IT-технологиялар, энергетика, автоматтандыру және есептеу техникасы

DOI: https://doi.org/10.53002/100

THE USE OF ARTIFICIAL INTELLIGENCE ENSURES DATA SECURITY

Seilkhanov A.

Yessenov university, Aktau, Kazakhstan
**Corresponding author e-mail: a.seilkhanov@ttc.kz*

Author information:
Seilkhanov Adlet, Yessenov University, Aktau, Kazakhstan, e-mail: a.seilkhanov@ttc.kz

Abstract — This paper presents an analysis of current approaches to the application of artificial intelligence (AI) technologies in the field of information security. The study examines the potential of machine learning, deep learning, and intelligent data analysis methods for detecting, preventing, and mitigating cybersecurity threats. Particular attention is given to the use of AI for network attack detection, anomalous user behavior analysis, malware protection, prevention of unauthorized access to information, and automation of information security monitoring and incident response processes. The study demonstrates that the application of intelligent algorithms significantly improves the efficiency of processing large volumes of data in real time, reduces the time required to detect cyber threats, and increases the accuracy of threat classification compared with traditional security methods. The advantages of adaptive security systems capable of learning from emerging attack patterns and continuously updating threat detection models with minimal human intervention are also discussed. The findings indicate the significant potential of artificial intelligence to enhance the protection of information resources and critical information infrastructures. The implementation of AI technologies contributes to preventing unauthorized access to information, timely identification of system vulnerabilities, prediction of potential cyberattacks, and reduction of the consequences of information security breaches. At the same time, it is emphasized that the effectiveness of intelligent security systems largely depends on the quality of training data, the robustness of AI models against adversarial attacks, and compliance with privacy and data protection requirements during information processing. The obtained results confirm the promising prospects for the further development and integration of artificial intelligence technologies into comprehensive information security systems. Their practical implementation will improve the reliability of digital resource protection, automate security decision-making processes, and enhance the resilience of information systems against modern cyber threats.
Keywords — cybersecurity, information security, artificial intelligence, provided, information.

ИННОВАЦИЯЛЫҚ МАТЕРИАЛДАРДЫҢ БЕРІКТІК СИПАТТАМАЛАРЫН ТАЛДАУ

Сейлханов А.

«Ш. Есенов атындағы Каспий мемлекеттік технологиялар және инжиниринг университеті» КеАҚ, Ақтау, Қазақстан
**Автор-корреспондент e-mail: a.seilkhanov@ttc.kz*

Автор туралы ақпарат:
Сейлханов Адлет, «Ш. Есенов атындағы Каспий мемлекеттік технологиялар және инжиниринг университеті», Ақтау, Қазақстан, e-mail: a.seilkhanov@ttc.kz

Аңдатпа — Жұмыста ақпараттық қауіпсіздікті қамтамасыз ету саласында жасанды интеллект (ЖИ) технологияларын қолданудың заманауи бағыттарына талдау жүргізілді. Машиналық оқыту, терең оқыту және деректерді интеллектуалды талдау әдістерін киберқауіптерді анықтау, алдын алу және олардың салдарын азайту мақсатында пайдалану мүмкіндіктері қарастырылды. Желілік шабуылдарды анықтау, пайдаланушылардың аномальды әрекеттерін талдау, ақпараттық жүйелерді зиянды бағдарламалық қамтамасыз етуден қорғау, ақпаратқа рұқсатсыз қол жеткізудің алдын алу, сондай-ақ ақпараттық қауіпсіздік оқиғаларын бақылау және оларға ден қою процестерін автоматтандыру мәселелеріне ерекше назар аударылды. Зерттеу нәтижелері жасанды интеллект алгоритмдерін қолдану нақты уақыт режимінде үлкен көлемдегі деректерді өңдеу тиімділігін айтарлықтай арттыратынын, қауіптерді анықтау уақытын қысқартып, дәстүрлі қорғау әдістерімен салыстырғанда оларды жіктеу дәлдігін жоғарылататынын көрсетті. Сонымен қатар, жаңа типтегі шабуылдарға өздігінен бейімделіп, қауіптерді анықтау модельдерін мамандардың елеулі араласуынсыз жаңарта алатын бейімделгіш

қауіпсіздік жүйелерінің артықшылықтары қарастырылды. Зерттеу қорытындылары жасанды интеллекттің ақпараттық ресурстар мен аса маңызды ақпараттық инфрақұрылымдардың қорғалу деңгейін арттырудағы әлеуетінің жоғары екенін дәлелдейді. Бұл технологияны пайдалану ақпаратқа рұқсатсыз қол жеткізудің алдын алуға, осалдықтарды уақтылы анықтауға, ықтимал кибершабуылдарды болжауға және ақпараттық қауіпсіздік бұзылуының салдарын азайтуға мүмкіндік береді. Сонымен қатар, интеллектуалды жүйелердің тиімділігі оқыту деректерінің сапасына, модельдердің қасақана әсерлерге төзімділігіне және ақпаратты өңдеу кезінде құпиялылық талаптарының сақталуына тәуелді екені атап өтілді. Алынған нәтижелер жасанды интеллект технологияларын ақпараттық қауіпсіздіктің кешенді жүйелеріне одан әрі дамыту мен енгізудің перспективалылығын растайды. Оларды тәжірибеде қолдану цифрлық ресурстарды қорғаудың сенімділігін арттырып, шешім қабылдау процестерін автоматтандыруға және ақпараттық жүйелердің заманауи киберқауіптерге төзімділігін күшейтуге мүмкіндік береді.
Түйін сөздер — инновациялық материалдар, беріктік сипаттамалары, композиттік материалдар, наноқұрылымдар, механикалық қасиеттер, талдау әдістері.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ДАННЫХ

Сейлханов А.

НАО «Каспийский университет технологий и инжиниринга имени Ш.Есенова», Актау, Казахстан
**Автор-корреспондент e-mail: a.seilkhanov@ttc.kz*

Информация об авторе:
Сейлханов Адлет, НАО «Каспийский университет технологий и инжиниринга имени Ш.Есенова», Актау, Казахстан, e-mail: a.seilkhanov@ttc.kz

Аннотация. **—** В работе проведен анализ современных направлений применения технологий искусственного интеллекта (ИИ) в области обеспечения информационной безопасности. Рассмотрены основные возможности использования методов машинного обучения, глубокого обучения и интеллектуального анализа данных для выявления, предотвращения и минимизации последствий киберугроз. Особое внимание уделено применению ИИ при обнаружении сетевых атак, анализе аномальной активности пользователей, защите информационных систем от вредоносного программного обеспечения, предотвращении несанкционированного доступа к данным, а также автоматизации процессов мониторинга и реагирования на инциденты информационной безопасности. В ходе исследования установлено, что использование интеллектуальных алгоритмов позволяет существенно повысить эффективность обработки больших объемов данных в режиме реального времени, сократить время обнаружения угроз и повысить точность их классификации по сравнению с традиционными методами защиты. Рассмотрены преимущества адаптивных систем безопасности, способных самостоятельно обучаться на новых типах атак и своевременно обновлять модели обнаружения угроз без значительного вмешательства специалистов. Сделаны выводы о высоком потенциале применения искусственного интеллекта для повышения уровня защищенности информационных ресурсов и критически важных информационных инфраструктур. Использование данной технологии способствует предотвращению несанкционированного доступа к информации, своевременному выявлению уязвимостей, прогнозированию возможных кибератак и снижению последствий нарушений информационной безопасности. Вместе с тем отмечено, что эффективность интеллектуальных систем во многом зависит от качества обучающих данных, устойчивости моделей к преднамеренным воздействиям и соблюдения требований конфиденциальности при обработке информации. Полученные результаты подтверждают перспективность дальнейшего развития и внедрения технологий искусственного интеллекта в комплексные системы информационной безопасности. Их практическое применение позволит повысить надежность защиты цифровых ресурсов, автоматизировать процессы принятия решений и обеспечить более высокий уровень устойчивости информационных систем к современным киберугрозам.
Ключевые слова — кибербезопасность, информационная безопасность, искусственный интеллект, данные, информация.

НЕГІЗГІ ЕРЕЖЕЛЕР

Жасанды интеллект технологияларын қолдану ақпараттық қауіпсіздік жүйелерінің тиімділігін арттырып, киберқауіптерді нақты уақыт режимінде анықтауға және олардың алдын алуға мүмкіндік береді.

Машиналық оқыту алгоритмдері пайдаланушылардың мінез-құлқын талдау, аномалияларды анықтау және жаңа қауіп-

қатерлерге автоматты түрде бейімделу арқылы ақпараттық жүйелердің қорғаныс деңгейін жоғарылатады. Жасанды интеллект негізіндегі биометриялық аутентификация, динамикалық қол жеткізуді басқару және автоматтандырылған қауіптерді талдау жүйелері дәстүрлі ақпараттық қауіпсіздік әдістеріне қарағанда жоғары сенімділік пен жылдамдықты қамтамасыз етеді.

КІРІСПЕ

Ақпараттық қауіпсіздік күннен-күнге кеңінен енгізіліп, қолданылып жатқан компьютерлік жүйелерді ескере отырып, қазіргі әлемде маңызды орын алады. Әрбір адам немесе компания өзінің ақпаратын ұрлау, жою немесе өзгерту қаупін азайтқысы келеді. Сол сияқты автоматтандырылған жүйеде де киберқауіпсіздік үлкен рөл атқарады [1-3].

IDC зерттеуіне сәйкес, «2020 жылға қарай ұйымдар киберқауіпсіздікке арналған бағдарламалық қамтамасыз етуге, қызметтерге және жабдықтарға 101,6 миллиард доллар жұмсайды».

Алдыңғы қатарлы ұйымдар ондаған қауіпсіздік өнімдерін біріктіргенімен, шабуылдарға осал болудан әлі де қорқады. Бұл қауіпсіздікке шығындардың артуына қарамастан, қауіпсіздік бұзушылықтарының тоқтау немесе баяулау белгілерін көрсетпейтінін білдіреді.

Киберқауіпсіздік саласындағы озық технологияларды енгізу уақытты талап етеді, бұл шабуылдарды егжей-тегжейлі анықтауға және оларды киберқауіпсіздік мамандарынан да жылдам шешуге мүмкіндік береді. Осындай технологиялардың бірі – жасанды интеллект [4-6]. ЖИ – бұл өзге мүмкіндіктерімен қатар (сурет 1), қатерлерді анықтап, оларды жою және болдырмау үшін қажетті әрекеттерді автоматты түрде жүзеге асыра алатын технология.

Зерттеудің маңыздылығы. Ақпараттық жүйелердің кеңінен қолданылуына және кибершабуылдардың күрделене түсуіне байланысты ақпараттық қауіпсіздікті қамтамасыз ету қазіргі қоғамның маңызды міндеттерінің біріне айналды. Дәстүрлі қауіпсіздік құралдары жаңа типтегі қауіп-қатерлерге әрдайым тиімді қарсы тұра алмайды. Осыған байланысты жасанды интеллект технологияларын қолдану қауіптерді ерте анықтауға, шабуылдарға жедел әрекет етуге және қорғау жүйелерінің тиімділігін арттыруға мүмкіндік береді. Зерттеу нәтижелері мемлекеттік мекемелерде, кәсіпорындарда және ақпараттық жүйелерде заманауи киберқауіпсіздік шешімдерін енгізуге ғылыми-тәжірибелік негіз бола алады.

Зерттеудің жаңалығы. Зерттеудің жаңалығы жасанды интеллект технологияларының ақпараттық қауіпсіздік жүйелеріндегі қолданылуын кешенді талдауында және олардың киберқауіптерді анықтау, биометриялық аутентификация, динамикалық қол жеткізуді басқару және шабуылдарға автоматты түрде әрекет ету мүмкіндіктерін жүйелеуінде жатыр. Сонымен қатар, машиналық оқыту алгоритмдерін пайдалану арқылы қауіп-қатерлерді болжау, жүйенің жаңа шабуыл түрлеріне бейімделуі және қауіпсіздік процестерін автоматтандырудың артықшылықтары негізделген. Зерттеу нәтижелері ақпараттық қауіпсіздікті қамтамасыз етуде жасанды интеллекттің тиімділігін арттыруға бағытталған ұсыныстарды ұсынады.

ӘДІСТЕР МЕН МАТЕРИАЛДАР

1. Әдебиеттерді талдау: ЖИ негізіндегі киберқауіпсіздік құралдарының теориялық негіздері мен қазіргі тәжірибесі зерттелді. Ғылыми мақалалар, зерттеу есептері және IDC сияқты аналитикалық деректер кеңінен қолданылды [1-6].
2. Құралдар мен технологияларды салыстыру: ЖИ технологияларын қолданатын әртүрлі биометриялық аутентификация, үлгіні тану, қауіптерді анықтау және динамикалық аутентификация жүйелері салыстырмалы түрде талданды. Әр құралдың артықшылықтары мен шектеулері анықталды.
3. Машиналық оқытуды қолдану: Қауіптерді анықтау және шабуылдарға жедел әрекет ету процестерінде машиналық оқыту алгоритмдері енгізілді. Бұл әдіс жүйенің зиянды әрекеттерді дербес және нақты уақыт режимінде тануына мүмкіндік береді.
4. Эмпирикалық бақылау: ЖИ құралдарының нақты қолдану сценарийлерінде тиімділігі тестіленді. Бұл биометриялық аутентификация, шабуылдарды алдын алу және динамикалық қол жеткізу құқықтарын өзгерту сияқты функцияларды қамтиды.

НӘТИЖЕЛЕР ЖӘНЕ ТАЛҚЫЛАУ

Инженерлік бақылау: ЖИ жүйелерінің жұмысын қадағалау үшін адам-инженерлердің қатысуы қажет, себебі кейбір ерекше жағдайлар машиналық алгоритмдерге толық көрінбеуі мүмкін. Бұл әдіс жүйенің қауіпсіздігін қамтамасыз ете отырып, дұрыс шешім қабылдауға мүмкіндік береді [7].

ЖИ негізіндегі құралдар киберқауіпсіздіктегі әртүрлі қажеттіліктерге жауап береді [8].

1. Биометриялық аутентификация.

Құпиясөздер бұзылуы мүмкін, бұл пайдаланушының, кәсіпорынның немесе мемлекеттік органның маңызды ақпаратын қатерге тігеді. Мұндай жағдайда ЖИ негізіндегі аутентификация, яғни саусақ ізін немесе алақанды сканерлеу әлдеқайда қауіпсіз болып саналады және жүйе оларды сенімді түрде сканерлей алады. Биометриялық логиндер құпиясөздермен байланысты болған кезде, пайдаланушы деректерін бұзу ықтималдығы айтарлықтай төмендейді.

2. Қауіптерді анықтауды жеделдету.

Кәдімгі киберқауіпсіздік жүйелері әртүрлі зиянды бағдарламалардың түрлерін бір уақытта өңдей алмайды. Бұдан бөлек, киберқауіпсіздік деңгейі ғана емес, хакерлер де өз стандарттарын көтеріп отыр. Кеңейтілген қауіп-қатерлерді жылдам анықтау үшін осындай мәселелерді шеше алатын озық қауіпсіздік құралдарын пайдалану қажет.

Компаниялар үнемі жаңартылып отыратын озық алгоритмдер мен кодтарды пайдалана отырып, үлгілерді тану арқылы қауіп-қатерді оңай анықтай алатын ЖИ негізіндегі басқарылатын жүйелерді енгізуде. ЖИ машиналық оқытумен бірге қолданылғанда сайтты айналып өту жолын, зиянды бағдарламалардың микро-мінез-құлқын және кез келген қасақана әрекеттерді талдауда тиімді, бұл қосымша дұрыс шешім қабылдауға көмектеседі.

3. Шабуылдарға жедел әрекет ету.

Қауіптерді нақты уақыт режимінде анықтау, егер жүйе олармен күресе алмай және оларды елеулі зиян келтірмей тұрып алдын ала алмайтын болса, ешқандай мәнге ие болмайды.

Хакерлер тобы жүйеге әртүрлі нүктелерден шабуыл жасағанда, ЖИ бұл нүктелерді дереу байланыстырып, шабуылды болдырмау жоспарларын автоматты түрде ұсынады. ЖИ зияткерлік талдауды қолданады, ол шабуылдарды анықтау мен жою үшін қарапайым әрі жылдам тәсіл болып табылады. Мысалы, ЖИ жүйесі жүйеден зиянды файл тапқанда, ол алдымен бұл файлды жүйеден оқшаулайды және оқиғаларды журналға тіркейді, бұл кейінгі талдауды жеңілдетеді.

4. Динамикалық аутентификация ортасын құру.

Деректер желілерде де ұсталып қалуы мүмкін. Бұл – жүйелерге қашықтан қол жеткізетін қызметкерлер үшін алаңдатарлық жағдай, яғни дәстүрлі аутентификация үлгілері енді қауіпсіз емес дегенді білдіреді. Осындай сәтте ЖИ көмекке келеді.

ЖИ жүйелері нақты уақыт режимінде жұмыс істейтін жаһандық аутентификация ортасын жасайды, ол көпфакторлы аутентификацияны қолдана отырып, қол жеткізу құқықтарын пайдаланушының орналасқан жеріне немесе желісіне сәйкес өзгертеді. Бұған қолданбада, құрылғыда және желіде пайдаланушының мінез-құлқын деректерге қашықтан қол жеткізу кезінде жинау және талдау кіреді.

5. Адамның қатысуын азайту.

Ешбір машина адамдардың шығармашылық әлеуетін, қиялын және ойлау қабілетін асыра алмайды. Бірақ инженерлер қабылдайтын шешімдер дұрыс деректер жиынтығымен, пікірлермен және ағымдағы үрдістермен де нығайтылады.

Маңызды деректерді зерттеу және пайдалану көп уақытты алады, ал жоғары тәуекелді тапсырманы жедел шешу мүмкін болмай қалады. Компаниялар ЖИ технологиясын қолданатын қауіпсіз қосымшалар жасағанда, қауіпсіздік қызметкерлері қауіп-қатерлерді анықтау мен алдын алуды автоматтандырудың арқасында адам араласуынсыз біраз жеңілдік алады.

Пайдаланушының мінез-құлқын үздіксіз талдау мен болжамдық талдау инженердің жүйені бірқатар шабуылдардан қорғаудағы араласуын азайтады. Үнемделген уақытты шығармашылық және жемісті бастамаларға жұмсауға болады [9,10].

6. ЖИ жүйелерінің интеграциясы және үздіксіз оқыту.

ЖИ шешімдері тек жеке компонент ретінде ғана емес, сонымен қатар ұйымның қауіпсіздік экожүйесіне толық интеграцияланған түрде тиімді жұмыс істейді. Машиналық оқыту алгоритмдері деректердің жаңа үлгілерін үздіксіз талдап, жүйені жаңа қауіп-қатерлерге бейімдеп отырады. Бұл тәсіл дәстүрлі қауіпсіздік жүйелерінің шектеулерін жеңіп, шабуылдарға қарсы белсенді қорғаныс қабілетін арттырады.

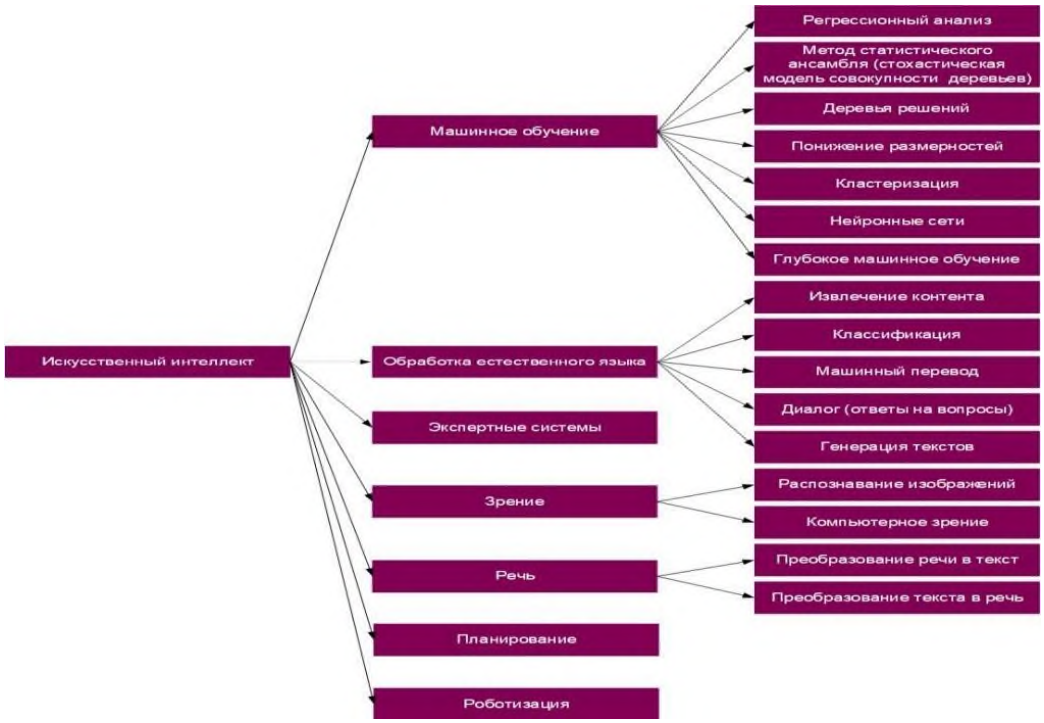
Сонымен қатар, ЖИ жүйелерінің интеграциясы келесі артықшылықтарды қамтамасыз етеді:

1) Үлкен деректерді талдау мүмкіндігі: ЖИ миллиардтаған желілік логтар, серверлік журналдар және қолданушылардың әрекеттерін талдай отырып, адам қабылдай алмайтын көлемде ақпаратты өңдей алады. Бұл кибершабуылдарды алдын ала анықтау мен қауіптерді классификациялау тиімділігін айтарлықтай арттырады.

2) Автоматтандырылған шешім қабылдау: Қауіп анықталған сәттен бастап ЖИ алдын ала сценарийлерді іске қосып, шабуылдардың әсерін минимизациялауға бағытталған әрекеттерді автоматты түрде жүзеге асыра алады. Мысалы, зиянды файлды оқшаулау, қолданушының қол жеткізу құқықтарын уақытша шектеу немесе желілік трафикті қайта бағыттау.

3) Үздіксіз оқыту және бейімделу: ЖИ жүйесі жаңа шабуыл үлгілері мен қауіп-қатер әдістерін үйреніп, алгоритмдерін жаңартады. Бұл әсіресе нөлдік күндік шабуылдар (zero-day attacks) сияқты алдын ала болжанбайтын қауіптерге қарсы күресте тиімді.

4) Интеграцияланған мониторинг және аналитика: ЖИ орталықтандырылған бақылау панелін пайдаланып, жүйелердің қауіпсіздік жағдайын нақты уақыт режимінде бақылауға мүмкіндік береді. Бұл инженерлерге тез арада дұрыс шешім қабылдауға және қауіпсіздік саясаттарын икемді түрде реттеуге мүмкіндік береді.



Сурет 1 - Жасанды интеллектті қолдану салалары

ҚОРЫТЫНДЫ

Жасанды интеллект жүйелері адамдар арқылы үйретіліп, басқарылады және кейбір жағдайларда адам-инженерлердің қажеттілігі міндетті болып табылады. Себебі олар машиналар анықтай алмайтын ауытқулардан тыс шығып, болжанған шабуылдың шын екенін растауға қабілетті. Сонымен қатар, ЖИ технологиялары киберқауіптерді алдын ала анықтау, шабуылдарға жылдам әрекет ету және жүйенің жалпы қауіпсіздік деңгейін арттыруда маңызды рөл атқарады. Адам мен ЖИ арасындағы үйлесім осы жүйелердің тиімділігін максималды түрде қамтамасыз етеді: ЖИ рутиналық және уақытты қажет ететін тапсырмаларды автоматтандырса, инженерлер стратегиялық шешімдер қабылдауға, жүйенің әлсіз тұстарын анықтауға және күрделі шабуылдарды болдырмауға бағытталады. Осылайша, жасанды интеллект және адам-инженерлердің бірлескен жұмысы заманауи киберқауіпсіздіктің тиімді және сенімді негізін құрайды.

МҮДДЕЛЕР ҚАҚТЫҒЫСЫ

Автор осы зерттеуді орындау және мақаланы жариялау барысында мүдделер қайшылығы жоқ екенін мәлімдейді.

ҚАРЖЫЛАНДЫРУ

Авторлар осы зерттеуді орындау кезінде сыртқы қаржыландырудың жоқтығын мәлімдейді.

АЛҒЫС

Автор қолжазбаны мұқият қарастырып, мақаланың мазмұны мен сапасын едәуір жақсартуға мүмкіндік берген құнды ескертулері мен ұсынымдары үшін журналдың редакторы мен рецензентіне шынайы алғысын білдіреді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

[1] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Hoboken, NJ, USA: Pearson, 2022.

[2] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2023 (reprint edition).

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 9th ed. Hoboken, NJ, USA: Pearson, 2024.

[4] W. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston, MA, USA: Addison-Wesley Professional, 2024.

[5] J. C. Cannon, Cybersecurity for Beginners. Birmingham, U.K.: Packt Publishing, 2022.

[6] M. Wooldridge, The Road to Conscious Machines: The Story of AI, Updated Edition. London, U.K.: Pelican Books, 2023.

[7] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD, USA: NIST, Jan. 2023.

[8] ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Geneva, Switzerland: International Organization for Standardization, 2022.

[9] ISO/IEC 23894:2023, Information Technology—Artificial Intelligence—Guidance on Risk Management. Geneva, Switzerland: International Organization for Standardization, 2023.

[10] ENISA, ENISA Threat Landscape 2024. Heraklion, Greece: European Union Agency for Cybersecurity, 2024.

REFERENCES

[1] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Hoboken, NJ, USA: Pearson, 2022.

[2] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2023 (reprint edition).

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 9th ed. Hoboken, NJ, USA: Pearson, 2024.

[4] W. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston, MA, USA: Addison-Wesley Professional, 2024.

[5] J. C. Cannon, Cybersecurity for Beginners. Birmingham, U.K.: Packt Publishing, 2022.

[6] M. Wooldridge, The Road to Conscious Machines: The Story of AI, Updated Edition. London, U.K.: Pelican Books, 2023.

[7] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD, USA: NIST, Jan. 2023.

[8] ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Geneva, Switzerland: International Organization for Standardization, 2022.

[9] ISO/IEC 23894:2023, Information Technology—Artificial Intelligence—Guidance on Risk Management. Geneva, Switzerland: International Organization for Standardization, 2023.

[10] ENISA, ENISA Threat Landscape 2024. Heraklion, Greece: European Union Agency for Cybersecurity, 2024.