**Жоба туралы қысқаша ақпарат**

| | |
|---|---|
| Жоба аты | AP19174716 «Компьютерлік жүйелерге басып кіруді анықтаудың тиімділігін арттыру үшін Байес желілері негізінде шешімдер қабылдауды қолдау жүйесін әзірлеу» (0123РК00972) |
| Жоба өзектілігі | Қолданыстағы басып кіруді анықтау жүйелерін және оқиғаларды жинау және корреляциялау жүйелерін (Security Information and Event Management, SIEM) талдау ақпараттандыру объектілерінің (АО) ақпараттық қауіпсіздігін (АҚ) және киберқауіпсіздігін (КҚ) ықтимал бұзушылардың әрекеттерін анықтау үшін пайдаланылатын деректерді талдау процестерін интеллектуализациялау үрдісін көрсетеді. Бұл әсіресе компьютерлік және ақпараттық жүйелердің жұмыс істеу процесін тұрақсыздандыруға бағытталған зиянды әрекеттердің саны мен сапасының артуынан байқалады. АО ақпараттық-коммуникациялық желілеріне енуді анықтаудың заманауи жүйелеріне (БКАЖ) арналған математикалық әдістерге жүргізілген талдау олардың бірқатар артықшылықтары мен кемшіліктерін анықтады. Бүгінгі күні қолданыстағы БКАЖ шабуылдардың жаңа түрлеріне қарсы, әсіресе, шабуыл белгілері әлсіз құрылымдалған деректермен немесе жаңа қауіптерді танудың тиісті тапсырмасындағы нақты емес критерийлермен сипатталатын жағдайларда әрдайым тиімді бола бермейді. Сондықтан, қорғаныс тарапының функционалдық мүмкіндіктерін кеңейту мақсатында шешім қабылдауды қолдаудың интеллектуалды жүйелерінің (ШҚҚЖ) құрамына интеграциялау арқылы БКАЖ үшін қалыптан тыс күйлерді сәйкестендірудің тиісті әдістерін әзірлеу БКАЖ-ге кибершабуылдардың жаңа түрлерін анықтауда тиімдірек болуға мүмкіндік береді. АО қауіпсіздігіне кибернетикалық қауіптер деңгейінің ұлғаюы мен КҚ-ға қойылатын талаптардың бір мезгілде жоғарылауымен сыртқы зиянды әсерлердің қарқындылығының артуы арасындағы айқын қарама-қайшылыққа сүйене отырып, АЖ-дағы белгілер мен анықталған ауытқулар туралы әлсіз құрылымдалған деректер жағдайында зияткерлік ШҚҚЖ үшін қолданыстағы әдістер мен модельдерді одан әрі дамыту және жаңа әдістер мен модельдерді әзірлеу маңызды ғылыми-техникалық міндет болып табылады. АҚ және КҚ зерттеу саласындағы көптеген теоретиктер көрсеткендей, теріс пайдалануды анықтаудың ең перспективалы бағыттарының бірі – айқын белгілермен бірге жүрмейтін ұзақ мерзімді кибершабуылдарды танумен байланысты жағдайларды талдауға бейімделген әдістер. Мұндай әдістерге Байес желілеріне (БЖ) және Байес классификаторларына негізделген әдістер толығымен кіреді, бұл біздің зерттеу тақырыбымыздың өзектілігін анықтайды. |
| Жоба мақсаты | Жобаның мақсаты - АО-дағы көп сатылы мақсатты кибершабуылдарды жүзеге асырудың күрделі ресімделген типтік емес жағдайларында Байес желілерін қолдануға |

| | |
|---|---|
| | негізделген тәсілді әзірлеу арқылы АО шабуылдаушысының қауіптерін іске асыру ықтималдығын бағалау сапасын арттыру. |
| Жоба міндеттері | Мақсатқа жету үшін келесі өзара байланысты міндеттер шешілуі керек:<br>1) басып кіруді анықтау жүйелеріне және оқиғаларды жинау және корреляциялау жүйелеріне талдау жүргізу (Security Information and Event Management, SIEM)<br>2)ақпараттандыру объектілерінің ақпараттық-коммуникациялық желілеріне (АКЖ) басып кіру қатерлері мен кезеңдерін болжау барысында БЖ шаблондарын және ШҚҚЖ есептеу ядросына арналған жаңа модельдерді әзірлеу;<br>3) динамикалық БЖ қолдану негізінде желілік басып кіруді анықтаудың ықтималдық модельдерін толықтыру;<br>4) БЖ пайдалану негізінде деректерді талдау міндеттерінде ШҚҚЖ әзірлеу және тестілеу. |
| Күтілетін және қол жеткізілген нәтижелер | Жоба аясында әзірленген ШҚҚЖ есептеу ядросына арналған БЖ шаблондары қауіп-қатерлер мен АО АҚЖ-ге басып кіру кезеңдерін болжау барысында АҚ талдаушыларына ШҚҚЖ көмегімен кездейсоқ айнымалылар жиынымен жұмыс істеуге және белгілі бір жағдайларда қауіп-қатерді немесе нақты басып кіру кезеңін жүзеге асыру ықтималдығын анықтауға мүмкіндік береді. Осыған ұқсас жұмыстармен салыстырғанда біздің жобада динамикалық БЖ қолдану негізінде желілік басып кірулерді анықтаудың ықтималдық модельдері толықтырылады. Сонымен қатар, ұсынылған тәсіл басып кірудің негізгі кезеңдерін ескеріп қана қоймай, сонымен қатар типтік басып кіру үлгілерін де, жаңадан синтезделген үлгілерді де қолдану негізінде шешім қабылдауға мүмкіндік береді. Барлық үлгілер мен модельдер әртүрлі кезеңдерде әлсіз құрылымдалған белгілермен сипатталуы мүмкін басып кіруді анықтау кезінде шешімдерді қолдау жүйесінің есептеу ядросын құрайды. |
| Зерттеу тобы мүшелерінің аты-жөні, идентификаторлары (Scopus Author ID, Researcher ID, ORCID, бар болса) және сәйкес профильдерге сілтемелер | 1. Ыдырышбаева Мөлдір Базарханкызы, жаратылыстану ғылымдарының магистрі, Индекс Хирша – 1, ORCID: https://orcid.org/0000-0002-5680-5444, Scopus Author ID: 57222863896<br>2. Ахметов Бахытжан Сражатдинович, профессор, техника ғылымдарының докторы, Индекс Хирша – 7, ResearcherID: ABI-3310-2020, ORCID: https://orcid.org/0000-0001-5622-2233, Scopus Author ID: 56829370400 |
| Жарияланымдар тізімі (URL, DOI көрсетілген) | |
| Патент туралы ақпарат | - |