді.

Ақпаратты қорғауда АИ қолдану:

1. Жаңа буын антивирустық жүйелері. AI зиянды бағдарламаларды тек қолтаңба арқылы емес, олардың мінез-құлқынан анықтауға мүмкіндік береді.

2. Интеллектуалды аутентификация жүйелері. Биометрия әдістері қолданылады (бетті, дауысты, саусақ іздерін тану). AI оларды дәлірек және контрафактілікке төзімді етеді.

3. Интрузияның алдын алу жүйелері (IPS/IDS). AI желілік трафикті талдайды және классикалық қолтаңба жүйелері үшін мүмкін емес белгісіз шабуылдарды анықтайды.

4. Оқиғаларға жауап беруді автоматтандыру. Жасанды интеллект қауіпті тіркеп қана қоймай, күдікті әрекеттерді өз бетінше бұғаттай алады. 5. Қауіптерді болжау. Өткен шабуылдарды талдау негізінде AI жаңа кибершабуылдардың ықтимал сценарийлерін болжай алады [4].

Жасанды интеллект ақпаратты қорғау саласындағы маңызды құралға айналуда. Оны енгізу қатерлерді анықтау және алдын алу тиімділігін арттыруға, инциденттерге ден қоюды жеделдетуге және дербес деректерді қорғауды қамтамасыз етуге мүмкіндік береді. Сонымен қатар, АИ қолдануға байланысты шектеулер мен тәуекелдерді, сондай-ақ құқықтық және этикалық сипаттағы мәселелерді ескеру қажет. Болашақта жасанды интеллектті киберқауіпсіздік жүйелерімен біріктіру цифрлық қоғам жағдайында ақпаратты қорғау стратегиясын анықтайды.

Жасанды интеллектті қолданудың практикалық мысалдары:

- Банк саласы. Ірі қаржы ұйымдарында AI транзакцияларды талдау және алаяқтық әрекеттерді анықтау үшін қолданылады. Мысалы, Машиналық оқыту алгоритмдері нақты уақыт режимінде клиенттің әдеттегі мінез-құлық үлгісіне сәйкес келмейтін күдікті операцияларды анықтай алады. Бұл қаражатты рұқсатсыз аударуға немесе ұрланған карталарды пайдалануға жол бермейді. Сонымен қатар, мінез-құлық биометриясы жүйелері банктік мобильді қосымшаларда қолданылады: пайдаланушының қолында PIN кодын немесе смартфонның қозғалысын енгізу әдісі талданады [5].

- Мемлекеттік құрылымдар. Мемлекеттік қауіпсіздік органдары мен арнайы қызметтер ашық көздерден келіп түсетін ақпараттың үлкен массивтерін талдау үшін, сондай-ақ мемлекеттік ақпараттық жүйелерге ықтимал кибершабуылдарды анықтау үшін АИ қолданады. Мысалы, мониторинг жүйелері Мемлекеттік желілердегі қалыптан тыс әрекеттерді автоматты түрде анықтай алады және оларды қорғау шараларын қолдана алады. Сонымен қатар, бетті тану технологиялары стратегиялық нысандарға кіруді бақылау үшін бейнебақылау жүйелерінде қолданылады.

- Телекоммуникациялық компаниялар. Байланыс желілерінде аі трафикті талдау және таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдарынан қорғау үшін қолданылады. Машиналық оқытуға негізделген жүйелер шабуылдың тән үлгісін тез тануға және зиянды трафикті қайта бағыттауға немесе сүзуге қабілетті.

- Корпоративтік жүйелер. Ірі халықаралық компаниялар инсайдерлік қауіптерге байланысты күдікті мінез-құлықты анықтайтын қызметкерлерді бақылаудың интеллектуалды жүйелерін пайдаланады. Мысалы, көшірілетін деректер көлемінің күрт өсуі немесе әдеттен тыс жұмыс уақытындағы белсенділік ақпараттың ағып кетуіне ықтимал әрекетті көрсетуі мүмкін.

Артықшылықтарға ақпараттың үлкен массивтерін өңдеу мен талдаудың жоғары жылдамдығы, адам факторына байланысты қателіктердің азаюы және статистикалық заңдылықтарды талдауға негізделген шабуылдардың жаңа түрлерін болжау мүмкіндігі жатады [6].

Дегенмен, шектеулер де бар. Біріншіден, жасанды интеллект жүйелерінің тиімділігі көбінесе олар оқытылатын бастапқы деректердің сапасына байланысты. Екіншіден, шабуылдаушылардың өздері шабуыл жасау үшін AI қолданады, бұл қорғаныс процесін қиындатады. Үшіншіден, Алгоритмдер жалған позитивтер бере алады, бұл мамандардың қосымша қатысуын талап етеді.

Жасанды интеллектке негізделген нақты қорғаныс жүйелерінің мысалдары:

- IBM QRadar advisor with Watson-қауіптерді талдау және ұсыныстар беру үшін AI мүмкіндіктерін пайдаланатын платформа.

- Darktrace-ауытқуларды өздігінен анықтайтын және блоктайтын машиналық оқытуға негізделген киберқауіпсіздік жүйесі.

- Kaspersky Adaptive Security-мақсатты шабуылдардың алдын алу үшін AI қолданатын шешімдер.

- Cylanceprotect-зиянды бағдарламалардың іске қосылуына жол бермейтін жасанды интеллектке негізделген антивирус. Болашақта AI технологиялары киберқауіпсіздікті қамтамасыз етуде шешуші рөл атқарады.

Дамудың келесі бағыттарын ажыратуға болады:

- Адами факторды толығымен жоққа шығаратын өзін-өзі басқаратын қорғаныс жүйелерін құру.

- Жүйенің қандай да бір шешім қабылдағанын түсінуге мүмкіндік беретін explainable аі (түсіндірілетін AI) технологияларын дамыту.

- Ақпаратты барынша қорғауды қамтамасыз ету үшін кванттық криптографиямен AI интеграциясы [7].

Ақпараттық қауіпсіздік саласында жасанды интеллектті қолдану деректерді

қорғау технологиялары эволюциясының табиғи кезеңі болып табылады. AI заманауи киберқауіптерден адаптивті, болжамды және автоматтандырылған қорғауды қамтамасыз ете алады. Алайда, оны енгізу айтарлықтай ресурстарды, мұқият бақылауды және алгоритмдерді үнемі жетілдіруді қажет етеді. Дәстүрлі қорғаныс әдістерін интеллектуалды жүйелермен біріктіретін кешенді тәсіл ғана цифрлық дәуірде қауіпсіздіктің жоғары деңгейін қамтамасыз ете алады.

Қорытынды. Жасанды интеллект ақпаратты қорғаудың маңызды құралына айналады. Ол ауытқуларды анықтауды, қауіптерді болжауды және кибершабуылдарға жауап беруді автоматтандыруды қамтамасыз етеді. Сонымен қатар, AI енгізу деректер сапасына, алгоритмдердің осалдығына және этикалық аспектілерге байланысты тәуекелдерді ескеруді талап етеді. "Адам + жасанды интеллект" гибридті жүйелерін дамыту, бұлтты платформаларға жасанды интеллект интеграциясы және криптографияда интеллектуалды әдістерді қолдану Киберқауіпсіздіктің болашағын анықтайды. Бұл жиынтықта XXI ғасырдың сенімді және тұрақты ақпараттық қауіпсіздік жүйесін құруға мүмкіндік береді.

Пайдаланылған әдебиеттер тізімі

1. Allen Dzh. Iskusstvennyj intellekt i kiberbezopasnost'. - M.: Infra-M, 2022.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. - MIT Press, 2016.
3. Bishop C. Pattern Recognition and Machine Learning. - Springer, 2006.
4. Kasperskij E. Kiberugrozy XXI veka. - M.: Al'pina, 2021.
5. Darktrace Research. The Future of AI in Cybersecurity. - 2022.
6. IBM Security. AI-Driven Threat Detection and Response. - 2023.
7. OpenAI Research. AI and Security: Challenges and Opportunities. - 2023.

List of references

1. Allen Dzh. Iskusstvennyj intellekt i kiberbezopasnost'. - M.: Infra-M, 2022.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. - MIT Press, 2016.
3. Bishop C. Pattern Recognition and Machine Learning. - Springer, 2006.
4. Kasperskij E. Kiberugrozy XXI veka. - M.: Al'pina, 2021.
5. Darktrace Research. The Future of AI in Cybersecurity. - 2022.
6. IBM Security. AI-Driven Threat Detection and Response. - 2023.
7. OpenAI Research. AI and Security: Challenges and Opportunities. - 2023.

Авторлар туралы мәліметтер

Мукашева Гульзира Ерсаиновна

Лауазымы: Семей қаласы, «Alikhan Bokeikhan University», «Ақпараттық-техникалық ғылымдар» кафедрасы, аға оқытушы, магистр

Почталық мекен-жайы: 071410, Қазақстан, Семей қаласы, К.Бөгенбайұлы көшесі, 36-53

Ұялы тел.: 87023973356

E-mail: gulzira_7777@mail.ru

Бейсебаева Жадыра Есенжоловна

Лауазымы: Семей қаласы, «Alikhan Bokeikhan University», «Ақпараттық-техникалық ғылымдар» кафедрасы, аға оқытушы, магистр

Почталық мекен-жайы: 071412, Қазақстан, Семей қаласы, 40-квартал көшесі, 1-7

Ұялы тел.: 87471418494

E-mail: beysebaeva.95@mail.ru

Сведения об авторах

Мукашева Гульзира Ерсаиновна

Должность: г.Семей, «Alikhan Bokeikhan University», кафедра «Информационно-технических наук», старший преподаватель, магистр
Почтовый адрес: 071410, Казахстан, г.Семей, ул.К.Богенбайулы, 36-53
Мобильный тел.: 87023973356
E-mail: gulzira_7777@mail.ru
Бейсебаева Жадыра Есенжоловна
Должность: г.Семей, «Alikhan Bokeikhan University», кафедра «Информационно-технических наук», старший преподаватель, магистр
Почтовый адрес: 071412, Казахстан, г.Семей, ул. 40-квартал, 1-7
Мобильный тел.: 87471418494
E-mail: beysebaeva.95@mail.ru

Information about the author
Mukasheva Gulmira Ersainovna
Position: Semey, «Alikhan Bokeikhan University», Department of «Information Technology Sciences», senior lecturer, master
Postal address: 071410, Kazakhstan, Semey, K. Bogenbayuly str., 36-53
Mobile phone: 87023973356
E-mail: gulzira_7777@mail.ru
Beisebayeva Zhadyra Yesenzholovna
Position: Semey, «Alikhan Bokeikhan University», Department of «Information Technology Sciences», senior lecturer, master
Postal address: 071410, Kazakhstan, Semey, 40th Street, 1-7
Mobile phone: 87471418494
E-mail: beysebaeva.95@mail.ru