БАПИЕВ ИДЕЯТ МЭЛСОВИЧТІҢ
6D070300 – «Ақпараттық жүйелер» мамандығы бойынша философии докторы (PhD) ғылыми дәрежені алу үшін диссертациясының
АҢДАТПАСЫ

Ақпараттық жүйелердің желілік ресурстарына шабуылдарға қарсы әрекеттің нейрожелілік модельдері мен әдістері

Тақырыптың өзектілігі. «Қазақстанның киберқалқаны» Киберқауіпсіздік тұжырымдамасына сәйкес [1], компьютерлік қылмыстықты және компьютерлік лаңкестікті білдіру ұлттық ақпарат жүйелерінің тұрақты және қауіпсіз қызмет етуіне кедергі жасайтын негізгі қауіп-қатерлерге жатады. Қазіргі жағдайларда кибершабуылдарға қарсы әрекет жүйелері ақпараттық жүйелердің желілік ресурстарын қорғаудың негізгі құралдарының бірі болып табылады. Дегенмен мұндай жүйелер әлдеқашан бірнеше онжылдықта қолданып жатқанымен, оларды әзірлеумен көптеген жоғары білікті мамандар айналысуда, ал сәйкес ғылыми-әдістемелік базаны жасауға жұмыстардың көптеген саны арналған, бірақ практикалық тәжірибе желілік кибершабуылдарға қарсы әрекет жүйелерінде бірқатар маңызды кемшіліктердің бар екенін көрсетеді. Олардың негізгілері желілік кибершабуылдардың бүкіл номенклатурасын танып білудің дәлдігі болып табылады, бұл бірқатар елдерде ақпаратты қорғау жүйелерін табысты бұзудың белгілі оқиғаларымен расталады. Одан басқа, отандық ақпараттық жүйелердің ақпаратты қорғау жүйелеріне желілік кибершабуылдарға қарсы әрекеттің белгілі құралдарын енгізу олардың пайдалану жағдайларының нұсқалығына күрделі бейімделу қажеттілігімен тудырылады. Сонымен қатар ақпараттық жүйелердің желілік ресурстарына кибершабуылдарына қарсы әрекеттің белгілі құралдарының кемшіліктері жоғары құны және толық ғылыми-техникалық құжаттаманың жоқтығы болып табылады.

Мұндай қойылуда отандық қолдану жағдайларына бейімделе алатын желілік кибершабуылдарға қарсы әрекеттің тиімді модельдерін, әдістерін және жүйелерін әзірлеу міндеті өзекті болып табылады.

Ғалымдар В.И. Васильевтің [3], А.В. Гришинның [4], Ю.Г. Емельяноваың [5], А.В. Крыжановскийдің [8], А.Г. Мустафаевтың [9], И.И. Слеповичевтің [10], А.А. Талалаевтың [12] және басқалардың зерттеулері желілік кибершабуылдарды танып білу құралдарын арттырудың келешектегі жолы оларда жасанды нейрондық желілер аппаратын пайдалану болып табылатынын көрсетеді. Бұл ұқсас міндеттерді ақпаратты қорғау құралдарының жетекші әзірлеушілерімен (Cisco, Symantec компаниялары) шешу үшін нейронды желілерді қолданудың дәлелденген тиімділігімен және қолданудың алуан түрлі жағдайларына нейрожелілік құралдардың (НЖҚ) дәлелденген бейімділігімен түсіндіріледі.

Шабуылдарға қарсы әрекет жүйелеріне нейрожелілік құралдарды тиімді енгізу үшін әдіснамалық пен теориялық негізін Б.Б. Ахметов [2], А.А. Корченко [6], В.Е. Сухов [11], И.А. Терейковский [13], А. Тимофеев [14], С.Т. Тынынбаев [7], А.Ф. Хафизов [15], В.А. Частикова [16] және т.б. сияқты

ғалымдардың ақпаратты қорғау жүйелерін теориялық әзірлемелері мен жасау тәжірибесі құрайды.

Осылайша, ақпараттық жүйелердың желілік ресурстарына кибершабуылдарға қарсы әрекеттің тиімді нейрожелілік модельдерін, әдістерін және құралдарын әзірлеу міндеті диссертациялық жұмыс арналған ғылыми зерттеулер мен әзірлемелердің өзектілігін қамтамасыз етеді.

Зерттеудің мақсаты мен міндеттері. Жұмыстың мақсаты пайдалану жағдайларына бейімделген және желілік кибершабуылдардың жаңа түрлерін жедел танып білуге қабілетті болатын кибершабуылдарға қарсы әрекеттің тиімді нейрожелілік модельдерін, әдістерін және құралдарын әзірлеуде тұрады.

Қойылған мақсатқа сәйкес зерттеудің келесідей негізгі міндеттері анықталған:

– ақпараттық жүйелердың желілік ресурстарына кибершабуылдарға қарсы әрекеттің нейрожелілік құралдарының мүмкіндіктеріне талдау жасау;

– ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекеттің әдіснамалық базасын дамыту;

– желілік кибершабуылдарға қарсы әрекеттің нейрожелілік модельдері мен әдістерін әзірлеу;

– желілік кибершабуылдарға қарсы әрекеттің нейрожелілік жүйесін әзірлеу және ұсынылған шешімдерін анықтауға бағытталған эксперименттік зерттеулерді жасау.

Зерттеу нысаны – ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға қарсы әрекеттің үдерістері.

Зерттеу заты – ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға қарсы әрекеттің нейрожелілік модельдері, әдістері және құралдары.

Зерттеу әдістері – сигналдарды, нейрондық желілерді, сараптамалық талдауды, математикалық статистиканы және оңтайландыруды цифрлық өңдеу теориясының әдістері.

Алынған нәтижелердің ғылыми жаңалығы теориялық пен тәжірибелік зерттеулер ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекет қағидаларын, модельдерін және әдістерін әзірлеуге және ғылыми негіздеуге мүмкіндік беруден тұрады.

Алғашқы рет:

– желілік кибершабуылдарға нейрожелілік қарсы әрекет үшін үйрететін іріктемені жасау әдісі әзірленген, ол іріктеменің рұқсат етілетін түрлерінің параметрлерін анықтаудың және эталондар жақындығының шығыс сигналында кибершабуылдардың түрлерін есепке алу есебінен нейрожелілік модельдердің рұқсат етілетін шеңберін анықтауға және оқу итерациясының санын азайтуды қамтамасыз етуге мүмкіндік береді;

– ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекет әдісі әзірленген, ол әзірленген нейрожелілік

модельдерді және үйретететін іріктемені жасаудың әзірленген әдісін пайдалану есебінен функционалдық мүмкіндіктерді кеңейтуге және танып білудің жеткілікті дәлдігін қамтамасыз етуге мүмкіндік береді.

Ары қарай дамуын алғандар:

− ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекеттің әдіснамалық базасы, ол осындай құралдарды жасау жағдайларын есепке алу есебінен қарсы әрекеттің тиімді нейрожелілік модельдері мен әдістерін жасау мүмкіндігін қамтамасыз етті;

− қарсы әрекеттің нейрожелілік модельдері, олар сараптық деректердің көмегімен үйрету мүмкіндігінің және құрамдастырылған үйретететін іріктемені пайдаланудың есебінен желілік кибершабуылдардың жаңа типтеріне жедел жауап қайтаруға мүмкіндік береді.

Алынған нәтижелердің тәжірибелік мәні. Ұсынылған нейрожелілік модельдер мен әдістер нейрожелілік жүйенің архитектурасын әзірлеуге мүмкіндік берді, ол жасау мен пайдалану жағдайларына бейімделе отырып, желілік кибершабуылдардың негізгі түрлерін жеткілікті дәлдікпен тапып білуге мүмкіндік береді, сонымен қатар аспаптық құралдарды жасау үшін пайдаланылуы мүмкін.

Тәжірибелік құндылығы келесіден тұрады:

− үйретететін іріктемені жасаудың әзірленген әдісін пайдалану нейрожелілік модельдің оқу итерацияларының санын шамамен 2,4 есе азайтуға мүмкіндік береді, бұл И.Сикорский атындағы КПИ «Тезис» ғылыми-зерттеу орталығының қызметіне енгізу актісімен расталады (11.08.2017 жылғы енгізу актісі);

− желілік кибершабуылдарды нейрожелілік танып білудің әзірленген әдісін қолдану желілік кибершабуылдарды нейрожелілік танып білу құралдарының тиімділігін шамамен 1,35 есе арттыруға мүмкіндік береді, бұл ««Дельта» ақпарат жүйелерінің қауіпсіздігі» ЖШҚ-ның қызметіне енгізу актісімен расталады (09.10.2017 жылғы енгізу актісі);

− ұсынылған модельдер мен әдістерді іске асыратын әзірленген бағдарламалар Ұлттық авиация университетінің (Киев, Украина) (25.07.2017 жылғы енгізу актісі) ақпараттық технологиялар қауіпсіздігі кафедрасындағы және Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университетінің ақпараттық жүйелер кафедрасындағы (04.09.2017 жылғы енгізу акті) оқу үдерісіне енгізілген.

Ізденушінің жеке үлесі. Бірлескен авторлықта жарияланған жұмыстарда ізденушіге: іріктеменің рұқсат етілетін түрлерінің параметрлерін анықтаудың және эталондар жақындығының шығыс сигналында кибершабуылдардың түрлерін есепке алу есебінен нейрожелілік модельдердің рұқсат етілетін шеңберін анықтауға және оқу итерациясының санын шамамен 2,4 есе азайтуын қамтамасыз етуге мүмкіндік беретін желілік кибершабуылдарға нейрожелілік қарсы әрекет үшін үйретететін іріктемені жасаудың жаңа әдісі әзірлеу; әзірленген нейрожелілік модельдерді және үйретететін іріктемені жасаудың әзірленген әдісін пайдалану есебінен

функционалдық мүмкіндіктерді кеңейтуге және кибершабуылдарды танып білудің жеткілікті дәлдігін қамтамасыз етуге мүмкіндік беретін ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекет әдісін әзірлеу тиесілі. Ұсынылған модельдер мен әдістерді пайдалану арқылы ақпараттық жүйелердің желілік ресурстарына кибершабуылдарға нейрожелілік қарсы әрекет жүйесі әзірленген және зерттелген. Танымал нейрожелілік құралдарға қарағанда, осы жүйеде нейрожелілік құралдарды жасаудың, бейімді үйретететін іріктемені қалыптастырудың жағдайларын анықтаудағы қосалқы жүйелерді пайдалану қарастырылған, бұл танып білудің жеткілікті дәлдігін және әзірлеу мен қолдану жағдайларына бейімділікті қамтамасыз етеді. Эксперименттік жолмен ұсынылған нейрожелілік жүйенің тиімділігінің ең озық ұқсас жүйелеріне қатысты шамамен 1,35 есе жоғары екені көрсетілген, ал қолданудың күтілетін жағдайдарында оны пайдалану желілік кибершабуылдарды танып білу қателігін 0,05 шектерінде қамтамасыз етуге мүмкіндік береді, бұл тәжірибелік пайдалану үшін жеткілікті.

Диссертация нәтижелерінің апробациясы. Диссертациялық жұмыстың негізгі нәтижелері Қ.И.Сәтбаев атындағы ҚазҰТЗУ «Ақпараттық технологиялар» кафедрасының семинарларында және халықаралық ғылыми-тәжірибелік конференцияларда баяндалған және талқыланған:

– «Киберқауіпсіздікті және ақпаратты қорғауды қамтамасыз етудің өзекті мәселелері» II халықаралық ғылыми-тәжірибелік конференция, Еуропалық университет (Украина, Киев қ., 24-27 ақпан 2016);

– I«Киберқауіпсіздікті және ақпаратты қорғауды қамтамасыз етудің өзекті мәселелері» III халықаралық ғылыми-тәжірибелік конференция, Еуропалық университет (Украина, Киев, 22-25 ақпан 2017);

– IV International scientific conference «Global and regional problems of informatizition in society and nature using'2016», National University of Life and Environmental Sciences of Ukraine (Ukraine, Kyiv, 23-24 of June 2016);

– V International scientific conference «Global and regional problems of informatizition in society and nature using'2017», NULES of Ukraine (Ukraine, Kyiv, 22-23 of June 2017);

– The 15th International Scientific Conference Information Technologies and Management, ISMA University – Satbayev University, (Latvia - Kazakhstan, Riga - Almaty, April 27-28, 2017);

– Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2017), Миколаїв – Коблево: МТУ «Миколаївська політехніка» (Украина, Николаево - Коблево, 20-23 июнь 2017г).

Жарияланымдар. Диссертациялық жұмысты орындау кезінде алынған негізгі нәтижелер 14 баспа жұмыстарында жарияланған, олардың ішінде 4 мақала ҚР БҒМ Білім және ғылым саласындағы бақылау комитетімен нұсқалған басылымда жарияланған, 1 мақала Scopus базасымен индексацияланатын басылымда жарияланған, 1 мақала – халықаралық журналда (Жаратылыстану Академиясы) жарияланған, 1 мақала – шетелдік

журналда (Украина) жарияланған, 6 мақала халықаралық ғылыми-тәжірибелік конференциялардың (Украина, Латвия) шетелдік жинақтарында жарияланған, 1 мақала халықаралық ғылыми-тәжірибелік конференцияның (Қазақстан) отандық жинағында жарияланған.

Диссертацияның көлемі мен құрылымы. Диссертация кіріспеден, төрт бөлімнен, қорытындыдан, 106 атаудан тұратын пайдаланылған әдеби көздердің тізімінен және 6 қосымшадан тұрады. Жұмыстың жалпы көлемі 124 бет. Жұмыста 25 сурет, 7 кесте бар.

ПАЙЛАНЫЛҒАН ӘДЕБИ КӨЗДЕРДІҢ ТІЗІМІ

1. 2017 жылғы 30 маусымдағы Қазақстан Республикасы Үкіметінің қаулысымен бекітілген №407 Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны»), [Электронды ресурс] – Қолжетімділік режимі: http://mdai.gov.kz/ru/pages/ koncepciya-kiberbezopasnosti-kibershchit-kazahstana (жүгіну күні: 16.12.2017)
2. Ахметов Б.Б. Ақпараттық жүйелердің желілік ресурстарына кибершабуылдарды танып білудің нейрожелілік құралдарының тиімділігін бағалау параметрлері / Б.Б. Ахметов, А.Г. Корченко, И.А. Терейковский, Ж.М. Алибиева // Reports of the national academy of sciences of the republic of Kazakhstan. ISSN 2224-5227. Volume 2, Number 312 (2017)
3. Васильев В.И. Internet желісінде шабуылдарды анықтаған кездегі нейрондық желілер (SYNFLOOD шабуылы мысалында) / В.И. Васильев, А.Ф. Хафизов // Ақпараттық пен сараптамалық жүйелердегі нейрокомпьютерлер. – М.: Радиотехника, 2007. – №6. – Б. 34-38.
4. Гришин А.В. Компьютерлік шабуылдарды анықтау міндеттеріндегі нейрожелілік технологиялар / А.В. Гришин // Информационные технологии и вычислительные системы – 2011. – №1. – Б. 53 - 64.
5. Емельянова Ю. Г. Ақпараттық ресурстарға желілік шабуылдарды анықтаудың нейрожелілік технологиясы / Ю. Г. Емельянова, А.А. Талалаев, И.П. Тищенко, В.П. Фраленко // Бағдарламалық жүйелер: теория және қосымшалар. – 2011. – №3(7). – Б. 3-15.
6. Корченко А.Г. Желілік ресурстарға кибершабуылдарды танып білудің нейрожелілік модельдерінің тиімді түрлерін анықтау / А.Г. Корченко, И.А. Терейковский, Л.А. Терейковская, Б.Б. Ахметов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (32), 2016 р.
7. Корченко А.Г. Интернет-бағдарланған ақпараттық жүйелердің қауіпсіздік параметрлерін бағалаудың нейрожелілік модельдері, әдістері және құралдары: монография / А. Корченко, И. Терейковский, Н. Карпинский, С. Тынымбаев. – К. : ТОВ «Наш Формат». – 2016. – 275 б.
8. Крыжановский А.В. Шабуылдарды анықтау жүйелерінде жасанды нейрондық желілерді қолдану / А.В. Крыжановский // Доклады ТУСУРа. – 2008. – № 2 (18), часть 1. – С. 37-41. URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennyh-neyronnyh-setey-v-sistemah-obnaruzheniya-atak

9. Мустафаев А.Г. Желілік трафикті талдаудың негізінде компьютерлік шабуылдарды анықтаудың нейрожелілік жүйесі // Қауіпсіздік мәселелері. – 2016. – № 2. – С.1-7. DOI: 10.7256/2409-7543.2016.2.18834. URL: http://e-notabene.ru /nb/article_18834.html.

10. Слеповичев И.И. Айқын емес нейрондық желінің DDoS-шабуылдарын анықтау / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Саратов университетінің хабарлары. – 2009. – Т. 9, сер. Математика. Механика. Информатика, шығ. 3. – Б. 84-89.

11. Сухов В.Е. Жасанды иммунды жүйелердің және нейрожелілік детекторлардың негізінде желілік трафигінің ауытқушылықтарын анықтау жүйесі // Вестник РГРТУ. – 2015. – № 54. Б.1. – Б. 84-90.

12. Талалаев А.А. Ауытқымалы желілік белсенділіктің мониторингінің нейрожелілік модулін әзірлеу / А.А. Талалаев, И.П. Тищенко, В.П.Фраленко, В.М. Хачумов // Нейрокомпьютерлер: әзірлеу және қолдану. — 2011. — № 7. — Б. 32-38.

13. Терейковський І. Нейронні мережі в засобах захисту комп’ютерної інформації: монографія / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 б.

14. Тимофеев А. Желілік шабуылдарды анықтау мен жіктеудің нейрожелілік әдісін зерттеу және модельдеу / А.Тимофеев, А. Браницкий // International Journal Information Technologies & Knowledge. – 2012. – Vol.6, Number 3. – P. 257-265

15. Хафизов А.Ф. WWW-серверде шабуылдарды анықтаудың нейрожелілік жүйесі: техн. ғыл. канд. дис. : 05.13.11 / А.Ф. Хафизов. – Уфа, 2004. –172 б.

16. Частикова В.А., Власов К.А., Картамышев Д.А. Үйрету алгоритмі ретінде бөлшектер тобы әдісін қолдану арқылы нейрондық желілер негізінде ddos-шабуылдарды анықтау / В.А. Частикова, К.А. Власов, Д.А. Картамышев // Іргелі зерттеулер. – 2014. – № 8-4. – Б. 829-832.