УДК 004

Р.Соловйов, магістр гр. КН-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ РОЗПОДІЛУ КЛЮЧІВ В МЕРЕЖІ CISCO SD-WAN, ЩО БАЗУЄТЬСЯ НА ХМАРНІЙ АРХІТЕКТУРІ

У статті розроблено програмне забезпечення, яке призначено для системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Метою розробки є дослідження та програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Об’єктом дослідження є процес розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Предметом дослідження є методи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Методи дослідження базуються на методах захисту інформації та хмарних обчислень, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, розподіл ключів, Cisco SD-WAN, хмарна архітектура

Постановка проблеми. Однією із ключових задач удосконалювання інформаційних комунікацій є задача побудови безпечної комп'ютерної мережі. Інтерес до неї обумовлюється зростаючими об'ємами переданими між учасниками інформаційного обміну конфіденційної інформації, і швидким ростом таких показників інформації, як вартість втрати конфіденційності, вартість схованого порушення цілісності, вартість втрати інформації. Цій проблемі присвячена велика кількість наукових робіт і монографій.

Захищеність комунікацій у безпечній мережі включає забезпечення конфіденційності й цілісності переданої інформації. Ці властивості забезпечуються використовуваними криптографічними системами, успішне функціонування яких припускає використання на приймальні й передавальній сторонах захищеного каналу криптографічних ключів, бінарних наборів достатньої довжини.

До 1976 року використовувалися лише симетричні криптосистеми, у яких ключі передавальної й приймаючої сторони повинні бути секретними й практично однаковими, що пов'язане із проблемою доставки ключа від одного учасника іншому або від довіреного центра обом учасникам. З винаходом У. Діффі, М. Хеллманом публічної криптографії один із ключів може бути відкритим і доставлятися його стороні, що використовує, не по закритому, а по автентичному каналі, що вимагає реєстрації цього ключа в центрах сертифікації інфраструктури розподілу відкритих ключів.

Помітимо, що використання криптосистем з відкритим ключем саме по собі не досить для забезпечення захищеності комунікацій у комп'ютерних мережах, оскільки алгоритми криптографії з відкритим ключем через необхідність виконання алгебраїчних операцій в алгебраїчних структурах високих порядків на три порядки повільніше алгоритмів симетричних криптосистем.

Тому криптосистеми з відкритим ключем можуть використовуватися для захисту лише невеликих обсягів інформації й в основному відіграють допоміжну роль, забезпечуючи захист передачі секретних ключів для симетричних криптосистем.

Безпосереднє використання цього способу доставки секретного ключа кожним

учасником комп'ютерної мережі приводить до багаторазового (по числу учасників) виконанню дорогих актів сертифікації й використанню ключів, що генерується учасниками без належного контролю їхньої якості.

Для спрощення процедури формування й доставки секретних ключів у криптографії запропоновані й досліджені різноманітні схеми попереднього розподілу ключів. У них процедура доставки секретного ключа учасникам комп'ютерної мережі виконується у два етапи: кожному учасникові довіреним центром доставляється пакет ключової інформації (у вигляді наборів двійкових слів достатньої довжини), склад якого (можливо, з деякою додатковою відкритою інформацією про ці слова) публікується.

При цьому кожний учасник, знаючи склади пакетів і опубліковані дані, може, використовуючи тільки набори зі свого пакета, обчислити для захищеної комунікації з будь-яким іншим учасником мережі ключ, що не може обчислити ніякий третій учасник.

Розвиваючи цей підхід, криптографи запропонували й схеми більш загального характеру, що дозволяють попередньо розподіляти ключову інформацію для обчислення ключів привілейованих груп учасників, недоступних забороненим групам учасників. Але й цей підхід зустрічає труднощі відносно до великих обчислювальних мереж, оскільки припускає використання єдиного центра генерації й доставки пакетів ключової інформації кожному учасникові мережі. Використання для доставки пакетів криптосистем з відкритим ключем припускає сертифікацію відритих ключів учасниками.

Розглянутий стан проблеми розподілу ключів дозволяє вважати **актуальними** наступні задачі:

– розробка й обґрунтування архітектурних мережевих рішень нецентралізованого попереднього розподілу ключової інформації в комп'ютерній мережі на основі незалежного попереднього її розподілу в сегментах або доменах мережі;

– розробка й обґрунтування способу реалізації попереднього розподілу ключової інформації в сегментах або доменах обчислювальної мережі на основі використання пропонованої модифікації протоколу Kerberos;

– розробка й обґрунтування нових схем попереднього розподілу ключів;

– розробка програмного забезпечення для обчислення пакетів ключової інформації й принципів побудови системного програмного забезпечення для обчислювальних систем з нецентралізованим попереднім розподілом ключів.

Варто підкреслити відповідність цих напрямків дослідження особливостям мобільних обчислювальних мереж, у яких практично важко реалізовані вимоги сертифікації відкритих ключів і актуальна задача обліку умови розширюваності мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

– Дослідження системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

– Програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

Об'єктом дослідження є процес розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

Предметом дослідження є методи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі.

Методи дослідження базуються на методах захисту інформації та хмарних обчислень, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис методу побудови схем попереднього розподілу ключів

У цьому розділі наведені приклади поліпшення схем попереднього розподілу системних ключів за рахунок аналізу привілейованого й забороненого сімейств.

Визначення: Нехай:

$\sum^1$ – множина всіх можливих KDP($\boldsymbol{P}_1$,$\boldsymbol{F}_1$)-схем.

$\sum^2$ – множина всіх можливих KDP($\boldsymbol{P}_2$,$\boldsymbol{F}_2$)-схем.

$\boldsymbol{S}^1$ – KDP($\boldsymbol{P}_1$,$\boldsymbol{F}_1$)-схема ($\boldsymbol{S}^1 \in \sum^{1)}$.

$\boldsymbol{S}^2$ – KDP($\boldsymbol{P}_2$,$\boldsymbol{F}_2$)-схема ($\boldsymbol{S}^2 \in \sum^{2)}$.

Схеми $\boldsymbol{S}^1$ і $\boldsymbol{S}^2$ є взаємозамінними, якщо $\boldsymbol{S}^1 \in \sum^2$ і $\boldsymbol{S}^2 \in \sum^{1\cdot}$

Для взаємозамінних схем по визначенню KDP-схеми виконано:

$$\forall P \in \boldsymbol{P}_1, F \in \boldsymbol{F}_1, P \cap F = \varnothing: \ \bigcap_{i \in P} S_i^2 \not\subset \bigcup_{j \in F} S_j^2, \tag{1}$$

$$\forall P \in \boldsymbol{P}_2, F \in \boldsymbol{F}_2, P \cap F = \varnothing: \ \bigcap_{i \in P} S_i^1 \not\subset \bigcup_{j \in F} S_j^1 \cdot \tag{2}$$

Помітимо, що відношення взаємозамінності є симетричні і рефлексивні, але не є транзитивні, тобто з того, що схеми $\boldsymbol{S}^1$ і $\boldsymbol{S}^2$ взаємозамінні, $\boldsymbol{S}^2$ і $\boldsymbol{S}^3$ взаємозамінні, не слідує, що $\boldsymbol{S}^1$ і $\boldsymbol{S}^3$ взаємозамінні. Відношення взаємозамінності є відношенням толерантності.

Твердження 1. Якщо $\boldsymbol{F}_1 \subseteq \boldsymbol{F}$, де $\boldsymbol{F}_1$ це сімейство всіх підмножин множини U потужності w, причому $\forall P \in \boldsymbol{P}: |P| + w < n$ $\left(\max_{P \in \boldsymbol{P}} |P| + w < n\right)$, то KDP($\boldsymbol{P}$,$\boldsymbol{F}$) і KDP($\boldsymbol{P}$,$\boldsymbol{F}'$)-схеми є взаємозамінними, де $\boldsymbol{F}'$ – це об'єднання сімейства $\boldsymbol{F}$ і всіх підмножин множини U потужність яких не перевершує w.

Твердження 2. Якщо існує сімейство $\boldsymbol{P}_1 \subseteq \boldsymbol{P}$, таке що $\boldsymbol{P}_1$ це сімейство всіх підмножин множини U потужності g, причому $\forall F \in \boldsymbol{F}: |F| + g < n$, то KDP($\boldsymbol{P}$,$\boldsymbol{F}$) і KDP($\boldsymbol{P}'$,$\boldsymbol{F}$)-схеми є взаємозамінними, де $\boldsymbol{P}'$ – це об'єднання сімейства $\boldsymbol{P}$ і всіх підмножин множини U, потужність яких не перевершує g.

Твердження 3. Якщо $g+w<n$, то схеми KDP(g,w) і KDP($\leq g$, $\leq w$) є взаємозамінними.

Для імовірнісного методу запропонована більше низька оцінка кількості системних ключів, необхідних для побудови схеми.

На основі вивчених методів запропонований метод побудови загального випадку схем розподілу системних ключів.

Суть імовірнісних методів полягає в тому, що формується деяким випадковим образом таблиця. Далі перевіряється, чи є сформована таблиця KDP-схемою. Якщо немає – то таблиця формується заново.

Розглянемо імовірнісний метод побудови KDP($\boldsymbol{P}$,$\boldsymbol{F}$)-схем.

Нехай елементи множини Ψ пронумеровані: $\{\psi_1, \psi_2, \ldots, \psi_k\}$.

Позначимо $X_{is} = \begin{cases} 1, & якщо\ \psi_s \in S_i \\ 0, & якщо\ \psi_s \notin S_i \end{cases}$, s=1, …, k; i=1, …, n...

Таблиця X заповнюється в такий спосіб:

$$X_{is} = \begin{cases} 1, & з\ ймовірністю\ \ p \\ 0, & з\ ймовірністю\ 1-p \end{cases}. \tag{3}$$

Верхня оцінка ймовірності того, що KDP-схема не буде побудована імовірнісним методом:

$$E = E(k, p) = \sum_{P \in \boldsymbol{P}} \sum_{\substack{F \in \boldsymbol{F} \\ P \cap F = \varnothing}} \prod_{s=1}^{k} \left(1 - \prod_{i \in P} p \prod_{j \in F} (1-p)\right) = \sum_{P \in \boldsymbol{P}} \sum_{\substack{F \in \boldsymbol{F} \\ P \cap F = \varnothing}} \left(1 - p^{|P|}(1-p)^{|F|}\right)^k \tag{4}$$

Розглянуто імовірнісний метод, що дозволяє побудувати KDP$(\boldsymbol{P}^g, \boldsymbol{F}^w)$ -схеми, де:

$$\boldsymbol{P}^g = \{P : P \in \boldsymbol{P}, |P| = g\},\ \boldsymbol{F}^w = \{F : F \in \boldsymbol{F}, |F| = w\}. \tag{5}$$

Мінімізуючи $E(k, p)$ по p, маємо:

$$p_0 = \frac{g}{w+g}. \tag{6}$$

Кількість ключів $k_0^{g,w}$, необхідних для побудови такої схеми обчислюється по формулі:

$$k_0^{g,w} = \left\lfloor \frac{(g+w)^{g+w}}{g^g w^w} \ln\left(\frac{\sum\limits_{P \in \boldsymbol{P}^g} \sum\limits_{\substack{F \in \boldsymbol{F}^w \\ P \cap F = \varnothing}} 1}{1 - \mathrm{E}} \right) \right\rfloor + 1. \tag{7}$$

Уведено поняття об'єднання KDP-схем і запропоновані способи зменшення об'єму ключового матеріалу за рахунок комбінування різних методів побудови схем KDP (або схем, одержуваних одним методом, але з різними параметрами).

Визначення. Нехай:

$\{S_1^1,\ldots,S_n^1\}$ – KDP($\boldsymbol{P}_1$,$\boldsymbol{F}_1$)-схема.

$\{S_1^2,\ldots,S_n^2\}$ – KDP($\boldsymbol{P}_2$,$\boldsymbol{F}_2$)-схема.

При цьому $\Psi_1 \bigcap \Psi_2 = \varnothing$.

Тоді об'єднанням KDP-схем KDP($\boldsymbol{P}_1$,$\boldsymbol{F}_1$)$\bigcup$ KDP($\boldsymbol{P}_2$,$\boldsymbol{F}_2$) є сімейство $\{S_1,\ldots,S_n\}$: $S_i = S_i^1 \bigcup S_i^2$.

Позначимо $G = \{g : \boldsymbol{P}^g \neq \varnothing\}$, $W = \{w : \boldsymbol{F}^w \neq \varnothing\}$.

Тоді:

$$\boldsymbol{P} = \bigcup_{g \in G} \boldsymbol{P}^g,\ \boldsymbol{F} = \bigcup_{w \in W} \boldsymbol{F}^w \text{ і } \mathrm{KDP}(\boldsymbol{P}, \boldsymbol{F}) = \bigcup_{w \in W, g \in G} \mathrm{KDP}(\boldsymbol{P}^g, \boldsymbol{F}^w). \tag{8}$$

При цьому можна використовувати різні методи побудови KDP$(\boldsymbol{P}^g, \boldsymbol{F}^w)$ -схем.

Розглянемо комбінування імовірнісних і тривіальних методів побудови схем попереднього розподілу системних ключів.

Якщо виконуються умови:

$$H_1(g,w) = \{ \sum_{g \in G} \min\{k_0^{g,w}, |\boldsymbol{P}^g|\} \geq |\boldsymbol{F}^w| \}, \tag{9}$$

або

$$H_2(g,w) = \{ \sum_{w \in W} \min\{k_0^{g,w}, |\boldsymbol{F}^w|\} \geq |\boldsymbol{P}^g| \}, \tag{10}$$

то для побудови KDP$(\boldsymbol{P}^g, \boldsymbol{F}^w)$ -схеми раціонально використовувати тривіальні методи, інакше – імовірнісні.

Таким чином, KDP($\boldsymbol{P}$,$\boldsymbol{F}$)-схема:

$$\bigcup_{\substack{w \in W, g \in G, \\ \neg H_1(g,w), \\ \neg H_2(g,w)}} \mathrm{KDP}(\boldsymbol{P}^g, \boldsymbol{F}^w) \bigcup \bigcup_{\substack{w \in W, \\ H_1(w,g)}} \mathrm{KDP}(\cdot, \boldsymbol{F}^w) \bigcup \bigcup_{\substack{g \in G, \\ H_2(g,w)}} \mathrm{KDP}(\boldsymbol{P}^g, \cdot) \tag{11}$$

Кількість системних ключів |Ψ|, необхідних для побудови схеми:

$$k_0 = \sum_{\substack{w \in W, g \in G, \\ \neg H_1(g,w), \\ \neg H_2(g,w)}} k_0^{g,w} + \sum_{\substack{w \in W, \\ H_1(w,g)}} |\boldsymbol{F}^w| + \sum_{\substack{g \in G, \\ H_2(g,w)}} |\boldsymbol{P}^g| \tag{12}$$

Імовірнісний метод побудови схеми попереднього розподілу ключів з геш-функцією.

Визначення. HAKDP(***P***,***F***,*L*)-схемою, де ***P*** і ***F*** – це сімейства підмножин множини *U* = {1, …, *n*}, називається всяка пара сімейств (***S***,***D***), ***S***={S_1,…,S_n} підмножин кінцевої множини $\Psi \subseteq \Omega$ (|Ψ|=*k*) і ***D***={D_1,…,D_n} підмножин множини {1,…,*L*}, причому |D_t| = |S_t| для *t*=1,…,*n*, задовольняючій умові: $\forall P \in \boldsymbol{P}, F \in \boldsymbol{F}, P \cap F = \varnothing : \bigcap_{i \in P} S_i \not\subset \bigcup_{j \in F} S_j$ або не виконана умова $D_{F,P} \le D_P$, де D_P – набір значень $\max_t(D_i(t))$ відповідним співпадаюніж елементам множин S_i з *P* і $D_{F,P}$ є набір значень $\min_t(D_i(t))$ всіх тих елементів з *F*, які відповідають співпадаюніж елементам множин S_i з *F*.

Зауваження. HAKDP(***P***,***F***,0)-схема є KDP(***P***,***F***)-схемою.

Приклад HAKDP(2,1,1)-схеми для *n*=4 абонентів і *k*=3 ключів:

S_1={1,2,3}, D_1=(1,1,1),

S_2={1,2}, D_2=(0,0),

S_3={1,3}, D_3=(0,0),

S_4={2,3}, D_4=(0,0)

Нехай, як і у випадку KDP-схем, таблиця *X* отримана деяким випадковим способом Pr{ X_{is} =1}=p_0. Таблиця ***D*** також отримана випадковим способом Pr{D_t(*s*)=*a*}=$\frac{1}{L}$, $a \in \{1,...,L\}$. При цьому p_0 обчислюється по формулі:

$$p_0 = \frac{2}{3(1+P_L)}, \tag{13}$$

кількість ключів, необхідних для побудови HAKDP(2,1,*L*)-схеми:

$$k = -\frac{\log(n(n-1)(n-2))}{\log(1-p^2(1-p)-p^3P_L)}, \tag{14}$$

де P_L – імовірність того, що $D_{rs} < D_i(s)$ і $D_r(s) < D_j(s)$.

Дану ймовірність можна порахувати по формулі:

$$P_L = \sum_{m=0}^{L} \frac{1}{L+1}\left(\frac{L-i}{L+1}\right)^2 = \frac{2L^2+L}{6L^2+12L+6}. \tag{15}$$

Переваги використання KDP і HAKDP-схем випливають із даних, представлених у таблиці 1 на прикладі KDP(10^4, 173) і HAKDP(10^4, 114, 10)-схем.

Таблиця 1 – Порівняння централізованої KDP і HAKDP-схем

	Без попереднього розподілу	KDP(10^4,173)-схема	HAKDP(10^4,114,10)-схема
Середня довжина пакета	9 999	115	71
Число переданих ключів	99 990 000	1 150 000	710 000

Пропонується три способи організації безпечної мережі на основі протоколу Kerberos і схем попереднього розподілу ключів.

Перший спосіб припускає використання стандартного протоколу Kerberos, у якому як сервер додатків виступає абонент мережі, якому адресується повідомлення.

Другий спосіб припускає використання стандартного протоколу Kerberos для попереднього розподілу ключового матеріалу в мережі, відповідно до KDP-схеми. При цьому KDP-схема й ключовий матеріал формується на стороні сервера додатків.

Третій спосіб припускає використання модернізованого протоколу Kerberos для

розподілу ключового матеріалу. При цьому KDP-схема й ключовий матеріал формуються на стороні сервера TGS.

Розглянемо нецентралізований розподіл ключової інформації. У складних мережах, що складаються з декількох доменів, використання централізованого розподілу ключової інформації може бути важко.

Опишемо технологію захищених комунікацій у комп'ютерній мережі, з використанням ключової інформації, попередньо розподіленої в її сегментах. Хоча б один з елементів у кожному сегменті відіграє роль сервера додатків. Інші елементи сегмента представляють мережевих клієнтів. Мережеві сервери додатка є довіреними вузлами для всіх елементів комп'ютерної мережі. Вони зашифровують і розшифровують конфіденційну інформацію користувачів, коли відповідний шифротекст одного сегмента передається користувачеві з іншого сегмента. При цьому використовуються ключі, що обчислюються по пачках, розподіленим елементам одного сегмента, для розшифрування й іншого для зашифрування.

Захищені комунікації в мережі здійснюються з використанням ключів, що обчислюються на підставі часток ключової інформації, виділюваних окремим елементам або різним парам елементів того самого домена (рисунок 1).

Дана технологія дозволяє зменшити час обчислення схем попереднього розподілу ключів, а також об'єм ключової інформації, переданої по секретних каналах від генератора до елементів комп'ютерної мережі.

Передбачаються наступні особливості мережі:

1) комп'ютерна мережа складається з N сегментів (або доменів) $D_1,\ldots, D_N$;

2) хоча б один учасник кожного домена виконує роль мережевого сервера додатків NAS (Network Application Server), інші елементи є клієнтами мережі.

3) кожний NAS є елементом двох сусідніх сегментів, він одержує свої частки ключової інформації, розподіленої в обох сегментах;

4) граф, вершини якого відповідають сегментам, а ребра – мережевим серверам додатків NAS зв'язний;

5) кожний учасник може передавати зашифровану інформацію будь-якому іншому учасникові по відкритих каналах;

6) мережеві сервери додатків NAS є довіреними вузлами для всіх елементів комп'ютерної мережі;

7) кожний мережевий сегмент (або домен) D_j, j=1,…,N, прикріплений до певного довіреного центра TA_j;

8) кожний довірений центр TA_j, j=1,…,N, виробляє схему попереднього розподілу ключів для прикріпленого сегмента й розподіляє між його елементами пакети обчисленої ключової інформації;

9) генерація схем розподілу ключів і доставка ключової інформації для елементів різних сегментів здійснюється незалежно й, можливо, одночасно.

10) конфіденційна комунікація між учасниками комп'ютерної мережі організується з використанням зашифрування-розшифрування й забезпечення цілісності тих самих або різних пакетів ключової інформації, що належать одному або декільком учасникам того самого сегмента.

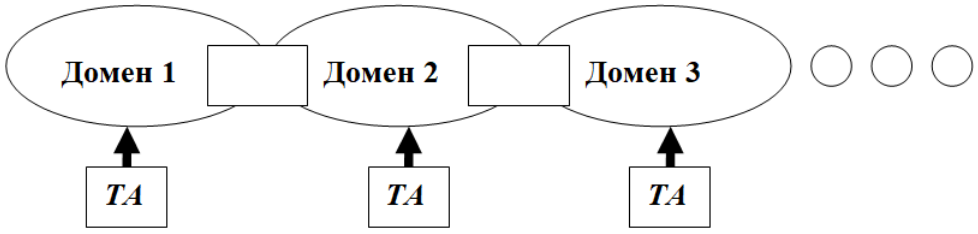

Рисунок 1 – Нецентралізований попередній розподіл ключів

Розглянемо окремий випадок мережі, у якій кожний абонент мережі може передати інформацію іншому абонентові мережі.

Розподіл ключової інформації здійснюється незалежно у всіх доменах мережі. Для цього в кожному домені будується KDP(2,1)-схема. Такі схеми можуть мати однакову або різні структури, але в кожній з них елементи ключової інформації, що розподіляється, виробляються випадково й незалежно.

Нехай по завершенню етапу попереднього розподілу ключів (централізованому для кожного домена образом, але незалежним у кожному домені) всі учасники комп'ютерної мережі мають пакети ключової інформації. Це дозволяє їм обчислити ключі для конфіденційного обміну в межах одного домена.

Для конфіденційної передачі інформації від абонента А абонентові В того самого домена, абонент А шифрує інформацію ключем k_{AB}, що будується на основі ключової інформації абонента А і KDP-схеми даного домена.

Для конфіденційної передачі інформації від абонента А абонентові В сусіднього (що має з доменом абонента А загальний сервер додатка С) домена, А передає С інформацію, зашифровану ключем k_{AC}. Сервер додатка С зашифровує інформацію за допомогою ключа k_{CB}, потім передає інформацію абонентові В, розшифровану ключем k_{AC}.

Для конфіденційної передачі інформації від абонента А абонентові В домена, що не має з доменом елемента А загального сервера додатків, будується шлях від абонента А до абонента В через сервера додатків C_1, C_2, …, C_l... Далі абонент А передає серверу додатків C_1 інформацію, зашифровану ключем k_{AC_1}. Сервер додатків C_1 зашифровує інформацію за допомогою ключа $k_{C_1C_2}$, потім передає інформацію серверу додатків C_2, розшифровану ключем k_{AC_1}, і так далі. Наприкінці сервер додатків C_l передає абонентові В інформацію, зашифровану ключем k_{C_lB}.

Помітимо, що відкритий текст відправника доступний для атак зловмисника через сервери додатків NAS, вони є довіреними вузлами для всіх учасників інформаційного конфіденційного обміну. Якщо шифратор відповідає властивості перестановочності (як, наприклад, блоковий шифратор у режимі гаммування), то розшифруванню в довірених вузлах зв'язку може передувати вторинне зашифрування, що було вище.

Для скорочення операцій розшифрування й зашифрування у вузлах зв'язку можливий наступний варіант: абонент А передає абонентові В ключ K_{AB}, обчислений на основі його ключового пакета, а потім здійснює передачу інформації, зашифрованої ключем K_{AB}.

Ключ зашифрування є значенням геш-функції, застосованої до ідентифікатора абонента В. Передача ключа K_{AB} і інформації здійснюється описаним вище способом.

У результаті виконання магістерської роботи досліджений також спосіб організації конференц-зв'язку коаліції абонентів з різних доменів в умовах нецентралізованого розподілу ключової інформації.

Модифікація протоколу Kerberos для генерації й розподілу ключової інформації

Генерація й розподіл ключової інформації для безпечної мережі може бути організована з використанням модифікації протоколу Kerberos. Запропонована модифікація протоколу Kerberos для генерації й розподілу ключової інформації в комп'ютерній мережі відрізняється тим, що в серверах TGS обчислюються пакети ключової інформації, що доставляються клієнтам із сервера додатків у складі посилок TGT.

Нехай є один або більше серверів автентифікації (AS) і, принаймні, така ж кількість серверів видачі квитків (TGS).

Кожний сервер TGS відповідає одному серверу AS. Кожний домен мережі зв'язується із сервером TGS і абоненти домена прив’язуються до цього TGS.

Якщо сервер додатків NAS утримується в декількох доменів, то він прив’язується до всіх TGS приналежних даним доменам. Всі абоненти мережі підтримують службу одноразових паролів OTPS (One-Time Password Service) з декількома AS, до яких прив'язані

відповідні TGS.

Сервер додатків NAS підтримує службу одноразових паролів однієї або більше OTPS. Абонент A_i і сервер автентифікації AS_j з OTPS мають одноразовий пароль k_{A_i,AS_j}.

На етапі ініціалізації (рисунок 2) кожний сервер AS_j обчислює ключі k_{A_i,TGS_t} для зв'язку з TGS_t і прив'язаних до нього абонентів A_i, k_{NAS_p,TGS_t} для зв'язку TGS_t і прив'язаних до нього NAS_p.

Припустимо, що в кожного AS_j є ключ k_{AS_j,TGS_t} для зв'язку із прив'язаними до нього TGS_t і кожний TGS будує KDP(P,F) - схему для відповідного домена мережі: для кожного абонента A_i або NAS_p цього домена обчислюються пакети S_i, S_s.

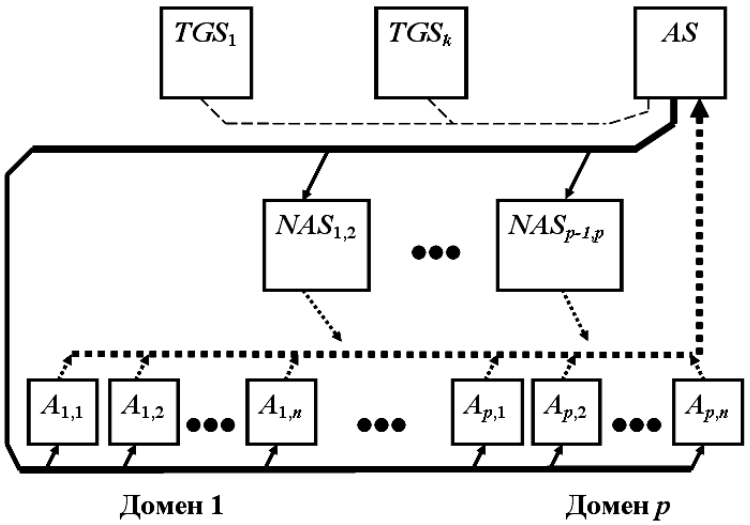

Рисунок 2 – Протокол обміну із сервером автентифікації з метою одержання дозволу на видачу ключової інформації

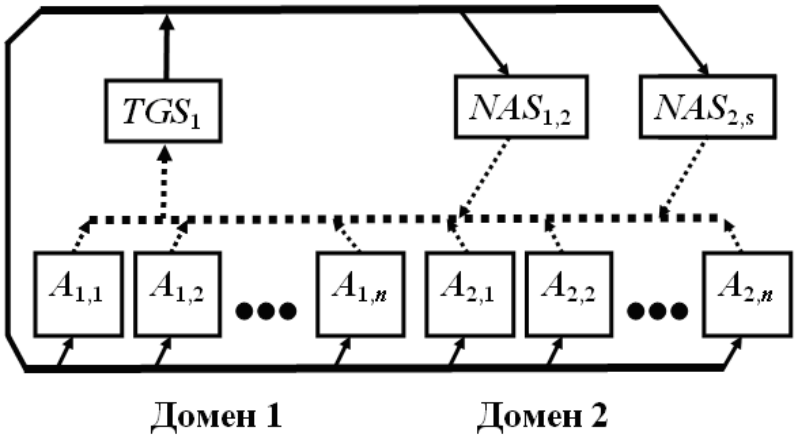

Рисунок 3 – Протокол обміну із сервером TGS з метою одержання ключового матеріалу абонентами мережі А і серверами додатків NAS

Тепер кожний учасник A_i підтримуючу службу одноразового пароля з відповідним сервером автентифікації AS_j, може одержати свій пакет K_i ключової інформації, ініціалізуя й виконуючи протоколи:

a) протокол обміну із сервером автентифікації, з метою одержання дозволу TGT на одержання ключової інформації (рисунок 2);

b) протокол обміну із сервером TGS, з метою одержання ключової інформації (рисунок 3);

Для безпечного обміну інформації між абонентами мережі використовується:

с) протокол комунікації абонентів мережі, у тому числі через сервер додатків NAS (рисунок 4).

Дано оцінки ключової інформації, необхідної для організації захищених комунікацій, для мереж різних типів.

Дані, представлені в таблиці 2 показують переваги використання нецентралізованих 10(KDP(1002, 56) і 10(HAKDP(1002, 56, 10)-схем.

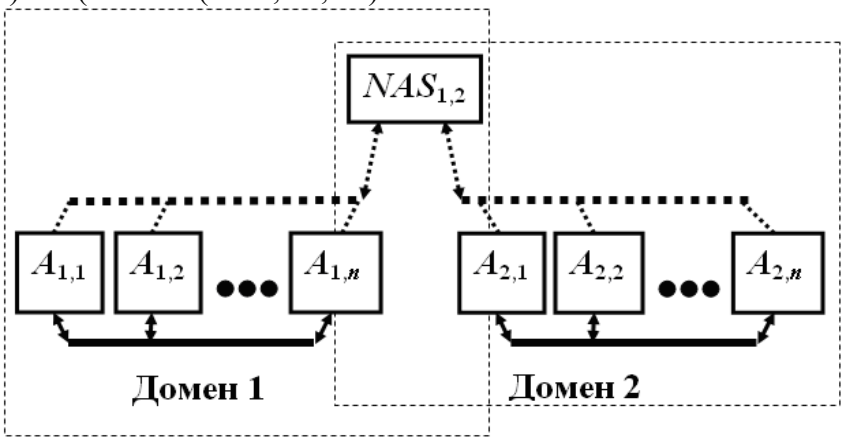

Рисунок 4 – Протокол комунікацій абонентів мережі, у тому числі через сервер додатків NAS

У нецентралізованій мережі в порівнянні із централізованої (таблиця 1), число ключів, що пересилаються від ТА учасникам, скорочується. Застосування схем з гешуванням приводить до ще більшого скорочення середньої довжини пакетів ключової інформації й об'єму ключової інформації, переданої від довіреного центра ТА.

Таблиця 2 – Порівняння нецентралізованої KDP і HAKDP

	Без попереднього розподілу	KDP(10^4,173)-схема	HAKDP(10^4,114,10)-схема
Середня довжина пакета	1 001	37	28
Число переданих ключів	10 030 020	370 740	280 560

Також досліджуються особливості побудови програмних засобів попереднього розподілу ключів. Показано, що при цьому перевага віддається імовірнісним методам двухетапного синтезу схем.

На першому етапі випадково генерується таблиця розподілу ключів, а на другому – перевіряється її відповідність умовам необхідної схеми. Аналітично обґрунтовані параметри керування імовірнісного етапу. Працездатність запропонованих методів підтверджена експериментами з використанням розроблених програмних засобів при різних параметрах вимог до мережі.

Розробка структурної схеми

Структурна схема розробленої системи показана на рисунку 5.

Для реалізації мережі WAN було вибрано технологію приватної мережі на орендованих каналах.

Мережа складається з головного офісу та декількох філіалів. У приміщенні головного офісу знаходяться наступні сервери:

1. Сервер автентифікації.
2. Сервер квитанцій (білетів).
3. Ресурсний сервер.

У приміщеннях філіалів знаходяться:

1. Ресурсні сервери.
2. Робочі станції (хости).

Орендовані територіальні канали прокладаються провайдером транспортних територіальних послуг у його первинній мережі FDM, PDH, SDH або мережі з інтегральними послугами ISDN. При оренді каналу в таких мережах підприємство ділить пропускну здатність магістральних каналів і комутаторів цієї мережі з іншими абонентами даного провайдеру.

На рисунку 5 показаний приклад використання орендованих каналів для побудови корпоративної мережі підприємства із трьома філіями.

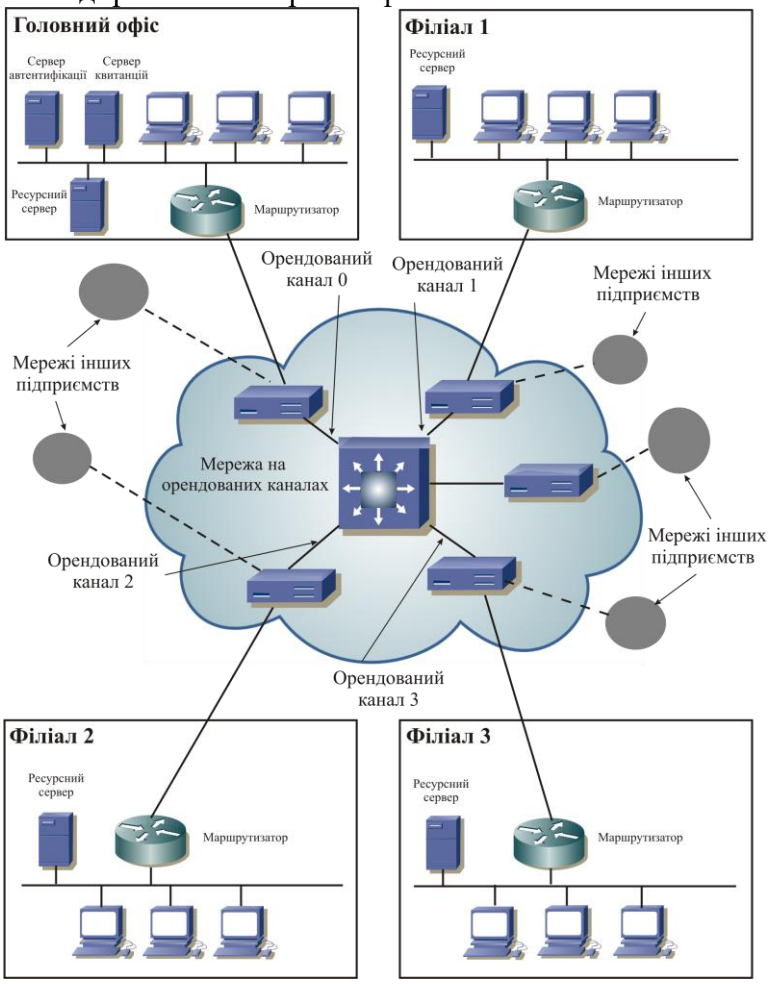

Рисунок 5 – Структурна схема розробленої системи

Канали, що зв'язують центральну мережу підприємства з мережами філій, проходять через мультиплексор, що поєднує канали всіх абонентів у магістральний канал. Незважаючи на те, що територіальні канали в цьому випадку не відносяться до власності підприємства, корпоративні мережі, побудовані на орендованих каналах, також називають часними, принаймні по двох причинах.

По-перше, смуга пропускання орендованого каналу повністю виділяється підприємству, і тому є в деякому змісті його "приватною власністю". Це повною мірою відноситься до орендованих цифрових каналів, які підтримуються провайдером на базі первинної цифрової мережі з технікою мультиплексування TDM. Орендар такого каналу одержує у своє повне розпорядження всю його пропускну здатність – 64 Кбіт/с, 128 Кбіт/с, 2 Мбіт/с, або вище. У застарілих мережах із частотним мультиплексуванням FDM орендар самостійно розпоряджається не пропускною здатністю, а заздалегідь відомою смугою пропущення каналу. У кожному разі, пропускну здатність каналу підприємство-орендар не

ділить ні з ким, і це дуже важливо для створення корпоративної мережі зі стабільними характеристиками.

Наявність гарантованої пропускної здатності дає можливість адміністраторові мережі планувати роботу додатків через глобальні канали зв'язку: розподіляти пропускну здатність каналу між додатками, оцінювати можливі затримки повідомлень, обмежувати обсяг генеруємого територіального трафіку, визначати максимальну кількість активних додатків і т.п.

По-друге, приватний характер мереж, побудованих на орендованих каналах, підтверджується достатньою конфіденційністю даних. Корпоративні дані практично не доступні для абонентів, що не є користувачами корпоративної мережі або співробітниками організації-провайдеру каналів. Дійсно комутацію каналів у первинних мережах може виконати тільки оператор мережі, а рядовому користувачеві така операція недоступна. Це спричиняє більший ступінь захищеності даних, переданих по каналах первинних мереж. Наприклад, тут неможлива типова для Інтернету атака – відгалуження й аналіз "чужого" трафіка іншим користувачем. Таким чином забезпечується прийнятна безпека переданих даних від зовнішніх атак.

Для мережі центрального офісу найкраще підійдуть маршрутизатори Cisco 3620 або Cisco 3640. Конкретна модель маршрутизатора й кількість установлених модулів буде залежати від покладеного на маршрутизатор завдання.

Моделі серії 3600 надають функціонально повне рішення для організації віддаленого доступу. Інакше кажучи, дані пристрої можуть використовуватися як потужний сервер доступу. Будь-яка модель Cisco 3600 може забезпечувати надійний доступ до Вашої WAN численних віддалених і мобільних користувачів. При цьому вони зможуть не тільки працювати з файловим господарством WAN, як зі своїм власним, але також використовувати загальні програмні додатки.

Дана серія маршрутизаторів є відмінними засобом вкладення коштів, при якому Ви зможете легко в майбутньому змінювати конфігурацію Вашої глобальної мережі в міру росту вимог до кількості з'єднань або в міру появи нових технологій для глобальних обчислювальних мереж. Все це забезпечує захист інвестицій у встаткування й, отже, економію грошей. Моделі Cisco 3600 мають достатню масштабованість. Наприклад, модель Cisco 3640 підтримує інтерфейси ISDN PRI (Primary Rate Interface) або ISDN BRI (Basic Rate Interface) у тому самому шасі: максимальне число підтримуваних PRI-з'єднань – шість, BRI-зєднань – 24, а модель Cisco 3620 може бути сконфігурована з одним портом Ethernet і одним портом ISDN PRI, або одним портом Ethernet і чотирма портами ISDN BRI. В усі моделі сімейства Cisco 3600 інтегрована міжмережева операційна система Cisco IOS, що підтримує встановлення з'єднань на вимогу, що забезпечує об'єднання локальних мереж, безпека доступу й даних і оптимізацію з'єднань із глобальними обчислювальними мережами. Завдяки підтримці повного набору функціональних можливостей Cisco IOS, маршрутизатори серії Cisco 3600 дають надійні й гнучкі засоби роботи з Інтернетом/Інтранетом мультимедійними додатками. Cisco IOS робить легкою не тільки роботу через Інтернет, але спрощує й підвищує ефективність роботи у корпоративній мережі Інтернет. Маршрутизатори сімейства Cisco 3600 надають відмінну можливість вибору конфігурації. Так, наприклад, модель Cisco 3640 має чотири слота під мережеві модулі, а модель Cisco 3620 – два слоти. У кожний слот по вибору можуть бути встановлені мережеві модулі для Інтернет і Token Ring, а також можна вибирати із цілого набору інтерфейсних карт для з'єднання із глобальними обчислювальними мережами. Кожне рознімання для мережевих модулів може прийняти інтерфесні карти мережевих модулів різного типу, включаючи ISDN PRI, ISDN BRI, і асинхронні/синхронні послідовні інтерфейси.

Інакше кажучи, по наявній лінії зв'язку можна легко об'єднати за допомогою Cisco 3640 WAN із чотирма іншими локальними мережами, розташованими в інших кінцях міста, і працювати в них, як у власній мережі й навіть використовувати їхнє устаткування (наприклад, високоякісний принтер).

Сімейство Cisco 3600 надає користувачеві можливість ефективного й недорогого використання додатків Інтернету/Інтранету і можливість масштабування подібних рішень при збільшенні потреб або зміні структури віддаленого доступу.

Пропонуючи повну інтеграцію мережевого маршрутизатора й сервера для ISDN, асинхронних і синхронних з'єднань WAN в одному продукті, Cisco 3600 дає користувачеві нову платформу для майбутніх додатків, що є негайним рішенням сьогоднішніх проблемам.

Для віддалених офісів (філій) найкраще підійдуть маршрутизатори серій Cisco 2500 або Cisco 2600. Конкретна модель маршрутизатора й кількість встановлених модулів буде залежати від покладеного на маршрутизатор завдання.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Досліджена система розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. На основі отриманих результатів досліджень створена програмна реалізація системи розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання розподілу ключів в мережі Cisco SD-WAN, що базується на хмарній архітектурі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
2. Смірнов О.А., Дрєєва Г.М., «Метод генерування фрактального трафіку за допомогою моделі генератора на графі» у Інформаційна безпека та інформаційні технології: монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139.
3. Смирнов А.А., Коваленко А.В. Комплекс математических моделей технологии тестирования web-приложений. Інформаційні технології: сучасний стан та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: ТОВ «ДІСА ПЛЮС», 2018. – 461 с.
4. Смирнов А.А., Коваленко А.В. Разработка метода управления рисками разработки программного обеспечения. Інформаційні технології: проблеми та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: Видавець Рожко С.Г., 2017. – 447 с.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98. 2022. (Фахове видання. Категорія «Б»)
6. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
7. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
8. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus).
9. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
10. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
11. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).

12. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus).
13. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus).
14. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379. (Scopus).
15. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
16. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
17. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).
18. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus).
19. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus).
20. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019. (Scopus).

УДК 811.161.1'276:33

Н. Глевацька, магістр гр. ПР-71м
Центральноукраїнський національний технічний університет

ДЕЯКІ ОСОБЛИВОСТІ ПЕРЕКЛАДУ УКРАЇНСЬКОЮ МОВОЮ МЕТАФОРИ НА МАТЕРІАЛАХ НАУКОВО-ЕКОНОМІЧНОГО СТИЛЮ

Стаття досліджує актуальну проблему перекладу метафор у науково-економічних текстах. Для досягнення цих цілей використовуються методи зіставного аналізу, метод словникових дефініцій, описовий метод та метод міжмовної перекладної особливості. Автор статті проводить аналіз специфіки економічного стилю, вивчає термінологію та виявляє особливості перекладу метафоричних висловів та концептів. Об'єкт дослідження є способи перекладу економічних термінів, а предметом дослідження є безпосередньо економічні тексти, які підлягають перекладу. Узагальнюючи, стаття пропонує важливий внесок у вивчення проблем перекладу метафор у науково-економічних текстах.

переклад метафор; українська мова; науково-економічний стиль; особливості перекладу; метафоричні вислови.

Постановка проблеми. Дослідження проблеми перекладу метафор на матеріалах науково-економічного стилю має велику актуальність в сучасному світі. Зростаюча глобалізація та міжнародна співпраця у галузі економіки створюють потребу в ефективному спілкуванні між різними мовами та культурами. Відповідно, переклад метафор у науково-економічних текстах має важливе значення для забезпечення чіткості, точності та зрозумілості інформації.

Проблема полягає у тому, що метафори в науково-економічному стилі мають специфічні концептуальні значення та контекстуальні нюанси, які можуть бути складні для передачі в інші мови. Додатково, культурні різниці та відмінності у менталітеті можуть