Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

ҒТАМР 32.70.10
ӘОЖ 004.056.5
DOI: 10.53002/100

Сейлханов А. Дж.

Ш.Есенов атындағы Каспий мемлекеттік технологиялар және инжиниринг университеті, Актау қ., Қазақстан
(E-mail.ru: a.seilkhanov@ttc.kz)

Жасанды интеллектті қолдану деректер қауіпсіздігін қамтамасыз етуде

Жасанды интеллектті қолданудың ықтимал жолдарына талдау жасалды ақпараттық қауіпсіздікті қамтамасыз ету саласындағы. Потенциал туралы қорытындылар жасаладырұқсат етілмеген технологияның алдын алу үшін осы жоғары технологияны пайдалану ақпаратқа қол жеткізу, сондай-ақ ақпараттық қауіпсіздікті бұзу кезіндегі салдарларды азайту.

Түйін сөздер: киберқауіпсіздік, ақпараттық қауіпсіздік, жасанды интеллект, берілген, ақпарат.

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.

Методология

1. Әдебиеттерді талдау: ЖИ негізіндегі киберқауіпсіздік құралдарының теориялық негіздері мен қазіргі тәжірибесі зерттелді. Ғылыми мақалалар, зерттеу есептері және IDC сияқты аналитикалық деректер 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.

Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

Зерттеу нәтижелері

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

ЖИ негізіндегі құралдар киберқауіпсіздіктегі әртүрлі қажеттіліктерге жауап береді.

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.

Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

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:

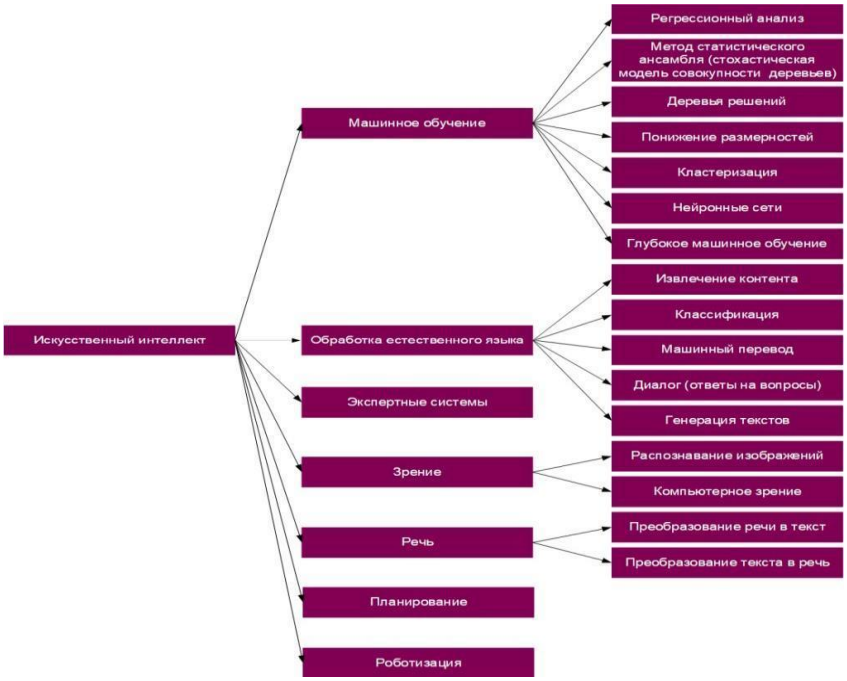
1) Үлкен деректерді талдау мүмкіндігі: ЖИ миллиардтаған желілік логтар, серверлік журналдар және қолданушылардың әрекеттерін талдай отырып, адам қабылдай алмайтын көлемде ақпаратты өңдей алады. Бұл кибершабуылдарды алдын ала анықтау мен қауіптерді классификациялау тиімділігін айтарлықтай арттырады.

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.

5) Болжау және алдын алу мүмкіндігі: ЖИ жүйесі өткен шабуыл үлгілерін және пайдаланушының мінез-құлқын талдап, әлеуетті қауіптерді алдын ала болжап, алдын алу шараларын ұсынады. Бұл жүйенің белсенді қорғаныс қабілетін арттырып, ұйымның қауіпсіздік мәдениетін күшейтеді.



1-сурет. Жасанды интеллектті қолдану салалары

Қорытынды

Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

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.

Әдебиеттер тізімі

1. Чипига А. Ф. Автоматтандырылған жүйелердің ақпараттық қауіпсіздігі. — М.: Гелиос АРВ, 2010. — 336 с.

2. Ефимова Л. Л., Кочерга С. А. Ақпараттық қауіпсіздік. Ресейлік және шетелдік тәжірибе: монография. — М.: Юнити, 2015. — 239 с.

3. Петров А. А. Компьютерлік қауіпсіздік. Қорғаудың криптографиялық әдістері. — М.: ДМК, 2000. — 448 с.

4. Russell S. Жасанды интеллект: заманауи тәсіл. — Pearson Education India, 2015. — 1164 с. б.

5. Taulli T. Жасанды интеллект негіздері: техникалық емес кіріспе. / 2-ші басылым. — Apress, 2019. — 200 с.

6. Андрейчиков А. В., Андрейчикова О. Н. Инновatикадағы стратегиялық шешімдерді жүйелік талдау және синтез: Инновацияларды жүйелік талдау мен синтездеудің математикалық, эвристикалық және интеллектуалдық әдістері: оқу құралы. — М.: Ленанд, 2015. — 306 с.

Сейлханов А. Дж.

Использование искусственного интеллекта в обеспечении безопасности данных

Проведен анализ возможных путей применения искусственного интеллекта в области обеспечения информационной безопасности. Выводы о потенциале заключаются в том, чтоиспользование этой высокой технологии для предотвращения несанкционированных технологий для доступа к информации, а также для уменьшения последствий нарушения информационной безопасности.

Ключевые слова: кибербезопасность, информационная безопасность, искусственный интеллект, данные, информация.

Seilkhanov A. Dz.

The use of artificial intelligence ensures data security

The analysis of possible ways of using artificial intelligence in the field of information security was carried out. Conclusions are drawn about the potentialuse of this high technology to prevent unauthorized access to information, as well as minimize the consequences in violation of Information Security.

Key words: cybersecurity, information security, artificial intelligence, provided, information.

References

Раздел 3. «IT-технологии, энергетика, автоматизация и вычислительная техника»

1. Chipiga A.F. Avtomattandırılğan jüýelerdiñ aqparattıq qauipsizdigi. – M.: Gelios ARV, 2010. – 336 s.

2. Efimova L.L., Koçerga S.A. Aqparattıq qauipsizdik. Reseylik jäne şeteldik täjiribe: monografïya. – M.: Yuniti, 2015. – 239 s.

3. Petrov A.A. Kompüterlik qauipsizdik. Qorğawdıñ krïptografïyalıq ädisteri. – M.: DMK, 2000. – 448 s.

4. Russell S. Jasandı intellekt: zamanaýı täsïl. – Pearson Education India, 2015. – 1164 s.

5. Taulli T. Jasandı intellekt negizderi: texnïkalıq emes kirïspe. / 2-şi basılım. – Apress, 2019. – 200 s.

6. Andreyçikov A.V., Andreyçikova O.N. Innovatïkadağı strategïyalıq şeşimderdi jüýelik taldaw jäne sïntez: Innovacïyalarni jüýelik taldaw men sïntezdewdiñ matematikalıq, evristikalıq jäne intellektualdıq ädisteri: oqw quralı. – M.: Lenand, 2015. – 306 s.