ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 004.738.5.056 doi: 10.32620/reks.2019.4.11

АХМЕД ВАЛІД АЛЬ-ХАФАДЖІ, О. О. СОЛОВЙОВ, Д. Д. УЗУН, В. С. ХАРЧЕНКО

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Україна

МЕТОД АНАЛІЗУ РИЗИКІВ ДОСТУПУ ДО АКТИВІВ В СИСТЕМАХ ФІЗИЧНОГО ЗАХИСТУ

Предметом вивчення в статті є методи аналізу ризиків доступу до активів всередині фізичного об'єкта. Як прикладі розглядається об'єкт системи фізичної безпеки наукової установи (як блок територіального елемента) з апаратним оточенням у вигляді пристроїв з низьким енергоспоживання і функціонуванням в середовищі Інтернету речей. Метою є створення теоретико-математичної моделі та методу аналізу внутрішніх компонентів системи безпеки і доступу до активам. Поставлені завдання охоплюють розробку підходу до аналізу рівня безпеки, яка забезпечується встановленою системою фізичної безпеки і формування підходу до проникнення з метою доступу до активів. При вирішенні завдань були використані такі методи, як просторовий аналіз фізичного розподілу елементів системи, формування графів маршруту, декомпозиція блоків і алгоритмів фізичного захисту, дослідження повного набору компонентів і індивідуально орієнтованого елемента забезпечення безпеки. Отримані наступні результати: розроблено підхід до аналізу рівня безпеки фізичного об'єкта з використанням базових параметрів, що складаються з фізичних та інформаційних змінних існуючих множинних активів, побудована математична модель компонентів системи, блочного орієнтування периметра об'єкта, запропонована послідовність етапів проникнення на захищений об'єкт з використанням безлічі маршрутів. Висновки: наукова новизна отриманих результатів полягає в наступному: удосконалено метод аналізу захищеності активів за рахунок використання змінних оточення і елементів контролю фізичної безпеки об'єкта, а також генерації та оцінювання маршрутів проникнення на об'єкт з метою доступу до критичних активів.

Ключові слова: *FMECA; PSMECA; куб критичності; фізична безпека; кібербезпека; система фізичної безпеки; аналіз приміщення; IoT; безпека; дерево атак.*

Вступ

Якщо брати до уваги те, що об'єктивно безперечно існує набір позитивних сценаріїв використання науково-технічних досягнень, то також, звичайно, необхідно враховувати потенційно деструктивні дії та/або сценарії. Однією з систем, на котру такі руйнівні дії можуть бути спрямованими, є системи фізичної безпеки (СФБ, англ. physical security systems, PSS) складних об'єктів (наприклад, будівлі державних установ, університети тощо).

Сучасні СФБ є складними комп'ютеризованими системами, призначені для забезпечення захисту фізичного простору, відповідних фізичних активів [1-3]. Вони мають відповідати загальним і спеціальним вимогам, зокрема, до надійності, кібербезпеки інформаційних ресурсів, швидкодії, тощо. При цьому важливо, щоб відповідні системні ресурси слід розподіляти відповідним чином, а засоби детектування – розподіляти у найкращій спосіб залежно від активів, які захищаються.

1. Постановка завдання і визначення початкових параметрів

У представленій статті розглядається задача аналізу рівня безпеки (захищеності активів), яка забезпечується системою фізичної безпеки. В процесі розробки визначаються і досліджуються такі параметри і поняття.

1. Фізичний двомірний простір (PhSp), котрий може бути описаний планом поверхів, щ являє собою набір кімнат з відомими із безлічі $\mathrm{SE} = \sum \mathrm{E_1 Y_1}$ входами, вікнами, товщиною стін [1].

2. Множина використовуваних засобів фізичного контролю [2], яка визначається датчиками переміщень, камерами відеоспостереження, контролю доступу та їх розміщення в просторі PhSp (рис. 1). Кожен з входів і вікон має свої координати $\left\{\mathrm{X_{El} Y_{El}}\right\}$ та $\left\{\mathrm{X_{Wq} Y_{Wq}}\right\}$ відповідно.

$$\mathrm{SSen} = \bigcup_{i=1}^{m} \mathrm{SSen}_j^i = \bigcup_{i=1}^{m} \bigcup_{j=1}^{mi} \mathrm{SSen}_j^i, \qquad (1)$$

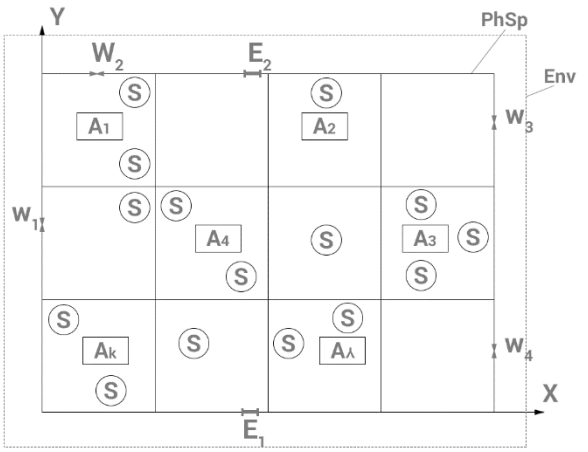

Рис. 1. Розміщення в просторі PhSp

де $SSen_j^i$ - множина сенсорів і-го типу;

m – число типів сенсорів, розміщених в просторі $PhSp(X_i Y)$;

$SSen_j^i$ – сенсор j з множини сенсорів і-го типу;

m_i - число сенсорів і-го типу, використаних для контролю. Тобто загальне число сенсорів, які використовуються в системі:

$$mS = \sum_{i=1}^{m} m_i. \qquad (2)$$

Кожному сенсору Sen_j^i відповідає вузол координат, а також ймовірність виявлення порушника P_{Si}, яка може здаватися в нечітких значеннях (Висока - L, Середня - M, Низька - S) [8].

3. Множина фізичних або інформаційних з відомих фізичних множин існуючих активів $SA = \{A_k\}_{k=1}$, котрі знаходяться в просторі PhSp. Кожному активу $A_k \in SA$, відповідають координати фізичного розміщення у просторі $\{X_{Ak} Y_{Ak}\}$, а також деякий показник важливості активу I_k:

$$A_k \sim \{X_{Ak}, Y_{Ak}, I_k\}. \qquad (3)$$

Активи можуть бути збудовані в ряд переваги з урахуванням показань I_k:

$$A_q > A_\lambda > \ldots > A_\beta, \qquad (4)$$

де > – знак переваги, який визначається значенням I_k, відранжувати за відносним значенням показника важливості активу δI_k, обчислюється за формулою:

$$\delta I_k = \frac{I_k}{\sum_{e=1}^{\lambda} I_e}. \qquad (5)$$

4. Вимоги до неврахованому ризику доступу до активу $A_k - Risk_R A_k$, який може здаватися ймовірністю доступу до активу P_{Ak} або в термінах нечітких змінних (низький, середній, високий, то що) [4]. Тоді вимоги до СФБ можуть формулюватися набором значень $\{Risk_R A_k\}_{k=1}$ або сумарною величиною незмінного ризику доступу до активів:

$$Risk_\Sigma A = \sum_{k=1}^{\lambda} RiskA_k. \qquad (6)$$

2. Послідовність рішення

1. Визначається підмножина активів $\Delta SA \subset SA$, для якого необхідно провести аналіз ризику доступу до них. Це підмножина або задається, або знаходиться виходячи з вимог до ФСБ. Далі розглядаємо варіант, коли один з активів визначено як пріоритетний, тобто $Card\Delta SA = 1$ і відомий A_k^* як пріоритетний. Особливості вирішення задачі для випадку $Card\Delta SA > 1$ будуть розглянуті далі [5].

2. Для актива A_k^* визначаються:

а) множина точок входу $SB = \left\{B_{A_k^*}\right\}_{i=1}^{k}$ від яких може бути розпочато рух порушника до активу A_k^*;

б) множина точок входу $SB_{A_k^*}$ є підмножиною об'єднаної множини SE та SW:

$$SB_{A_k^*} \subset SE \bigcup SW. \qquad (7)$$

Множина маршрутів $SR_{A_k^*}$ можливого руху порушника до активу A_k^*, яке є об'єднанням підмножин таких маршрутів для кожної з точок $B_{A_k^* z} \in SB_{A_k^*}$, тобто:

$$SR_{A_k^*} = \bigcup_{v:B \in B_{A_k^*}} \bigcup_{\mu=1}^{вх} SR_{A_{k\mu v}^*} \qquad (8)$$

Слід зазначити, що маршрути $SR_{A_{k\mu v}^*}$ можуть прив'язуватися до координат сенсорів, які знаходяться на цьому маршруті і можуть виявити порушника [6]. Тоді будь-який шлях $SR_{A_{k\mu v}^*}$ може бути представлений безліччю сенсорів, в які можуть попе-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

редньо зафіксувати порушника (якщо знехтувати відстанню між сенсорами і природними перешкодами на шляху) [12]:

$$\forall SR_{A^*_{k\mu\nu}} \sim Sen_{k,\mu,\nu,\varepsilon=1}^{\lambda k,\mu,\nu}, \quad (9)$$

де $\lambda k,\mu,\nu$ – число таких сенсорів на шляху $SR_{A^*_{k\mu\nu}}$. Множина таких шляхів може бути представлено на графі: $G\left(A^*_k\right) = \{V, \Psi\}$, у якому V – множина вершин, що складається з вершин [7], яким відповідають активи A^*_k та сенсори з безлічі $SR_{A^*_k}$:

$$V = \left\{A^*_k, SR_{A^*_k}\right\}, \quad (10)$$

коли Ψ – відображення елементів множини самих на себе ребер графа. В даному випадку воно є виродженим, оскільки відображення описує послідовність елементів - сенсорів в сумі $\left\{Sen_{k,\mu,\nu,\varepsilon=1}^{\lambda k,\mu,\nu}\right\}$ [13]. Загальний вигляд графа представлений на рис. 2;

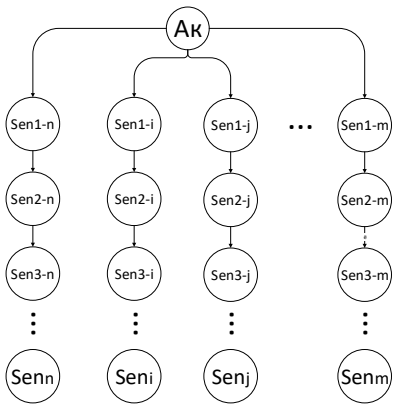

Рис. 2. Загальний вид графа

в) здійснюється аналіз маршрутів і для кожного маршруту $SR_{A^*_{k\mu\nu}} \in SR_{A^*_k}$ оцінюється ризик не виявлення порушника. Для цього:

- кожному маршруту $SR_{A^*_{k\mu\nu}}$ встановлюється відповідно коефіцієнт значень ризику (ймовірності) не виявлення порушника [14]:

$$\overline{P}_s(SR_{A^*_{k\mu\nu}}) \sim \left\{\overline{P}_{s\lambda}\right\},\ Sen_\lambda \in SR_{A^*_{k\mu\nu}}; \quad (11)$$

- обчислюється загальне значення ймовірності виявлення / невиявлення порушника:

$$P_s / \overline{P}_s(SR_{A^*_{k\mu\nu}}); \quad (12)$$

г) визначається підмножина маршрутів з незначними ризиками доступу до активу, тобто таких, для яких:

$$\overline{P}_s(SR_{A^*_{k\mu\nu}}) > RiskA^*_k. \quad (13)$$

У цьому завданню розглядається ситуація з одноразовою спробою проникнення до активу A^*_k;

д) для маршрутів з недоречними ризиками формується рекомендації [9] щодо зниження ризику методом:

- установки додаткових сенсорів;
- виявлення сенсорів з більшою ймовірністю виявлення;
- переміщення активу в пристрої PhSp.

3. План досліджуваного приміщення

Даний макет являє собою план будівлі наукової організації, в якому проводиться навчання студентів (рис. 3). У будівлі є приміщення для проведення лекцій, семінарів, лабораторних робіт, учнівські бібліотеки, адміністративні кімнати для розміщення персоналу. Також є об'ємний хол, пункт прийому їжі, наскрізна шахта ліфта і дублюючі її ступені, санітарні вузли, зони контролю входу та виходу для співробітників та учнів. Конструктивно будівля являє собою монолітне будова з зовнішніми і внутрішніми несучими стінами. Внутрішнє зонування приміщень виконано з використанням роздільних стін з комбінованих матеріалів.

4. Аналіз системи безпеки об'єкта

Формування звіту про безпеку системи починається з побудови маршруту потенційного зловмисника в умовах визначеного об'єкта від точок входу до критичної зони. Маршрутний вектор враховує можливі варіанти доступу до критичної інформації відштовхуючись від координаційної розташування периметра, будови, кімнати і детального розміщення спеціалізованого обладнання [13]. У схему маршруту вноситься також склад фізичних матеріалів, щільність поверхні, елементи взаємодії. Нижче наведена загальна схема потенційних маршрутів (рис. 4). Кожна гілка маршруту відповідає за певний порядок дій зловмисника. Певний вузол відображає стан або ж тип елемента, який зустрічається в процесі процедури проникнення. Побудова дерева може здійснюватися в двох напрямках.

Перший варіант - це побудова від вузла критичної інформації до точки входу. Третій варіант - від точки входу до вузла критичної інформації. Кількість

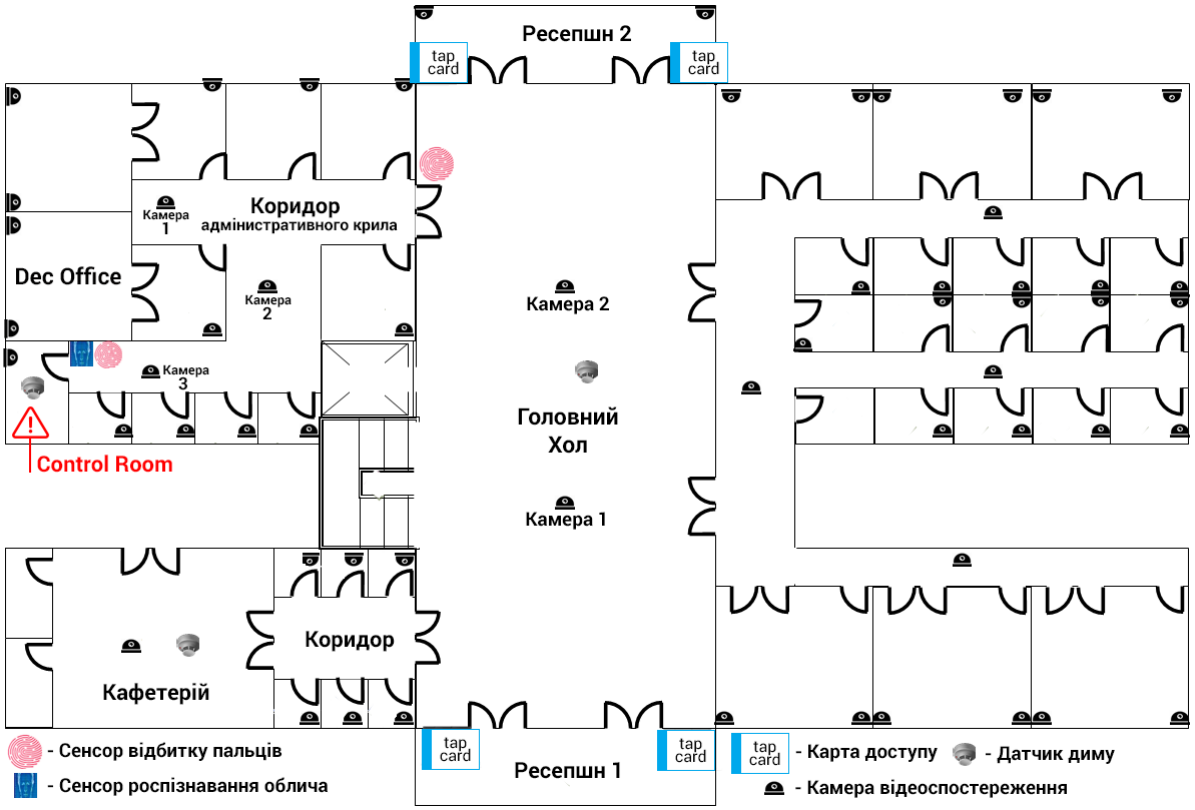

Рис. 3. План досліджуваного приміщення

вузлів може зростати в залежності від типу маршруту, наявності багаторівневих точок входу і елементів системи безпеки. Далі представлений потенційний маршрут зловмисника до критичної зоні CR (Controll Room).

Маршрут 1. Проникнення в приміщення починається через вузол «Ресепшн 1». Для доступу в головний «Хол» використовується «Карта доступу». У головному холі є спрямована на вхід «Камера відеоспостереження 1» і «Датчик диму» по центру приміщення. Через «Хол» маршрут проляже в прохідній «Коридор» без систем безпеки. Далі в центрі «Кафетерію» встановлена спрямована на портал між прохідним «Коридором» і «Кафетерієм» «Камера відеоспостереження» і «Датчик диму».

Портал між кафетерієм і клієнтським холом кафетерію не проглядається. Дана область не передбачає систем безпеки. Внутрішня площа «Кафетерія» межує із зовнішньою стіною критичної зони. Виходячи з плану об'єкта, можна зробити висновок, що зовнішня стіна критичної зони не є несучою. Цей факт створює можливість фізичного проникнення в «Control Room» і отримання доступу до вразливої інформації. Усередині «Control Room» також є «Камера відеоспостереження» і «Датчик диму».

Маршрут 3. Проникнення в приміщення починається через вузол «Ресепшн 2» Периметр вузла проглядається за допомогою двох «Камер відеоспостереження». Для доступу в «Головний хол» використовується «Карта доступу». У «Головному холі» є спрямована на вхід «Камера 2» і «Датчик диму» по центру приміщення. Перехід з холу в «Коридор адміністративного крила» контролюється «Сенсором відбитку пальців». Периметр коридору проглядається трьома камерами відеоспостереження. «Камера 1» фіксує вхід в коридор і входи в сторонні адміністративні приміщення. «Камера 2» фіксує геометричне викривлення коридору. «Камера 3» не фіксує рух в процесі проникнення.

В кінці коридору є глуха стіна, яка дозволяє в разі фізичного руйнування отримати доступ в «Dec Office».

Внутрішня площа «Dec Office» межує із зовнішньою стіною критичної зони. Виходячи з плану об'єкта, можна зробити висновок, що зовнішня стіна критичної зони не є несучою. Цей факт створює можливість фізичного проникнення в «Control Room» і отримання доступу до вразливої інформації. Усередині «Control Room» є «Камера відеоспостереження» і «Датчик диму».

Побудова маршрутів дає можливість детально вивчити існуючі компоненти, які зустрічаються на шляху зловмисника в процесі проникнення. Таким чином, визначаються найбільш вразливі елементи

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

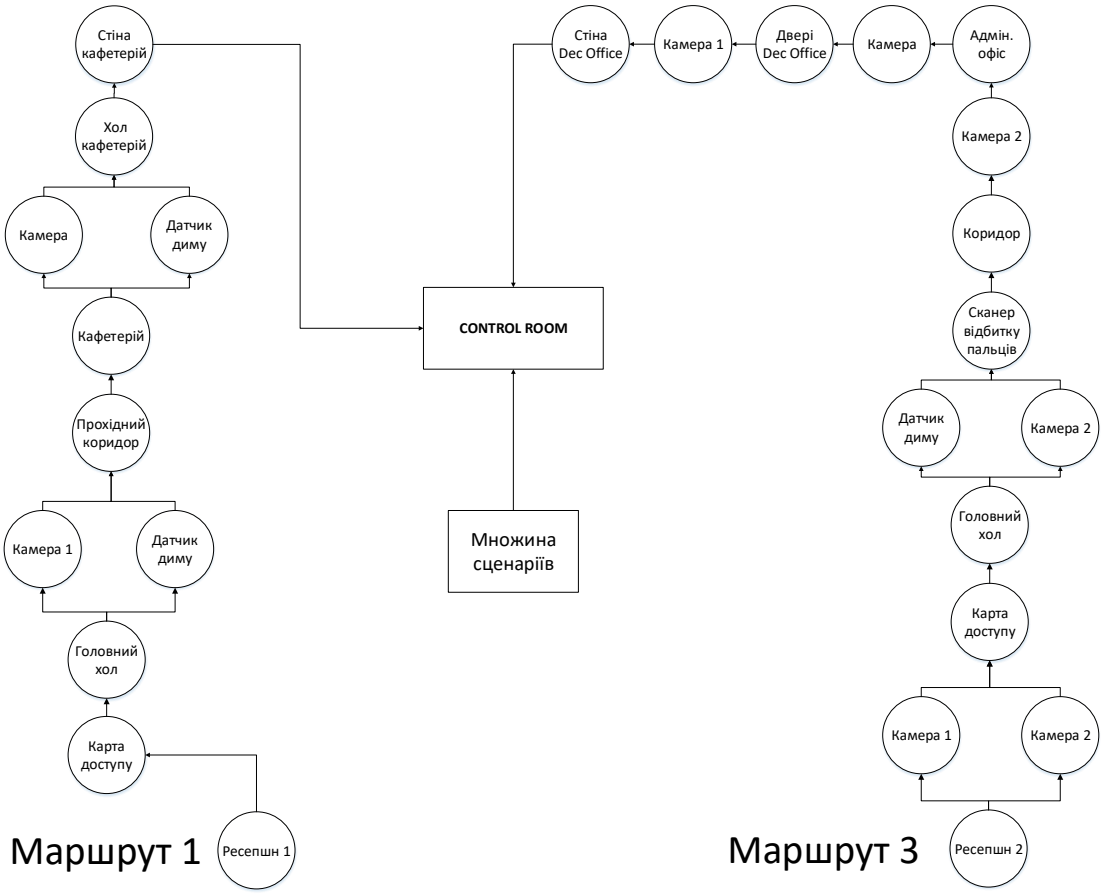

Рис. 4. Схема потенційних маршрутів

системи. Наступним етапом є формування графа компонентів і розстановка вагових коефіцієнтів для кожного вузла безпеки [13].

Знаходження y_i дає можливість порівняти рівень вразливості маршруту, використовуючи підхід із застосуванням нечіткої логіки (fuzzy logic). Для цього необхідно визначити мінімальне і максимальне значення всіх вузлових коефіцієнтів на певних маршрутах.

5. Обробка коефіцієнтів

Кожен вузол безпеки має свій ваговий коефіцієнт. Розмір коефіцієнта залежить від класифікації та рівня устаткування, яке використовується всередині як окремого приміщення, так і системи в цілому (табл. 1).

Загалом конструктивному плані системи може бути безліч приладів забезпечення безпеки, такі як камери високої роздільної здатності, датчики руху, датчики диму, біометричні системи розпізнавання відбитків пальців і сканування сітківки ока, системи зчитування обсягу і ваги, інфрачервоні прилади зчитування положення предметів, карти, чипи зонування простору та інше [3].

Класифікація і рівень обладнання безпосередньо пов'язаний з призначенням приладу або ж компонента, точності даних, одержуваних в процесі взаємодії, типом надійності і стійкості до фізичних та електронним втручанням у функціонування. Загальний формат вагових коефіцієнтів поділяється на три рівні: Low, Medium, High. Нижче наведена таблиця з розстановкою вагових коефіцієнтів приладів, використовуваних у цій системі безпеки (табл. 2).

Загальний вигляд графа коефіцієнтів компонентів системи являє собою послідовність перешкод, які повинен подолати зловмисник в процесі отримання доступу до критичної інформації (рис. 5).

Для виконання прорахунку вузлових коефіцієнтів використовується формула:

$$y_i = \sum x_n, \qquad (13)$$

Таблиця 1

Прилади системи безпеки

Назва	Розміщення	Призначення	Пояснення	Рівень	Значення
Камера	Приміщення	Відеофіксація оточення	CCTV. Базовий елемент системи безпеки. Фіксує стан довіреного периметра	Medium	2
Датчик диму	Приміщення	Фіксація задимлення	Реагує на домішки хімічних елементів в повітрі.	Low	1
Сканер дактилоскопії	Приміщення	Система доступу	Біометрична система зонування простору	High	3
Сканер сітківки ока	Приміщення	Система доступу	Біометрична система зонування простору	High	3
Карта доступу	Приміщення	Система доступу	Фізична система зонування простору	Medium	2
Стіна	Приміщення	Зонування простору	Фізична система зонування простору	Low	1
Стіна несуча	Приміщення	Конструктивне	Фізична система зони	Medium	2

Таблиця 2

Вагові коефіцієнти

Рівень	Значення
Low	1
Medium	2
High	3

де y_i – значення всіх вузлових коефіцієнтів на і-му маршруті, x_n – вага n-го вузлового коефіцієнта на певному і-му маршруті. Такий підхід дозволяє розглянути і деталізувати всі елементи маршруту.

$$\min = f(y_1, y_2, \ldots y_i), \quad \max = f(y_1, y_2, \ldots y_i). \tag{14}$$

Спираючись на отримані значення min і max, отримуємо максимально і мінімально уразливі маршрути, де min – максимально уразливий маршрут, max – мінімально уразливий маршрут відповідно.

Такий підхід дозволяє визначити вразливість системи в цілому, виявити сприятливий для проникнення маршрут і виконати заходи з модернізації з метою модифікації систем безпеки і підвищення рівня захищеності. Розглядаючи показники декількох маршрутів з'являється можливість захистити об'єкт за рахунок модифікацій всіх доступних максимально вразливих маршрутів до певної межі S, який визначається середнім значенням від максимальної величини найбільшої суми вузлових коефіцієнтів маршрутів. Далі для прикладу виконується розрахунок вузлових коефіцієнтів для кожного маршруту індивідуально.

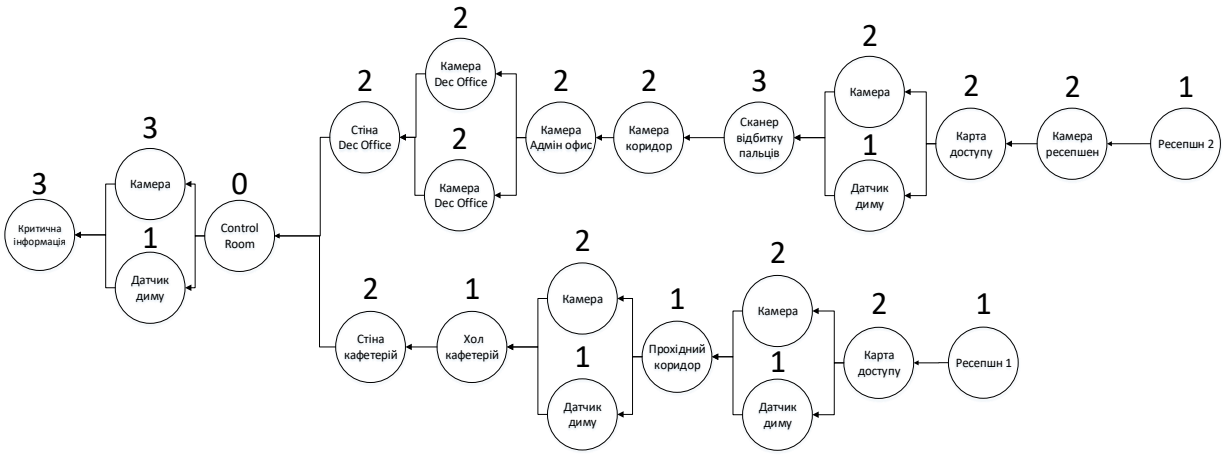

Рис. 5. Загальний граф коефіцієнтів компонентів системи

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Маршрут 1. Відштовхуючись від формули (13) розраховується кількість вузлів. Кожен вузол має свій ваговий коефіцієнт, який закріплений виходячи з технічної інформації про застосовуваний приладі. У загальному уявленні ми маємо наступний вид :

$$y_1 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9,$$

при детальному розгляді виходить:

$$\begin{aligned} y_{\text{маршрут1}} &= 1_{\text{Вхід}} + 2_{\text{Карта доступу}} + \\ &+2_{\text{Камера}} + 1_{\text{Датчик диму}} + 1_{\text{Прохідний коридор}} + \\ &+2_{\text{Камера}} + 1_{\text{Датчик диму}} + 1_{\text{Хол кафетерія}} + \\ &+2_{\text{Стіна кафетерія}}, \end{aligned} \quad (15)$$

де сума всіх коефіцієнтів дорівнює $y_1 = 9$. За аналогією прораховуються наступні маршрути.

Маршрут 3.

$$\begin{aligned} y_{\text{маршрут3}} &= 1_{\text{Вхід}} + (2_{\text{Камера ресепшн}}) \times 2 + \\ &+2_{\text{Карта доступу}} + 2_{\text{Камера}} + 1_{\text{Датчик диму}} + \\ &+3_{\text{Сканер відбитка}} + (2_{\text{Камера коридора}}) \times 2 + \\ &+2_{\text{Камера Адмін офіс}} + \left(2_{\text{Камера Dec Office}}\right) \times 2 + \\ &+2_{\text{Стіна Dec Office}}, \end{aligned} \quad (16)$$

де сума всіх коефіцієнтів дорівнює $y_3 = 13$.У підсумку отримуємо характеристику маршрутів зображену на таблиці 3

Таблиця 3

Прилади системи

Маршрут	Кількість вузлів	Сума вузлових коефіцієнтів
y_1	9	13
y_3	13	25

З отриманих вузлових коефіцієнтів визначаємо мінімальне і максимальне значення. У разі якщо коефіцієнти рівні, пріоритет вибору розглядається в сторону більшої кількості вузлів

$$\min = f(y_1, y_3), \quad \min = f(13, 23) = 13. \quad (17)$$

Отже, максимально уразливий маршрут є маршрут y_1, який має 9 елементів безпеки

$$\max = f(y_1, y_3), \quad \max = f(13, 25) = 25. \quad (18)$$

Значення мінімально уразливого маршруту дорівнює 25. У разі збігу зі значеннями сум вузлових коефіцієнтів в маршрутах, наприклад, y_2 и y_3, має сенс відштовхуватися від кількості вузлів в маршрутах, пріоритет вразливості буде присвоєно маршруту y_3, тому що він використовує більшу кількість елементів безпеки.

Далі слідує побудова PSMECA таблиці елементів, використовуючи компоненти з критичної зони і максимально уразливого маршруту.

6. Побудова PSMECA таблиці

Процес створення PSMECA таблиць починається з розроблення подібних (базових або початкових) FMECA таблиць, які модифікуються відповідно до розробленої теоретико-множинної моделі компонентів системи фізичної безпеки. Основною метою такої модифікації є поглиблення структури аналізованих джерел відмов системи, щоб забезпечити більш строго формалізований підхід, заснований на додаткових елементах структури та рівнях ієрархії.

Таким чином, для аналізу проекту першого поверху досліджуваного об'єкта першим етапом буде розробка FMECA таблиці охоронних систем головного приміщення (табл. 4). Під головним приміщенням ми розглядаємо головну кімнату контролю безпеки об'єкта [14, 15].

Для забезпечення охорони та доступу до головної кімнати контролю безпеки об'єкта використовується біометрична система сканування обличчя та відбитку пальців. У приміщенні, навпроти вхідної двері, встановлена CCTV камера. На стелі встановлено датчик диму, на випадок задимлення приміщення у випадку пожежі або стороннього впливу. FMECA таблиця для підсистеми, що функціонує в нормальному режимі модифікована у схожу PSMECA таблицю у відповідності до теоретико-множинної моделі компонентів системи фізичної безпеки. Розроблена PSMECA таблиця (табл. 5) може використовуватися для встановлення більш детальних причинних зв'язків між підсистемами, їх типами відмов та ризиками безпеки PSS [14, 15].

Базуючись на отриманих даних, створюється PSMECA матричне подання до вразливостей в вигляді таблиці можливого взлому (табл. 6).

Подібний підхід побудови PSMECA таблиць застосовується і до елементів безпеки (табл. 7) раніше визначених уразливих маршрутів. Виходячи з отриманих даних, максимально вразливим маршрутом є y_1, який має 9 елементів безпеки.

Деякі елементи можуть дублюватися і мати різну координаційну орієнтацію, зі збереженням рівного функціоналу [11]. Це створює необхідність для наочності представити перелік елементів в таблиці для подальшого аналізу.

Таблиця 4

FMECA таблиця для елементів підсистеми критичної зони, що функціонує в нормальному режимі

Підсистема	Тип відмови	Режим відмови	Причина відмови	Наслідок відмови	P	S	M	C
Елемент керування камерою	HW	Не запускається	Помилка установки або аварійне припинення (переривання)	Моніторинг руху в межах контрольованого периметру вимкнено	L	H	L	H
		Неправильне функціонування			M	M	M	M
	SW	Не працює	Помилка персоналу або проектна помилка		L	H	M	H
		Немає відгуку			L	M	M	M
Біометрична система розпізнавання обличчя	HW	Не запускається	Помилка установки або аварійне припинення (переривання)	Несанкціонований доступ до захищеної зони	L	H	L	H
		Неправильне функціонування			M	M	M	M
	SW	Неправильне функціонування	Помилка персоналу або проектна помилка		L	M	M	M

Таблиця 5

PSMECA таблиця для елементів підсистеми критичної зони, що функціонує в нормальному режимі

Підсистема	Тип відмови			Режим відмови	Причина відмови	Наслідок відмови	P	S	M	C
Елемент керування камерою	HW	pf	hpf	Не запускається	Помилка установки або аварійне припинення (переривання)	Моніторинг руху в межах контрольованого периметру вимкнено	L	H	L	H
		df	hif				M	M	L	H
		hf	hpf	Неправильне функціонування			M	M	M	M
			hif				M	M	L	M
		if	pif	ip(n)f			M	M	L	M
							M	M	L	M
	SW	df	hpf	Не працює	Помилка персоналу або проектна помилка		L	H	M	H
		hf	hif	Немає відгуку			L	M	M	M
		if	ipf	ip(a)f			M	L	L	L
			iif	ii(n)f			L	L	M	L
							L	L	M	L
Біометрична система розпізнавання обличчя	HW	pf	hpf	Не запускається	Помилка установки або аварійне припинення (переривання)	Несанкціонований доступ до захищеної зони	L	H	L	H
		df	hif				L	H	L	H
		hf	hpf	Неправильне функціонування			M	M	M	M
		if	ipf				M	L	L	M
			iif				M	L	L	M
	SW	df	hif	Неправильне функціонування	Помилка персоналу або проектна помилка		L	M	M	M
		hf	hpf				L	M	M	M

Таблиця 6

Матриця можливого взлому

Ймовірність відмови	Тяжкість взлому		
	Низька	Середня	Висока
Низька	L	M	**H**
Середня	M	M	**H**
Висока	**H**	**H**	**H**

Таблиця 7

Елементи безпеки

Назва	Взаємодія	Кількість
Вхід	Фізична	1
Карта доступу	Електрона	1
Камера	Електрона	2
Датчик диму	Електрона	2
Прохідний коридор	Фізична	1
Хол Кафетерія	Фізична	1
Стіна кафетерія	Фізична	1

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Наступним етапом є аналогічна побудова FMECA та PSMECA таблиці підсистем, які використовуються в уразливому маршруті. Після проведених розрахування та аналізу системи формується за допомогою спеціалізованого програмного забезпечення [10] об'єктне уявлення PSMECA розрахунків у вигляді куба критичності (рис. 6)

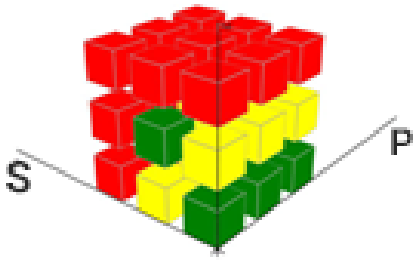

Рис. 6. Представлення PSMECA таблиці

Таким чином, на основі отриманих результатів від таблиць PSMECA можна визначити слабкі сторони системи на основі уразливого маршруту з метою доповнення, модернізації або повторного розгляду підбору компонентів системи безпеки.

Висновки

На основі досліджуваної схеми фізичної безпеки були отримані наступні результати роботи:

- розроблено структурна декомпозиція системи фізичної безпеки;

- запропоновані прикладні рішення для реалізації стандартних функцій підсистем у об'єкті дослідження, а деякі з них були розглянуті в роботі;

- проаналізовано теоретико-множинну модель компонентів, середовища и відмов системи фізичної безпеки, а також е основні результати методики PSMECA оцінювання;

- проведений експериментальний розрахунок уразливості елементів фізичної безпеки із застосуванням підходу складання маршрутів атаки і взаємодії з окремо взятими елементами фізичної безпеки.

Дана стаття описує систему, що виконує робочі заходи в нормальному режимі функціонування. Формат атаки розглядається як мануальний перебір можливих комбінацій, з урахуванням взаємодії з обладнанням без доповнення процедур часовими інтервалами, витраченими на маршрут і елементи системи.

Майбутні дослідження можуть бути спрямовані на розробку динамічних сценаріїв фізичних і кібератак, що охоплюють багаторівневі загрози і множинні відмови мають залежність від програмного, апаратного або людського оточення.

Література

1. Павлов, Д. М. Забезпечення фізичної безпеки ядерних об'єктів в Україні в умовах зростання військово-терористичної загрози: організаційно-правовий аспект [Текст] / Д. М. Павлов // Юридична наука. – 2015. – № 2. – С. 21–27.

2. Niles, S. Physical Security in Mission Critical Facilities [Text] / Suzanne Niles // Schneider Electric. – 2004. – 22 p.

3. Physical Security Systems [Text] // Hitachi Review – 2014. – Vol. 53, No. 2. – P. 73–78.

4. Basic concepts and taxonomy of dependable and secure computing [Text] / A. Avizienis, J. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – No. 1. – P. 11–33.

5. Yastrebenetsky, M. Nuclear Power Plants Instrumentation and Control Systems for Safety and Security [Text] / V. Yastrebenetsky, V. Kharchenko. – Hershey PA, USA, 2014. – 470 p. – (IGI Global).

6. Qahtan Abdulmunem, M. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models [Text] / M. A.-S. Qahtan Abdulmunem, V. Kharchenko // Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry. – 2016. – P. 302–307.

7. Charlie, F. Physical Protection Principles [Text] / F. Charlie, M. Brayon // Nuclear Installation Dept. AELB. – 2014. – 10 p.

8. Harris, S. Physical and Environmental Security. [Text] / S. Harris // CISSP Exam Guide. – 2013. – P. 457–502.

9. Conrath, J. Structural Design for Physical Security: State of the Practice [Text] / J. Conrath. – ASCE Reston: Task Committee, Structural Engineering Institute, 1999. – 264 p.

10. Monk, S. Programming the Raspberry Pi: Getting Started with Python [Text] / S. Monk. – McGraw Hill Professional, 2015. – 192 p.

11. Blum, J. Exploring Arduino: Tools and Techniques for Engineering Wizardry [Text] / J. Blum. – Jonh Willey & Sons, 2013. – 384 p.

12. Wireless Sensor Node with Passive RFID for Indoor Monitoring System [Text] / N. M. Nadzir, M. Rahim, F. Zubir // International Journal of Electrical & Computer Engineering. – 2017. – P. 1459–1466.

13. IoT-based physical security systems: Structures and PSMECA analysis [Text] / A. K. A. Waleed, V. Kharchenko, D. Uzun, O. Solovyov // IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – 2017. – P. 870–873.

14. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring [Text] / A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov // Lecture Notes in Computer Science. – 2006. – Vol. 4157. – P. 153–167.

15. Illiashenko, O. Choosing FMECA-based techniques and tools for safety analysis of critical systems [Text] / O. Illiashenko, E. Babeshko // Information & Security: An International Journal. – 2012. – No. 28(2). – P. 275–285.

References

1. Pavlov, D. M. Zabezpechennya fizychnoyi bezpeky yadernykh ob"yektiv v Ukrayini v umovakh zrostannya viyskovo-terorystychnoyi zahrozy: orhanizatsiyno-pravovyy aspect [Physical security of nuclear facilities in Ukraine in terms of growth of military-theoretical threat, organizational and legal aspects]. *Yurydychna nauka – Jurisprudence*, 2015, no. 2, pp. 21–27. (in Ukrainian).

2. Niles, S. *Physical Security in Mission Critical Facilities Suzanne Niles*. Schneider Electric, 2004. 22 p.

3. Physical Security Systems. *Hitachi Review*, 2014, vol. 53, no. 2, pp. 73–78.

4. Avizienis, A., Laprie, J., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 2004, no. 1, pp. 11–33.

5. Yastrebenetsky, V., Kharchenko, V. *Nuclear Power Plants Instrumentation and Control Systems for Safety and Security*. Hershey PA, USA, 2014. 470 p.

6. Qahtan Abdulmunem, M., Kharchenko, V. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models. *Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry*, 2016, pp. 302–307.

7. Charlie, F., Brayon, M. *Physical Protection Principles*. Nuclear Installation Dept. AELB, 2014. 10 p.

8. Harris, S. *Physical and Environmental Security*. CISSP Exam Guide, 2013, pp. 457–502.

9. Conrath, J. *Structural Design for Physical Security: State of the Practice*. ASCE Reston: Task Committee, Structural Engineering Institute, 1999. 264 p.

10. Monk, S. *Programming the Raspberry Pi: Getting Started with Python*. McGraw Hill Professional, 2015. 192 p.

11. Blum, J. *Exploring Arduino: Tools and Techniques for Engineering Wizardry*. Jonh Willey & Sons, 2013. 384 p.

12. Nadzir, N. M., Rahim, M., Zubir, F. Wireless Sensor Node with Passive RFID for Indoor Monitoring System. *International Journal of Electrical & Computer Engineering*, 2017, pp. 1459–1466.

13. Waleed, A. K. A., Kharchenko, V., Uzun, D., Solovyov, O. IoT-based physical security systems: Structures and PSMECA analysis. *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017, pp. 870–873.

14. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A. *F(I)MEA-technique of Web Services Analysis and Dependability Ensuring*. Lecture Notes in Computer Science, 2006, vol. 4157, pp. 153–167.

15. Illiashenko, O., Babeshko, E. Choosing FMECA-based techniques and tools for safety analysis of critical systems. *Information & Security: An International Journal*, 2012, no. 28(2), pp. 275–285.

Надійшла до редакції 3.12.2019, розглянута на редколегії 10.12.2019

МЕТОД АНАЛИЗА РИСКОВ ДОСТУПА К АКТИВАМ В СИСТЕМАХ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

Ахмед Валид Аль-Хафаджи, А. А. Соловьёв, Д. Д. Узун, В. С. Харченко

Предметом изучения в статье являются методы анализа рисков доступа к активам внутри физического объекта. В качестве примере рассматривается объект системы физической безопасности научного учреждения (как блок территориального элемента) с аппаратным окружением в виде устройств с низким энергопотреблением и функционированием в среде Интернета вещей. **Целью** является создание теоретико-математической модели и метода анализа внутренних компонентов системы безопасности и доступа к активам. Поставленные задачи охватывают разработку подхода к анализу уровня безопасности, которая обеспечивается установленной системой физической безопасности и формирования подхода к проникновению с целью доступа к активам. При решении задач были использованы такие методы, как пространственный анализ физического распределения элементов системы, формирование графов маршрута, декомпозиция блоков и алгоритмов физической защиты, исследования полного набора компонентов и индивидуально ориентированного элемента обеспечения безопасности. **Получены следующие результаты**: разработан подход к анализу уровня безопасности физического объекта с использованием базовых параметров, состоящих из физических и информационных переменных существующих множественных активов, построена математическая модель компонентов системы, блочного ориентирования периметра объекта, предложена последовательность этапов

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

проникновения на защищенный объект с использованием множества маршрутов. **Выводы**: научная новизна полученных результатов заключается в следующем: усовершенствован метод анализа защищенности активов за счет использования переменных окружения и элементов контроля физической безопасности объекта, а также генерации и оценивания маршрутов проникновения на объект с целью доступа к критическим активам.

Ключевые слова: FMECA; PSMECA; куб критичности; физическая безопасность; кибербезопасность; система физической безопасности; анализ помещения; IoT; безопасность; дерево атак.

ASSET ACCESS RISK ANALYSIS METHOD IN THE PHYSICAL PROTECTION SYSTEMS

Ahmed Waleed Al-Khafaji, A. A. Solovyov, D. D. Uzun, V. S. Kharchenko

The subject of study in the article is asset access risk analysis methods inside a physical object. As an example, we consider the object of the physical security system of a scientific institution (as a block of a territorial element) with a hardware environment in the form of devices with low energy consumption and functioning in the Internet of things. The goal is to create a theoretical and mathematical model and method for analyzing the internal components of a security system and access to assets. The tasks set to cover the development of an approach to the analysis of the level of security, which is ensured by the established system of physical security and the formation of an approach to penetration to access assets. In solving the problems, methods were used such as spatial analysis of the physical distribution of system elements, the formation of route graphs, decomposition of blocks and physical protection algorithms, the study of a complete set of components and an individually oriented security element. The following results were obtained: an approach to the analysis of the security level of a physical object using basic parameters consisting of physical and information variables of existing multiple assets was developed, a mathematical model of the system components, block orientation of the perimeter of the object was built, a sequence of stages of penetration into a protected object using multiple routes was proposed. Conclusions: the scientific novelty of the results is as follows: the method of analyzing asset security through the use of environment variables and physical security controls of the facility, as well as the generation and evaluation of penetration routes to the facility to access critical assets, has been improved.

Keywords: FMECA; PSMECA; criticality cube; physical security; gate security; physical security system; room analysis; IoT; security; attack tree.

Ахмед Валід Аль-Хафаджі– здобувач каф. комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Соловйов Олександр Олександрович – аспірант каф. комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Узун Дмитро Дмитрович – канд. техн. наук, доцент, доцент каф. комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, професор, зав. каф. комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Ahmed Waleed Al-Khafaji – PhD Candidate, Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: eng_ahmed.waleed@yahoo.com.

Solovyov Oleksandr Oleksandrovich – PhD Student, Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: a.solovyov@csn.khai.edu.

Uzun Dmytro Dmytrovich– Associate professor Computer Systems, Networks and Cybersecurity Department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: d.uzun@csn.khai.edu, ORCID Author ID: 0000-0001-5574-550X

Kharchenko Vyacheslav Serhiiovych – DrS on Engineering, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: v.kharchenko@csn.khai.edu, ORCID Author ID: 0000-0001-5352-077X,
Scopus Author ID: 22034616000, ResearcherID: A-7719-2017,
https://scholar.google.com/citations?hl=ru&user=FQ4dH4EAAAAJ