УДК 32.973.202 (004.8) **DOI 10.52167/1609-1817-2022-129-6-128-136**

Ж.К. Алимсеитова[1,2], Е.Т. Каламан[1]
[1]Satbayev University, Алматы, Қазақстан
[2]Алматы технологиялық университеті, Алматы, Қазақстан
E-mail: zhuldyz_al@mail.ru

ОҚУ ОРНЫНЫҢ ТАРАТЫЛҒАН ЖЕЛІСІНІҢ АҚПАРАТТЫҚ САҚТАЛУ МОДЕЛІ

Аңдатпа. Қазіргі заманғы ақпараттық қауіпсіздік объектілерінің, оның ішінде Қазақстан Республикасының ірі университеттерінің есептеу жүйелері мен желілері өз архитектурасында көптеген күрделі элементтерді біріктіреді. Өз кезегінде, мұндай элементтердің әрқайсысы компьютерлік шабуылдаушылардың шабуылына ұшырауы мүмкін. Тиісінше, есептеу желісінің архитектурасын құрайтын элементтердің әрқайсысы кибернетикалық қауіптердің жеткілікті санына ұшырайды. Бұл қауіптердің есептеу желісінің ақпараттық қауіпсіздігіне әсерін азайту және кейбір жағдайларда келтірілген залалдың алдын алу үшін әртүрлі ақпаратты қорғау құралдары желі архитектурасына біріктірілген. Зерттеу барысында оқу орнының таратылған желісінің ақпараттық сақталу моделі толықтырылды, онда қолданыстағы модельдерден айырмашылығы, оқу орнының таратылған есептеу желісі үшін ақпараттық сақталудың бұзылу қаупінің көрсеткіштері ескерілді.

Түйінді сөздер. Ақпараттық қауіпсіздік, есептеу желісі, университет, ақпараттың сақталғандығы.

Кіріспе.

Оқу орындарының таратылған есептеу желілеріне (ТЕЖ) кибернетикалық шабуыл сценарийлерінің саны мен күрделілігінің өсуі жағдайында [1], шешім қабылдаудағы қатенің «бағасы» тез өсуде. Оқу орындарының есептеу желілерін (ЕЖ немесе ТЕЖ) жобалау барысында қабылданатын шешімдердің жоғары кәсіби деңгейін қамтамасыз ету үшін әртүрлі математикалық әдістер мен модельдер, сондай-ақ мамандандырылған бағдарламалық қамтамасыз ету (БҚ) қолданылады. Мұндай бағдарламалық қамтаманың нәтижесі көбінесе шешім қабылдаушыларға (ШҚ) ұсыныстар болып табылады. Мұндай ұсынымдардың сапасы қабылданған шешімдердің, оның ішінде университеттік ТЕЖ ақпараттық қауіпсіздігін (АҚ) қамтамасыз ету мәселелеріне қатысты шешімдердің тиімділігіне тікелей әсер етеді. Университеттік ТЕЖ АҚ-ны қамтамасыз ету міндеттеріндегі модельдердің күрделілігін үнемі арттыру АҚ-ға әсер ететін факторлар жиынтығын барабар және егжей-тегжейлі көрсетуді талап етеді. Университеттердің ТЕЖ үшін АҚ жүйелерін оңтайландыру кезінде ақпаратты қорғаудың тетіктері мен құралдарын (АҚҚ) барынша тиімді анықтау міндеті басым болып табылатынын ескеріңіз. Жоғарыда айтылғандардың барлығы біз жүргізген зерттеудің өзектілігін анықтады.

Әдебиеттерге шолу және талдау. Барған сайын киберқауіптер субъектілері көп векторлы шабуылдарға жүгінеді. Мысалы, шамамен он жыл бұрын бопсалау бағдарламалары тек деректерді шифрлауға назар аударды. Енді мұндай БҚ деректерді ұрлауды, DDoS және басқа қауіптерді қамтиды. Университеттерге көптеген кибершабуылдарды жүргізудегі басты сын-қатер оқу орнының құнды деректеріне қол жеткізу болып табылады [1-6].

Жалпыға ортақ пайдаланылатын желілермен (ЖОПЖ) байланысы болуы керек қауіпсіз және сенімді корпоративтік желіні (немесе таратылған есептеу желісін) құру

міндеті қойылған кезде, сұрақ туындайды: Корпоративтік желіні ЖОПЖ-ге қосуды ұйымдастыру тәсілі (принципі) бұл көрсеткіштерге қалай әсер етеді?».

ТЕЖ қауіпсіздігі мен сенімділігінің көрсеткіштері ғана емес, сонымен қатар таңдалған ТЕЖ негізінде қосылу және іске асыру әдістерін іске асыруға жұмсалатын ресурстардың (қаржылық, ұйымдастырушылық және т.б.) мөлшері де қосылу әдісін таңдауға байланысты болады.

Көптеген заманауи ақпараттық қауіпсіздік объектілерінің (АҚО) есептеу жүйелері немесе ТЕЖ архитектурасында көптеген күрделі элементтерді біріктіреді. Өз кезегінде, мұндай элементтердің әрқайсысы компьютерлік шабуылдаушылардың шабуылына ұшырауы мүмкін. Тиісінше, ТЕЖ архитектурасын құрайтын әрбір элемент кибернетикалық қауіптердің жеткілікті санына ұшырайды. Бұл қауіптердің ТЕЖ АЖ-ға әсерін азайту және кейбір жағдайларда келтірілген залалдың алдын алу үшін әртүрлі АҚҚ желілік архитектураға біріктірілген. Немесе ықтимал қауіптердің әртүрлілігін ескере отырып – АҚ-ны қамтамасыз ету шаралары мен құралдары.

Университеттің ТЕЖ үшін АҚ құралдарын көбейту, демек, жұмсалған ресурстардың, ең алдымен қаржылық ресурстардың көлемін ұлғайту әрқашан күтілетін нәтиже бермейтіні бұрыннан дәлелденген [1, 2].

ТЕЖ-да қолданылатын АҚ құралдары мен шаралары әртүрлі бағытта болуы мүмкін. Мысалы, бұл кез келген зиянды бағдарламалық жасақтаманың ТЕЖ соңғы түйіндеріне енуіне жол бермейтін АҚ құралдары болуы мүмкін. Немесе жүйелік әкімшілер арасында танымал жалпы ТЕЖ-тің де, оның жеке компоненттерінің де жұмысына мониторинг жүргізуге арналған бағдарламалар.

АҚ-ға қауіп-қатер ландшафты үнемі өзгеріп отыратындығына және ТЕЖ архитектурасы күрделене түскен сайын қауіптер саны артып келе жатқандығына сүйене отырып, желілердің қауіпсіз және сенімді жұмысын қамтамасыз ету мәселелерін шешу айтарлықтай қаржылық инвестицияларды қажет етеді.

Алайда, [6-10] еңбектерінде көрсетілгендей, көптеген компаниялар, бюджеттік ұйымдарды (соның ішінде оқу орындарын) айтпағанда, АҚ шаралары мен қаражатына инвестиция салуға дайын емес. АҚО менеджментін сендіру үшін көбінесе АҚҚ-ны нығайтудың орындылығы туралы жалпы пайымдауды, есептеулердің нақты нәтижелерімен күшейту қажет.

Айта кетейік, әрбір АҚО (соның ішінде университет) өзінің ақпараттық қажеттіліктерімен, нақты ақпараттық активтерімен, әртүрлі ақпараттық ағындарымен сипатталады. Осылайша, АҚО АҚ үшін қауіптер де әртүрлі болуы мүмкін. Бұл өз кезегінде болжамды айқын етеді. Әртүрлі АҚО (және олардың ТЕЖ) үшін жобаланатын АҚ жүйелеріне «құн-сапа» критерийі бойынша бірдей талаптар қойылмайды.

Егер АҚО ТЕЖ-да айналатын ақпараттық ағындардың ерекшеліктерін басшылыққа алсақ, онда АҚ үшін өзекті қауіптерді дәл ажыратуға болады. Тиісінше, дәл осы өзекті қауіптерден қорғауға осы АҚО АҚ қызметтері шоғырланған. Нәтижесінде АҚ тәуекелдері және өзекті қауіптер іске асырылған жағдайда АҚ-ға келтірілуі мүмкін ықтимал залал азаяды. Бұл тәсіл АҚҚ құнына айтарлықтай шектеулер болған кезде негізделген. Мұндай жағдайларда қорғау тарапының әзірлеушілер ұсынған АҚ-ның барлық құралдарын пайдалануға мүмкіндігі жоқ. Бұл өз кезегінде АҚО үшін шығындарды азайтатын осындай қорғау схемасын жасауға байланысты міндеттерді тудырады.

Университеттерде көбінесе ақпараттық активтер көп болады. Сонымен қатар, бұл инновациялық әзірлемелер болуы мүмкін, мысалы, озық ғылыми-техникалық зерттеулер саласында. Бұл жалпы университеттерді, сондай-ақ олардың ақпараттық жүйелері мен желілерін киберқылмыскерлер үшін тартымды нысанаға айналдырады.

Сонымен қатар, жыл сайын жаңа студенттердің пайда болуы және белгісіз беделге ие қызметкерлерді жалдау немесе айналдыру университеттердегі ақпараттық қауіпсіздік тәуекелдері мен қиындықтарын күшейтеді.

Зерттеудің мақсаты. Университет желісі ресурстарының ақпараттық сақталуын бұзу тәуекелдері көрсеткіштерінің ерекшелігін ескере отырып, оқу орнының таратылған желісінің ақпараттық сақталу моделін дамыту.

Материалдар мен тәсілдер.

Таратылған есептеу желісінің әрбір құрамдас бөлігінің ресурстары, мысалы, оқу орнының, әрқайсысының cl_{kl} іске асырылуы $\{x_{jkl}\}$ бар CL_l сыныптың ықтимал қауіптілігіне ие болсын [11, 12].

Ақпаратты қорғау құралының (әдіс, бағдарламалық қамтамасыз ету (мысалы, антивирустық бағдарламалық қамтамасыз ету немесе IDS/IPS, SIEM), аппаратура) қауіптің нақты іске асырылуының нақты тиімділігі EFA_{ijkl}, мұндағы $i-$ қорғау құралдарының индексі $(i=1,2,...,I)$, $j-$ АҚ үшін қауіптерді іске асыру тәсілінің индексі $(j=1,2,...,J)$, $k=1,2,...,K$ индексімен тең.

Оқу орнының желісі үшін АҚҚ тиімділігі уақыт бірлігі үшін динамикалық түрде өлшенеді [1].

Оқу орнының желісіндегі ақпаратты қорғау шараларының тиімділігі (EFE_{ijkl}) $i-$ ші АҚҚ қауіптерін бейтараптандыру әдісіне байланысты.

Қорғау тиімділігінің EFE_{ijkl} бір типтегі (сыныптағы) қолданылатын АҚҚ санына тәуелділігін анықтауға болады:

$$EFE_{ijkl} = f\left(EFA_{ijkl}, n_i\right), \tag{1}$$

мұнда n_i- оқу орнының ТЕЖ ақпараттық қауіпсіздігін қамтамасыз ету үшін пайдаланылатын $i-$ ші АҚҚ саны.

ТЕЖ жеке компонентінің жұмыс істеу кезеңінің T қорғау тиімділігіне EFE_{ijkl} тәуелділігін құрамыз және оқу орнының ТЕЖ АҚ ішкі жүйесінің құрамында бір мезгілде қолданылатын АҚҚ максимумын $n_{i\max}$ анықтаймыз.

Оқу орнының ТЕЖ ресурстарын қорғаудың келесі деңгейінде АҚҚ бір мезгілде өзара әрекеттеседі. Сондықтан мультипликативті модельді қолданған жөн [12].

Мысалы, осы деңгейдегі АҚҚ тиімділік дәрежесін келесі өрнек арқылы сипаттауға болады:

$$Q_{ikj} = 1 - \prod_{i=1}^{I}\left[1 - EFE_{ijkl}\left(EFA_{ijkl}, n_i\right)\right], \tag{2}$$

мұнда $I-$ оқу орнының ТЕЖ үшін барлық АҚҚ индекстер көптігі.

Немесе, мысалы, келесі түрлі функцияларымен:

$$Q_{ikj} = \prod_{i=1}^{I} \zeta_i^{\alpha_i}, \tag{3}$$

мұнда $\zeta_i^{\alpha_i} - Q_{ikj}$ көрсеткішіне $\left(EFA_{ijkl}, n_i\right)$ әсерін ескеретін функция.

Параметрлер барабарлық функционалын логарифмдеу арқылы өзгертілген ең кіші квадрат әдісімен анықталады.

Анықталған параметрлерді ескере отырып, осы деңгейдегі қорғаудың тиімділік дәрежесін анықтаймыз.

Екінші деңгейдегі - W_{jk} $k-$ші қауіпі үшін іске асырылатын $j-$ші әдіс ықтималдығының тәуелділігі қауіптен қорғалу дәрежесіне Q_{kj} байланысты. Бұл ретте келесі қағидатты қолданамыз: неғұрлым тиімді қорғау шарасы - АҚ үшін қауіптің іске асырылу ықтималдығы аз.

$W_{jk} = W_{jk}\left(Q_{kj}\right)$ тәуелділік оқу орнының ТЕЖ қауіпсіздік жүйесінің тиімділігін бағалауға мүмкіндік береді.

Оқу орнының ТЕЖ үшін ақпараттық сақтаудың бұзылу қаупінің көрсеткішін бағалайық. Бұл көрсеткіш R_{jkl} шамасымен анықталады, мұнда $l-$оқу орнының ТЕЖ компоненттер көптігінен:

$$R_{jkl} = 1 - \left[W_{jk}\left(Q_{kj}\right)\cdot\left(1 - Q_{kj}\right)\right]. \quad (4)$$

Келесі деңгейде оқу орнының ТЕЖ АҚ үшін жекелеген қатерді іске асырудың барлық әдістері мен тәсілдерінің тең (қорғалуын) қамтамасыз ету мақсаты қойылады. Яғни, АҚ-ны бұзу тәуекелі R_{jkl} ($k-$ші қауіп-қатерден) қорғауды жүзеге асырудың барлық тәсілдері арасында қорғаудың минималды сапасымен анықталады.

Әрі қарай, қауіп-қатерлердің баламасы және қауіп дәрежесі бойынша осы қауіптердің саралау шартында оқу орнының ТЕЖ жекелеген компоненттерін барлық қауіптерден қорғаудың тең сенімділігін қамтамасыз ету мақсаты қойылады. Қауіптерді саралау рангтік коэффициенттері Q_{kl} арқылы жасауға болады.

Бірінші жағдайда тәуекел келесі өрнекпен анықталады:

$$R_l = \max R_{kl}, \quad \forall k \in K_l, \quad (5)$$

мұнда $\{R_{kl}\}-$ оқу орындары желілерінің жұмыс істеу ерекшелігін ескере отырып, оқу орнының ТЕЖ қауіпті $l-$ші құрамдас бөлігі үшін көптеген қауіптер бойынша АҚ тәуекелінің көптеген көрсеткіштері.

Екінші жағдайда ТЕЖ АҚ үшін талданатын тәуекел келесі өрнек арқылы анықталады:

$$R_l = \max_{\{R_{kl}\}} R_{kl} Q_{kl}, \quad \forall k \in K_l. \quad (6)$$

Оқу орнының ТЕЖС қорғау жұмысының негізгі мақсаты - ТЕЖ компоненттерін барлық өзекті қауіптерден қорғаудың тең сенімділігін қамтамасыз ету. Бұны келесідей ұсынуға болады:

$$\{R_{kl} Q_l\}, \quad \forall l \in L, \quad (7)$$

мұндағы Q_l-оқу орнының ТЕЖ құрамында l компонентінің маңыздылық коэффициенті.

Нәтижелер және талқылау.

Оқу орнының ТЕЖ құрамында l компонентінің маңыздылығын бағалау - сараптамалық немесе эвристикалық. Мысалы, желілік экрандарды таңдау кезінде қорғау

жүйесін жобалау кезеңінде мұндай өнімдерге төмен бағаны уәде ететін жарнамалық акцияларға сенуден гөрі сарапшылардың пікіріне сүйенген дұрыс.

Оқу орнының ТЕЖ АҚ тәуекелді басқарудың тиімділігін EF келесідей бағалауға болады:

$$EF = \frac{100\left(R - \overline{R}\right)}{R}, \tag{8}$$

мұндағы $\overline{R}$ – тәуекел дәрежесі максимум бойынша (оқу орнының ТЕЖ үшін талданатын тәуекелдер жиынтығы бойынша).

ТЕЖ сегментінің қорғалу өлшемі қауіпсіздік сегментінің ақпараттық доменінің құрамдас бөліктерін ескеретін есептеу формулалары негізінде АҚ қауіптерінің көрсеткіші болуы мүмкін.

Мысалы, $\{R_{md}E_{md}\}$, $\forall m \in M$ көптігі бойынша $R_d = \max\left(R_{md}E_{md}\right)$, мұнда M – оқу орнының көптеген ТЕЖ сегменттері, соның ішінде ағымдағы деп саналатын d сегменті бар.

Сол сияқты бүкіл университет үшін жалпы қорғалғандық көрсеткіші анықталады:

$$R = \max\left(R_d F_d\right), \quad \forall d \in D, \tag{9}$$

мұнда D – қорғауға жататын жүйе объектілерінің саны; F_d – оқу орнының бизнес-процестері үшін объектіні қорғаудың маңыздылық дәрежесі.

Қосымша тапсырма мүмкін, мысалы, оқу орнының ТЕЖ қорғаудың белгілі бір компонентін қолданудың тиімділігін эксперименталды түрде анықтау. Мысалы, серверлік виртуалдандыру жүйесі негізінде IPS Suricata және SIEM Splunk пайдалану мүмкіндігі қарастыру. PVE басқаратын хосттарда IPS Suricata қауіп-қатерді анықтау жүйесі, Splunk платформасы және Pi-Hole DNS мекенжай сүзгісі орналастырылды. Бұл АҚ құралдары ақысыз немесе ақысыз нұсқалары бар, бірақ функционалдығы шектеулі.

АҚО АҚ (атап айтқанда, оқу орнының ТЕЖ) қамтамасыз етудің магистральдық мақсатына әртүрлі тәсілдермен қол жеткізуге болады. Мысалы, математикалық модельдеу әдістерін қолдана отырып, желіге орналастырылатын АҚҚ жиынтықтарын алдын-ала бағалауға болады. Бұл жағдайда, мысалы, белгілі бір АҚҚ – «баға-сапа» бағалаудың ең қол жетімді критерийіне сүйене отырып, АҚ-ны қамтамасыз ету міндеттерін қажетті деңгейде ең көп қамтуды қамтамасыз ететін АҚҚ-ны таңдауға болады. Осылайша, АҚ-ның ең маңызды қауіптері жойылады. Демек, математикалық модельдеуді қолдана отырып, ең қолайлы бағасымен АҚҚ-ның жиынтығын аналитикалық түрде қалыптастыруға болады. Бұл жағдайда сенімділік параметрлері жақшаның артында қалады деп болжаймыз. Бұл бөлек тапсырма және ол төменде талданады. Нәтижесінде, АҚ-ны қамтамасыз ету жобаларын талдаудың алғашқы кезеңінде математикалық модельдеу мүмкіндіктеріне жүгініп, АҚ-ны қажетті деңгейде қамтамасыз ету үшін аппараттық және бағдарламалық қамтамасыз етудің аздығымен есептеуге болады.

Университеттің ТЕЖ АҚ контурларын нарықта ұсынылған ақпаратты қорғаудың аппараттық-бағдарламалық құралдарының алуан түрлілігіне сүйене отырып қалыптастыруға болады. Айта кетейік, соңғы кездері ТЕЖ АҚ-ны қамтамасыз етуге арналған бағдарламалық құралдар, сондай-ақ ілеспе міндеттерді шешу үшін, мысалы, желінің жай-күйін бақылау және шабуылдарды анықтау үшін үлкен танымалдылыққа ие болды. Сонымен қатар, жоғарыда көрсетілгендей, бұл құралдардың бір бөлігі Open Sources санатына жатады. Мұндай бағдарламалық жасақтама ТЕЖ-дағы осалдықтардың санын, сондай-ақ ТЕЖ түйініне ұшырауы мүмкін АҚ қауіптерін азайтуға мүмкіндік

береді. Мамандандырылған бағдарламалық жасақтаманы пайдалану кезінде оқу орнының ТЕЖ архитектурасын өзгерту қажет емес. Тіпті дәстүрлі түрде кеңінен қолданылатын антивирустық бағдарламалық өнімдер, рұқсатсыз қол жеткізуден қорғау құралдарыы, IDS/IPS, SIEM, АҚО АҚ көрсеткіштерін айтарлықтай жақсартады.

Мамандандырылған бағдарламалық жасақтаманы қолдану ТЕЖ АҚ-ны қамтамасыз ету мәселесінде бірқатар мәселелерді шешсе де, сонымен бірге бұл бағдарламалық жасақтама ТЕЖ соңғы түйіндерінің өнімділігін төмендетеді. Бұл өз кезегінде жалпы ТЕЖ үшін ақауларға төзімділік деңгейінің төмендеуіне әкелуі мүмкін.

Сондықтан, егер қаржылық ресурстар мүмкіндік берсе, онда АҚО, мысалы, университет, арнайы есептеу серверлерін қолданған жөн. Мысалы, мұндай арнайы сервер көбінесе қашықтықтан оқыту жүйесін (ҚОЖ) құруға негіз болады. Немесе кейбір жағдайларда, мысалы, 6В061 Ақпараттық-коммуникациялық технологиялар; 6В062 Телекоммуникация; 6В063 Ақпараттық қауіпсіздік және т.б. сияқты мамандықтарды дайындау кезінде оқыту тиімділігін арттыру және практикалық сабақтарды ұйымдастыру үшін мамандандырылған полигондарды ұйымдастыру үшін пайдалануға болады.

Бұл жағдайда аталған мамандандырылған бағдарламалық жасақтама (IDS/IPS, SIEM, осалдық сканерлері, желіні бақылауға арналған бағдарламалық жасақтама және т.б.) тікелей серверге орнатылады. Сервер ішінара осындай бағдарламалық жасақтамамен жұмыс істеу кезінде өзіне жүктеме алады.

ТЕЖ АҚ бойынша бірқатар міндеттерді шешуге арналған бағдарламалық жасақтаманың ықтимал кемшіліктерін ескере отырып, көптеген ірі ТЕЖ жобалау кезеңінде бастапқыда аппараттық және бағдарламалық жасақтаманы қамтитын аралас шешімдерді қолдануды қарастырады. Мысалы, ірі ТЕЖ-да аппараттық брандмауэрлер өздерін жақсы дәлелдеді.

Бағдарламалық және аппараттық брандмауэрлердің артықшылықтары мен кемшіліктерін аздап салыстырмалы талдауы 1-кестеде жинақталған.

1 кесте - Бағдарламалық және аппараттық брандмауэрлердің артықшылықтары мен кемшіліктерін салыстырмалы талдау

Атауы	Артықшылықтары	Кемшіліктері
Бағдарламалық брандмауэрлер	1. Салыстырмалы түрде төмен бағасы. 2. Желі түйіндерін ішінен қорғау мүмкіндігі. 3. ТЕЖ сегменттерін икемді бөлу мүмкіндігі 4. Оларды қолданыстағы серверлерге орналастыру мүмкіндігі. 5. Кеңейтілген функционалдылық.	1. Орналастыру және теңшеу үшін жеткілікті жоғары біліктілік қажет. 2. Функционалдылық кеңейген сайын, мысалы, жүктемені теңестіру модульдерін қосқанда, IDS/IPS және сол сияқтылардың қосқанда бағасы күрт артады.
Аппараттық брандмауэрлер	1. Орналастыру және пайдалану оңай (салыстырмалы). 2. Төмен қуат тұтыну. 3. Жинақы. 4. Сенімділік.	1. Аппараттық брандмауэрлер ТЕЖ-дегі әрбір жеке жұмыс станциясын қорғауды қамтамасыз ете алмайды. 2. Аппараттық брандмауэрлер ТЕЖ ішіндегі шабуылдарда дәрменсіз. 3. Аппараттық брандмауэрлер дербес деректердің ақпараттық жүйелерінде саралауды орындай алмайды. 4. Әртүрлі өндірушілердің аппараттық брандмауэрлерін орнату кезінде тәжірибе қажет. 5. Аппараттық брандмауэр орналасқан бөлмені бөлек қорғау қажет.

Бағдарламалық және аппараттық брандмауэрлері жоғары шығындармен сипатталса да, оларды қолдану ТЕЖ соңғы түйіндеріндегі есептеу жүктемесін азайтуға көмектеседі. Нәтижесінде ол сенімді және ақауларға төзімді болады. Бұл, атап айтқанда, аппараттық брандмауэрлерді қолдану күрделі ТЕЖ-дің әр элементі арасында жүктеменің таралуына ықпал етеді. Осыған ұқсас тәсіл IDS/IPS сегментінде, қорғалған деректер қоймаларында (бұл әсіресе университеттің ҚОЖ үшін маңызды) біріктірілген аппараттық-бағдарламалық шешімдерді, және т. б. пайдаланған кезде де байқалады.

Көбінесе университеттің ТЕЖ түйіндерін қорғау ішкі құралдармен шектеледі. Мұндай ішкі құралдарға, мысалы, антивирустық бағдарлама, рұқсатсыз қол жеткізуден қорғау жүйесі, университеттің деректер қоймасын қорғау жүйесі жатады. Бұл ретте, әдетте, университеттік ТЕЖ-ға кіре берісте пакеттерді сүзетін брандмауэрлер орнатылған. Университет желілерінің жұмысын ұйымдастырудың бұл схемасы сыртқы желіден келетін АҚ қауіптерін жоюға байланысты жұмыстардың көп бөлігі соңғы түйіндерге түсетіндігіне әкеледі. Алайда, АЖ-ны ТЕЖ-дің маңызды түйіндерімен қамтамасыз ету қажет болған жағдайда, АҚЖ-ның минималды жиынтығымен ғана шектелу жеткіліксіз.

Қорытындылар.

Зерттеу барысында оқу орнының таратылған желісінің ақпараттық сақталу моделі толықтырылды, онда қолданыстағы модельдерден айырмашылығы, оқу орнының ТЕЖ үшін ақпараттық сақталудың бұзылу қаупінің көрсеткіштері зерттелді.

ӘДЕБИЕТТЕР

[1] Ахметов, Б., & Лахно, В. Защита информации и кибербезопасность цифровой образовательной среды университета / Вестник КазАТК, 2022, 120(1), с. 134-141.

[2] Ulven, J. High level information security risk in higher education / Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2020, pp. 1-6.

[3] Yilmaz, R.; Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. TEM J. 2016, 5, pp. 180–191.

[4] Adams, A.; Blanford, A. Security and Online Learning: To Protect and Prohibit / In Usability Evaluation of Online Learning Programs; IGI Global: Hershey, PA, USA, 2003; pp. 331–359.

[5] Schneider, F. BCybersecurity education in universities / IEEE Security & Privacy, 2013, 11(4), pp. 3-4.

[6] Muthuppalaniappan, M., & Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health / International Journal for Quality in Health Care, 2021, 33(1), mzaa117.

[7] Олейник, А. С., Якунина, Т. А., Тагирова, Э. И., Зыкова, А. В., & Щербаева, Л. А. Анализ внешних факторов, влияющих на кибербезопасность высшего военного учебного заведения / Управление образованием: теория и практика, 2022, (5 (51)), с. 221-230.

[8] Мулланурова А. Р., Ковтун Д. Б. Стратегии обеспечения кибербезопасности в высших учебных заведениях. – 2022. – С. 76.

[9] Alexei, L. A., & Alexei, A. Cyber security threat analysis in higher education institutions as a result of distance learning / International Journal of Scientific and Technology Research, 2021, (3), pp.128-133.

[10] Whitman, M. Management of Information Security; Cengage Learning, Inc.: Boston, MA, USA, 2018; ISBN 9780357691205.

[11] Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. Information security management frameworks and institution: a systematic review / Annals of Telecommunications, 2021, 76(3), pp. 255-270.

[12] Науразова, Э. А., & Шамилев, С. Р. Модель информационной безопасности в распределенных сетях. / Экономика. Бизнес. Информатика, 2016, 2(4), с. 27-37.

REFERENCES*

[1] Ahmetov, B., & Lahno, V. Zashhita informacii i kiberbezopasnost' cifrovoj obrazovatel'noj sredy universiteta / Vestnik KazATK, 2022, 120(1), s. 134-141.

[2] Ulven, J. High level information security risk in higher education / Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2020, rr. 1-6.

[3] Yilmaz, R.; Yalman, Y. A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. TEM J. 2016, 5, rr. 180–191.

[4] Adams, A.; Blanford, A. Security and Online Learning: To Protect and Prohibit / In Usability Evaluation of Online Learning Programs; IGI Global: Hershey, PA, USA, 2003; pp. 331–359.

[5] Schneider, F. BCybersecurity education in universities / IEEE Security & Privacy, 2013, 11(4), rr. 3-4.

[6] Muthuppalaniappan, M., & Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health / International Journal for Quality in Health Care, 2021, 33(1), mzaa117.

[7] Olejnik, A. S., Jakunina, T. A., Tagirova, Je. I., Zykova, A. V., & Shherbaeva, L. A. Analiz vneshnih faktorov, vlijajushhih na kiberbezopasnost' vysshego voennogo uchebnogo zavedenija / Upravlenie obrazovaniem: teorija i praktika, 2022, (5 (51)), s. 221-230.

[8] Mullanurova A. R., Kovtun D. B. Strategii obespechenija kiberbezopasnosti v vysshih uchebnyh zavedenijah. – 2022. – S. 76.

[9] Alexei, L. A., & Alexei, A. Cyber security threat analysis in higher education institutions as a result of distance learning / International Journal of Scientific and Technology Research, 2021, (3), rr.128-133.

[10] Whitman, M. Management of Information Security; Cengage Learning, Inc.: Boston, MA, USA, 2018; ISBN 9780357691205.

[11] Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. Information security management frameworks and institution: a systematic review / Annals of Telecommunications, 2021, 76(3), rr. 255-270.

[12] Naurazova, Je. A., & Shamilev, S. R. Model' informacionnoj bezopasnosti v raspredelennyh setjah. / Jekonomika. Biznes. Informatika, 2016, 2(4), s. 27-37.

Zhuldyz Alimseitova, PhD, associate professor, Satpayev University, senior lecturer, Almaty Technological University, Almaty, Kazakhstan, zhuldyz_al@mail.ru

Yerbolat Kalaman, master's degree, lecturer, Satpayev University, Almaty, Kazakhstan, politeh.kalaman@gmail.com

A MODEL OF INFORMATION SECURITY OF A DISTRIBUTED NETWORK OF AN EDUCATIONAL INSTITUTION

Abstract. Computing systems and networks of most modern information security facilities, including large universities of the Republic of Kazakhstan, integrate a large number of complex elements in their architecture. In turn, each of these elements can potentially become an

object of attack by computer attackers. And, accordingly, each of the elements that make up the architecture of a computer network is exposed to a sufficiently large number of cybernetic threats. In order to reduce the impact of these threats on the information security of the computer network, and in some cases to prevent the damage caused, a variety of information security tools are integrated into the network architecture. In the course of the study, the information security model of the distributed network of an educational institution was supplemented, in which, unlike existing models, the risk indicators of information security violations for the distributed computing network of an educational institution were taken into account.

Keywords. information security, computer network, university, safety of information.

Жулдыз Алимсеитова, PhD, ассоциированный профессор, Satpayev University, сениор-лектор, Алматинский технологический университет, Алматы, Казахстан, zhuldyz_al@mail.ru

Ерболат Каламан, магистр, преподаватель, Satpayev University, Алматы, Казахстан, politeh.kalaman@gmail.com

МОДЕЛЬ ИНФОРМАЦИОННОЙ СОХРАННОСТИ РАСПРЕДЕЛЕННОЙ СЕТИ УЧЕБНОГО ЗАВЕДЕНИЯ

Аннотация. Вычислительные системы и сети большинства современных объектов информационной безопасности, в том числе крупных университетов Республики Казахстан, интегрируют в своей архитектуре большое количество сложных элементов. В свою очередь, каждый из таких элементов потенциально может стать объектом атаки со стороны компьютерных злоумышленников. И, соответственно, каждый элементов, составляющих архитектуру вычислительной сети подвергается достаточно большому числу кибернетических угроз. Чтобы снизить влияние этих угроз на информационную безопасность вычислительной сети, а в некоторых случаях предотвратить наносимый ущерб, в архитектуру сети интегрируют разнообразные средства защиты информации. В ходе исследования была дополнена модель информационной сохранности распределенной сети учебного заведения, в которой в отличие от существующих моделей, учтены показатели риска нарушения информационной сохранности для распределенной вычислительной сети учебного заведения.

Ключевые слова. Информационная безопасность, вычислительная сеть, университет, сохранность информации.

****