ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

3

АЛМАТЫ
АЛМАТЫ
ALMATY

2017

МАМЫР
МАЙ
MAY

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
www: nauka-nanrk.kz, bulletin-science.kz

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 3, Number 367 (2017), 54 – 64

G. Beketova[1], B. Akhmetov[1], A. Korchenko[2], A. Lakhno[3]

[1]Kazakh national research technical university after K. I. Satpayev, Almaty, Kazakhstan,
[2]National aviation university, Kiev, Ukraine,
[4]European university, Ukraine.
E-mail: Beketova_gs@mail.ru

SIMULATION MODELING OF CYBER SECURITY SYSTEMS IN MATLAB AND SIMULINK

Abstract. In the article some aspects of simulation application in MATLAB and Simulink are considered for solving the problems of information security of the components of information protection means for critical computer systems. A number of important qualities for creating an effective model are presented, such as the detailed implementation of protocols that are involved in cyberattacks; the ability to connect their own modules to implement the agent approach, in particular using models; the possibility of changing the parameters of simulation modeling during making experiments; independence from the platform on which simulation modeling is performed; advanced graphical interface; cost of a software product for carrying out simulation modeling; an opportunity to assess the damage from cyberattacks. It is established that the use of simulation modeling in MATLAB and Simulink makes it possible to unite the heterogeneous mathematical models of the elements that make up critical computer systems and is one of the innovative methods that allow to evaluate the effectiveness of critical computer systems cyber security systems and their reaction to attempts to perturb some indicators.

Key words: critical computer systems, means of information protection, simulation modeling, firewall.

ӘОЖ 004.056

Г. Бекетова[1], Б. Ахметов[1], А. Корченко[2], А. Лахно[3]

[1]Қ. И. Сатпаев атындағы Қазақ ұлттық зерттеу техникалық университеті им. К. И. Сатпаева,
Алматы, Қазақстан,
[2]Ұлттық авиациялық университет, Киев, Украина,
[3]Еуропалық университет, Киев, Украина

MATLAB 7/2009 ЖӘНЕ SIMULINK-те КИБЕРҚОРҒАУ ЖҮЙЕСІНІҢ ИМИТАЦИЯЛЫҚ МОДЕЛЬДЕНУІ

Аннотация. Мақалада критикалық маңызды компьютерлік жүйелерде ақпаратты қорғау құралдары компоненттерінің ақпараттық қауіпсіздігін қамтамасыз ету тапсырмаларын шешу үшін MATLAB және Simulink-те имитациялық модельдеуді қолданудың кейбір аспектілері қарастырылған. КМКЖ құрамына кіретін элементтердің әртүрлі математикалық модельдерін өзара біріктіретін MATLAB және Simulink-те имитациялық модельдеуді қолдану КМКЖ кибер қорғау жүйесінің тиімділігін бағалауға мүмкіндік беретін инновациялық әдістерінің бірі болып табылатындығы анықталды.

Түйін сөздер: критикалық маңызды компьютерлік жүйелер, средства защиты информации, имитационное моделирование, межсетевой экран.

Кіріспе. Программалық-аппараттық платформалар кибер қаупінің жаңа типтері мен кластарын танып-білуге бейімделу негізінде ақпараттық ағындарды бақылауды қамтамасыз етудің ауқымды жүйесі ғана ақпараттық қауіпсіздікке тұрақсыздандырылған әсердің үнемі өсіп отырған кезінде тиімді.

Ақпаратты қорғау құралдары кешендерімен жабдықталған үлкен жүйелер, олардың ішінде аса маңызды компьютерлік жүйелер, жүздеген, кей жағдайларда мыңдаған элементтерден тұрады. Оған қоса, элементтер арасындағы байланыстар саны соңғыларынан онға көбеюі мүмкін. Критикалық маңызды компьютерлік жүйелер (КМКЖ) элементтер мен байланыстардың біртекті еместігімен сипатталады. Жеке элементтер мен байланыстар дискретті математиканың немесе бұқаралық қызмет көрсету теориясының модельдерімен сипатталатындығына қарамастан киберқорғау мен ақпараттық қауіпсіздік (АҚ) жүйелері туралы бұлай айтуға болмайды. Жалғыз баламасы КМКЖ және олардың ақпараттық қауіпсіздікті қамтамасыз ететін ішкі жүйелерінің құрамына кіретін элементтердің әртүрлі математикалық модельдерінің өзара байланысуына мүмкіндік беретін имитациялық модельдеуді қолдану болып табылады. Осылайша, жобалау этаптарында КМКЖ ақпараттық қауіпсіздік жүйелері (АҚЖ) тиімділігін және оның көрсеткіштер қатары бойынша кибер шабуыл әрекетіне реакциясын бағалауға мүмкіндік беретін имитациялық модельдің әрі қарай даму мәселесі өзекті болып табылады.

Жұмыстың мақсаты. Жұмыстың мақсаты КМКЖ-лер үшін АҚЖ-сінің компоненттерінің ақпараттық қауіпсіздігін қамтамасыз ету мәселесін зерттеу барысында синтезделген имитациялық моделінің жұмысқа қабілеттілігін тексеру болып табылады.

Алдыңғы зерттеулерге шолу. КМКЖ АҚЖ-рін құру кезіндегі имитациялық модельдеу көмегімен төмендегі міндеттерді шешуге болады:

– АҚ жүйесінің техникалық, технологиялық, сонымен бірге ұйымдастырушылық қайта құрылуының түрлі нұсқаларын талдау негізінде КМКЖ үшін АҚЖ-лер, оның ішінде кибер қорғаудың даму бағыттарын анықтау және жетілдіру, сонымен қатар қабылданған шешімдердің нәтижелерін зерттеу;

– АҚЖ-лер программалық қамсыздандыруы мен техникалық компоненттерін қалыптастыру құрылымы мен режимдерінің түрлі нұсқаларын ғана емес, сонымен бірге КМКЖ АҚЖ-ді қалыптастырудың түрлі режимдерін өңдеу.

Көптеген КМКЖ-дің АҚ жүйелерінің моделдеу құралдарын құру кезінде кілттік шешім модельдерді құрудың программалық ортасын таңдау болып табылады, және осыдан имитациялық тәжірибені жүргізу, модельдің нәтижелері мен жөндеу мүмкіндіктері тәуелді болады. Бұған қоса тиімді модель құру үшін маңызды қасиеттері төмендегілер болып табылады: [1-5]:

– кибер шабуылдарда іске қосылған хаттамалардың детальды берілуі;

– агенттік енудің берілуі үшін өз модульдеріне қосылу мүмкіндіктері;

– тәжірибе жүргізу кезінде имитациялық модельдеу параметрлерін өзгерту мүмкіндіктері;

– имитациялық модельдеу орындалатын платформадан тәуелсіздік;

– дамыған графикалық интерфейс;

– имитациялық модельдеуді жүргізуге программалық өнімнің құны;

– кибер шабуылдан болған залалды бағалауды орындау мүмкіндігі.

Әдеттегідей, ақпаратты қорғау мен АҚ проблемасымен байланысты тапсырмаларды шешу кезінде желілік процесстердің талдауы үшін неғұрлым сай келетін төмендегі программалық өнімдерді қолданады[6-8 және т.б.]:

– NS-2 – C++-та модельдер ядросына қосылу мүмкіндігі бар программалық өнім;

– COMNET III – локальды және глобальды желілер мен АЖ-лерді модельдеудің объектіге-бағытталған жүйесі;

– Netmaker – ЛЕЖ топологиясын жобалау, сонымен қатар, желіге жүктеуді жобалау мен талдауға арналған жүйе;

– OPNET – компьютерлік жүйелер, қосымшалар мен таратылған жүйелердің локальды және глобальды желілерін модельдеу мен жобалауға арналған программалық пакет;

– OMNeT++ – ақпараттық жүйелер (АЖ) мен локальды есептеуіш жүйелердің (ЛЕЖ) ішкі қарапайым модульдері орындалатын дискретті оқиғалардың симуляторы.

ПП мәліметтерінде бар барлық жетістіктері кезінде, төмендегі кемшіліктерге ие болады:

– «қызмет көрсетуден бас тарту» типті шабуылдың берілуі кезінде ЛЕЖ-нің және АЖ-дің өнімділігінің модельдеуіне бағытталуы;

– симуляторларға жазылған скрипттерді жөндеудің қиындығы;

– модельге жаңа объектілерді қосу күрделілігі және сәйкесінше, кибер қорғау объектісін сипаттайтын функциялардың математикалық берілуінің күрделілігі.

Құрылғылардың анықталған шектеулеріне [4, 8-10] талдау жасау негізінде желілерді модельдеу мен КМКЖ-дің таратылған локальды тораптарындағы АҚ мониторингінің проблематикалары құрылған құралдардың төмендегі көрсеткіштеріне негізделген:

– КМКЖ АҚ жүйесінің математикалық модельдеуі базасының толықтығы;

– КМКЖ АҚ жүйесінің математикалық модельдеуі базасын қолданушымен кеңейту мүмкіндігі;

– КМКЖ-лер үшін АҚЖ-лері компоненттерін зерттеу мен өңдеу құралдарының қол жетімдігі;

– КМКЖ-лер үшін кибер қорғау объектілерінің имитациялық модельдеу деңгейіндегі есептің барынша дәлдігі;

– компанияның ақпараттық қауіпсіздік саласында модельдеу мәліметтерін эксперттермен бірлесе қолдану мүмкіндігі.

КМКЖ-дің кибер қорғаулары мен АҚЖ жұмыстарын имитациялық модельдеу үшін Simulink пакеті таңдалды, бұл пакеттің негізгі міндеті жүйелер мен құрылғыларды имитациялық модельдеуге негізделген [11,12].

Сыртқы оқиғалар (жағдайлар) әсер ететін жүйелер мен құрылғыларды модельдеу оқиғалық немесе жағдайлық модельдеу деп аталады. Simulink + MATLAB жүйесінде ол Stateflow арнайы кеңейтілуі көмегімен орындалады [11, 12]. Stateflow оқиғалық модельдеу пакеті соңғы автоматтар теориясына негізделген. Ол кибер шабуылдың белгілі сценарийін беретін жақ ретінде де, жауап қайтаратын әрекетті орындаушы АҚЖ ретінде де оқиға мен іс-әрекетке сәйкес қойылатын ережелер тізбегі негізінде жүйені қалыптастыруға мүмкіндік береді. Stateflow пакеті төмендегідей жүйелерді талдау, модельдеу және жобалау үшін арналған:

– басқарудың анықталған жүйесі;

– түрлі сандық құрылғылар, оның ішінде КМКЖ құрамындағы АҚЖ-лері мен АЖО-ның (ДК) программалық-аппараттық құрылғылары;

– адам-машиналық интерфейс элементтері (Men Machine Interface – MMI);

– Simulink құралдары кеңейтілу пакетінің тізбегі (Control System, Digital Signal Processor және т.б.);

– тағы басқалар.

Simulink + MATLAB-та берілген кибер қорғаудың ішкі жүйесінің имитациялық модельдеуі. Осылайша, КМКЖ кибер қауіпсіздік бойынша мамандармен, оның ішінде территориалды локальды тораптарда жұмыс жасайтындармен талап етілген АҚЖ-ді модельдеудің жалпы сызбасы 1-суретте көрсетілген.

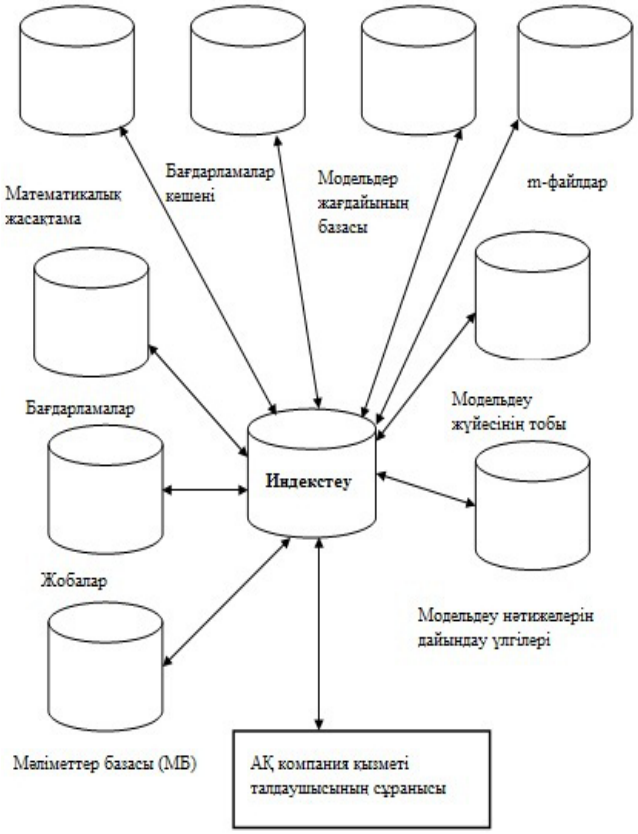
Жұмыста көрсетілген барлық модельдер кибер шабуылдардың түрлі нұсқаларына кері әрекет жағдайында КМКЖ-дің жұмыс режимін ары қарай зерттеу үшін, сонымен бірге алынған тәуелділіктерді баламалыққа тексеру үшін MATLAB пакетінде берілген [27].

MATLAB-пен КМКЖ АҚЖ модельдерінің клиенттері, өнімдері және ресурстары өзара әрекет ету технологиясы 2-суретте көрсетілген.

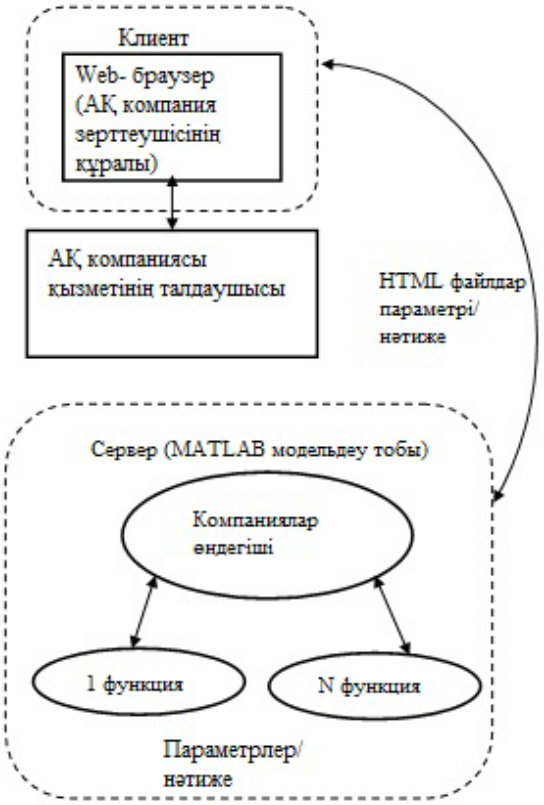
3, 4-суреттерде ақпаратты жинау, сақтау және тасымалдаудың технологиялық процестерін принципиалды құрылымдық сызбасының негізінде, сонымен бірге компьютерлік компоненттердің – ДҚ серверлері, клиенттік бекеттер, телекоммуникациялық құрылғылардың АЖ-лерінде берілуі есебінен құрылған КМКЖ-дің негізгі модульдерінің имитациялық модельдерінің ішкі жүйелері көрсетілген.

КМКЖ-дің ішкі жүйелерінің көп саны ретінде, сонымен бірге кейбір ішкі жүйелер мысалы, бапталатын параметрлері бар типтік ЛЕЖ-лер MATLAB кітапханаларының құрамында болатын жағдайларда, мақалада Simulink компоненттерінің қолданылуымен құрылған тек аутентикалық сызбалар келтірілген [11, 12, 26].

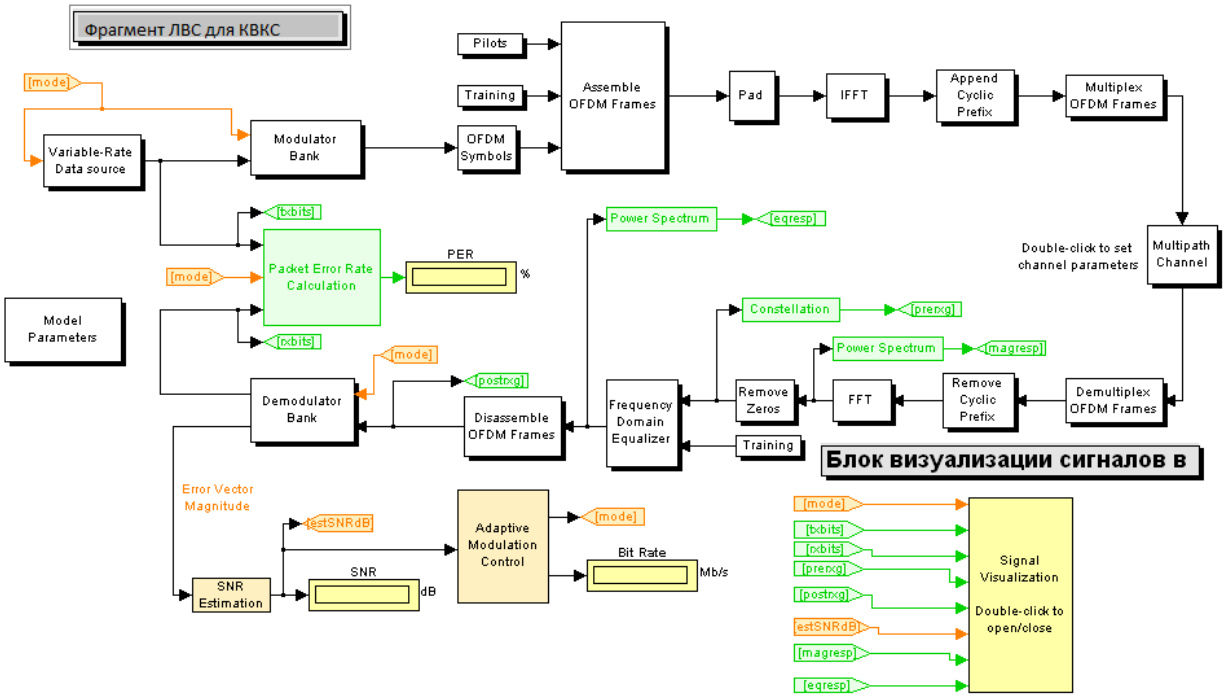
Жұмыста ұсынылған модельдер мен алгоритмдерді қолдана отырып [27], КМКЖ-дің неғұрлым осал компоненттеріне (коммутаторлар, желі аралық экран, АЖО, серверлер) шабуылдарды анықтау мүмкіндіктерін зерттеу үшін КМКЖ компьютерлік желілері сегментіне имитациялық эксперимент жүргізілген, 3, 4-суреттерді қараңыз.



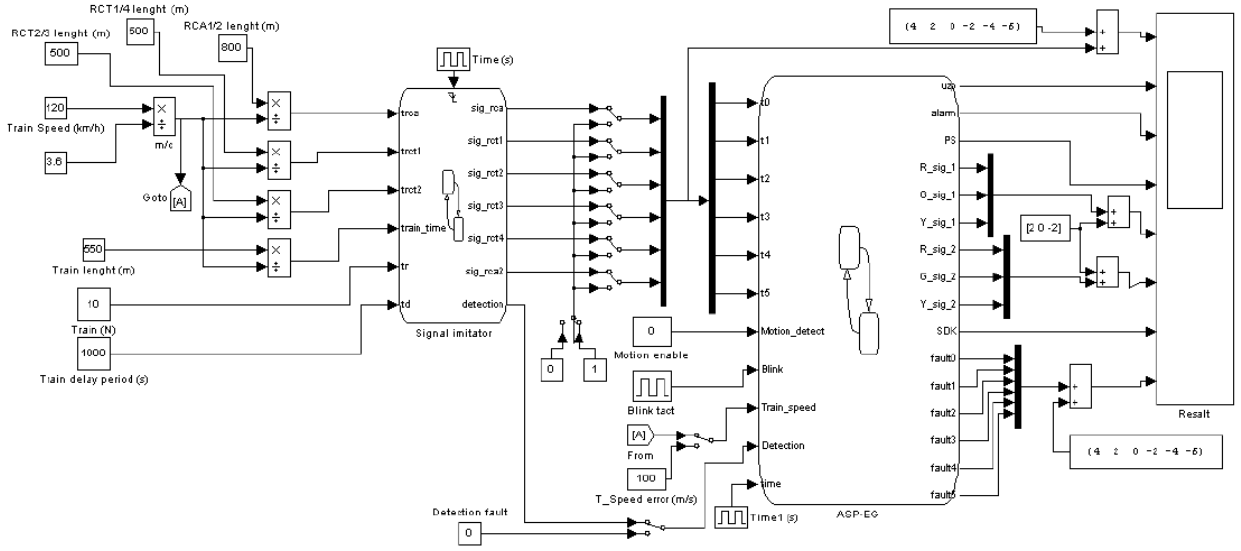
1-сурет –
КМКЖ АҚ модельдеудің физикалық құрылымы



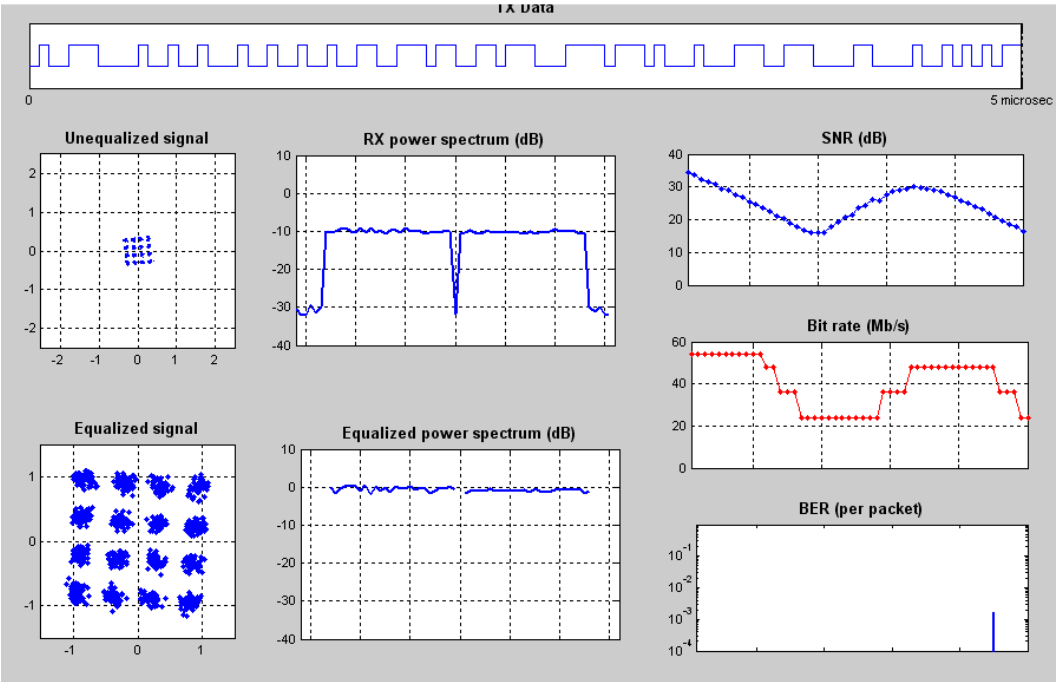
2-сурет – КМКЖ АҚ клиенттері, өнімдері мен ресурстарының өзара әрекеттесу технологиясы



3-сурет – КМКЖ-лер үшін ЛЕЖ сегментінің моделі



4-сурет – КМКЖ құрамында АЖО үшін желілік байланысу жүйесін басқару моделі



5-сурет – КМКЖ ЛЕЖ сегментінде сигналдарды визуалдау нәтижелері

Сигналдарды визуалдау үшін мәліметтер пакетін беру деңгейінде, соның ішінде КМКЖ-ге шабуылдың түрлі типтерінің әсері кезінде, ЛЕЖ-дің негізгі параметрлерін талдауға мүмкіндік беретін «Signal Visualization» арнайы блогы жобаланды, 5-суретті қараңыз.

Трафик генераторы көмегімен желілік шабуылдардың келесі типтерінің бірі модельденді – DoS, буфердің толуы, U2R, R2L және Probe, сонымен қатар вирустардың түрлі типтерінің КМКЖ құрамында ЛЕЖ-нің өнімділігіне әсері зерттелді.

КМКЖ желілік компоненттері үшін кибер шабуылдардың 4 негізгі компоненттері қарастырылды: DoS/DDoS, U2R, R2L және Probe [13, 14]. Шабуыл типтерінің мәліметтерін анықтау және топтастырудың ұстанымдарына сәйкес [9, 15-20] желілік байланысуды сипаттайтын 8-ден 20-ға дейін параметрлер жеткілікті. Имитациялық эксперимент кезінде қолданылатын параметрлер тізімі 1-кестеде көрсетілген.

1-кесте – Имитациялық эксперимент кезінде қарастырылатын параметрлер

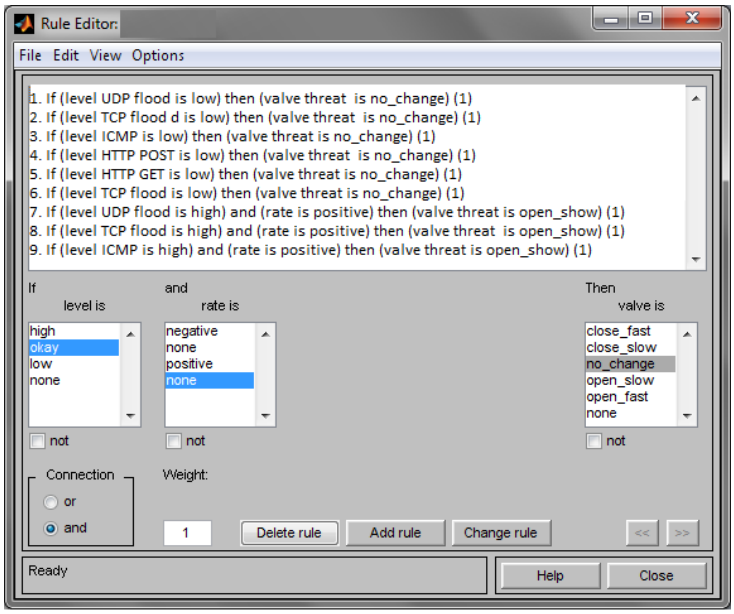
Параметр	Параметрдің сипатталуы
1. duration	Байланыстың ұзақтығы
2. src_byte	Бастапқы көзден қабылдағышқа берілетін байт саны
3. dst_byte	Қабылдағыштан бастапқы көзге берілетін байт саны
4. land	Жіберуші портының қабылдаушы портымен теңдігі
5. wrong fragment	Жойылған пакеттер саны
6. urgent	URG жалаушасы бар пакеттер саны
7. hot	hot-индикаторлар саны
8.count	Қашықтағы хост пен жергілікті хост арасындағы байланыс саны
9. srv_count	Жергілікті қызметке қосылулар саны
10. serror rate	Берілген хост-көзге арналған SYN типті қатесі бар байланыстың пайыздық саны
11. srv serror rate	Берілген қызметтік көзге арналған SYN типті қатесі бар байланыстың пайыздық саны
12. rerror rate	Берілген хост-көзге арналған REJ типті қатесі бар байланыстың пайыздық саны
13. srv rerror rate	Берілген қызметтік көзге арналған REJ типті қатесі бар байланыстың пайыздық саны
14. same_srv_rate	Қызметке қосылудың пайыздық саны
15. diff_srv_rate	Түрлі қызметтерге қосылудың пайыздық саны
16. srv_diff_host_rate	Түрлі хосттарға қосылудың пайыздық саны
17. dst_host_count	Қашықта орнатылған жергілікті хостқа қосылу саны
18. dst_host_srv_count	Қашықта орнатылған және бір ғана қызметті қолданатын жергілікті хостқа қосылу саны
19. st_host_same_srv_rate dst_host_diff_srv_rate dst_host_same_src_port_rate dst host srv diff host rate	Байланыстың пайыздық саны, сәйкесінше: – қашықта орнатылған және бір ғана қызметті қолданатын жергілікті хостқа; – қашықта орнатылған және түрлі қызметтерді қолданатын жергілікті хостқа; – бастапқы көз портының ағымдағы номері кезінде берілген хостқа; – түрлі хосттар қызметіне.
20. dst_host_serror_rate dst_host_srv_serror_rate dst_host_rerror_rate dst_host_srv_rerror_rate	Төмендегідей типті қателері бар байланыстың пайыздық саны: – берілген хост-қабылдағышқа арналған SYN; – қабылдағыштың берілген қызметіне арналған SYN; – берілген хост-қабылдағышқа арналған REJ; – қабылдағыштың берілген қызметіне арналған REJ.

КМКЖ компоненттеріне және оқыту ережелері шешетін белгілер қорлары бар (матрицалар) кестелер негізінде кибер шабуылдауды интеллектуалды тану процедурасын модельдеу процесін, сонымен бірге MATLAB ортасындағы (Fuzzy Logic Toolbox кеңейтілу пакеті) білімдер базасын [27] беру үшін аномалия, кибер шабуыл және қауіпті тану блогында қолданылатын оқуға арналған объектілерді (интеллектуалды агенттер) оқу үшін сәйкес ережелер құрылды, 6-суретті қараңыз.

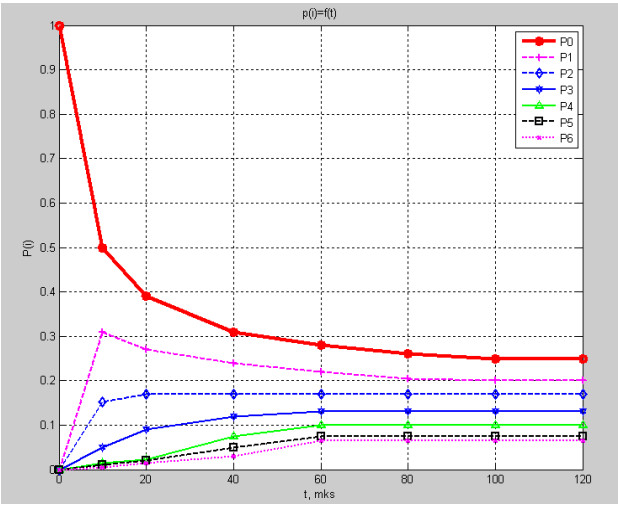
КМКЖ басқа жүйелермен коммутатор арқылы байланысатындықтан, кибер қорғау жүйесінің бірінші эшелоны ереже бойынша желіаралық экран (ЖЭ) мен коммутатор деңгейінде құрылады, имитациялық модельдеу нәтижелері мақаланың келесі пунктінде көрсетілген.

КМКЖ кибер қорғау ішкі жүйесін имитациялық модельдеу нәтижелері. Коммутаторды модельдеу аясында байланыс орнату кезінде қауіп төндірушінің байланысын ұстап қалу мүмкін емес, сонымен бірге жағдайлар арасында өту қарқыны байланысу қарқынына сәйкес келеді. Байланысты болдырмау арнайы сипаттамаға [21, 22] сәйкес жүргізіледі, және ЖЭ баптауларына байланысты. Имитациялық модельдеу аясында байланысты болдырмауды ЖЭ арнайы сипаттамасына сәйкес елемеуге болады. Пакет өмірінің уақыты бірнеше ондаған секундтардан аспайды, осы жұмыста оны 50–75 секундқа тең деп есептейміз.

7-суретте 4 кадр буфер ұзындығы бар коммутатордың қабылдау трактының ықтимал жағдайларын модельдеу нәтижелері көрсетілген. (КМКЖ ЛЕЖ-лер сегментінің моделі үшін 3-суретте көрсетілген).



6-сурет – Аномалия, кибер шабуыл және қауіпті тану блогында қолданылатын оқуға арналған логикалық процедуралар түріндегі ережелер жүйесі



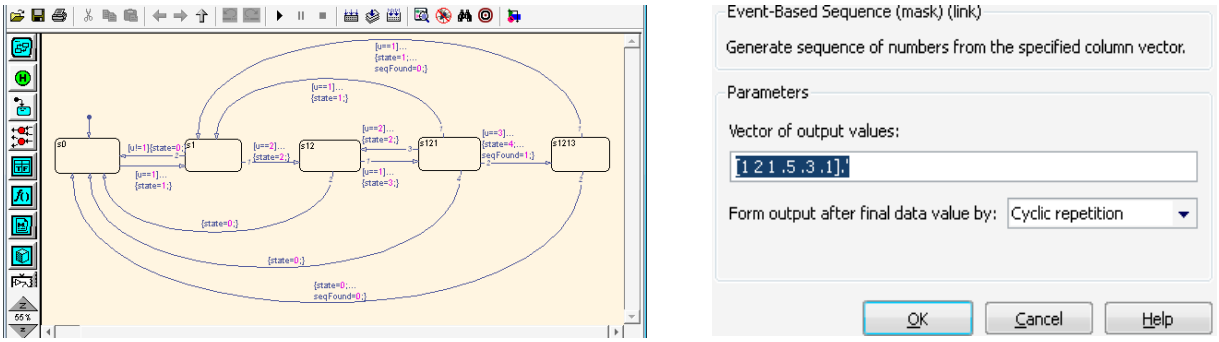
7-сурет – Коммутатордың қабылдау тракты ықтималдылық жағдайы

Осылайша, [21, 23, 24] жұмыстарда берілген эксперименталь мәліметтермен сәйкес келетін модельдеу нәтижелері негізінде коммутатормен кадрларды қабылдау этабында кадрларды жоғалту ықтималдығы ((P_6) желілік шабуылды сәтті беру) 0,08-ден аспайды, және одан кейінгі есептеулерде оны елемеуге болады.

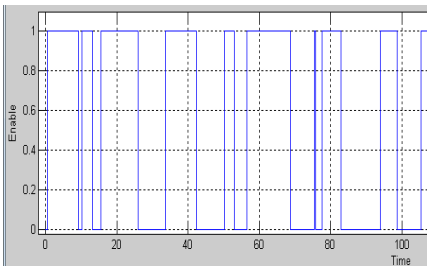
КМКЖ ЛЕЖ-рінде шабуылдары үшін тарфиктер мен сұраныстар ағынының нұсқаларын модельдеу үшін сұраныстар генераторы (кіріс ағындар векторы) түріндегі параметрлер берілді, 8-суретті қараңыз.

Имитациялық модельдеу кезінде желідегі сұраныстар саны және трафиктің басқа сипаттамалары, сонымен бірге өтінімдерді таратуы бойынша заң өзгерді, 1-кестеде қараңыз [1, 5, 25].

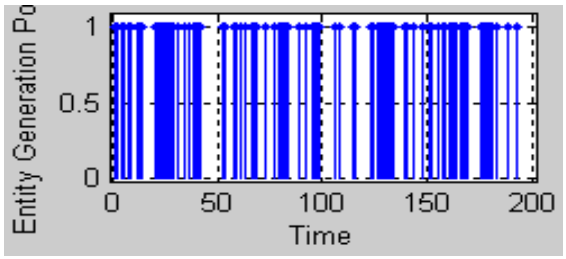
2-кесте мен 9 а)-суретте көрсетілген графиктер мен нәтижелерден көрсетілген, КМКЖ сервері қалыптасуының қарапайым режимінде, (таратылудың көрсеткіштік заңы [5, 26]), сұраныстарға қызмет көрсету уақыты қол жетімді шектерде болады, осылайша кезек қалыптасып үлгермейді. Дегенмен егер шабуылдаушы жақ нәтижесінде шабуылдар сұраныстардың артықтық ағынын қалыптастырса, 9 б)-сурет, жағдай түбегейлі өзгереді. Мысалы, егер шабуылдаушы жақ КМКЖ-ге



8-сурет – КМКЖ жағдайының өзгеру графы модельдеу нәтижелері 9-суретте және 2-кестеде көрсетілген



а) КМКЖ-лердегі сұраныстар ағынының көрсеткіштік заңы бойынша таратылуы



б) Орындаудың түрлі артықшылықтары бар сұраныстар ағынының таратылуы (буфердің толып кету мен DoS класы шабуылдарының берілуі кезіндегі конфликтік сұраныстар)

9-сурет – Кезектің уақыты мен ұзындығына қызмет көрсету КМКЖ-де өтінімдерге ену көздерінің таратылу тәуелділігі

2-кесте – DoS / DDoS шабуылдары жағдайында КМКЖ-нің берілген желілерін имитациялық модельдеу нәтижелері

Модельдеу сеанстарының саны	n	15
Сұраныстарды жоғалту жиілігінің орташа саны	V_{zap}	4,6E-2
Сұраныстарды жоғалту жиілігінің орташа ауытқуы	F_{zap}	1,02E-3
Сұраныстарды жоғалту ықтималдығының есептік бағалауы	P_{zap}	4,41E-2
Орташа қате	ΔP_{zap}	3,87E-4

сұраныстың бірнеше қарқынды кіріс ағынын қалыптастырса, біріншіден, сұраныстар ағынын құсу мен есептерді бір өлшемді түрде көрсету мүмкін емес, екіншіден, конфликтік сұраныстар түрінде өтінімдерге уақыттың қиылыспайтын интервалында қызмет көрсетіледі. Бұдан басқа, ағындарға қызмет көрсетуге кибер қорғау жүйесімен тосқауыл қойылған кездегі қол жетпестік интервалдар бөлінеді.

Қорытынды. Жүргізілген зерттеулер нәтижесінде төмендегідей қорытындылар жасалды.

1. КМКЖ құрамына кіретін элементтердің әртүрлі математикалық модельдерін өзара біріктіретін MATLAB және Simulink-те имитациялық модельдеуді қолдану КМКЖ кибер қорғау жүйесінің тиімділігін бағалауға мүмкіндік беретін инновациялық әдістерінің бірі болып табылатындығы анықталды. КМКЖ АҚЖ-сін құру кезінде MATLAB және Simulink ортасында имитациялық модельдеу көмегімен, техникалық, технологиялық, сонымен қатар ұйымдастырушылық қайта құру мен қабылданған шешімдер салдарын оқу негізінде кибер қорғауды және АҚ-ті жетілдіру жолын анықтау бойынша есептер шығарылатындығы анықталды.

2. DoS кибер шабуылы типтік кластарының, буфердің толып кетуі кезіндегі жүйенің аномальды жағдайын анықтауда сұраныстарды болдырмау ішкі жүйесі үшін шешуші ережелердің алгоритмін қалыптастыруының жұмысқа қабілеттілігін тексеру орындалды.

ЛИТЕРАТУРА

[1] Моделирование информационных систем: учебное пособие / Под ред. О. И. Шелухина. – М.: Радиотехника, 2005. – 368 с.

[2] Моделювання витрат на розробку програмного забезпечення в залежності від типу ліцензіу [Давиденко А.М., Головань С.М., Чернова Ю.О., Дубчак О.В.] // Моделювання та інформаційні технологіу Зб. наук. Пр. ІПМЕ НАН Украγни. – 2007. – Вип. 44. – С. 60-72.

[3] Особенности защиты информации в распределенных системах телекоммуникаций и корпоративных системах связи. В 3-х т. / О.В. Есиков, Р.Н. Акиншин, А.С. Кислицын // Обеспечение информационной безопасности в экономической и телекоммуникационной сферах: Коллективная монография / Под ред. Е. М. Сухарева. – М.: Радиотехника, 2003.

[4] Павлов В.А. Формализованное представление реализации конфликтного компонента в телекоммуникационных системах / Павлов В.А., Толстых Н.Н. // Тр. науч.-техн. конф.: Радиолокация, навигация и связь (24–26 апреля 2001, Воронеж). С. 80-84.

[5] Рыков В.В. Управляемые системы массового обслуживания / Рыков В.В. // Сб. Теоретическая кибернетика. АН СССР. С. 146-154.

[6] Методы и средства защиты информации [Текст]: В 2 т. / С. В. Ленков [и др.]. – К. : Арий, 2008 . – ISBN 978–966–498–21–7.

[7] Pawar S.N. Intrusion detection in computer network using genetic algorithm approach: a survey. International Journal of Advances in Engineering Technology. – 2013. –Vol. 6, Iss. 2. P. 730–736.

[8] Raiyn J. A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications. – 2014. – Vol.8, No.1, P. 247–256

[9] Ахмад Д.М. Защита от хакеров корпоративных сетей / Дубровский И., Флинн Х. пер. с англ. – 2–е изд. – М.: Компаний АйТи; ДМК – Пресс, 2005. – 864 стр.: ил.

[10] Omar S., Ngadi A., Jebur H.H. Machine learning techniques for anomaly detection: an overview. International Journal of Computer Applications. – 2013. – Vol. 79, No. 2. P. 33–41.

[11] Дьяконов В. П. MATLAB. Анализ, идентификация и моделирование систем. Специальный справочник. / Дьяконов В. П., Круглов В. В. – СПб.: ПИТЕР, 2002. – 576 с.

[12] Дьяконов В. П., Круглов В. В. Математические пакеты расширения MATLAB. Специальный справочник. – СПб.: ПИТЕР, 2001. – 674 с.

[13] Бияшев Р.Г. Многокритериальное атрибутное разграничение доступа в современных вычислительных средах / Р.Г. Бияшев, М.Н. Калимолдаев, О.А. Рог // Труды II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика», Алматы, Казакстан, 3–4 декабря, 2015 года. – С. 67–70

[14] Бочков М.В. Активный аудит действий пользователей в защищенной сети / Бочков М.В., Логинов В.А., Саенко И.Б. // Защита информации. Конфидент. 2002, № 45. С. 94–98.

[15] Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.

[16] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко – К. : «МК-Пресс», 2006. – 320с.

[17] Chung M. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems / Chung M, Mukherjee B., Olsson R. A., Puketza N. //Proc. of the 18th NISSC, 1995.

[18] Gorodetsk, V. Attacks against Computer Network: Formal Grammar–based Framework and Simulation Tool. RAID 2000 / Gorodetsk, V., Kotenko I. //LNCS. – 2002. Vol. 2516.

[19] Knight J. The Willow Architecture: Comprehensive Survivability for Large–Scale Distributed Applications / Knight J., Heimbigner D., Wolf A.L., Carzaniga A., Hill J., Devanbu P., Gertz M. // Proceedings of International Conference Dependable Systems and Networks (DSN 02). Bethesda, MD, USA, 2002. P.17–26.

[20] Kumar S. An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR / Kumar S., Spafford E. H. – Purdue University, 1994

[21] Иванов К.В. Расчет буферной памяти и времени задержки кадров в коммутаторе OptiSwitch / Иванов К.В. // КГТУ – 2007. – № 4. – С. 57–60.

[22] Козиол Дж. Искусство взлома и защиты систем. / Козиол Дж., Личфилд Д., Эйтэл Д. и др. – СПб.: Питер, 2006. 416 с.

[23] Лахно В.А. Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок [Текст] / В.А. Лахно, А.С. Петров. - Луганск: ВНУ им. В.Даля, 2010. – 280 с.

[24] Норткат С. Анализ типовых нарушений безопасности в сетях. / Норткат С. – М.: «Вильямс», 2006. – 424 с.

[25] Тынымбаев С. Сравнительный анализ сумматоров двоично-десятичных чисел при реализации криптографических алгоритмов / С. Тынымбаев, Е. Айтхожаева, Г. Жангисина, В. Щербина // Безпека інформациу. – 2013. – Т. 19, № 3. – С. 193–197.

[26] Прохоров Ю.В. Теория вероятностей. / Прохоров Ю.В., Розанов Ю.А. – М. Изд–во. Наука. 1973. – 395 с.

[27] lakhno V.A., Petrov O.S., Hrabariev A.V., Ivanchenko V.V., Beketova G.S. Improving of information transport security under the conditions of destructive influence on the information-communication system / Journal of Theoretical and Applied Information Technology, 31st July 2016. Vol.89. No.2, p.352-361

REFERENCES

[1] Modeling of Information Systems: Textbook / Ed. OI Shelukhina. Moscow: Radio Engineering, 2005. - 368 p.

[2] Modelyuvannya vitrat on the package of software for storage in the hallway type of litigation [Davidenko AM, Golovan SM, Chernova Yu.O., Dubchak OV] // Modeluvannya ta informatsionnyi tehnologii Zb. Sciences. Etc. ІПМЕ НАН Украγни. - 2007. - Vip. 44 - P. 60 - 72.

[3] Features of information security in distributed telecommunications systems and corporate communication systems. In 3 volumes / O.V. Yesikov, RN Akinshin, A.S. Kislitsyn // Ensuring information security in the economic and telecommunications spheres: Collective monograph. Ed. EAT. Sukharev. - Moscow: Radio Engineering, 2003.

[4] Pavlov VA Formalized representation of the implementation of the conflict component in telecommunication systems. / Pavlov VA, Tolstykh N.N. // Tr. Scientific-techn. Conf .: Radiolocation, navigation and communication (April 24-26, 2001, Voronezh). Pp. 80-84.

[5] Rykov V.V. Managed queuing systems / Rykov VV // Sat. Theoretical Cybernetics. Academy of Sciences of the USSR. "Pp. 146-154.

[6] Methods and means of information protection [Text]: in 2 volumes / S.V. Lenkov [and others]. - K.: Arius, 2008. - ISBN 978-966-498-21-7.

[7] Pawar S.N. Intrusion detection in computer network using genetic algorithm approach: a survey. International Journal of Advances in Engineering Technology. – 2013. –Vol. 6, Iss. 2. P. 730–736.

[8] Raiyn J. A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications. –2014. – Vol.8, No.1, P. 247–256

[9] Ahmad D.M. Protection against hackers corporate networks / Dubrovsky I., Flynn H. per. With the English. - 2 nd ed. - Moscow: Company IT Co.; DMK - Pres, 2005. - 864 p.

[10] Omar S., Ngadi A., Jebur H.H. Machine learning techniques for anomaly detection. International Journal of Computer Applications. - 2013. - Vol. 79, No. 2. P. 33-41.

[11] MATLAB Dyakonov. Analysis, identification and modeling of systems. Special reference book. / Dyakonov V. P., Kruglov V. V. - St. Petersburg .: Peter, 2002. - 576 p.

[12] VP Dyakonov, VV Kruglov. Mathematical packages of the MATLAB extension. Special reference book. - St. Petersburg: Peter, 2001. - 674 p.

[13] RI Biyashev Multi-criteria attribute access in modern computing environments / RG Biyashev, M.N. Kalimoldaev, OA Rig // Proceedings of the II International Scientific and Practical Conference "Information and Telecommunication Technologies: Education, Science, Practice", Almaty, Kazakstan, December 3-4, 2015. - 67-70 p.

[14] M. Bochkov Active audit of user actions in a secure network / Bochkov MV, Loginov VA, Saenko IB // Data protection. Confidential. 2002, No. 45. P. 94-98.

[15] Grishchuk R. V. Theoretical basis of modeling processes in attacking information using the methods of differential programming and differential translation: monograph / RV Grischuk. - Zhitomir: RUTA, 2010. - 280 h.

[16] A.G. Korchenko Construction of information security systems on fuzzy sets. Theory and practical solutions / A.G. Korchenko-K.: "MK-Press", 2006. – 320 p.

[17] Chung M. Simulating Concurrent Intrusions for Testing Intrusion Detection Systems / Chung M, Mukherjee B., Olsson R. A., Puketza N. //Proc. of the 18th NISSC, 1995.

[18] Gorodetsk, V. Attacks against Computer Network: Formal Grammar–based Framework and Simulation Tool. RAID 2000 / Gorodetsk, V., Kotenko I. //LNCS. – 2002. Vol. 2516.

[19] Knight J. The Willow Architecture: Comprehensive Survivability for Large–Scale Distributed Applications / Knight J., Heimbigner D., Wolf A.L., Carzaniga A., Hill J., Devanbu P., Gertz M. // Proceedings of International Conference Dependable Systems and Networks (DSN 02). Bethesda, MD, USA, 2002. P.17–26.

[20] Kumar S. An Application of Pattern Matching in Intrusion Detection. Technical Report CSDTR / Kumar S., Spafford E. H. – Purdue University, 1994

[21] Ivanov K.V. Calculation of the buffer memory and time delay frames in the switch OptiSwitch / Ivanov K.V. // KSTU - 2007. - № 4. - P. 57-60.

[22] Koziol J. The art of hacking and protecting systems. / Koziol J., Lichfild D., Eitel D. et al. - St. Petersburg: Peter, 2006. 416 p.

[23] Lakhno V.A. Ensuring the security of automated information systems of transport enterprises in case of traffic intensification [Text] / V.A. Lakhno, A.S. Petrov. - Lugansk: VNU them. V.Dalya, 2010. - 280 p.

[24] Nortkat S. Analysis of typical security breaches in networks. / Northcat S. - M .: Williams, 2006. - 424 p.

[25] Tynimbaev S. Comparative analysis of adder of binary-decimal numbers in the implementation of cryptographic algorithms / S. Tynymbayev, E. Aitkhozhaeva, G. Zhangisina, V. Scherbina // Bezpeka Informatsii. - 2013. - T. 19, No. 3. - P. 193-197.

[26] Prokhorov Yu.V. Probability theory. / Prokhorov Yu.V., Rozanov Yu.A. - Moscow Publishing House. The science. 1973. - 395 p.

[27] lakhno V.A., Petrov O.S., Hrabariev A.V., Ivanchenko V.V., Beketova G.S. Improving of information transport security under the conditions of destructive influence on the information-communication system / Journal of Theoretical and Applied Information Technology, 31st July 2016. Vol.89. No.2, p.352-361

Г. Бекетова[1], Б. Ахметов[1], А. Корченко[2], А. Лахно[3]

[1]Казахский национальный исследовательский технический университет им. К. И. Сатпаева, Алматы, Казахстан,
[2]Национальный авиационный университет, Киев, Украина,
[3]Европейский университет, Киев, Украина

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СИСТЕМ КИБЕРЗАЩИТЫ В MATLAB И SIMULINK

Аннотация. В статье рассмотрены некоторые аспекты применения имитационного моделирования в MATLAB и Simulink для решения задач обеспечения информационной безопасности компонентов средств защиты информации критически важных компьютерных систем (КВКС). Установлено, что использование имитационного моделирования в MATLAB и Simulink, позволяет объединить между собой разнородные математические модели элементов, входящих в состав КВКС, и является одним из инновационных методов, позволяющих оценивать эффективности систем киберзащиты КВКС и их реакцию на попытки возмущения по ряду показателей.

Ключевые слова: критически важные компьютерные системы, средства защиты информации, имитационное моделирование, межсетевой экран.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Д. С. Аленов, Т. М. Апендиев*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 24.05.2017.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
19,4 п.л. Тираж 2000. Заказ 3.