**МРНТИ 50.47**
**УДК 004.056**

**https://doi.org/10.51889/2021-4.1728-7901.12**

*В.А. Лахно[1], Б.С. Ахметов[2], М.Б. Ыдырышбаева[3*], А. Ербол[2]*
**e-mail: moldir.ydyryshbaeva@gmail.com*

*[1]Биоресурстар және табиғатты пайдалану ұлттық университеті, Киев қ., Украина*
*[2]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан*
*[3]әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы қ., Қазақстан*

# КИБЕРШАБУЫЛДАРДЫ ТАНУ ҮШІН ШЕШІМДЕРДІ ҚОЛДАУ ЖҮЙЕЛЕРІ ТУРАЛЫ БІЛІМ БАЗАСЫН ҚАЛЫПТАСТЫРУ МОДЕЛЬДЕРІ

*Аңдатпа*

Ақпараттандыру объектілерінің (АО) ақпараттық-коммуникациялық желілеріне (АКЖ) басып кіру қатерлері мен кезеңдерін болжау барысында шешімдер қабылдауды қолдау жүйесінің есептеу ядросы үшін Байес желілерінің (БЖ) үлгілері әзірленді. Ұсынылған БЖ үлгілері көптеген кездейсоқ айнымалылармен жұмыс істеуге және кибернетикалық қауіптің немесе берілген жағдайларда басып кірудің нақты кезеңінің ықтималдығын анықтауға мүмкіндік береді. Динамикалық Байес желілерін (ДБЖ) қолдану негізінде желілік шабуылдарды анықтаудың ықтималды модельдері толықтырылды. EM-алгоритм негізінде Байес желілерінің параметрлері оқытылды. Ұсынылған тәсілдің қолданыстағы шешімдерден айырмашылығы, басып кіруді анықтаудың негізгі кезеңдерін ескеріп қана қоймай, стандартты басып кіруді анықтау үлгілерін, жаңадан синтезделген үлгілерді қолдану арқылы шешім қабылдауға мүмкіндік береді. Барлық үлгілер мен модельдер басып кіруді анықтау кезінде ШҚҚЖ есептеу ядросын құрайды. Әзірленген модельдердің тиімділігі бұрын оқытуда қолданылмаған тест үлгілерінде тексеріледі.

**Түйін сөздер:** шешім қабылдауды қолдау жүйелері, басып кіруді тану, байес желілері, модельдер.

*Аннотация*

# МОДЕЛИ ФОРМИРОВАНИЯ БАЗ ЗНАНИЙ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ РАСПОЗНАВАНИЯ КИБЕРАТАК

*В.А. Лахно[1], Б.С. Ахметов[2], М.Б. Ыдырышбаева[3], А. Ербол[2]*
*[1]Национальный университет биоресурсов и природопользования, г. Киев, Украина*
*[2]Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан*
*[3]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан*

Разработаны шаблоны байесовских сетей (БС) для вычислительного ядра системы поддержки принятия решений (СППР) в ходе прогнозирования угроз и этапов вторжения в информационно-коммуникационные сети (ИКС) объектов информатизации (ОБИ). Предложенные шаблоны БС, позволяют оперировать множеством случайных переменных и определять вероятность реализации кибернетической угрозы или конкретного этапа вторжения при заданных условиях. Дополнены вероятностные модели выявления сетевых вторжений на основе применения динамических сетей Байеса (ДСБ). Проведено обучение параметров байесовских сетей на основе EM-алгоритма. В отличие от существующих решений, предложенный подход дает возможность не только учитывать основные этапы вторжений, но и более обоснованно принимать решения на основе применения как типовых шаблонов вторжений, так и вновь синтезируемых шаблонов. Все шаблоны и модели составляют вычислительное ядро СППР в ходе выявления вторжений. Эффективность разработанных моделей проверена на тестовых выборках, которые ранее не использовались в обучении.

**Ключевые слова:** система поддержки принятия решений, распознавание вторжений, байесовские сети, модели.

*Abstract*

# MODELS FOR FORMING KNOWLEDGE DATABASES FOR DECISION SUPPORT SYSTEMS FOR RECOGNIZING CYBERATTACKS

*Lakhno V.A.[1], Akhmetov B.S.[2], Ydyryshbayeva M.B.[3], Yerbol A.[2]*
*[1]National University of Life and Environmental Sciences, Kiev, Ukraine*
*[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan*
*[3]Al Farabi Kazakh National University, Almaty, Kazakhstan*

Patterns of Bayesian networks (BN) have been developed for the computing core of the decision support system (DSS) in the course of threats prediction and stages of intrusion into information and communication networks (ICN) of

informatization objects. The proposed Bayesian networks (BN) templates allow one to operate with a variety of random variables and determine the probability of a cyber threat or a specific stage of an invasion under given conditions. Probabilistic models for detecting network intrusions based on the use of dynamic Bayesian networks (DBN) have been added. The training of Bayesian networks parameters based on the EM-algorithm was carried out. In contrast to existing solutions, the proposed approach makes it possible not only to take into account the main stages of intrusions but also to make more reasonable decisions based on the use of both typical intrusion patterns and newly synthesized patterns. All templates and models make up the decision support system (DSS) computing core for intrusion detection. The effectiveness of the developed models was tested on test samples that were not previously used in training.

**Keywords:** Decision support system, intrusion recognition, Bayesian networks, models.

**1. Кіріспе**

Ақпараттандыру объектілеріне (АО) заңсыз әсер ету күрделілігінің тұрақты өсуіне, аномалияларды зияткерлік тану жүйелерін және кибернетикалық шабуылдарды пайдалану арқылы қарсы тұруға болады [1]. Шабуыл сценарийлерінің күрделенуі жағдайында көптеген компаниялар басып кіруді анықтау жүйелерін (БКАЖ) жасаушылар интеллектуалды шешімдерді қолдау жүйелерін (ШҚҚЖ) өз өнімдеріне біріктіре бастады. Қазіргі заманғы ШҚҚЖ негізі оның есептеу ядросын құрайтын әртүрлі модельдер мен әдістерден тұрады [2].

Әртүрлі АО ақпараттық қауіпсіздігін кепілдікті қамтамасыз етудің (АҚ) күрделі жағдайларында шешімдер қабылдау процесі ақпаратты қорғау құралдары (АҚҚ) мен кибернетикалық қауіпсіздік жүйелері (КҚ) сарапшылармен белсенді өзара іс-қимыл жасаған жағдайда жүргізілетін болады. Жоғарыда аталған жағдайлар БКАЖ құрамындағы ШҚҚЖ есептеу ядросы үшін модельдерді синтездеу саласындағы зерттеулеріміздің өзектілігін анықтады.

**2. Әдебиеттерге шолу және талдау**

[2] көрсетілгендей, осы саладағы зерттеулердің перспективалық бағыты АҚ саласындағы ШҚҚЖ [3] әдістері, модельдері мен бағдарламалық кешендерін және сараптамалық жүйелерді (ЭС) [4] дамыту бойынша жұмыстар болды.

[5, 6] еңбектерде АҚ есептеріндегі Data Mining технологиялары қарастырылды. Бұл зерттеулерде АО АҚ қамтамасыз етумен байланысты жағдай эволюциясының заңдылықтарын анықтау міндетіне баса назар аударылады. Қарастырылған жұмыстар бағдарламалық кешендер түрінде практикалық іске асырылмады.

[7] еңбекте АО АҚ есептерінде интеллектуалды модельдеу әдістемесі талданады. Авторлар ұсынған әдістеме АО-ға басып кіруді жүзеге асырудың әртүрлі сценарийлерін талдауға және шешім қабылдауға арналған. Алайда, бұл зерттеулер аппараттық немесе бағдарламалық жасақтамаға жеткізілмеген.

АҚ есептеріне талдау жасау және шешім қабылдауды қолдау қиын, шабуылдардың жаңа кластары пайда болған кезде АҚ-ны қамтамасыз ету есептерін формализациялау және құрылымдау әлсіз берілетін болып табылады. Бұл жағдайда АО АҚ күйінің параметрлері сапалық көрсеткіштермен ұсынылуы мүмкін.

Авторлардың пікірінше [8] АО-ның қорғалу дәрежесін талдау және мақсатты кибершабуылдарға қарсы іс-қимыл жоспарларын әзірлеудің алдында негізгі қауіптерді анықтау кезеңі болуы керек. Авторлар [9] тиісті ШҚҚЖ-сыз осындай мәселені сапалы шешу қиын екенін айтады. Зерттеушілер олардың дамуының практикалық нәтижелерінің сипаттамасын бермеді.

[10] еңбектерінде АҚҚ құрудың аталған аспектілерін Байес желілерінің (БЖ) қолданылуына негізделген тәсілде ескеруге болатындығы көрсетілген. Деректерді талдаудың қолданыстағы әдістерімен салыстырғанда, олар өз тұжырымдарына көрнекі және интуитивті түсінік береді. Сондай - ақ, БЖ (көбінесе динамикалық, ДБЖ) логикалық түсіндіруді және есеп айнымалылары арасындағы қатынастардың құрылымын өзгертуді қамтиды. Мысалы, АО АКЖ үшін БЖ-ны графтар түрде ұсыну оны кибернетикалық қатерлерді іске асыру ықтималдығын бағалау мәселесін шешудің ыңғайлы құралы етеді.

Әзірленген ШҚҚЖ есептеу ядросының негізі білім базасын (ББ) құрайтын ықтималды модельдерге негізделген. Мұндай ықтималдық модельдер деректер әлсіз құрылымдалған немесе статистикалық талдау үшін жеткіліксіз болған жағдайда процестерді сипаттай алады. Білім базасының ықтималды модельдерін қолдану негізінде шешілуі мүмкін есептер ықтималдылықты анықтау процедураларын да қолдануы керек. АО АКЖ-де болатын әр түрлі процестер өздерінің деректер тізбегін жасайды. Бұл мәліметтер тізбегі әр процестің барысын сипаттауда көрініс табуы

керек. Жоғарыда келтірілген талдау кибершабуылдарды тану процесінде ШҚҚЖ білім базасын қалыптастырудың жаңа модельдерін жасау саласындағы зерттеулер маңызды екенін көрсетті.

**3. Зерттеудің мақсаты**

Зерттеудің мақсаты – күрделі кибернетикалық шабуылдарды анықтау барысында шешімдерді қолдау жүйесінің есептеу ядросының білім базасы үшін Байес желісіне негізделген модельдерді дамыту.

**4. Модельдер мен әдістер**

ШҚҚЖ алынған түсініктемелердің ұсынылуы пайдаланушылардың ақпараттық қажеттіліктеріне сәйкес келетініне кепілдік бермейді.

Алайда, мақалада БЖ модельдерін және ШҚҚЖ есептеу ядросының сәйкес үлгілерін әзірлеуге ұсынылған тәсіл қолданушыларға қауіптер мен осалдықтар туралы мәліметтер болатын жағдайларды түсіндіру мәселесін қолдау, егер шабуыл туралы мәліметтер әлсіз құрылымдалған немесе толық статистикалық бағалауда олардың саны аз болса, ақпараттық технологиялар мен сәйкес бағдарламалық өнімдерді пайдалануға мүмкіндік береді.

Шабуылдаушының АКЖ-дағы рұқсатсыз әрекеттері оның жұмысында тиісті ауытқуларды тудырады. Бұл тұрғыда, АКЖ-ның өзі мүлдем оқшауланған емес, бірақ белгілі бір сыртқы ортада (қызметкерлер, бәсекелестер, заң шығарушы және бақылаушы органдар және т.б. кіретін қоршаған орта) орналасады. Мұндай орта, көбіне өте әлсіз құрылымдалған, өйткені компоненттер арасындағы байланыс әрдайым нақты анықталмайды және осы ортада аномалиялар тудырған кибершабуылдарды анықтау мәселелерін шешу үшін көптеген түрлі белгілер мен сипаттамалардың шабуылын анықтау үшін тиісті құралдар мен әдістер қажет. Басып кіру белгілері мен олардың параметрлерін таңдаудың негізгі критерийі статистикалық маңыздылық деңгейі болып табылады. Бірақ желіге кіру белгілерінің өзі KDD99 [11] 41 (1 -кестені [11] қараңыз) сәйкес келетіндіктен, осы белгілердің ішіндегі ең ақпараттыларының санын азайту кезеңі қажет. Алайда, [12, 13] жұмыстарда көрсетілгендей ақпараттық белгілердің санын азайтуға болады. Мұндай қысқарту алдыңғы мысалдағыдай, БКАЖ үшін басып кіруді анықтау логикасын модельдеу үшін Байес желісін құруға мүмкіндік береді. Осылайша, ақпараттылық сипаттамаларды талдау мен іріктеу үшін параметрлердің жалпы санын барынша азайту процедурасынан кейін параметрлер саны 41 -ден (2.2- кесте) 8 -ге дейін төмендеді. 1-кестеде сұр түспен белгілеу желілік шабуылдарды анықтау үшін ең ақпаратты деп танылған белгілері бар жолдарды көрсетеді [13].

Дәл осы 8 белгі Probe, U2R, R2L, Dos/DDos типтік желілік шабуылдардың болуын 99% дәлдікпен тануға мүмкіндік береді.

Таңдалған ақпараттық белгілердің кейбірі (атап айтқанда, 1-кестенің 23 және 28-жолдары) динамикалық және 0-2 с уақыт аралығында олардың мәнін өзгертеді.

Сондықтан, ШҚҚЖ жобалау және оның білім базасын Байес желілерінің тиісті үлгілерімен толтыру үшін ішкі есепте динамикалық Байес желісін –ДБЖ (DBN) қолданған дұрыс. Динамикалық Байес желілері - көрші уақыт қадамдарындағы айнымалылармен байланысқан қарапайым Байестік желілер. Шын мәнінде, ДБЖ- 1-ші қатарға жатқызуға болатын Марков процесі.

Жобаланған ДБЖ екі желіден тұрады. Бірінші БЖ ретінде $(B1)$, екінші БЖ ретінде $(B2)$ белгілейміз. $B1$ желі бастапқы болады, $B2$ желі транзиттік болып табылады. Бастапқы желі $(B1)$ қолжетімді модельдің априорлық таралуын $(P(z(1)))$ анықтайды. Транзиттік модель $(B2)$ уақыт аралығы арасындағы ауысу ықтималдығын анықтайды.

*Кесте 1. БЖ құру үшін желілік трафик параметрлері ([14] деректері бойынша)*

| *№ п/п* | *Параметр* | *Сипаттамасы* |
|---|---|---|
| *1.* | *duration* | *Байланыс ұзақтығы (секундпен)* |
| *2.* | *protocol_type* | *Хаттама түрлері (TCP, UDP, т.б.)* |
| *3.* | *service* | *Шабуыл жасалатын сервис* |
| *4.* | *src_bytes* | *Көзден қабылдағышқа дейін байттар саны* |

| | | |
|---|---|---|
| 5. | dst_bytes | Клиентке жауап байттарының саны |
| 6. | flag | Байланыс жалаулары (флагтары) |
| 7. | land | 1, егер байланыс бір хосттан/бір хостқа дейін болса /порта |
| 8. | wrong_fragment | "Жалған" фрагменттер саны |
| 9. | urgent | Шұғыл пакеттер саны |
| 10. | hot | "Ыстық" индикаторлардың саны |
| 11. | num_failed_logins | Тіркелудің сәтсіз әрекеттерінің саны |
| 12. | logged_in | 1, егер сәтті кіру болса; 0 сәтсіз |
| 13. | num_compromised | "Ымыраға келу" шарттарының саны |
| 14. | root_shell | 1, егер root shell алынса; болмаса 0 |
| 15. | su_attempted | 1, егер "su root" орындалса; болмаса 0 |
| 16. | num_root | "root" қолжетімділік саны |
| 17. | num_file_creations | Файл құру операцияларының саны |
| 18. | num_shells | Қабықша беруге сұраныстар саны |
| 19. | num_access_files | Файлдарды басқаруға қол жеткізу операцияларының саны |
| 20. | num_outbound_cmds | FTP сессиясына арналған шығыс командаларының саны |
| 21. | is_hot_login | 1, егер логин "ыстық" тізімге жататын болса |
| 22. | is_guest_login | 1, егер "қонақ" кіру |
| 23. | count | Соңғы 2 с ағымдағы сессиядағы хостқа қосылу саны |
| 24. | serror_rate | % "SYN" қателері бар қосылыстар |
| 25. | rerror_rate | % "REJ" қателері бар қосылыстар |
| 26. | same_srv_rate | % бірдей қызмет көрсететін қосылыстар |
| 27. | diff_srv_rate | % әр түрлі қызметтерге қосылу |
| 28. | srv_count | Соңғы 2 с үшін осындай сервиске қосылыстар саны |
| 29. | srv_serror_rate | % «SYN» пакетінде қате бар қосылымдар |
| 30. | srv_rerror_rate | % "REJ" қателері бар қосылыстар |
| 31. | srv_diff_host_rate | % басқа хосттардан қосылыстар |
| 32. | dst_host_count | Жергілікті хостқа қашықтан (удаленной) орнатылған қосылулар саны |
| 33. | dst_host_srv_count | Қашықтағы тарап орнатқан және бір қызметті пайдаланатын жергілікті хостқа қосылу саны |
| 34. | dst_host_same_srv_rate | % Қашықтағы тарап орнатқан және бір Қызметті пайдаланатын жергілікті хостқа қосылу |
| 35. | dst_host_diff_srv_rate | % Қашықтағы тарап орнатқан және әртүрлі қызметтерді пайдаланатын жергілікті хостқа қосылу |
| 36. | dst_host_same_src_port_rate | % ағымдағы порт нөмірі кезінде осы хостқа қосылу |
| 37. | dst_host_srv_diff_host_rate | % әр түрлі хосттардың қызметіне қосылу |
| 38. | dst_host_serror_rate | % осы хост қабылдағыш үшін SYN типті қате қосылымдар |
| 39. | dst_host_srv_serror_rate | % осы қабылдағыш қызмет үшін SYN типті қате қосылымдар |
| 40. | dst_host_rerror_rate | % берілген хост қабылдағыш үшін REJ типті қате қосылымдар |
| 41. | dst_host_srv_rerror_rate | % осы қабылдағыш қызмет үшін REJ типті қате қосылымдар |

Содан кейін, жоғарыда айтылғандарды ескере отырып, 1-кестенің 2-4, 23, 26-28, 34 жолдарында белгіленген айнымалылар үшін ДБЖ құрамыз. Сонымен қатар, ДБЖ-ге *type* айнымалын қосамыз, ол шын мәнінде желілер арасындағы $(B1)$ және $(B2)$ ауысу сәтін көрсетеді.

ДБЖ жобалау үшін GeNIe Modeler редакторы қолданылды. Қолжетімді модельдерді бөлу графының төбелері арасында ауысуға арналған ДБЖ-ның ықтималды моделі төменде көрсетілген:

$$p(Z_t \mid Z_{t-1}) = \prod_{t=1}^{N} p\left(p\left(Z_t^i \mid Pa\left(Z_t^i\right)\right)\right), \tag{1}$$

$$p(Z_{1:t}) = \prod_{t=1}^{N}\prod_{i=1}^{N} p\left(Z_t^i \mid Pa\left(Z_t^i\right)\right), \tag{2}$$

Мұндағы $Z_t - t$ уақыт моменті үшін БЖ кесу; $Z_t^i - t$ уақыт кезіндегі БЖ түйін; $Pa\left(Z_t^i\right) - Z_t^i$ БЖ түйініне арналған көптеген ата-аналық түйіндер; $N -$ БЖ кесуге арналған түйіндер саны. (2) өрнегі БЖ түйіндері арасындағы ауысу ықтималдығын сипаттайды.

Егер модель $(V_t)$ байқалмайтын айнымалылар жиынына, сондай-ақ $(U_t)$ тіркелетін айнымалылар жиынына бөлінсе, онда бұл жағдайда (1) өрнекті (2) өрнегімен толықтыру керек, ол сәйкесінше күй моделін ғана емес, сонымен қатар бақылау моделін де орнатады.

Жобаланған тест желісі үшін трафиктің қасиеттерін талдауда артықшылық мәселесін шешу үшін 1-суретті қараңыз, бұл трафиктің ақпараттық сипаттамаларын талдау арқылы жүзеге асырылады.

Мақалаларды талдау негізінде ақпараттық сипаттамаларды талдау барысында [14,15] ақпараттың өсу критерийін қолдану ұсынылды – $I(V,U)$.

Осы өлшемге сәйкес ақпаратты бір атрибуттан $I(V,U)$ екінші атрибутқа ұлғайту (мысалы, 3 жол – $V$ атрибут , 23жол – $U$ атрибут ) $V$ мәндер белгілі болған кезде, $U$ мәнге қатысты белгісіздік азаятынын көрсетеді .

Сәйкесінше, $I(V,U) = H(U) - H(U \mid V)$, мұндағы $H(U), H(U \mid V) - (U \mid V)$ және $U$ атрибут энтрапиясы. $U$ және $V$ мәндері дискретті және $\{u_1,...,u_k\}$ и $\{v_1,...,v_k\}$, диапазондағы мәндерді қабылдай алатындықтан, $U$ атрибут үшін энтропия мәндері келесідей анықталды:

$$H(U) = -\sum_{i=1}^{i=k} P(U = u_i) \cdot \log_2\left(P(U = u_i)\right). \tag{3}$$

Шартты энтропияны келесідей табуға болады:

$$H(U \mid V) = -\sum_{j=1}^{j=l} P(V = v_i) \cdot H(U \mid V = v_i). \tag{4}$$

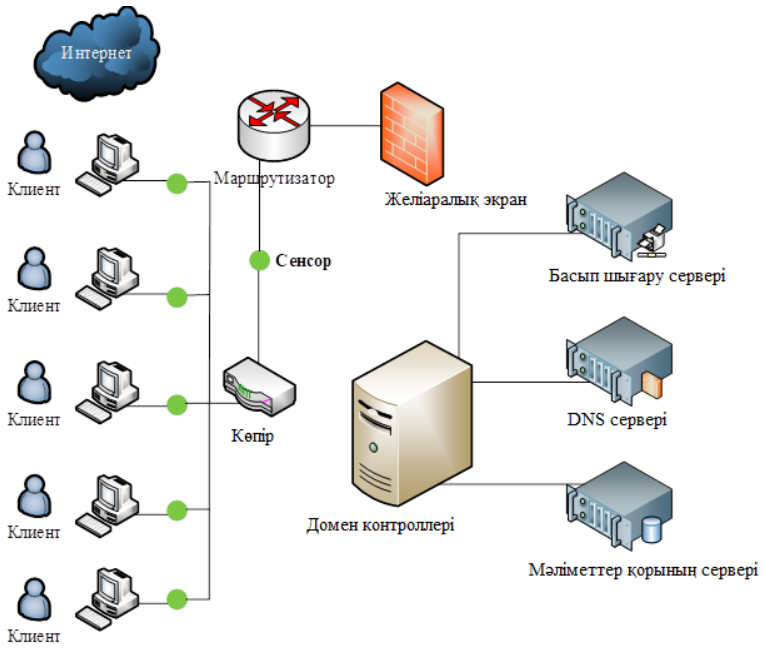
Дискретті мәндер үшін есептеу жүргізілгендіктен, жиындардағы мәндерді таңдау қажет болды. $\{u_1,...,u_k\}$ и $\{v_1,...,v_k\}$ есептеу дискретті мәндер үшін жүргізілгендіктен, жиындардан алынған мәндерді $I(V,U)$ дискреттеуге тура келді.

Тест эксперименттері кезінде іріктеу үшін бірдей жиілік интервалдары әдісі қолданылды. Осы әдіске сәйкес атрибут мәнінің кеңістік мәні бөлімдердің еркін санына бөлінуі керек. Әр бөлімде тиісті мәліметтермен сипатталған нүктелер саны бірдей болады. Бұл әдісті қолдану деректер мәндерін жүйелі жіктеуге қол жеткізуге мүмкіндік берді.

Ақпараттың өсуі $I(V,U)$ сәйкес атрибуттардың мәндерінің санына байланысты болады. Сондықтан мәндердің саны артқан сайын атрибуттың энтропиялық мәні төмендейді.

Ақпараттық атрибуттарды күшейту коэффициентінің көмегімен таңдауға болады [13]:

$$G(U \mid V) = \frac{I(U,V)}{H(V)} = \frac{H(U) - H(U \mid V)}{H(V)}.$$




*Сурет 1. Тестілік желі*

Ақпараттың пайда болуы нәтижені ШҚҚЖ-ге ұсыну үшін қажет $G(U|V)$ оның мөлшерін ғана емес, ағымдағы $(V)$ атрибут бойынша ақпаратты бөлу үшін $H(V)$ қажет болады.

ШҚҚЖ ББ үшін ДБЖ жобалаудың келесі мысалын қарастырамыз. Ол үшін біз келесі болжамдарға сүйенеміз. Әдетте, желіге басып кіру (ену) үш сатылы схемада жүзеге асады. Бірінші қадамда шабуылдаушы желіні қарап шығуды (сканерлеу) орындайды $(S)$. Екінші кезеңде АКЖ осалдықтарына $(E)$ әсер етеді. Соңғы үшінші кезеңде шабуылдаушы АКЖ-ға backdoor $(B)$ арқылы қол жеткізуге тырысады.

Қазіргі заманғы шабуылдар көбінесе қашықтан жүреді және шабуылдаушылар шабуылдайтын желі туралы барлық ақпаратты білмейді. Шабуылдаушы шабуыл объектісі туралы мүмкіндігінше көп мәліметтер жинауы керек. Кері жағдайда барлық белгілі осалдықтарды сұрыптауға тура келеді және бұл өте ұзақ процедура. Желіні сканерлеу процестері желілік трафикке өз ізін қалдырады. Бірақ, шабуылдаушы ақпаратты алған кезде, ол желілік құрылғылардағы, қызметтердегі, операциялық жүйелердегі және қолданбалы БҚ-дағы әлеуетті осалдықтарға мақсатты түрде назар аудара алады. Бұл жағдайда желіге әсер ету трафиктің өзгеруіне әкеледі. Шабуылшылардың әрекеттерінің реттілігі жеткілікті түрде нақты сипатталған, сондықтан шабуылдың жағдайы мен техникасына терең үңілместен, басып кірудің әртүрлі кезеңдеріндегі желілік күйлердің ықтималды моделін сипаттайтын ДБЖ құрылысына назар аударамыз. Егер шабуыл кезеңдері $(S),(E),(B)$ қорғаныс қызметтері байқалмаса жасырын болып саналады.

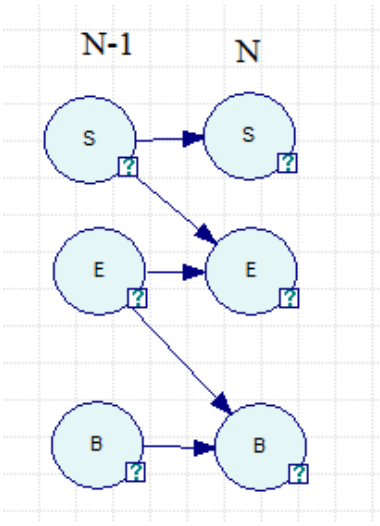
2–суретте $(S),(E),(B)$ басып кіру кезеңдеріне арналған жалпы ДБЖ-ның моделі ұсынылған. Модель басып алу процесіне сәйкес келетін екі тілімді көрсетеді.

Шабуыл кезеңдері жасырын. Бұл желілік трафиктің параметрлерін бақылау статистикасын жинау қажеттілігін тудырады (1-кесте). 1-кесте (3-6, 12, 25, 25, 29, 30, 38, 39 жолдар) бақыланатын параметрлердің өзара байланысының мысалы 3-суретте көрсетілген.

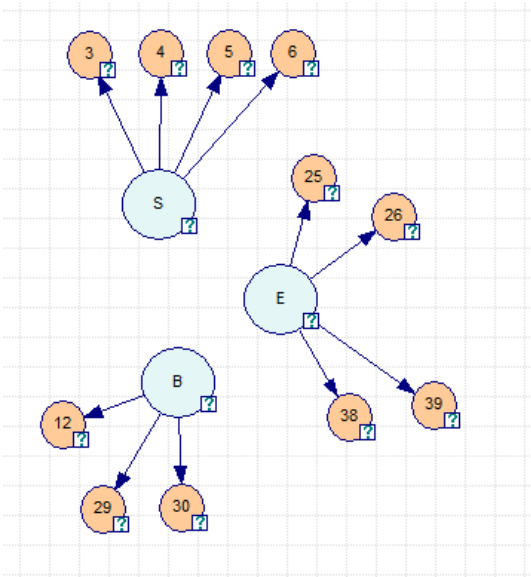
Шабуылға алынған желінің күй графын модель түрінде сипаттай аламыз:

$$P(V(n)|\,Pa(V(n))) = \prod_{i=1}^{3} P(v_i(n)|\,Pa(v_i(n))), \tag{5}$$

$$\prod_{i=1}^{3} P(v_i(n)|\,Pa(v_i(n))) =$$
$$= P(s(n)|\,s(n-1))\cdot P(e(n)|\,e(n-1),s(n-1))\cdot P(b(n)|\,b(n-1),e(n-1)). \tag{6}$$




*Сурет 2.* $(S),(E),(B)$ *басып кіру кезеңдеріне арналған жалпы ДБЖ моделі*




*Сурет 3. 1-кесте (3-6, 12, 25, 25, 29, 30, 38, 39 жолдар) бақыланатын параметрлердің өзара байланысының мысалы*

Мысалы, 3-суретте көрсетілген БЖ нұсқасы үшін желілік трафик бақыланатын айнымалылардың байланысын және күйден графтың төбелерінің күйіне өту ықтималдығын сипаттайтын модель келесідей болады:

$$P(U(n)\,|\,Pa(U(n))) = \prod_{j=1}^{11} P\left(u_j^N(n)\,|\,Pa\left(u_j^N(n)\right)\right), \tag{7}$$

$$\prod_{j=1}^{11} P\left(u_j^N(n)\,|\,Pa\left(u_j^N(n)\right)\right) = \prod_{j=1}^{4} P\left(u_j^N(n)\,|\,Pa(s(n))\right)\times \tag{8}$$

$$\times \prod_{j=5}^{8} P\left(u_j^N(n)\,|\,Pa(e(n))\right)\times \prod_{j=9}^{11} P\left(u_j^N(n)\,|\,Pa(b(n))\right),$$

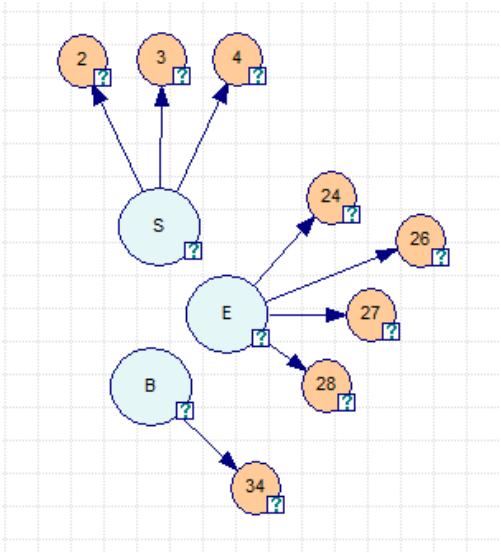
$$\begin{aligned} P\left(u_j^N(n)\,|\,Pa(s(n))\right) &= P\left(u_1^3(n)\,|\,s(n)\right)\cdot P\left(u_2^4(n)\,|\,s(n)\right)\cdot \\ &\cdot P\left(u_3^5(n)\,|\,s(n)\right)\cdot P\left(u_4^6(n)\,|\,s(n)\right), \end{aligned} \tag{9}$$

$$\begin{aligned} P\left(u_j^N(n)\,|\,Pa(e(n))\right) &= P\left(u_5^{25}(n)\,|\,e(n)\right)\cdot P\left(u_6^{26}(n)\,|\,e(n)\right)\cdot \\ &\cdot P\left(u_7^{38}(n)\,|\,e(n)\right)\cdot P\left(u_8^{39}(n)\,|\,e(n)\right), \end{aligned} \tag{10}$$

$$\prod_{j=9}^{11} P\left(u_j^N(n)\,|\,Pa(b(n))\right) = P\left(u_9^{12}(n)\,|\,b(n)\right)\cdot P\left(u_{10}^{29}(n)\,|\,b(n)\right)\cdot P\left(u_{11}^{30}(n)\,|\,b(n)\right) \tag{11}$$

Мұндағы, желі күйлерінің графы үшін байқалатын (3 суретте көрсетілгендей) $j = 1,...,11-$ айнымалылар саны, 1 кестеден алынған (трафик параметрі) $N = 1,...,41-$ тиісті.

Содан кейін 4-суретте көрсетілгендей, 1-кестенің 2-4, 23, 26-28, 34-жолдарының DDoS шабуылының бұрын таңдалған ақпараттық белгілері үшін ДБЖ келесідей болады.




*Сурет 4. Бақыланатын параметрлердің өзара байланысының мысалы (1-кестенің 2-4, 23, 26-28, 34-жолдары)*

Тиісінше, осы шабуыл үлгісі үшін желілік трафикте бақыланатын айнымалылардың байланысын және күйден граф төбелерінің күйіне өту ықтималдығын сипаттайтын модель келесідей болады:

$$P(U(n)\,|\,Pa(U(n))) = \prod_{j=1}^{8} P\left(u_j^N(n)\,|\,Pa\left(u_j^N(n)\right)\right), \tag{12}$$

$$\prod_{j=1}^{8} P\left(u_j^N(n)\,|\,Pa\left(u_j^N(n)\right)\right) = \prod_{j=1}^{3} P\left(u_j^N(n)\,|\,Pa(s(n))\right)\times \tag{13}$$

$$\times \prod_{j=4}^{6} P\left(u_j^N(n)\,|\,Pa(e(n))\right)\times P\left(u_6^7(n)\,|\,Pa(b(n))\right).$$

$$P\left(u_j^N(n)\,|\,Pa(s(n))\right) = P\left(u_1^2(n)\,|\,s(n)\right)\cdot P\left(u_2^3(n)\,|\,s(n)\right)\cdot \\ \cdot P\left(u_3^4(n)\,|\,s(n)\right), \tag{14}$$

$$P\left(u_j^N(n)\,|\,Pa(e(n))\right) = P\left(u_4^{23}(n)\,|\,e(n)\right)\cdot P\left(u_5^{26}(n)\,|\,e(n)\right)\cdot \\ \cdot P\left(u_6^{27}(n)\,|\,e(n)\right)\cdot P\left(u_7^{28}(n)\,|\,e(n)\right), \tag{15}$$

$$P\left(u_j^N(n)\,|\,Pa(b(n))\right) = P\left(u_7^{34}(n)\,|\,b(n)\right). \tag{16}$$

Жоғарыда келтірілген есептеулерге сүйене отырып Probe, U2R, R2L, Dos/DDos түрдегі шабуылдар үшін желілік трафикте бақыланатын айнымалылардың байланысын сипаттайтын БЖ үлгілерін және сәйкес модельдерді құруға және күйден графтың төбелерінің күйіне өту ықтималдығын модельдеуге болады. БЖ үлгілері және тиісті модельдер ШҚҚЖ білім базасының негізін құрайды.

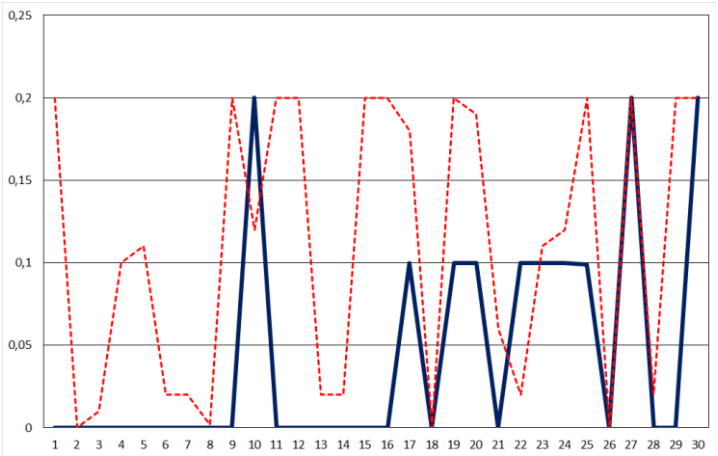
**5. Есептеу эксперименттері.**

Төменде 3 және 4 суреттерде ШҚҚЖ ББ арналған БЖ үлгілерін тестілеу нәтижелері көрсетілген. Тестілік талдауда әр үлгі үшін 30 жазба болды. Тест үлгілерін тексеру тест желісінде жүзеге асырылғандығын 1-суреттен көруге болады. Желілерді оқыту үшін PC алгоритмі және EM алгоритмі [10] қолданылды.

Эксперименттердің нәтижелері 5 және 6 суреттерде көрсетілген. Диаграммаларда оқытылған желілер үшін dos/DDos түрдегі шабуылдарды РС алгоритмі (1-жол) және ЕМ алгоритмін (2-жол) қолдану арқылы дұрыс анықтау және түсіндіру ықтималдығын модельдеу нәтижелері көрсетілген.

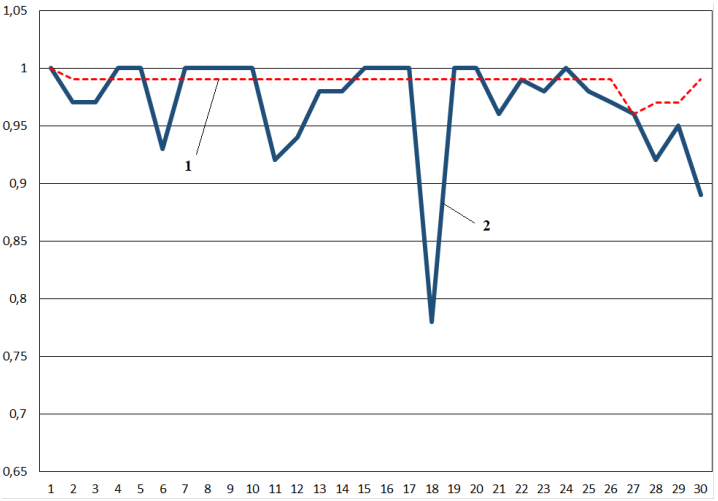
Алынған БЖ үшін модельдеу нәтижелерін талдау (3 және 4 суреттерде көрсетілген) 1-ші және 2-ші типтегі қателерді бағалау бағытында жүргізілді.

Шешім қабылдауды қолдау үшін пайдаланылған және БЖ оқытуға қатыспаған 60 жазбаның ішінде алғашқы 30 жазба тест шабуылын (2-ші типтегі қате) өткізіп жіберуді тексеру үшін дұрыс деректер. Қалған 30 жазба жалған позитивтерді тексеру үшін пайдаланылды (1-ші типтегі қате).




*1 – ЕМ алгоритмі; 2 – РС алгоритмі*

*Сурет 5. Әр түрлі алгоритмдерді қолдана отырып оқытылған БЖ үшін DDoS түрдегі шабуылды түсіндіруде 1-ші типтегі қатенің дұрыс анықталу ықтималдығы*




*1 – ЕМ алгоритмі; 2 – РС алгоритмі*

*Сурет 6. Әр түрлі алгоритмдерді қолдана отырып оқытылған БЖ үшін DDoS типті шабуылды түсіндіруде 2-ші типтегі қатенің дұрыс анықталу ықтималдығы*

**6. Есептеу экспериментінің нәтижелерін талқылау.**

5 және 6 суреттерде 1-ші және 2-ші типтегі қателер көрсетілген. РС және ЕМ алгоритмдері [10] өзінің тиімділігін растады. БЖ тестілеуі әзірленген үлгілер шабуылды 95-96% ықтималдықпен дұрыс түсіндіретінін көрсетті.

Жоғарыда сипатталған эксперименттер көрсеткендей, жүргізілген эксперименттер Байес пікірлері схемадағы әр компонент үшін ықтимал көріністі анықтауға мүмкіндік беретінін растады. Шаблондарды құрастырудың кейбір күрделілігі, егер барлық әзірленген үлгілер ШҚҚЖ білім базасының бөлігіне айналса, оларды айтарлықтай өзгертусіз бірнеше рет қолдану мүмкіндігімен өтеледі.

Гипотетикалық түрде, циклдік емес барлық ықтимал модельдер жиынтығын құру үшін БЖ қарапайым тест көмегімен құрылуы мүмкін. Алайда, [10] жұмыстар бұл тәсіл оңтайлы емес екенін

көрсетеді. Бұл 7 төбеден көп мөлшерде толық есептеу айтарлықтай есептеу ресурстарын қажет ететіндігімен және ұзақ уақытты алатындығымен байланысты. Сондықтан, дамып келе жатқан ШҚҚЖ және оның білім базасы үшін шабуыл үлгілерін алдын-ала құру, жасырын айнымалыларды азайту және шапқыншылықты анықтау дәлдігіне шешуші әсер етпейтін аз ақпараттық айнымалыларды алып тастау қолайлы нұсқа болып табылады.

ВЖ оқыту нақты бір есеп үшін жеке төбелердің параметрлерін дұрыс конфигурациялаудан, желілік шабуылдардың белгілі бір түрін анықтаудан тұрады. Осылайша, 1-кестеде көрсетілгендей оқу кезеңінде жеке куәліктердің априорлық үлестірілуі мен шартты үлестірілуін анықтау қажет. Тест мысалдарында көрсетілгендей, "мұғаліммен бірге оқыту" өте тиімді. Мұндай оқыту БЖ үлгісі жасалмаған шабуылдардың жаңа түрлерінде нәтиже бермесе де, жаңа үлгілерді оңай синтездеуге болады. Ол үшін жаңа БЖ төбелерін сипаттайтын статистикалық материал қажет. Бұл жаңа БЖ шабуылдың жаңа түрін сипаттайтын мәліметтер жиынтығы үшін тиісті кіріс және шығыс мәндерін қамтиды. Жаңа БЖ үшін тәуелсіз және жеткілікті күрделі міндет БЖ төбелерінің шартты ықтималдық кестелері үшін сандық мәндерді алу болады. Деректерді сараптамалық жолмен немесе нейрондық желі аппаратын қолдану арқылы да алуға болады.

Бұл зерттеуді дамытудың болашағы – жоғары деңгейлі алгоритмдік тілдерде ШҚҚЖ бағдарламалық қамтамасыздандыруды енгізу және осы ШҚҚЖ мен оның білім базасын АО нақты желілерінің сегменттерінде тесттен өткізу.

**Қорытынды**

АО АКЖ-ге басып кірудің қауіптері мен кезеңдерін болжау барысында ШҚҚЖ есептеу ядросы үшін Байес желілерінің (БЖ) үлгілері әзірленді.

Құрылған БЖ үлгілері көптеген кездейсоқ айнымалылармен жұмыс істеуге және кибернетикалық қауіптің немесе берілген жағдайларда басып кірудің нақты кезеңінің ықтималдығын анықтауға мүмкіндік береді. Басып кіруді болжаудың тиімділігін арттыру үшін желі параметрлерін оқыту жүргізілді. ЕМ алгоритмі және РС алгоритмі, сондай-ақ тест желісі үшін қолда бар статистикалық мәліметтер қолданылды. БЖ қолдану негізінде желілік шабуылдарды анықтаудың ықтималды модельдері сипатталған. Қолданыстағы модельдерден айырмашылығы, ұсынылған тәсіл басып кірудің негізгі кезеңдерін ескеріп қана қоймай, сонымен қатар стандартты басып кіру үлгілерін де, жаңадан синтезделген үлгілерді де қолдану негізінде шешім қабылдауға мүмкіндік береді. Барлық үлгілер мен модельдер басып кіруді анықтау кезінде ШҚҚЖ есептеу ядросын құрайды.

Әзірленген модельдердің тиімділігі бұрын оқытуда қолданылмаған тест үлгілерінде тексеріледі. Алынған нәтижелер АКЖ үшін кибернетикалық қауіптерді танудың жоғары сапалы нәтижесін алу үшін ЕМ алгоритмін қолданудың орындылығын көрсетеді.

*References:*

*1 Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95-99.*

*2 Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, (1 (2)), 4-15.*

*3 Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment, Decision Support Systems, Vol. 86, P. 13–23.*

*4 Atymtayeva, L., Kozhakhmet, K., Bortsova, G. (2014). Building a Knowledge Base for Expert System in Information Security, Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing, Vol. 270, P. 57–76.*

*5 Dua S., Du, X. (2016). Data Mining and Machine Learning in Cybersecurity, CRC press, p. 225.*

*6 Buczak, A. L., Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, Vol. 18, Iss. 2, P. 1153 – 1176.*

*7 Ben-Asher, N., Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection, Computers in Human Behavior, Vol. 48, P. 51–61.*

*8 Kanatov, M., Atymtayeva, L., Yagaliyeva, B. (2014). Expert systems for information security management and audit, Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), P. 896 – 900.*

*9 Lakhno, V.A., Lakhno, M.V., Sauanova, K.T., Sagyndykova, S.N., Adilzhanova, S.A. (2020). Decision support system on optimization of information protection tools placement, International Journal of Advanced Trends in*

*Computer Science and Engineering. P. 4457-4464.*

*10 Shin, J., Son, H., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. Reliability Engineering & System Safety, 134, 208–217.*

*11 Özgür, A., & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ Preprints, 4, e1954v1.*

*12 Lakhno, V. A., Kravchuk, P. U., Malyukov, V. P., Domrachev, V. N., Myrutenko, L. V., & Piven, O. S. (2017). Developing of the cyber security system based on clustering and formation of control deviation signs. Journal of Theoretical and Applied Information Technology, 95(21), 5778–5786.*

*13 Lakhno, V. A., Hrabariev, A. V., Petrov, O. S., Ivanchenko, Y. V., & Beketova, G. S. (2016). Improving of information transport security under the conditions of destructive influence on the information-communication system. Journal of theoretical and applied information technology, 89(2), 352–361.*

*14 Özgür, A., & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ Preprints, 4, e1954v1.*

*15 Lakhno, V. A., Hrabariev, A. V., Petrov, O. S., Ivanchenko, Y. V., & Beketova, G. S. (2016). Improving of information transport security under the conditions of destructive influence on the information-communication system. Journal of theoretical and applied information technology, 89(2), 352–361.*