ҒТАХР 44.29.01

10.51889/2959-5894.2024.86.2.018

Е.Т. Каламан[1*], Ж.К. Алимсеитова[1], Қ.Ж.Сабраев[2]

[1]Сатпаев университеті, Алматы қ., Қазақстан
[2]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан
[*]*e-mail: politeh.kalaman@gmail.com*

УНИВЕРСИТЕТТІҢ ЕСЕПТЕУ ЖЕЛІСІНІҢ ОСАЛДЫҚ КӨРСЕТКІШТЕРІН МОДЕЛЬДЕУГЕ НЕГІЗДЕЛГЕН АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕСІ

Аңдатпа

Ақпараттандыру объектісінің таратылған есептеу желісі үшін ақпараттық қауіпсіздік жүйесін қалыптастыру әдістемесі ұсынылды. Әдістеменің бірінші кезеңінде математикалық модельдеуді қолдану ұсынылады. Атап айтқанда, осалдық коэффициентін есептеу үшін ықтималдық теориясы аппаратын пайдалану негізінде математикалық модель көрсетілген. Бұл коэффициент ақпараттану объектісі желісінің ақпараттық қауіпсіздік деңгейін бағалауға мүмкіндік береді. Ақпараттық қауіпсіздік үшін тәуекелдердің рұқсат етілген және сыни деңгейін бағалау критерийлері де ұсынылған. Әрі қарай, таратылған есептеу желісінің ақпараттық қауіпсіздігі жүйесін қалыптастыру әдістемесінің екінші кезеңінде таратылған есептеу желісінің ақпараттық қауіпсіздігі компоненттерін имитациялық модельдеу және виртуалдандыру әдістері қолданылады. Эксперименттік зерттеулер барысында қорғалған таратылған есептеу желісінің моделі жасалды. Эксперименттік модельде желілік құрылғылар мен таратылған есептеу желісінің ақпараттық қауіпсіздігі компоненттері виртуалды машиналарда эмуляцияланды. Таратылған есептеу желісінің ресурстары Proxmox VE виртуализация жүйесі арқылы ойнатылды. PVE басқаратын таратылған есептеу желісі хосттарында IPS Suricata орналастырылды. SIEM ретінде Splunk жүйесі қолданылды. Таратылған есептеу желісі үшін ақпараттық қауіпсіздік жүйесін қалыптастырудың ұсынылған әдістемесі және осалдық коэффициентінің моделі ақпараттану объекті таратылған есептеу желісінің осалдық деңгейлерінің сандық бағасын алуға мүмкіндік бергені көрсетілген.

Түйін сөздер: ақпараттық қауіпсіздік, ақпараттандыру объектісі, таратылған есептеу желісі, математикалық модель, осалдық коэффициенті, виртуализация, IDS, SIEM.

Е.Т. Каламан[1], Ж.К. Алимсеитова[1], К.Ж. Сабраев[2]
[1]Сатпаев университет, г. Алматы, Казахстан
[2]Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан

СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МОДЕЛИРОВАНИЯ ПОКАЗАТЕЛЕЙ УЯЗВИМОСТИ УНИВЕРСИТЕТСКОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Аннотация

Предложена методика формирования системы информационной безопасности для распределенной вычислительной сети объекта информатизации. На первом этапе методики предлагается использовать математическое моделирование. В частности, изложена математическая модель на основе задействования аппарата теории вероятностей для расчета коэффициента уязвимости. Данный коэффициент позволяет оценить уровень информационной безопасности сети объекта информатизации. Также предложены критерии для оценивания допустимого и критического уровня рисков для информационной безопасности. Далее на втором этапе методики формирования системы информационной безопасности распределенной вычислительной сети используются методы имитационного моделирования и виртуализации компонентов информационной безопасности распределенной вычислительной сети. В ходе экспериментальных исследований была построена модель защищенной распределенной вычислительной сети. В экспериментальной модели сетевые устройства и компоненты информационной безопасности распределенной вычислительной сети были эмулированы на виртуальных машинах. Ресурсы распределенной вычислительной сети были воспроизведены с помощью системы виртуализации Proxmox VE. На хостах распределенной вычислительной сети под управлением PVE была развернута IPS Suricata. В качестве SIEM

использовалась система Splunk. Показано, что предложенная методика формирования системы информационной безопасности для распределенной вычислительной сети и модель коэффициента уязвимости позволили получить количественную оценку уровней уязвимости распределенной вычислительной сети объекта информатизации.

Ключевые слова: информационная безопасность, объект информатизации, распределенная вычислительная сеть, математическая модель, коэффициент уязвимости, виртуализация, IDS, SIEM.

E.T. Kalkaman[1], Zh.K. Alimseitova[1], K.J. Sabrayev[2]
[1]Satpayev University, Almaty, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

FORMATION SECURITY SYSTEM BASED ON MODELING OF VULNERABILITY INDICATORS OF THE UNIVERSITY COMPUTER NETWORK

Abstract

A method of forming an information security system for a distributed computer network of an informatization object is proposed. At the first stage of the methodology, it is proposed to use mathematical modeling. In particular, a mathematical model is presented based on the use of the apparatus of probability theory to calculate the vulnerability coefficient. This coefficient allows us to assess the level of information security of the network of the informatization object. Criteria for assessing the acceptable and critical level of risks for information security are also proposed. Further, at the second stage of the methodology for the formation of an information security system of a distributed computer network, methods of simulation modeling and virtualization of information security components of a distributed computer network are used. In the course of experimental research, a model of a secure distributed computing network was built. In the experimental model, network devices and information security components of a distributed computing network were emulated on virtual machines. The resources of the distributed computing network were reproduced using the Proxmox VE virtualization system. IPS Suricata was deployed on the hosts of a distributed computing network under PVE management. The Splunk system was used as a SIEM. It is shown that the proposed methodology for the formation of an information security system for a distributed computer network and the vulnerability coefficient model made it possible to obtain a quantitative assessment of the vulnerability levels of a distributed computer network of an informatization object.

Keywords: information security, informatization object, distributed computing network, mathematical model, vulnerability coefficient, virtualization, IDS, SIEM.

Негізгі ережелер

Мақаланың мақсаты таратылған есептеу желісі осалдық көрсеткіштерін модельдеу негізінде ақпаратты қорғау жүйесін қалыптастыру әдістемесін, сондай-ақ ақпараттандыру объекті желісінің осалдық коэффициентін сипаттайтын модельді дамыту. Мақсатқа жету үшін осалдық коэффициентін есептеу үшін ықтималдық теориясы аппаратын пайдалану негізінде математикалық модель жасалған, ақпараттық қауіпсіздік үшін тәуекелдердің рұқсат етілген және сыни деңгейін бағалау критерийлері ұсынылған. Эксперименттік зерттеулер барысында қорғалған таратылған есептеу желісінің моделі жасалды. Таратылған есептеу желісі үшін ақпараттық қауіпсіздік жүйесін қалыптастырудың ұсынылған әдістемесі және осалдық коэффициентінің моделі ақпараттану объекті таратылған есептеу желісінің осалдық деңгейлерінің сандық бағасын алуға мүмкіндік бергені көрсетілген.

Кіріспе

Компаниялардың (бұдан әрі ақпараттандыру объектілері немесе АОБ) ақпараттық қауіпсіздігіне (бұдан әрі АҚ) қауіп-қатерлердің ландшафты үздіксіз өзгеріп отыратын жағдайында, сондай-ақ компьютерлік зиянкестердің тактикасы мен стратегиясын жетілдіруге қарай АҚ жөніндегі мамандар көбінесе ақпаратты қорғау жүйелері (бұдан әрі АҚЖ) жұмысының тиімділігі мен сенімділігіне сүйенеді. Мұндай АҚЖ-ның негізгі міндеті ақпараттық жүйелерден (бұдан әрі АЖ) тыс ақпараттың (көбінесе құпия) ағып кетуіне жол бермеу болып табылады. Бірқатар зерттеулерде көрсетілгендей [1], ақпараттың ағып кетуіне

байланысты АҚ оқиғаларының көпшілігі қызметкерлердің қателіктеріне байланысты [2]. Ағып кетудің шамамен 25%-ы ғана хакерлердің [3], инсайдерлердің әрекеттерінен немесе АЖ пайдаланушыларының жаман ниетінен туындайды.

Инсайдерлер де, сыртқы құқық бұзушылар да ақпараттық қауіпсіздік құралдарын (немесе ақпаратты қорғау жүйесін - АҚЖ) жеңуге тырысатыны түсінікті. Бұл әсіресе мақсатты шабуылдар кезінде маңызды. Шабуылшы жақ пен қорғау жағының мұндай қарсыласуының нәтижесі көптеген факторларға байланысты. Нәтижесінде ақпараттандыру объектісінің АҚ жүйесі (бұдан әрі АҚЖ) қаншалықты мінсіз болса да, қорғаудың сәттілігіне алдын-ала кепілдік беру мүмкін емес.

Шабуылдардың саны да [4], шабуылдардың күрделілігі де [5], күрделене түскен сайын қазіргі заманғы көп тізбекті АҚЖ басқа мәселелерді де шешуге арналғанын айта кету керек [6]. Мұндай қосалқы міндеттерге мыналар жатқызылуы мүмкін: АЖ ішінде де, сыртқа да қажетсіз жіберу жағдайларының алдын алу; персонал АЖ ресурстарын өздерінің жеке мақсаттары үшін пайдаланатын жағдайларға жол бермеу; АОБ және/немесе оның АЖ таратылған есептеу желісінде трафикті мониторингтеу және деректерді жіберу арналарының жүктемесін оңтайландыру; персонал немесе бөгде адамдар қажетсіз ақпаратты жіберуге тырысатын жағдайларға жол бермеу (мысалы, спам немесе ақпараттың шамадан тыс көлемі); жіберілетін хабарламаларды архивтеу, бұл, мысалы, АҚ бойынша оқиғаны тереңірек талдау қажет болған жағдайда керек; персоналдың жұмыс орындарында болуын бақылау [7].

Егер АҚ-ті сыртқы бұзушылардан қорғау туралы айтатын болсақ, онда шабуылдарды анықтау жүйелері бүгінде көптеген компаниялар мен ұйымдардың таратылған есептеу желісі (ТЕЖ) АҚ контурларының ажырамас бөлігі болды. Бұл ретте, басып кіруді анықтау жүйелері (IDS) және басып кіруді болдырмау жүйелері (IPS) немесе біріктірілген IDS/IPS шешімдері қолданылады. Соңғы жағдайда бағдарламалық-аппараттық жасақтама болып табылатын IDS/IPS жүйелері желіні рұқсатсыз кіруден қорғауға қызмет етеді.

АОБ желісінің АҚ қамтамасыз етудің жүйелік тәсілін іске асыру үшін қорғау тарапына ақпаратты қорғаудың техникалық құралдарының арсеналын ғана қолдану жеткіліксіз. Мұндай АҚЖ жүйесін жобалау кезеңінде ғылыми әдістерді қолдану қажет. Мұндай ғылыми әдістерге, мысалы, белгілі бір АОБ үшін АҚ жүйелері мен процестерін математикалық немесе имитациялық модельдеу жатады. Мұндай модельдеудің басым мақсаты АОБ АҚ жүйесін басқаруға байланысты оңтайлы шешімдерді табу болып табылады. Сонымен қатар, әдетте, қосымша міндеттер туындайды, мысалы, жоғарыда аталған IDS/IPS сияқты белгілі бір АҚ механизмдерін қолдану тиімділігін бағалауға байланысты. Белгілі бір АОБ үшін АҚЖ модельдеудің бүкіл процесін шартты түрде екі компонентке бөлуге болады:

- модельдерді құру, мысалы, математикалық, физикалық немесе имитациялық;
- АҚЖ қажетті сипаттамаларын алу мақсатында модельдерді іске асыру.

Жоғарыда айтылғандардың барлығы зерттеу тақырыбының өзектілігін анықтады. Атап айтқанда, АОБ осалдық көрсеткіштерін математикалық және имитациялық модельдеу негізінде ТЕЖ АҚ жүйесін қалыптастыру әдістемесін дамыту.

Әдебиеттерге шолу

Белгілі бір АОБ үшін АҚ жүйесін құру туралы сөз болғанда, әдетте қорғау жағы екі мүмкін жағдайдың біріне тап болады.

Бірінші жағдайда АОБ үшін "нөлден" АҚ жүйесін құру керек. Шын мәнінде, АҚ жүйесі қорғау объектісінде бар шешімдерге сүйенбей және АОБ АҚ қамтамасыз етудің кешенді тәсілінің маңыздылығын түсінбей әзірленеді. Екінші жағдайда, АОБ-де АҚ кейбір құралдары бар. Ал қорғау жағында оның тиімділігін арттыру міндеті тұр. Мысалы, бұған АҚЖ құрамын оңтайландыру арқылы қол жеткізуге болады. Немесе қолда бар құралдарды АОБ-дағы ең құнды ақпараттық активтерді қорғау үшін қайта бөлу. Екінші нұсқа әлдеқайда жиі кездеседі [8]. Кибернетикалық шабуылдар туралы көңіл көншітпейтін статистикаға қарамастан [9] көбінесе АОБ менеджменті АҚ мәселелеріне тиісті назар аудармайды [10], егер

ол өзінің ақпараттық активтерін әлсіз қорғаудан немесе оның болмауынан туындаған мәселелерге тап болмаса [11].

Алайда, егер АОБ басшылары АҚ-дың дұрыс емес жағдайынан туындаған нақты мәселелерге тап болса [12], олар АҚ-ға үлкен қаржылық инвестиция салуға дайын. Мұндай жағдайлардың қайталануына жол бермеу басымдыққа ие болады [13].

[14] көрсетілгендей, АОБ АҚ-дың берілген деңгейіне жету өзара байланысты міндеттер кешенін сәтті шешуге байланысты. Мұндай міндеттерге, мысалы, мыналар кіруі мүмкін: АҚЖ әзірлеу және енгізу кезінде шешілетін техникалық-технологиялық, қаржылық, ұйымдастырушылық және басқа міндеттер.

Осылайша, жоғарыда айтылғандарға сүйене отырып, қазіргі АОБ-дің көпшілігінің ажырамас бөлігі ретінде ТЕЖ осалдық көрсеткіштерін модельдеу негізінде АҚ жүйесін қалыптастыру әдістемесін дамыту міндеті өзекті болып қала береді деп айтуға болады.

Зерттеу әдіснамасы

ТЕЖ осалдық көрсеткіштерін модельдеу негізінде АҚ жүйесін қалыптастыру әдістемесін, сондай-ақ АОБ желісінің осалдық коэффициентін сипаттайтын модельді дамыту.

Зерттеу нәтижелері

АОБ үшін белгілі бір АҚ жүйелерін таңдау мәселесін шешу үшін АҚ қауіптерінің пайда болуының бірыңғай динамикалық коэффициентін қарастыру қажет [15]. Бұл коэффициент $P^{DT} \in [0;1]$ АҚ қауіптерінің динамикасын ескеруге мүмкіндік береді, мысалы, АОБ ТЕЖ үшін, сондай-ақ ТЕЖ үшін қауіптердің ықтималдығын модельдеу.

Әдетте, белгілі бір уақыт аралығында жұмыс істейтін әрбір ұйымда немесе компанияда АҚ инциденттері бойынша белгілі бір статистика бар. Демек, қауіптерді іске асырудың статистикалық ықтималдығы туралы айтуға болады $P_{stat} \in [0;1]$. Сондай-ақ, АОБ ТЕЖ үшін қауіп-қатерлерді сараптамалық бағалауға сенуге болады $P_{\text{expert}} \in [0;1]$.

[15] ТЕЖ үшін АҚ қауіптерінің динамикалық компонентін ($DC \in [0;1]$) қарастыру ұсынылады:

$$DC = \begin{cases} P_{stat}^{n-1} > P_{stat}^{n}, & \left(\dfrac{P_{stat}^{n-1} - P_{stat}^{n}}{P_{stat}^{n}} \right); \\ P_{stat}^{n-1} \le P_{stat}^{n}, & \left(-\dfrac{P_{stat}^{n-1} - P_{stat}^{n}}{P_{stat}^{n}} \right), \end{cases} \quad (1)$$

мұнда $n-$ АҚ қауіптері туралы статистика, мысалы, АОБ ТЕЖ үшін. Деректер, мысалы, SIEM көмегімен АҚ оқиғаларын бақылау нәтижесінде немесе IPS/IDS жұмыс деректері негізінде қабылданады.

Әрі қарай, АОБ ТЕЖ қорғау элементтерін анықтаймыз. Бұл кезеңде, мысалы, сарапшының көмегімен ТЕЖ үшін осалдықтар мен қауіптердің гистограммалары жасалады.

Қауіп іске асырылған жағдайларда қорғау тарапы төтенше жағдайға тап болады. Мұндай жағдай қауіптерді жүзеге асырудың барлық ықтимал салдарын қарастыруды талап етеді. Мысалы, бұл АОБ үшін моральдық, материалдық, ақпараттық шығындарға және т.б. байланысты.

Қауіптерді іске асыру ықтималдығының максималды мәнін $P_{\max}^{DT}$ және минималды мәнін $P_{\min}^{DT}$ деп қабылдаймыз. Мұны осылай түсіндіруге болады:

- егер $P_n^{DT} > P_{\max}^{DT}$, онда бұл қауіп P_n^{DT}, мысалы, АОБ ТЕЖ үшін тереңірек талдау үшін қабылданады. Оған автоматты түрде жоғары басымдық беріледі және оның алдын алу шаралары қабылданады;

- егер $P_{\min}^{DT} > P_n^{DT} > P_{\max}^{DT}$, онда бұл қауіп P_n^{DT} орташа басымдыққа ие болады;

- егер $P_n^{DT} > P_{\min}^{DT}$, онда бұл қауіп P_n^{DT} төмен басымдықпен сипатталады.

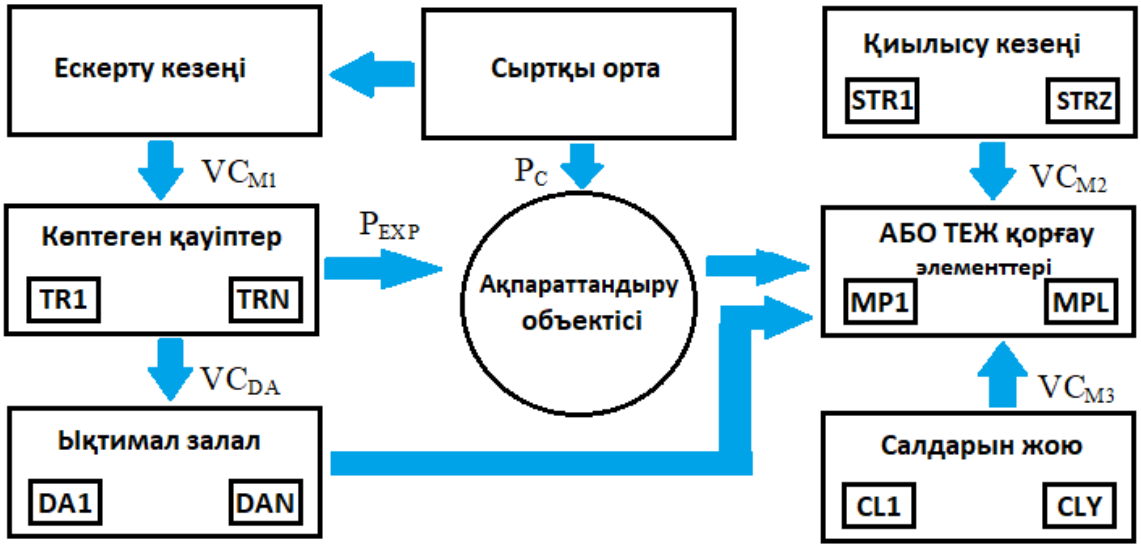
Демек, бірінші кезеңде АОБ АҚ бөлімінің қызметкерлеріне қауіптерді талдау және бағалау, мысалы, ТЕЖ үшін АҚЖ бар құрамымен қауіптерді сүзуді жүзеге асыруға мүмкіндік береді.

Әрі қарай, ТЕЖ осалдық коэффициентін қарастырамыз.

Осалдық деп ТЕЖ қорғау элементінің, мысалы, брандмауэрдің қауіп-қатерге ұшырау қасиеті түсініледі. Яғни, осы АҚЖ-ға тұрақсыздандырушы факторлар әсер етуі мүмкін. Брандмауэрге әсер ететін қарапайым тұрақсыздандырғыш факторлар ретінде бөлек қарастыруға болады:

- ТЕЖ АОБ-ге сенімсіз қосымшаға қол жеткізу;
- RAW Socket қолданумен ТЕЖ АОБ-ге қол жеткізу;
- АОБ ТЕЖ сенімді процестеріне бөгде DLL енгізу;
- ТЕЖ АОБ-дің сенімді процестерінде трояндық ағындарды құру;
- сенімді процестердің машиналық кодын өзгерту;
- сенімсіз процесті жасыру;
- және т. б.

АОБ ТЕЖ осалдық коэффициентін қазіргі уақыттағы АҚ деңгейін сандық бағалау ретінде түсіндіруге болады. Сонымен қатар, мұндай бағалау ТЕЖ және жалпы АОБ жұмысының нақты жағдайларымен байланысты. ТЕЖ осалдық коэффициентін (немесе жалпы АОБ) қалыптастыру тәсілі сурет 1-де көрсетілген.



Сурет 1. Университет желісінің осалдық коэффициентін қалыптастыру тәсілі

Сонда ТЕЖ осалдық коэффициентінің мәнін (VC), [15] жұмыс нәтижелерін ескере отырып осылай көрсетіміз:

$$VC = \sum_{i=1}^{N} VC_i \cdot \frac{\sum_{j}^{M} DC_{ij}}{\max \sum_{j}^{M} DC_{ij}}, \qquad (2)$$

мұндағы VC_i – ТЕЖ АҚ үшін i – ші қауіп төнген кезде осалдық коэффициентінің мәні; DC_{ij} – АҚ үшін i – ші қауіп төнген кезде ТЕЖ j – ші компоненті (мысалы, АҚ құралдары) үшін зиян коэффициентінің мәні; N – ТЕЖ АҚ үшін қауіптер саны; M – ТЕЖ элементтерінің саны, оның ішінде АҚЖ.

Қауіптерді жою үшін әдетте ұйымдастырушылық шаралар жеткіліксіз. Тиімді қорғау, әдетте, ақпаратты қорғаудың техникалық құралдарын сатып алуға, персоналды оқытуға, жоғары білікті мамандарды тартуға және т. б. қаржылық инвестицияларды қажет етеді.

АҚЖ санын, олардың АҚ интегралды метрикаларына негізделген техникалық параметрлерін таңдау мәселесін шешу үшін АОБ ТЕЖ үшін мақсатты функция ретінде жылдық келтірілген шығындар қабылданды:

$$C = p \cdot \sum_{i=1}^{n} CE_i + \sum_{i=1}^{m} OC_i, \tag{3}$$

мұнда p – талданатын АОБ үшін ТЕЖ АҚ-ға күрделі салымдардың салыстырмалы тиімділігін сипаттайтын коэффициент, CE_i, OC_i – сәйкесінше ТЕЖ АҚ-ға күрделі және пайдалану шығындарының і-ші бабы; n, m – сәйкесінше ТЕЖ АҚ-ға күрделі және пайдалану шығындарының құрамдас бөліктерінің саны.

Модельді жеңілдету үшін ТЕЖ АҚ үшін жылдық келтірілген шығындар бұл ТЕЖ АҚ жүйесіне инвестициялау тиімділігін бағалаудың негізгі критерийі болып табылады. Мұндай жеңілдету модельдің жалпы жұмыс өнімділігін көрсетуге мүмкіндік береді. Мақсатты функцияның (МФ) есептеу формуласының қарапайымдылығы ТЕЖ үшін оңтайлы АҚЖ құрамын анықтау мәселесін шешу үшін модельдің сәйкестігіне нәтижелерді талдауды жеңілдетуге мүмкіндік береді.

ТЕЖ АҚ үшін нақты АҚЖ (қауіптердің нақты класы шеңберінде, мысалы, брандмауэр, IPS/IDS, SIEM және т. б.) сатып алуға арналған шығындарды келесі функциясымен ұсынылсын:

$$CE_{1u} = a_1 + a_2 \cdot IPI, \tag{4}$$

мұнда IPI – белгілі бір кластағы АҚЖ тиімділігінің интегралды көрсеткіші (мысалы, брандмауэр, IPS/IDS, SIEM және т.б.); a_1, a_2 – сызықтық жуықтауға арналған коэффициенттер.

Сол сияқты, ТЕЖ үшін басқа АҚЖ сыныптарын сатып алуға, монтаждауға, қосылуға, мысалы, АОБ ақпараттық жүйесіне, байланысты күрделі шығындарды білдіруге болады (мысалы, қол жеткізуді басқару құралдары),

Пайдалану шығындары мен шектеулерді ұқсас тәсілді ұстанумен білдіруге болады, [16, 17] жұмыстарда көрсетілгендей жуықтауға арналған өрнектер міндетті түрде сызықтық емес.

Ұсынылған әдістемеде ТЕЖ (немесе АОБ) үшін АҚ жүйесінің сипаттамасын егжей-тегжейлі көрсету үшін қажет болатын көптеген негізгі жеке критерийлерді CR енгіземіз:

$$CR = \{CR_1, CR_2, CR_3, CR_4, CR_5\}, \tag{5}$$

мұнда CR_1 – белгілі бір сыныпқа жататын АҚЖ құны; CR_2 – тиісті АҚЖ-мен жабылатын АОБ АҚ үшін қауіптер кластарының саны; CR_3 – ТЕЖ үшін АҚЖ-ның бір немесе басқа сыныбының арқасында азаятын нивелирленген тәуекел мөлшері; CR_4 – тиісті АҚЖ үшін АҚ

сертификаттарының болуы; CR_5 – жалпы қорғау кешеніндегі және АОБ АҚ-дағы жеке АҚЖ үйлесімділік көрсеткіші.

Жоғарыда көрсетілген жеке критерийлерінің әрқайсысы 0-ден 1-ге дейін диапазонда өзгеруі мүмкін. Мысалы, CR_5 үшін, егер белгілі бір АҚЖ қорғалған ТЕЖ түйінінде орналасқан құралдар тобындағы басқалармен үйлесімді болса, онда $CR_5 = 1$ мәні (керісінше $CR_5 = 0$). Критерий CR_1, үшін түсіндіру келесідей болуы мүмкін:

$$CR_1 = \begin{cases} 1, \quad if \quad C_{ist} < C_{ist}^{\max}; \\ 0{,}5 \quad if \quad 0{,}5 \cdot C_{ist}^{\max} \le C_{ist} \le C_{ist}^{\max}; \\ 0 \quad if \quad C_{ist} > C_{ist}^{\max}, \end{cases} \tag{6}$$

мұнда $C_{ist}, C_{ist}^{\max}$ – талданатын класс шеңберіндегі АҚЖ-ның орташа құны (мысалы, брандмауэр, қол жеткізуді шектеу құралдары, басып кіруді анықтау жүйелері және т.б.) және максималды құны. Критерий CR_2, үшін түсіндіру келесідей болуы мүмкін:

$$CR_2 = \begin{cases} 1, \quad if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = |IST|; \\ 0{,}5 \quad if \quad 0{,}5 \cdot |IST| \le \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le |IST|; \\ 0{,}25 \quad if \quad 0 < \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot |IST|; \\ 0 \quad if \quad \sum_{i=1}^{n} m_{ISR_{ii}}^{ist_k} = 0, \end{cases} \tag{7}$$

мұнда IST – ТЕЖ АҚ үшін қауіптер көптігі (шамасы тұрақты емес және сыртқы факторларға тәуелді); n – нақты ТЕЖ үшін өзекті қауіптер саны; $m_{ISR_{ii}}^{ist_k}$ – қолданыстағы және жоспарланған қорғау құралдары мен ТЕЖ АҚ-мен өзекті кибернетикалық қауіптердің қабаттасу матрицасы. Критерий CR_3, үшін түсіндіру келесідей болуы мүмкін [16]:

$$CR_3 = \begin{cases} 1, \quad if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} < R_a; \\ 0{,}5 \quad if \quad R_a \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le 0{,}5 \cdot R_{cr}; \\ 0{,}25 \quad if \quad 0{,}5 \cdot R_{cr} \le \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \le R_{cr}; \\ 0 \quad if \quad \sum_{i=1}^{n} R_{ISR} \cdot m_{ISR_{ii}}^{ist_k} \ge R_{cr}, \end{cases} \tag{8}$$

мұнда, R_a, R_{cr} – тиісінше, АОБ ТЕЖ үшін АҚ тәуекелінің рұқсат етілген және сыни деңгейлері; n – нақты ТЕЖ үшін өзекті қауіптер саны; $m_{ISR_{ii}}^{ist_k}$ – қолданыстағы және жоспарланған АҚЖ мен АҚ үшін өзекті қауіптердің қабаттасу матрицасы.

Жеке критерийлерге арналған ұқсас есептеулер ғылыми әдебиеттерде бірнеше рет сипатталған, мысалы, [10], [12].

Сонда ұсынылған жеке критерийлерді қолдана отырып, ТЕЖ үшін бүкіл АҚ жүйесінің тиімділігін (EF) векторымен ұсынуға болады:

$$EF = \{1, 1, 1, 1, 1\}. \tag{9}$$

Шын мәнінде, бұл формада ТЕЖ үшін АҚЖ тиімділігін бағалау үшін қолданылатын анықтамалық жеке критерийлерді алуға болады.

Сонда жоғарыда айтылғандарды ескере отырып ТЕЖ осалдық коэффициентін келесідей көрсетуге болады:

$$VC = \sum_{j=1}^{M} \frac{EF\left\lfloor P_{\text{expert (i)}} \cdot \left(P_{stat\,(\text{i})} + DC_i\right)\right\rfloor}{\sum_{j}^{M} \alpha_{ij} \cdot CEF_{ij}}, \tag{10}$$

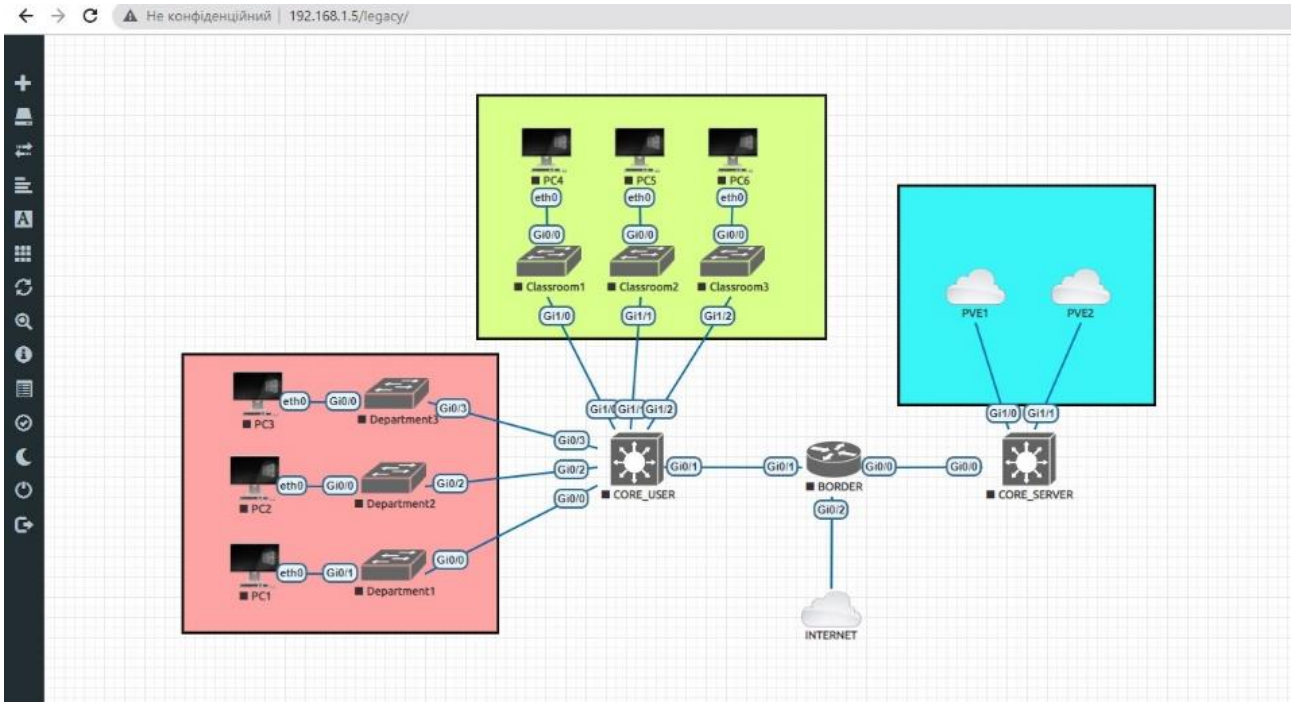
мұндағы α_{ij} – ТЕЖ АҚ-ға төнетін i – ші қауіпті бұғаттаудың тиісті кезеңдерінде ТЕЖ АҚ-ның j – ші құралының әсер ету дәрежесін сипаттайтын салмақ коэффициенттерінің мәндері; CEF_{ij} – ТЕЖ АҚ-ға төнетін i – ші қауіпті бұғаттаудың тиісті кезеңдерінде ТЕЖ АҚ-ның j – ші құралының (мысалы, брандмауэр, IPS/IDS, SIEM және т.б.) тиімділігін сипаттайтын салмақ коэффициенттерінің мәндері.

АОБ АҚ жүйесін қалыптастырудың ұсынылған әдістемесінің тиімділігін эксперименттік тексеру үшін шартты АОБ виртуалды желісі жобаланды. Windows 10 ОЖ басқаратын компьютерде орнатылған VmWare Workstation платформасы қолданылды. Компьютердің өзі Intel Xeon E5 1650 серверлік процессорына негізделген және 32 Гб жедел жады орнатылған, бұл виртуалды машиналарды (ВМ) құру және жүйелерді модельдеу операциялары үшін жеткілікті.

Барлығы 3 виртуалды машина жасалды, оның ішінде 2-і Proxmox VE ОЖ-мен басқарылады, оған басқа ВМ-ды орналастыру үшін гипервизор ретінде әрекет етеді. Үшінші ВМ-да Ubuntu Server операциялық жүйесі орнатылды. Сондай-ақ, бұл ВМ-да EVE-NG желілерін модельдеуге арналған қосымша орнатылды.

Инфрақұрылымды ыңғайлы басқару үшін кластерлік шешімдер қолданылды. Бұл бірнеше серверлерді бір жүйеге біріктіруге мүмкіндік берді, бұл ресурстарды резервтеу мен орталықтандырылған басқаруды қамтамасыз етті. Proxmox VE бұл мүмкіндікті қолдайтындықтан, 2 серверді бір кластерге біріктіру туралы шешім қабылданды. Кластер құрылғаннан кейін кез-келген хосттың мекен-жайына өтіп, екі сервер және олардың барлық ресурстары (ВМ, контейнерлер, қоймалар және т.б.) туралы ақпаратты көруге болады. Кластерді құру көптеген артықшылықтар берді. Олардың бірі серверлердегі ВМ-ны кластердің басқа түйіндеріне көшіру мүмкіндігі болды, сурет 2-ні қараңыз.

Жоғарыда айтылғандай, желілік құрылғыларда АОБ желісінің моделін құру үшін EVE-NG қосымшасы қолданылды. 1 маршрутизатор (және брандмауэр рөлін атқарады) және 2 ядро коммутаторы қосылды. Біріншісі сервер сегментіне, екіншісі пайдаланушы сегментіне жауап береді. Сондай-ақ, пайдаланушы сегментіне жауап беретін ядро коммутаторына қосылған қол жеткізу коммутаторлары қосылды.



Сурет 2. АОБ желісінің диаграммасы

Тиісінше, осы 2 сегменттегі пайдаланушыларға қол жеткізу саясаты әр түрлі деп қабылданды – менеджментінің коммутаторлары арқылы қосылған пайдаланушыларда АОБ серверлерінде орналасқан жергілікті ресурстарға қол жеткізу құқықтары көбірек болады, 2 суретті қараңыз. Барлық құрылғылар VmWare виртуалды интерфейстеріне қосылады. VmWare интерфейстері өз кезегінде дербес компьютердің желілік интерфейсіне қосылған. Компьютердің өзі провайдердің желісіне қосылған маршрутизаторға қосылған.

АОБ АҚ кешенді жүйесін қалыптастыру әдістемесін зерттеу аясында АОБ желісінің параметрлерін сыртқы шабуылдарға қорғалған етіп өзгерту туралы шешім таңдалды. Ядро коммутаторларын және олардың өздері мен маршрутизатор арасындағы байланыстарын резервтеу туралы шешім қабылданды. Ол үшін серверлерден және пайдаланушылардың қол жеткізу коммутаторларынан екі ядро коммутаторларына да байланыс жасау керек. Бүгінгі күні қол жеткізу коммутаторларының көпшілігінде бұл үшін 2-4 жоғары порттар бар, сондай-ақ серверлерде кем дегенде 2 портқа арналған желілік карталар бар.

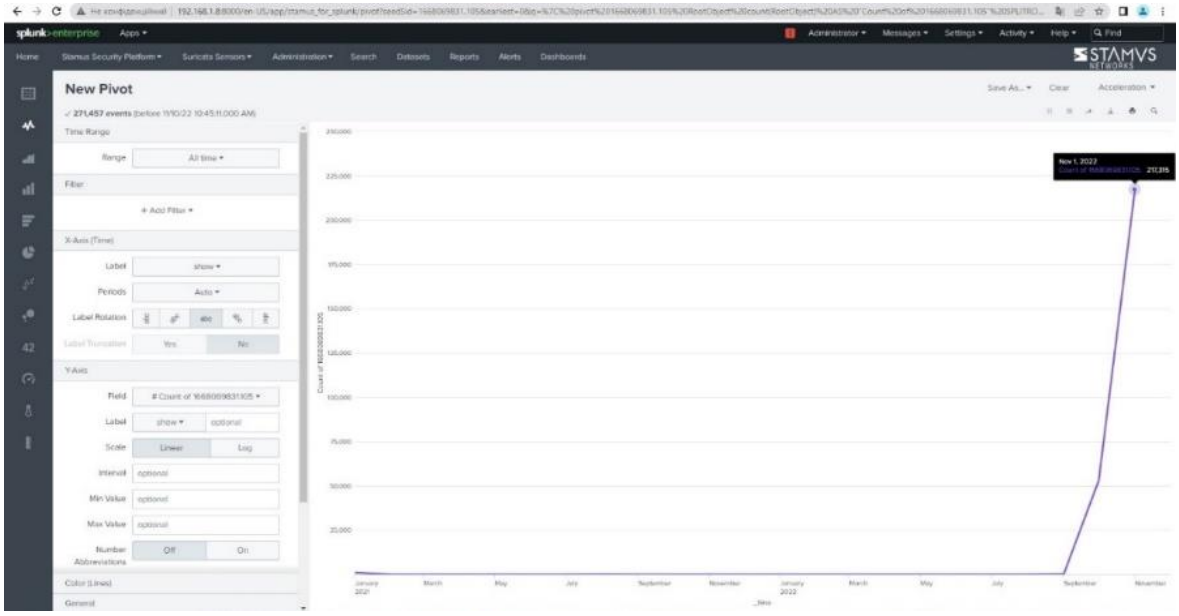
Маршрутизатор мен ядро коммутаторларын байланыстыру үшін динамикалық маршруттау хаттамасы орнатылды.

Содан кейін ядро коммутаторларында виртуалды желілер (VLAN) құрылды. Бұл шектеулі қолжетімділікті қамтамасыз ету үшін АОБ ресурстарын АҚ қамтамасыз ету үшін трафикті ішкі желілерге бөлуге мүмкіндік берді. Сондай-ақ, желілік ілмектердің пайда болуын болдырмау үшін коммутаторларда STP хаттамасы орнатылды. Сонымен қатар, снуппинг DHCP хаттамалары, ARP пакеттерін тексеру, Flood шабуылдары үшін трафикті сүзу орнатылды. АОБ желісін қорғауды одан әрі күшейту үшін, оның жеке түйіндерінде қауіпсіздікті қамтамасыз етуден және DNS мекенжайларын сүзуден басқа, кибершабуылдарды анықтау үшін трафикті талдайтын ВМ жүйесіне қосқан жөн. Біз IPS Suricata орнатылған Kali Linux (Debian) негізінде жеке ВМ құру туралы шешім қабылдадық.

АОБ қауіпсіз желіні орнату аяқталғаннан кейін жұмыс өнімділігі тексерілді. Ол үшін Pi-Hole бар ВМ барлық құрылғыларда және шеткі маршрутизаторда негізгі DNS сервері ретінде көрсетілген. Pi-Hole қосымшасының өзі нақты уақыт режимінде қандай сұраулар бұғатталғанын және қайсысына рұқсат берілгенін көруге мүмкіндік берді. Pi-Hole көмегімен

АОБ АҚ әкімшісі статистиканы диаграмма түрінде көрсетуге және олардың мәліметтерін көруге ыңғайлы болды.

Алынған нәтижелерден, сурет 3-ті қараңыз, виртуалды ТЕЖ үшін сыналған АҚ жүйесі (ұсынылған әдістеме негізінде құрастырылған) 5 сағат жұмыс ішінде 3700-ден астам зиянды сұраныстарды бұғаттады, бұл АОБ желісіне кіретін барлық трафиктің > 41% құрайды. Осылайша, АОБ желісінің АҚ арттыру үшін IDS және SIEM жүйелерін пайдалану бойынша қабылданған шешімдердің дұрыстығы эксперименталды түрде расталды. IDS Suricata және SIEM Splunk орнатылғаннан кейін, соңғысы біріншісінен жүйелік хабарламалар ала бастады. Бір сағаттың ішінде жүйе бойынша АОБ АҚ ережелерін бұзу және тиісті трафикті бұғаттау туралы 20 хабарлама жіберілді. Бұл мұндай жүйелер АОБ қауіпсіздік контурында өзін ақтайды деген қорытынды жасауға мүмкіндік берді.



Сурет 3. IDS Suricata-дан ескертулерінің Splunk-те графикалық бейнелеу

Тек ТЕЖ емес, жалпы АОБ-де, АҚ деңгейін бағалау үшін осы математикалық тәсілдің мүмкіндігін атап өткен жөн. Ағымдағы кезеңдегі зерттеудің кемшілігі ретінде ТЕЖ немесе жалпы АОБ үшін қауіптердің толық тізімі қарастырылмағанын атап өтуге болады. Сондай-ақ, эксперимент барысында оларды бейтараптандыру үшін таңдалған АҚ шараларының тізімі шектелді.

Дискуссия

Көптеген заманауи ақпараттық қауіпсіздік объектілерінің есептеу жүйелері немесе ТЕС олардың архитектурасында көптеген күрделі элементтерді біріктіреді. Өз кезегінде, мұндай элементтердің әрқайсысы компьютерлік шабуылдаушылардың шабуылына ұшырауы мүмкін. Тиісінше, ТЕС архитектурасын құрайтын әрбір элемент кибернетикалық қауіптердің жеткілікті санына ұшырайды. Бұл қауіптердің ТЕС АЖ-ға әсерін азайту және кейбір жағдайларда келтірілген зиянды болдырмау үшін желі архитектурасына әртүрлі ақпаратты қорғау құралдары біріктірілген. Немесе ықтимал қауіптердің әртүрлілігін ескере отырып – АҚ-ны қамтамасыз ету шаралары мен құралдары.

ТЕС үшін ақпараттық қауіпсіздік құралдарын көбейту, демек, жұмсалатын ресурстардың, ең алдымен қаржылық ресурстардың көлемін ұлғайту әрқашан күтілетін нәтиже бермейтіні бұрыннан дәлелденген. ТЕС-та қолданылатын АҚ құралдары мен шаралары әртүрлі бағытта болуы мүмкін. Мысалы, бұл кез - келген зиянды бағдарламалық жасақтаманың маңызды ТЕС түйіндеріне енуіне жол бермейтін АҚ құралдары болуы мүмкін. Немесе жүйелік әкімшілер

арасында жалпы ТЕС-тің де, оның жеке компоненттерінің де жұмысына мониторинг жүргізуге арналған танымал бағдарламалар.

АҚ-ға қауіп-қатер ландшафты үнемі өзгеріп отыратындығына және ТЕС архитектурасы күрделене түскен сайын қауіптер саны артып келе жатқандығына сүйене отырып, желілердің қауіпсіз және сенімді жұмысын қамтамасыз ету мәселелерін шешу көп көңіл бөлуді және қосымша зерттеулерді қажет етеді. Сондықтан таратылған есептеу желісі үшін ақпараттық қауіпсіздік жүйесін қалыптастырудың ұсынылған әдістемесі және осалдық коэффициентінің моделі ақпараттану объекті таратылған есептеу желісінің осалдық деңгейлерінің сандық бағасын алуға мүмкіндік бергені көрсетілген.

Қорытынды

Осылайша жүргізілген зерттеулер келесі нәтижелерге қол жеткізуге мүмкіндік берді:

Университеттік есептеу желісіне (немесе ТЕЖ) арналған АҚ жүйесін қалыптастыру әдістемесіне нақтылау ұсынылды.

Әдістеменің бірінші кезеңінде ықтималдық теориясының аппаратын пайдалану негізінде математикалық модельдеуді қолдану ұсынылады. Ұсынылған тәсіл ТЕЖ осалдық коэффициентін есептеу үшін аналитикалық өрнек алуға мүмкіндік берді (қажет болған жағдайда жалпы АОБ үшін).

ТЕЖС АҚ жүйесін қалыптастыру әдістемесінің екінші кезеңінде АОБ желісінің АҚ компоненттерін имитациялық модельдеу және виртуалдандыру әдістері қолданылады.

Эксперименттік зерттеулер барысында АОБ қорғалған желісінің моделі жасалды. Эксперименттік модельде желілік құрылғылар мен АҚ компоненттері виртуалды машиналарда (ВМ) эмуляцияланды. АОБ желісінің ресурстары Proxmox VE серверлік виртуалдандыру жүйесінің арқасында қайталанды. АОБ желісінің хосттарында PVE басқаруымен IPS Suricata қауіп-қатерді анықтау жүйесі орналастырылды, Splunk жүйесі SIEM ретінде пайдаланылды.

ТЕЖ үшін АҚ жүйесін қалыптастырудың ұсынылған әдістемесі және осалдық коэффициентінің моделі ТЕЖ әртүрлі элементтерінің осалдық деңгейлерін сандық бағалауға мүмкіндік беретіні көрсетілген. Сондай-ақ, ұсынылған модель АҚ желісінің жүйесін жобалау сатысында АОБ осалдығының болжамды деңгейін бағалауды орындауға және қауіптер мен осалдықтарды бейтараптандыру үшін қарсы шараларды қолдану тиімділігін алдын ала бағалауды жүзеге асыруға мүмкіндік береді.

Пайдаланылған дереккөздер тізімі

[1] Evans, M., He, Y., Maglaras, L., & Janicke, H. HEART-IS: A novel technique for evaluating human error-related information security incidents. // Computers & Security. 2019. 80. P. 74-89. https://doi.org/10.1016/j.cose.2018.09.002

[2] Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation. // Information Technology & People. 2019. 32(5). P. 1262-1275. https://doi.org/10.1108/ITP-06-2018-0261

[3] Schlette, D., Caselli, M., & Pernul, G. A comparative study on cyber threat intelligence: the security incident response perspective. // IEEE Communications Surveys & Tutorials. 2021. 23(4). P. 2525-2556. https://doi.org/10.1109/COMST.2021.3117338

[4] Zegzhda, D. P., Lavrova, D. S., & Pavlenko, E. Y. Management of a dynamic infrastructure of complex systems under conditions of directed cybe attacks. // Journal of Computer and Systems Sciences International. 2020. 59(3). P. 358-370. http://dx.doi.org/10.1134/S1064230720020124

[5] Ahmetoglu, H., & Das, R. A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. // Internet of Things. 2022. 100615. https://doi.org/10.1016/j.iot.2022.100615

[6] An, P., Wang, Z., & Zhang, C. Ensemble unsupervised autoencoders and Gaussian mixture model for cyberattack detection. // Information Processing & Management. 2022. 59(2). 102844. https://doi.org/10.1016/j.ipm.2021.102844

[7] Aribisala, A., Khan, M. S., & Husari, G. (2021, October). Machine Learning Algorithms and Their Applications in Classifying Cyber-Attacks On a Smart Grid Network. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0063-0069). IEEE. http://dx.doi.org/10.1109/IEMCON53756.2021.9623067

[8] Angelini, M., Blasilli, G., Catarci, T., Lenti, S., & Santucci, G. Vulnus: Visual vulnerability analysis for network security. // IEEE transactions on visualization and computer graphics. 2018. 25(1). P. 183-192. http://dx.doi.org/10.1109/TVCG.2018.2865028

[9] Yeboah-Ofori A, Islam S. Cyber Security Threat Modeling for Supply Chain Organizational Environments. // Future Internet. 2019. 11(3):63. https://doi.org/10.3390/fi11030063

[10] Tanwar, R., Choudhury, T., Zamani, M., & Gupta, S. (Eds.). Information Security and Optimization. CRC Press. 2020. https://books.google.de/books?hl=en&lr=&id=F1cBEAAAQBAJ&oi=fnd&pg=PP1&dq=related:NTArO56bNTwJ:scholar.google.com/&ots=2qdbsP1NG3&sig=ps37g1m7bE7pqPqeRNVJoXIvMtY

[11] Almohri, H. M., Watson, L. T., Yao, D., & Ou, X. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. // IEEE Transactions on Dependable and Secure Computing. 2015. 13(4). P. 474-487. http://dx.doi.org/10.1109/TDSC.2015.2411264

[12] Bouyeddou, B., Harrou, F., Kadri, B., & Sun, Y. Detecting network cyber-attacks using an integrated statistical approach. // Cluster Computing. 2021. 24(2). P. 1435-1453. https://link.springer.com/article/10.1007/s10586-020-03203-1

[13] Utzerath, J., & Dennis, R. Numbers and statistics: data and cyber breaches under the General Data Protection Regulation. // International Cybersecurity Law Review. 2021. 2(2). P. 339-348. https://doi.org/10.1365/s43439-021-00041-8

[14] Schatz D., Bashroush R. Economic valuation for information security investment: a systematic literature review. // Information Systems Frontiers. 2017. T. 19. №.5. P. 1205-1228. DOI https://doi.org/10.1007/s10796-016-9648-8

[15] Оладько В. С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности. 2016. №1 (14). С.17-23. URL: https://cyberleninka.ru/article/n/model-vybora-ratsionalnogo-sostava-sredstv-zaschity-v-sisteme-elektronnoy-kommertsii

[16] Прокушев Я.Е., Пономаренко С.В., Пономаренко С.А. Моделирование процессов проектирования систем защиты информации в государственных информационных системах // Computational nanotechnology. 2021. Т. 8. № 1. С. 26–37. DOI: 10.33693/2313-223X-2021-8-1-26-37 https://cyberleninka.ru/article/n/modelirovanie-protsessov-proektirovaniya-sistem-zaschity-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah/viewer

[17] 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). P. 255-270. https://doi.org/10.1007/s12243-020-00783-2

References

[1] Evans, M., He, Y., Maglaras, L., & Janicke, H. HEART-IS: A novel technique for evaluating human error-related information security incidents. // Computers & Security. 2019. 80. P. 74-89. https://doi.org/10.1016/j.cose.2018.09.002

[2] Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance: An empirical investigation. // Information Technology & People. 2019. 32(5). P. 1262-1275. https://doi.org/10.1108/ITP-06-2018-0261

[3] Schlette, D., Caselli, M., & Pernul, G. A comparative study on cyber threat intelligence: the security incident response perspective. // IEEE Communications Surveys & Tutorials. 2021. 23(4). P. 2525-2556. https://doi.org/10.1109/COMST.2021.3117338

[4] Zegzhda, D. P., Lavrova, D. S., & Pavlenko, E. Y. Management of a dynamic infrastructure of complex systems under conditions of directed cybe attacks. // Journal of Computer and Systems Sciences International. 2020. 59(3). P. 358-370. http://dx.doi.org/10.1134/S1064230720020124

[5] Ahmetoglu, H., & Das, R. A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. // Internet of Things. 2022. 100615. https://doi.org/10.1016/j.iot.2022.100615

[6] An, P., Wang, Z., & Zhang, C. Ensemble unsupervised autoencoders and Gaussian mixture model for cyberattack detection. // Information Processing & Management. 2022. 59(2). 102844. https://doi.org/10.1016/j.ipm.2021.102844

[7] Aribisala, A., Khan, M. S., & Husari, G. (2021, October). Machine Learning Algorithms and Their Applications in Classifying Cyber-Attacks On a Smart Grid Network. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0063-0069). IEEE. http://dx.doi.org/10.1109/IEMCON53756.2021.9623067

[8] Angelini, M., Blasilli, G., Catarci, T., Lenti, S., & Santucci, G. Vulnus: Visual vulnerability analysis for network security. // IEEE transactions on visualization and computer graphics. 2018. 25(1). P. 183-192. http://dx.doi.org/10.1109/TVCG.2018.2865028

[9] Yeboah-Ofori A, Islam S. Cyber Security Threat Modeling for Supply Chain Organizational Environments. // Future Internet. 2019. 11(3):63. https://doi.org/10.3390/fi11030063

[10] Tanwar, R., Choudhury, T., Zamani, M., & Gupta, S. (Eds.). Information Security and Optimization. CRC Press. 2020.
https://books.google.de/books?hl=en&lr=&id=F1cBEAAAQBAJ&oi=fnd&pg=PP1&dq=related:NTArO56bNTwJ:scholar.google.com/&ots=2qdbsP1NG3&sig=ps37g1m7bE7pqPqeRNVJoXIvMtY

[11] Almohri, H. M., Watson, L. T., Yao, D., & Ou, X. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. // IEEE Transactions on Dependable and Secure Computing. 2015. 13(4). P. 474-487. http://dx.doi.org/10.1109/TDSC.2015.2411264

[12] Bouyeddou, B., Harrou, F., Kadri, B., & Sun, Y. Detecting network cyber-attacks using an integrated statistical approach. // Cluster Computing. 2021. 24(2). P. 1435-1453. https://link.springer.com/article/10.1007/s10586-020-03203-1

[13] Utzerath, J., & Dennis, R. Numbers and statistics: data and cyber breaches under the General Data Protection Regulation. // International Cybersecurity Law Review. 2021. 2(2). P. 339-348. https://doi.org/10.1365/s43439-021-00041-8

[14] Schatz D., Bashroush R. Economic valuation for information security investment: a systematic literature review. // Information Systems Frontiers. 2017. T. 19. №.5. P. 1205-1228. DOI https://doi.org/10.1007/s10796-016-9648-8

[15] Olad'ko, V. S. (2016). Model' vybora racional'nogo sostava sredstv zashchity v sisteme elektronnoj kommercii [A model for choosing a rational composition of security tools in the e-commerce system]. Voprosy kiberbezopasnosti. №1 (14). 17-23 (in Russian). https://cyberleninka.ru/article/n/model-vybora-ratsionalnogo-sostava-sredstv-zaschity-v-sisteme-elektronnoy-kommertsii

[16] Prokushev, YA. E., Ponomarenko, S. V., & Ponomarenko, S. A. Modelirovanie processov proektirovanija sistem zashhity informacii v gosudarstvennyh informacionnyh sistemah [Modeling of design processes of information security systems in state information systems]. Computational nanotechnology. 2021. №1. 26-37. (in Russian). DOI: 10.33693/2313-223X-2021-8-1-26-37
https://cyberleninka.ru/article/n/modelirovanie-protsessov-proektirovaniya-sistem-zaschity-informatsii-v-gosudarstvennyh-informatsionnyh-sistemah/viewer

[17] 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). P. 255-270. https://doi.org/10.1007/s12243-020-00783-2