Қорытынды

Компьютерлік жүйелер бойында ақпарат қауіпсіздігін қамтамасыз ету үшін, желі периметрі бойында оның барлық ерекшеліктерін есепке ала отырып, біріншіден барлық желі бойындағы ақпараттармен жұмыс істеу үшін қолданушы аутентификациядан өтуі керек, екіншіден, желі трафигіне жіберіліп жатқан шабуылдар тұрақты түрде бақыланып отыруы керек, ол үшін LanAgent жүйесін қолдандық. Сонымен, компьютерлік жүйелердің қорғанысын ұйымдастыру барысында осы қорғаныс әдістерінің барлық ерекшеліктері есепке алынып, ішкі және сыртқы периметрлерде шабуылдарды анықтауға арналған программалық-аппараттық жиыннан тұратын жүйе құрылды.

Әдебиеттер

1. *Рапх В.В.* Разработка математической модели информационного обмена в ЛВС и метода сетевой защиты информации. –М.: 2009, - 197 с.
2. *Тұрым А.Ш.* Ақпарат қорғау және қауіпсіздендіру негіздері . –Алматы:, 2002.
3. *Корнеев В.В.* Защита информации в офисе. –М.:ТК Велби, Изд-во Проспект. 2008, -333 с.

Казыбек Р., Байгелов К.Ж.

МОДУЛИ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ

Аннотация В данной работе рассматривается использование протокола Kerberos и модулей направленных на организацию защиты компьютерных систем для использования секретного индентификатора основанного на методах аутентификации.

*Ключевые слова:*Компьютерная система, атака, защита, протокол, идентификация, аутентификация, сервер, трафик.

Kazybek R., Baigelov K.

MODULE FOR COMPUTER SYSTEMS SECURITY

Annotation In this paper, we consider the use of the Kerberos protocol and modules aimed at organizing the protection of computer systems for the use of the identifier secret based authentication methods.

Keywords: Computer system, attack, defence, protocol, authentication, authentification, server, traffic.

ӘОЖ 681.3.053

Қазыбек Р., Байгелов Қ.Ж.

Қазақ ұлттық аграрлық университет

ШАБУЫЛДАРДЫ ІСКЕ АСЫРУ ҮРДІСІН МОДЕЛДЕУ ЖӘНЕ ОНЫҢ ЫҚТИМАЛДЫЛЫҚ ПАРАМЕТРІН БАҒАЛАУ

Андатпа

Шабуылдарды іске асыру үрдісін моделдеу барысы қарастырылып, осы шабуылдың пайда болу ықтималдылығының таралған заңы ретінде Пуассон заңы таңдалған, құрылған тәуекел-модель адекваттылыққа тексерілді.

Кілт сөздер: Компьютерлік жүйе, шабуыл, қорғаныс, тәуекел-модель.

Кіріспе

Мақалада парольді таңдау арқылы операциялық жүйеге қол жеткізу мәселелеріне шолу жасалып, компьютерлік жүйелерде орын алған шабуылдардың салдарынан келтірілген зиянның сандық көрсеткішін есепке ала отырып құрылған тәуекел-модель негізінде ақпаратты қорғау деңгейін көтеру жолдарына талдау жасалып, бағаланған. Ұсынылған мақсатқа жету үшін келесі тапсырмалар тұжырымдалып шешімін тапты: технологияның жалпы сипаттамасы мен оның жеке элементтерін қарастыру, ақпаратты қорғаудағы оның құрамдас саласындағы ең негізгілерін табу, алынған нәтижелерді талдау, құрылымдау және кілттік тапсырмалар тізімін қалыптастырудың шешімі қабылданып, ақпаратты қорғау деңгейін жоғарлату үшін шабуылдың пайда болу ықтималдылығының таралған заңы ретінде Пуассон заңын қолдану жолдары қарастырылған.

Компьютерлік жүйе бойымен таратылатын ақпараттың үлкен көлеміне қарамастан, жүйенің қорғанысын ұйымдастыру тәуекел-модельдің көмегімен бағаланып, белгілі бір уақыт аралығында аса жоғары көлемде зиян келтіретін шабуылдардың ықтимал шамасы анықталды.

Кілттік кезең, барлық деңгейдегі ақпараттарды қорғаудың сапалы қорғаныс жүйесін тиісті деңгейде іске асыруды қамтамасыз етуге мүмкіндік береді [1].

Парольді таңдау арқылы операциялық жүйеге қол жеткізу

Операциялық жүйеге қол жеткізудің бірінші кезеңін қарастырамыз, таңдалған компьютерлерден жүйелік файлдарды ұрлау барысы әр түрлі әдістермен іске асырылады. Бұл кезеңнен өту үшін қаскүнемнің қолында операциялық жүйеге қосымша болатын жүктеуші, ауыспалы тасымалдаушы диск болуы керек. Файлдық жүйелер ретінде FAT32 және NTFS алынды.

Парольді таңдау арқылы операциялық жүйеге ену үш кезеңнен тұратынына көз жеткіздік:

1) Керекті компьютерге кіру үшін SAM және SYSTEM файлдарын ұрлау керек.
2) Қаскүнемнің компьютердегі паролді шешуі қажет.
3) Таңдалған парольдерді қолданып компьютердің операциялық жүйесіне қол жеткізуі керек.

Тәуекел (риск) деп, компьютерлік жүйеге келтірілетін зиянның сандық көрсеткішін айтады. Тәуекел шамасы **P** ықтималдылықтың мәнімен және **U** зиянның сандық көрсеткішімен анықталады [2].

Құрылатын тәуекел-модельді, зерттелетін көптеген қауіптердің әсерін есепке ала отырып математикалық модель түріне келтірдік. Бұл моделдің шығыс параметрлері компьютерлік жүйеге төнетін қауіптің интегралданған тәуекелінен тұрады.

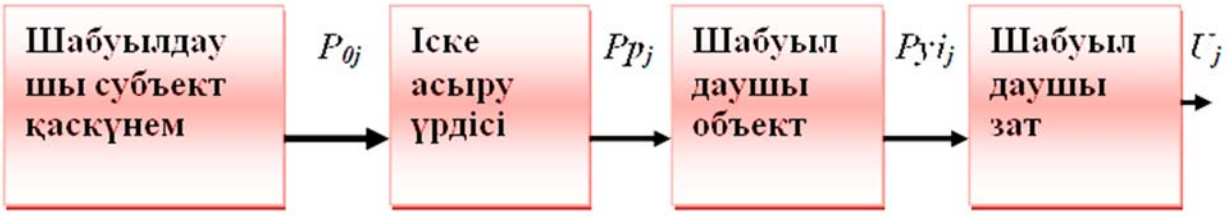
Сонымен, тәуекелдерді реттеу қорғаныс құралдарының жиынын қолдану арқылы іске асырылды. Анықталған тәуекел шамасы негізінде зерттелетін компьютерлік жүйелердің оптимум жиынын таңдап алындық.

Сандық талдау жүргізу барысында параметрлерді қажетті талапқа сай таңдау үшін, қорғалатын объектке келесі әсер ету сатыларын қолданады [1]:

1) Әсер ету субъектті (қауіп көзі) – үрдістің белсенді құрамы, басқа құрамдас бөліктерге әр түрлі әрекеттерді орындау арқылы әсер етуге мүмкіншілігі бар.
2) Әсер етуді іске асыру үрдісі - субъекттің өз мақсатына жету үшін қолданатын нақты операция немесе сценарий.
3) Әсер ету объекті – субъекттің әсерінің арасында болатын үрдістің селқос құрамы.
4) Әсер ету тұлғасы – субъекттің әрекеттері немесе оның белгілі бір мәні.

Тәуекел-модельді құру және оны адекваттылыққа бағалау

Келтірілген құрылымды іске асырылатын шабуылдар мен қашықтықтан қол жеткізуді компьютерлік жүйенің элементтеріне төндіретін қауіп тұрғысынан қарастырамыз (1-сурет).



1-сурет. Компьютерлік жүйелерге шабуылдар және оның параметрлері.

P_{0j} – i - шабуылдың пайда болу ықтималдылығы,
Pp_j – i - шабуылдың іске асыру ықтималдылығы.
Pyi_j – i - шабуылды іске асыру негізінде j – зиян орын алатындығының ықтималдылығы.
u_j – j түріндегі келтірілетін зиянның шамасы.

Аталған параметрлердіанықтау жолдарын қарастырамыз. Ол үшін әр түрлі зиян түрлері үшін тәуекелдердің тәуелсіз таралуын қарастырып, келтірілетін зиян түрін компьютерлік жүйеге жасалатын шабуылдың типімен байланыстырамыз.

Іске асырылған шабуыл түрлері – желі трафигін ұстап алу, өтірік объектті енгізу, сниффинг бумалар, осы әрекеттер тиімді іске асырылған жағдайда, қаскүнем барлық бумаларды оқи алады, ал криптографиялық әрекеттер қолданылмаса ақпараттың конфиденциалдығы бұзылады [2].

Шабуылдың пайда болу ықтималдылығының таралған заңы ретінде Пуассон заңын таңдап алдық. Тәуекелдің адекваттылығын бағалау, жүйеде Т уақыт аралығында болған шабуылдарға талдау жасау арқылы іске асырдық.

Бұл есептегі ықтималдылықтың таралуының дұрыстығын Пуассон заңының көпшілікке қызмет көрсету теориясы тұрғысынан қарастырдық. Пуассон таратуы, тұрақты уақыт аралығында болып өткен оқиғалардың санынан тұратын кездейсоқ шамаларды моделдейді, мұнда оқиғалар тұрақты орташа интенсивтілікпен және бір-бірімен байланыссыз іске асырылады.

Көпшілік жағдайда кіріс ағындар басқарылмайды және бірнеше кездейсоқ факторлармен байланысты болады. Уақыт бірлігінде іске асырылатын шабуылдар саны кездейсоқ шама болып табылады. Кездейсоқ шамаға сонымен қатар, көрші шабуылдардың іске асырылу уақытының интервалы да жатады. Бірақ, уақыт бірлігінің арасында орын алған шабуылдардың орташа саны мен көрші шабуылдар арасындағы орташа уақыт аралығында алдын-ала белгілі деп саналады [3].

Зерттеу жүргізілген уақыт аралығындағы орташа шабуылдардың санын, шабуылдардың келтірілген интенсивтілігі деп атайды және келесі түрде анықтайды (1):

$$\lambda = \frac{T}{T_0}, \qquad (1)$$

Мұндағы, $\mathbf{T_0}$ – шабуылдар арасындағы уақыт интервалының орташа мәні, б.а. интенсивтілік мәні зерттелетін уақыт аралығында болып жатқан шабуылдардың орташа санымен анықталады.

Көптеген нақты үрдістер үшін оқиғалар ағыны Пуассоның таратуы заңымен жақсы сипатталады. Мұндай ағын жәй деп аталады. Жәй ағын бірнеше маңызды қасиеттерге ие:

1. Тұрғылықтылық қасиеті. Уақыт бойынша ағынның ықтималдылық режимінің өзгермейтіндігін сипаттайды. Бірдей уақыт аралығында болып жатқан оқиғалардың саны, орташалап алғанда тұрақты болуы керек. Егер үлкен уақыт аралығын қарастыратын болсақ компьютерлік жүйеде орын алатын күрделі өзгерістер және оның жұмыс атқару ортасы үшін бұл қасиетті қоданууға болады.

2. Аяққы әсердің жоқтық қасиеті. Қиылыспайтын уақыт аралығындағы оқиғалар санының өзара тәуелсіздігін қамтамасыз етеді. Басқаша айтқанда, осы уақыт аралығында

түсіп жатқан оқиғалардың саны, оның алдында түсіп жатқан оқиғалардың санына байланысты емес. Қарастырылып отырған жүйенің күрделілігіне байланысты, жасалатын қорытынды, шабуылды іске асыру саны өте көп, сондықтан, бір тектес шабуылдарды тәуелсіз деп санауға болады.

3.Ерекшелік қасиеті. Бір мезетте екі немесе одан да көп оқиғалардың түсуінің мүмкін еместігін білдіреді (бұл оқиғаның ықтималдылығы қарастырылатын уақыт аралығына қарағанда өте аз, егер уақыт нөлге ұмтылатын болса). Тәжірибеде үрдіс стационарлы емес (күннің әр түрлі мерзімдерінде, айдың әр түрлі күндерінде өзгеріп отырады, ертемен немесе айдың соңғы күндері). Аяққы әсердің орын алуы интервалдың аяғында шабуылдың саны оның бас кезіндегі эффективтілігіне байланысты. Егер бірнеше қаскүнемдер біртектес шабуылдарды іске асыратын болса, онда біртексіздік бейнесі орын алады. Бірақ, Пуассонның тарату заңы жоғары дәлдікпен көптеген көпшілікке қызмет көрсету заңдарын сипаттайды, сондықтан, шабуылдың пайда болу ықтималдылығы тарату барысында қолданылады [1].

Бұл тұжырымдама көптеген жағдайда дұрыс болып саналады, сонымен қатар, ол А.Я.Хинчиннің жалпы теоремасымен дәлелденеді, тәжірибелік және теориялық құны жоғары [3]. Бұл теорема бойынша, кіріс ағынды, барлық тәуелсіз ағындардың үлкен қосындысы түрінде көрсетуге болады, сонымен қатар, оны интенсивтілігі жағынан ешқайсысын қосынды ағынмен салыстыруға болмайтын жағдайда қолдануға болады. Бұл есепте жалпы шабуылды, әр жеке қаскүнем іске асыра алатын, әр түрлі шабуылдардың ағынына бөлуге болады.

Шабуылдардың ағынына қорғаныс қоюдың мақсаты - қатынас құруға рұқсат етілмеген арналарды ақпараттың түрін өзгертуге, ақпаратты жоғалтуға және сыртқа келтіруге бағытталған әсерлерден сенімді түрде сақтауды қамтамасыз ететін өзара байланысты бөгеттердің біріңғай жүйесін құру. Жүйе жұмысын қалыпты режимде көзделмеген осындай оқиғалардың біреуінің пайда болуы рұқсат етілмеген қатынас құру деп саналады.

Қорғаныш жүйесінің міндеттері: жасырын және өте жасырын ақпараттарды онымен рұқсатсыз танысудан және оның көшірмесін жасап алудан қорғау; деректер мен программаларды рұқсат етілмеген кездейсоқ немесе әдейі өзгертуден қорғау; деректер мен прогграммалардың бұзылуының салдарынан болатын шығындан көлемін азайту; есептеу техника құралдарының көмегімен орындалатын қаражаттық қылмыстардың алдын алу және т.б.

Шабуылдар ағынынан қорғаныс жүйесі - деп белгіленген қорғаныш мәселелерін шешу үшін онда көзделетін барлық құралдар, әдістер және шаралардың ұйымдастырылған жиынтығын айтады.

Ақпараттық қорғаныс жүйесін құрудың жалпы әдістемелік ұстанымдары: тұжырым/дамалық тұтастық-бірлік, талаптарға барабарлық, икемділік, функционалдық тәуелсіздік, пайдалану ыңғайлығы, берілетін құқықтарды шектеу, бақылаудың толық-тығы, қарсы әрекет жасаудың белсенділігі, тиімділік [2].

Жәй ағындар кезінде орын алған шабуылдарды тарату, Пуассонның тарату заңына бағынады [3]. Жалпы жағдайда таңдап алынған компьютерлік жүйенің жұмыс атқару ұзақтығын, Т уақыт интервалын есепке ала отырып есептеуге болады (2):

$$p_k = \frac{(\lambda_0 T)^k}{k!} e^{-\lambda_0 T}. \qquad (2)$$

Интенсивтілік λ_0 таңдап алынған **Т** интервалдың бірлік өлшеміне сәйкес болатын уақыт аралығындағы шабуылдардың санына тең (3).

$$\lambda = \lambda_0 T, \qquad (3)$$

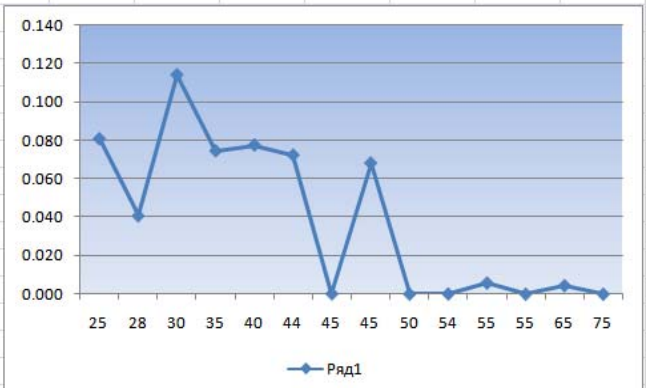
Бірақ, егер **λ** шамасын енгізетін болсақ, онда Т уақыт аралығында дәл ***k*** шабуыл болатындығының ықтималдалығы келесі формуламен есептеледі (4):

$$p_k = \frac{\lambda^k}{k!} e^{-\lambda}. \qquad (4)$$

Келтірілген зиянды есептеу шабуылдардың жалпы ағынын әр шабуылдың тигізетін зияны бойынша ағындарға бөлу арқылы есептелді (2-сурет).

	Lymbda	T	k шабуыл	Pk	k!
2	0.5	25	15	0.081	1.3077E+12
3	0.5	28	19	0.041	1.2165E+17
4	0.4	30	12	0.114	479001600
5	0.6	35	18	0.075	6.4024E+15
6	0.6	40	22	0.078	1.124E+21
7	0.6	44	24	0.073	6.2045E+23
8	0.7	45	14	0.000	8.7178E+10
9	0.4	45	21	0.068	5.1091E+19
10	0.7	50	15	0.000	1.3077E+12
11	0.7	54	18	0.000	6.4024E+15
12	0.5	55	16	0.006	2.0923E+13
13	0.8	55	14	0.000	8.7178E+10
14	0.6	65	25	0.004	1.5511E+25
15	0.8	75	25	0.000	1.5511E+25

$$p_k = \frac{(\lambda_0 T)^k}{k!} e^{-\lambda_0 T}.$$



Сурет 2. Т уақыт аралығында k шабуыл болатынының ықтималдылығы

Сонымен, зерттеу қорытындысы бойынша алынған көрсеткіштерді өңдеу барысында, келесі тұжырымдаманы жасауға болады: уақыт интервалы 25-тен 45 минутқа дейін өзгергенде, желі бойындағы шабуылдардың пайда болу ықтималдылығының ең үлкен көрсеткіші 0,114 тең болды, ал уақыт 50 минуттан жоғарылаған сайын, шабуылдардың пайда болу ықтималдылығы нөлге жақын көрсеткішке ие болды.

Қорытынды

Келтірілетін зиян компьютерлік жүйенің түрлеріне байланысты әр түрлі деңгейде іске асырылады және ол жүйеге келтірілетін әсердің маңыздылығына байланысты. Сондықтан тәуекел-моделдеу барысында зиянның көлемі ретінде қауіптерге сәйкескелетін, тиімді іске асырылған зияндардың санын алу қажеттігі анықталды, ал әр шабуыл түріне байланысты зиянды жеке есептеу керек.

Әдебиеттер

1. *ЧипигаА.Ф., Пелешенко В.С.* Формализация процедур обнаружения и предотвращения сетевых атак//Известия ТРТУ Таганрог 2006 С 96-101
2. *Тұрым А.Ш.* Ақпарат қорғау және қауіпсіздендіру негіздері . –Алматы:, 2002.
3. *Хинчин А.Я.* Риск-модели информационных систем при реализации угроз непосредственного и удаленного доступа. –М.: РадиоСофт, 2009. -134с.

Казыбек Р., Байгелов К.Ж.

МОДЕЛИРОВАНИЕ ПРОЦЕССА ОРГАНИЗАЦИИ АТАК И ОЦЕНКА ИХ ВЕРОЯТНОСТНЫХ ПАРАМЕТРОВ

Аннотация В данной работе рассматривается моделирования процесса организации атак, для оценки появления атак выбран закон распределения вероятности, закон Пуассона, построенная риск-модель проверена на адекватность.

*Ключевые слова:*Компьютерная система, атака, защита, риск-модель.

Kazybek R., Baigelov K.

MODELING OF ATTACKS AND ASSESSMENT OF THEIR PROBABILISTIC PARAMETERS

Annotation This paper deals with modeling the process of organizing the attacks, to assess the of attacks chosen the law of probability distribution, the Poisson law, based risk model was validated for adequacy.

*Keywords:*Computer system, attack, defence, risk-model.

УДК 631.352

Марзуова М., Нуржан Д.Ж., Ундирбаев М.С., Абдрашев Ж.К.

Казахский национальный аграрный университет

ТЕХНОЛОГИЯ УБОРКИ ЛЮЦЕРНЫ В КРЕСТЬЯНСКИХ ХОЗЯЙСТВАХ ЮГА КАЗАХСТАНА

Аннотация

В условиях становления рыночных отношений в сельском хозяйстве Юга Казахстана, для удовлетворения потребностей животноводства в полноценном корме необходимо создать прочную кормовую базу. Из всех заготавливаемых видов кормов на повышение удоев молока и привесов мяса лучше влияет люцерна. Зеленая масса люцерны хорошо поедается всеми сельскохозяйственными животными. Например, при скармливании крупному рогатому скоту, коэффициент использования ее составляет 92,6 %. По богатству белками люцерновое сено превосходит многие другие корма, так в 100 кг люцернового сена содержится 11,6 кг пере варимого протеина, 1,77 кг кальция, 0,22 кг фосфора и 4,5 г каротина.

Ключевые слова: Южно-Казахстанская область, люцерна, урожайность, агротехнические требования, технологический процесс.

Введение

Успешное решение задач увеличения поголовья скота и повышения продуктивности животноводства в экологических условиях В юге Казахстана во многом зависит от своевременной заготовки кормов и перевода кормопроизводства на промышленную основу.

Увеличить производство высококачественных кормов можно за счет внедрения высокоурожайных сортов, применения новых ресурсосберегающих технологий возделывания и уборки, оптимальной организации производственных процессов возделывания и повышения эффективности использования технических средств.