МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2020

МАТЕРІАЛИ

X міжнародної науково-технічної конференції

19-24 березня 2020 року

м. Київ (Україна), м. Шарм-ель-Шейх (Египет)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: X міжнародна науково-технічна конференція, 19-24 березня 2020 р. – К.: НАУ, 2020. – 59 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників IX міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів захисту інформації, консолідації інформації та бізнес-аналітики.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – системи захисту інформації, 21.05.01 – інформаційна безпека держави, студентам вищих навчальних закладів, які отримують вищу освіту за спеціальностями: 125 – Кібербезпека (напрями: «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою» («Адміністративний менеджмент у сфері захисту інформації»), «Системи і технології кібербезпеки») та 124 – Системний аналіз (напрям «Консолідована інформація»), а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Кафедра безпеки інформаційних технологій Національного авіаційного університету;
- Наукове товариство студентів, аспірантів, докторантів та молодих учених НАУ;
- Європейський університет;
- Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ ім. І. Сікорського»;
- Національна академія Служби безпеки України;
- Університет в Бєльсько-Бялій (Польща);
- Satbayev University (Казахстан);
- ТОВ «Акксон Софт»;
- ТОВ «Безпека інформаційних систем «Дельта»;
- Всеукраїнська громадська організація «Співтовариство ІТдиректорів України»;
- Всеукраїнська громадська організація «Українська федерація професіоналів безпеки»;
- Студентське науково-технічне товариство «CyberTag»;
- Редакція наукового журналу «Безпека інформації»;
- Редакція наукового журналу «Захист інформації».

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова д.т.н., проф. **Олександр Корченко**
Національний авіаційний університет (м. Київ, УКРАЇНА)

Заступник голови д.т.н., доц. Іванченко Євгенія
Національний авіаційний університет (м. Київ, УКРАЇНА)

Відповідальний секретар Коломієць Марина
Національний авіаційний університет (м. Київ, УКРАЇНА)

Члени програмного комітету

д.т.н., проф. **Володимир ГОЛОВКО**, Брестський державний технічний університет (м. Брест, БІЛОРУСЬ)

к.т.н., доц. **Геворг МАРҐАРОВ**, Державний інженерний університет Вірменії (м. Єреван, ВІРМЕНІЯ)

д.т.н., проф. **Бахитжан АХМЄТОВ**, Казахский национальный педагогический университет имени Абая (м. Алмати, КАЗАХСТАН)

к.т.н., доц. **Нургуль СЄЙЛОВА**, Казахський національний технічний університет ім. К.І. Сатпаєва
(м. Алмати, КАЗАХСТАН)

д.т.н., проф. **Микола КАРПІНСЬКИЙ**, Університет у Бєльсько-Бялій(м. Бєльсько-Бяла, ПОЛЬЩА)

д.т.н., проф. **Станіслав РАЙБА**, Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, ПОЛЬЩА)

д.т.н., с.н.с., проф., **Володимир БУРЯЧОК**, Київський університет імені Бориса Грінченка (м. Київ, УКРАЇНА)

д.т.н., проф. **Євген ВАСІЛІУ**, Одеська національна академія зв'язку ім. О.С. Попова (м. Одеса, УКРАЇНА)

д.ю.н., проф. **Анатолій МАРУЩАК**, Національна академія Служби безпеки України(м. Київ, УКРАЇНА)

д.т.н., проф. **Володимир МОХОР**, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова (м. Київ, УКРАЇНА)

д.т.н., проф. **Андрій ПЕЛЕЩИШИН**, Національний університет «Львівська політехніка» (м. Львів, УКРАЇНА)

д.т.н., проф. **Катерина СОЛОВЙОВА**, Харківський національний університет радіоелектроніки
(м. Харків, УКРАЇНА)

к.психол.н., с.н.с. **Олександр ФАРМАГЕЙ**, Національна академія Служби безпеки України (м. Київ, УКРАЇНА)

Зміст

Стратегія захисту розподіленої інформаційної системи

УДК 004.732

Шестак Яніна[1], Мірутенко Лариса[2], Оксіюк Олександр[3]

Київський національний університет імені Тараса Шевченка,

[1] lucenko.y@ukr.net, [2] myrutenko.lara@gmail.com, [3] oksiuk@ukr.net

На сьогоднішній день при побудові розподіленої інформаційної системи пріоритетним завданням є врахування вимог по масштабуванню апаратного комплексу, що включає у себе збільшення кількості робочих станцій, впровадження мультиядерних процесорів та організацію багатопотокової архітектури. Зазначені вимоги призводять до того, що розробка стратегії захисту інформаційної системи від зовнішніх загроз, підтримка стабільної роботи апаратно-програмного комплексу за умов економії обчислювальних ресурсів і енергоспоживання загальної системи постає перед дослідниками у якості нетривіальної задачі.

Метою даної роботи є розробка методики оцінки захищеності складних розподілених інформаційних систем шляхом впровадження алгоритмів визначення ефективності і функціональності систем захисту, а також побудови математичної моделі захисту апаратно-програмного комплексу.

У рамках поставленого завдання було розглянуто аспекти впровадження технології оцінки захищеності розподілених інформаційних систем. З метою визначення систем оцінки впливу методик розподілення навантаження на продуктивність роботи апаратно-програмного комплексу запропоновано процедуру структурування графу завдань на рівні списків, груп і підгруп. На основі зазначеного підходу розроблено багаторівневу схему оптимізації розподілу апаратних ресурсів. Запропонована схема оптимізації розподілу апаратних ресурсів визначається через обмеження довжини графу завдань та параметру енергоспоживання у межах списків, груп та підгруп завдань, що дозволяє побудувати наступні рівні аналізу: 1) Оптимізація розподілу апаратних ресурсів інформаційної системи у межах однієї підгрупи завдань; 2) оптимізація розподілу апаратних ресурсів інформаційної системи на рівні взаємодії між підгрупами завдань; 3) оптимізація розподілу апаратних ресурсів РІТС на рівні взаємодії між групами завдань; 4) оптимізація розподілу апаратних ресурсів РІТС на рівні взаємодії між списками завдань.

Для аналізу ефективності впровадження розробленої схеми була побудована математична модель та отримані значення нормалізованого графа завдань і нормалізованого розподілу енергії. Вказана модель була застосована при моделюванні наступних методів роботи з графами завдань: 1) обчислення за ієрархічною структурою; 2) алгоритми розбиття графу; 3) методи на базі алгебраїчної теорії графів; 4) структурування типу «Diamond Dags». Отримані результати математичного моделювання були надалі співставленні зі статистичними даними, що визначались для наступних видів розподілу: 1)

рівномірний розподіл; 2) біноміальний розподіл; 3) геометричний розподіл. Результати показали вискоку точність прогнозування на рівні визначення максимального значення відносної похибки моделювання.

Порівняння різних моделей характеристичних векторів для JPEG-стеганоаналізу

УДК 004.056; 004.415.24

Наталія Кошкіна

Інститут кібернетики імені В.М. Глушкова НАН України,
nata.koshkina@gmail.com

При практичному стеганоаналізі основними критеріями вибору методу детектування прихованих повідомлень є його точність та швидкодія. Проте здійснити порівняння методів навіть одного класу, базуючись на даних з наукових публікацій, досить складно через відмінності в умовах чисельних експериментів. Тому, дослідження, що дозволяють порівняти ефективність сучасних методів стеганоаналізу в однакових умовах, є актуальними, а їх результати можуть бути використані для практичної організації систем виявлення стеганографічних прихован. Також вони можуть слугувати базою для подальшого вдосконалення стеганоаналітичних методів і систем.

Метою даної роботи є здійснення порівняльного аналізу ефективності різних статистичних моделей характеристичних векторів для стеганоаналітичних систем на базі машинного навчання, на основі якого можна буде вибрати оптимальну модель для заданих практичних умов.

Для проведення чисельних експериментів було обрано три програми, що здатні здійснювати приховування у файли формату JPEG: Jsteg, Jphide та Steganos Privacy Suite 2012 (модуль Crypt&Hide). Вихідний тестовий набір містив 1330 кольорових зображень розмірами 512×384 пікселі, в кожне з них вищезгаданими програмами вкраплювалося 1 Кб випадкового тексту.

Обравши класичний класифікатор – метод опорних векторів (англ. SVM, support vector machine) та зафіксувавши однакові умови експериментів ми прорахували точність та швидкодію стеганоаналізу на базі наступних відомих статистичних моделей для JPEG-контейнерів: CHEN, CC-CHEN, LIU, CC-PEV, CC-C300, GFR, DCTR.

В таблиці 1 наведена кількість елементів характеристичного вектора для кожної з вищезазначених моделей, а також швидкість створення характеристичного вектора, отримана на ПК з процесором Intel Core i5-661 3.33 Ггц і 8 Гб ОЗУ та усереднена за 100 обчисленнями.

Таблиця 1

Параметри характеристичних векторів для різних моделей

№ п/п	Параметри / Модель	Кількість елементів вектора	Швидкість обчислення вектора, сек
1	CHEN	486	0.2
2	CC-CHEN	972	0.9
3	LIU	216	44.2
4	CC-PEV	548	1.5
5	CC-C300	48600	1.1
6	GFR	17000	6.2
7	DCTR	8000	2.0

Швидкість обчислення характеристичних векторів впливає на швидкість роботи стеганоаналітичної системи як на етапі її навчання, так і на етапі детектування стегановкладок. Особливо критичною ця характеристика є для систем реального часу. Як бачимо з даних таблиці 1 різниця в швидкості обчислення характеристичних векторів для різних моделей досить помітна. Найшвидше обчислюються характеристичні вектори для моделі CHEN, найповільніше – для LIU. Тобто коли в моделі LIU буде опрацьований тільки один файл, в моделі CHEN таких файлів буде більше ніж 200.

Точність виявлення стеганоконтейнерів, яка була усереднена за 10 повторами стеганоаналізу з випадковим поділом контейнерів на навчальну та контрольну вибірки, представлена у таблиці 2. Також в дужках після точності наведено усереднену кількість хибно позитивних та хибнонегативних тривог для 557 пустих та 557 заповнених контейнерів контрольної вибірки.

Таблиця 2

Точність виявлення стеганоконтейнерів на базі різних статистичних моделей

№ п/п	Атака на / Модель	Jsteg	Jphide	Steganos
1	CHEN	97.9% (0; 24)	83.1% (89; 99)	83.1% (67; 50)
2	CC-CHEN	98.0% (0; 23)	88.2% (61; 71)	94.9% (32; 25)
3	LIU	99.8% (0; 2)	88.8% (57; 68)	98.0% (5; 17)
4	CC-PEV	84.0% (75; 104)	76.9% (79;179)	76.9% (81; 177)
5	CC-C300	99.1% (4; 6)	91.6% (51; 43)	95.7% (25; 24)

6	GFR	96.3% (19; 22)	91.6% (66; 27)	92.0% (40; 50)
7	DCTR	98.6% (13; 3)	93.1% (45; 32)	97.1% (14; 18)

За результатами цих експериментів в трійку лідерів потрапили моделі LIU, CC-C300 та DCTR. Найкращу точність при виявленні стеганоконтейнерів, створених програмами Jsteg та Steganos Privacy Suite 2012 забезпечила модель LIU, при виявленні Jphide стегановкладок – модель DCTR. Найгірша точність класифікації для всіх трьох варіантів стеганопрограм отримана для моделі CC-PEV. Також незалежно від стеганопрограми модель CC-CHEN має перевагу над вихідною моделлю CHEN.

Зауважимо, що у випадках, коли допустиме зниження швидкодії, є резерви покращення точності. Так, можна не обирати якусь одну модель формування характеристичних векторів, а використовувати декілька ефективних для даного типу контейнерів та стеганоперетворення. При цьому можна як комбінувати чи усереднювати результати на базі різних моделей (наприклад, байесівське усереднення), так і навчити окрему модель тому, яку саме з наявних моделей використати для передбачення (наприклад, дерево прийняття рішень).

Крім того в загальному випадку стегоаналітична система повинна мати можливість працювати в режимі мультикласифікації, тому було виконане також порівняння ефективності і для подібних сценаріїв.

В подальшому планується перевірити точність розглянутих та інших статистичних моделей при виявлення вдосконалених стеганоперетворень, таких як nsF5, YASS, HUGO, WOW, UNIWARD.

Кількісна оптимізація побудови мереж відповідно заданому рівню захищеності

УДК 004.056.53

Сергій Зибін
Національний авіаційний університет, zysv@ukr.net

При дослідженні і розробці шляхів передачі інформації в захищених мережах необхідно враховувати побудову структур інформаційних потоків, які визначаються раціональними факторами: кількісним, топологічним, якісним і часовим.

Метою даної роботи являється оптимізація організації захищеної мережі за кількісним фактором.

Виконання поставленого завдання починається з побудови інформаційних структур $G_n^{(1)}$, $(\mathrm{n} = \overline{1,\mathrm{n}_0})$, що представляють собою зв'язані орієнтовані графи. Вершинами графів являються задачі взаємодії макрорівня $M_i^{\mu_i}$, $(i = \overline{1,i_0},\ \ \mu_i = \overline{1,(\mu_i)_0})$, що здійснюють інформаційний обмін між ресурсами системи і зовнішніми джерелами, а дугами являються інформаційні потоки. Відповідним чином задачі $M_i^{\mu_i}$ представляють собою зв'язані орієнтовані підграфи, вершинами яких служать задачі взаємодії мікрорівня $U_i^{\lambda_i}$, $\lambda_i = \overline{1,(\lambda_i)_0}$, що забезпечують обмін інформаційними потоками між ресурсам системи S_i, а дугами – інформаційні потоки.

Задачі взаємодії макрорівня і мікрорівня поділимо на три типи.

$$M_i^{\mu_i} = A_i^{\alpha_i} \cup B_i^{\beta_i} \cup D_i^{\delta_i};\ (\alpha_i,\beta_i,\delta_i) = \overline{1,(\mu_i)_0};\ \alpha_i \neq \beta_i \neq \delta_i;\ i = \overline{1,i_0}$$

$$U_i^{\lambda_i} = X_i^{\phi_i} \cup Y_i^{\psi_i} \cup Z_i^{\xi_i};\qquad (\phi_i,\psi_i,\xi_i) = \overline{1,(\lambda_i)_0};\ \phi_i \neq \psi_i \neq \xi_i;\ i = \overline{1,i_0},$$

де $(A_i^{\alpha_i}, X_i^{\phi_i})$ – ресурси-джерела, що виконують збір, підготовку і передачу інформації; $(B_i^{\beta_i}, Y_i^{\psi_i})$ – ресурси-транзити, які обробляють і передають інформацію; $(D_i^{\delta_i}, Z_i^{\xi_i})$ – ресурси-користувачі, ОПР або користувачі. Даного виду ресурси-споживачі формують рішення або виконуються дії в мережі S_i', в результаті обробки інформації.

Оптимізація структур за кількісним фактором здійснюється в локальній задачі обчислення раціональних об'ємів інформації.

Під об'ємом інформації будемо розуміти кількість елементарних символів. Слід відзначити, що мова йде про об'єми інформації, які складаються з базових, а не синтетичних показників.

Раціональний об'єм повинен відповідати вимогам повноти інформації, що ставиться задачею-споживачем.

Якщо об'єм інформації менше потрібного, то елемент мережі, споживач або вся мережа відчуватиме нестачу інформації. У випадку надлишку потрібного об'єму виникають непродуктивні затрати на формування, обробку і передачу інформації або результатів рішення задач.

Позначимо через $Q_{ki}^{(M')_k^{\mu_k}(U')_k^{\lambda_k},(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}$, $Q_{ii}^{(M'')_i^{\mu_i}(U')_i^{\gamma_i}(U'')_i^{\lambda_i}}$, $Q_{ij}^{(M')_i^{\mu_i}(U')_i^{\lambda_i},(M'')_i^{\mu_j}(U'')_i^{\lambda_j}}$, $Q_{ii}^{(M'')_k^{\mu_k}(U')_i^{\lambda_i}(U'')_i^{\nu_i}}$ об'єми відповідної інформації завдань взаємодії $W_{ki}^{(M')_k^{\mu_k}(U')_k^{\lambda_k},(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}$, $W_{ii}^{(M'')_i^{\mu_i}(U')_i^{\gamma_i}(U'')_i^{\lambda_i}}$, $W_{ij}^{(M')_i^{\mu_i}(U')_i^{\lambda_i},(M'')_j^{\mu_j}(U'')_j^{\lambda_j}}$, $W_{ii}^{(M'')_i^{\mu_i}(U')_i^{\lambda_i}(U'')_i^{\nu_i}}$, $(\nu_i = \overline{1,(\lambda_i)_0}, \nu_i \neq \lambda_i)$. Нехай $(Q_{IN})_i^{(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}$, $(Q_{IN})_i^{B_i^{\beta_i}Y_i^{\psi_i}}$ визначають об'єми даних, які необхідні для виконання відповідно задач $(M'')_i^{\mu_i}(U'')_i^{\lambda_i}$, $B_i^{\beta_i}Y_i^{\psi_i}$, а $(Q_{OUT})_i^{(M')_i^{\mu_i}(U')_i^{\lambda_i}}$ і $(Q_{OUT})_i^{B_i^{\beta_i}Y_i^{\psi_i}}$ ідентифікують об'єми результатів розв'язку задач $(M')_i^{\mu_i}(U')_i^{\lambda_i}$ і $B_i^{\beta_i}Y_i^{\psi_i}$.

Використовуючи позначення, які були прийняті сформулюємо математичну постановку локальної задачі: необхідно оптимізувати структуру $G_n^{(3)}$ за кількісним фактором Q

$$G_n^{(4)} = \underset{Q}{opt} G_n^{(3)}$$

тобто, необхідно забезпечити виконання кількісного критерію K_Q

$$K_Q = [\underset{G_n^{(4)}}{\forall}(M'')_i^{\mu_i}(U'')_i^{\lambda_i} \times (\vartheta_Д \sum_{(M')_k^{\mu_k}(U')_k^{\lambda_k} I^*(M'')_i^{\mu_i}(U'')_i^{\lambda_i}} \frac{(Q_{ki}^{(M')_k^{\mu_k}(U')_k^{\lambda_k},(M'')_i^{\mu_i}(U'')_i^{\lambda_i}})^{\vartheta_{II}}}{(Q_{IN})_i^{(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}} +$$

$$+ \sum_{(U')_i^{\gamma_i} I^*(U'')_i^{\lambda_i}} \frac{(Q_{ii}^{(M'')_i^{\mu_i}(U')_i^{\gamma_i}(U'')_i^{\lambda_i}})^{\vartheta_n}}{(Q_{IN})_i^{(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}}) \to 1],$$

де $\vartheta_Д$ – коефіцієнт достовірності, ($\vartheta_Д \leq 1$), $\vartheta_{П}$ – коефіцієнт повноти, ($\vartheta_{П} \leq 1$).

Алгоритм обчислення об'ємів інформації починається з послідовного аналізу задач і пошуку в них задач-користувачів. Використовуючи опис задачі макрорівня і коефіцієнти об'ємів, обчислюємо об'єми інформації.

Послідовно розглядаючи всі задачі, визначимо об'єми інформації.

За порядком обчислення об'єми вносимо в опис структури або в опис задачі взаємодії макрорівня.

Після закінчення процедури визначення об'ємів інформаційних потоків отримаємо:

$$G_n^{(4)} = \{(A_k^{\alpha_k}) \cap (W_{ki}^{A_k^{\alpha_k}(U')_k^{\lambda_k},(M'')_i^{\mu_i}(U'')_i^{\lambda_i}} Q_{ki}^{A_k^{\alpha_k}(U')_k^{\lambda_k},(M'')_i^{\mu_i}(U'')_i^{\lambda_i}}),$$

$$A_k^{\alpha_k}(U')_k^{\lambda_k} I^*(M'')_i^{\mu_i}(U'')_i^{\lambda_i} \cap (W_{ki}^{(M')_k^{\mu_k}(U')_k^{\lambda_k},B_i^{\beta_i}(U'')_i^{\lambda_i}} Q_{ki}^{(M')_k^{\mu_k}(U')_k^{\lambda_k},B_i^{\beta_i}(U'')_i^{\lambda_i}}) B_i^{\beta_i},$$

$$(M')_k^{\mu_k}(U')_k^{\lambda_k} I^* B_i^{\beta_i}(U'')_i^{\lambda_i} \cap (W_{ij}^{B_i^{\beta_i}(U')_i^{\lambda_i},(M'')_j^{\mu_j}(U'')_j^{\lambda_j}} Q_{ij}^{B_i^{\beta_i}(U')_i^{\lambda_i},(M')_j^{\mu_j}(U'')_j^{\lambda_j}}),$$

$$B_i^{\beta_i}(U')_i^{\lambda_i} I^*(M'')_j^{\mu_j}(U'')_j^{\lambda_j} (W_{ij}^{(M')_i^{\mu_i}(U')_i^{\lambda_i},D_{\delta_j}(U'')_j^{\lambda_j}} Q_{ij}^{(M')_i^{\mu_i}(U')_i^{\lambda_i},D_{\delta_j}(U'')_j^{\lambda_j}}) D_j^{\delta_j}\}$$

Реализация алгоритма UMAC на крипто-кодовых конструкциях

УДК 681.3.06

Ольга Король[1], Алла Гаврилова[2]

Харьковский национальный экономический университет имени Семена Кузнеца, [1]olha.korol@hneu.net, [2]alla.gavrylova@hneu.net

В условиях современных угроз и реализации алгоритмов криптоанализа с применением полномасштабных квантовых компьютеров в будущем, использование известных алгоритмов SHA-3 и Европейского криптографического конкурса NESSIE в алгоритмах аутентификации и цифровой подписи из-за возможности их взлома ставится под сомнение.

Целью данной работы является обоснование расчетным путем на основании алгоритма UMAC необходимости использования крипто-кодовых конструкций Мак-Элиса с эллиптическими кодами для выявления модификаций открытого текста при передачи через открытый канал.

При разработке математической модели формирования хеш-кода в алгоритме UMAC, используется псевдослучайная последовательность, которая обеспечивает криптостойкость данного хеш-кода. В качестве алгоритма формирования подложки выступает крипто-кодовая конструкция Мак-Элиса на эллиптических кодах (ЕС).

Кодирование открытого сообщения отправителя для передачи по каналам связи выполнялось на основании следующих процедур.

I процедура. Формирование хеш-кода в алгоритме UMAC. Указанные преобразования проводим параллельно с формированием кодограммы. Данная процедура является итеративной и складывается из трехслойной структуры: 1) Y_{L1M} – первый слой, который является значением функции UHASH-hash первого уровня хеширования; 2) Y_{L2M} – второй слой, который является значением функции POLY-hash второго уровня хеширования; 3) Y_{L3M} – третий слой, который является значением функции Carter-Wegman-hash третьего уровня хеширования.

II процедура. Формирование криптограммы (C_X) с учетом одноразового сеансового секретного ключа *e.*

III процедура. Формирование псевдослучайной подкладки/подложки (*Pad*) для обеспечения криптостойкости алгоритма UMAC проводим с помощью функции *PDF*, причем различные части *Pad* можно будет использовать как дополнительный вектор инициализации.

IV процедура. Формирование кода контроля целостности и аутентичности кодограммы *Tag* рассчитывается на основании значений функций Y_{L3M} и *Pad*.

V процедура. Формирование значения суммарного кода достоверности передаваемого текста *(Y)* проведем на основании найденного значения хеш-кода Y_{L3M} и *Tag*.

Верификация хеш-кода на приемной стороне с использованием алгоритма UMAC осуществлялась следующим образом.

I процедура. Строим вектор, который является кодовым словом кода с порождающей матрицей *G*, искаженной не более чем в *t* разрядах.

II процедура. Получаем синдром ошибок S .

III процедура. Находим многочлен локатора ошибок ($\Lambda(x)$) с последующей локализацией ошибок по процедуре Ченя.

IV процедура. Определяем кратности ошибочных позиций, решив систему уравнений (расчет S').

V процедура. Получаем криптограмму C_X^* с учетом вектора ошибок e' .

VI процедура. C_X^* используется в качестве основы для формирования подложки по алгоритму UMAC.

Таблиця 1

Формализация показателей и результаты расчетов

№	***Показатель***	***Формула расчета***	***Значение показателя***
1	Y_{L3M} ,	$((Y_{L1I} \bmod(2^{36}-5)) \bmod 2^{32}) xor Y_{L32I}$,	10000000010
2	C_X	$I \times G_X^{EC} + e$	23023322
3	*Pad*	$PDF(K, Nonce, Taglen)$,	1101010
4	*Tag*	$Y_{L3M} \oplus Pad$	10001101100
5	*Y, Y'*	$Y_{L3M} \oplus Tag$	1101110
6	C_X^*	$C_X \times D^{-1} \times P^{-1}$	22202221
7	S	$C_X^* \times H^T$	1,1,1,0,0,0
8	$\Lambda(x)$	$a_{00} + a_{10}x + y = 0$	$x + y = 0$
9	S'	$H \times e'$	00020003
10	$C_X^{'}$	$C_X^* + e'$	22222224

Результат верификации, полученный при проведенных расчетах положителен, так как при сравнении хеш-кодов (полученного от отправителя и сформированного получателем) их длины совпадают. Следовательно, открытый текст, полученный через открытый канал получателем, не модифицирован.

В результате исследований разработаны практические алгоритмы формирования хеш-кода и его верификации на основе алгоритма UMAC с использованием крипто-кодовых конструкций Мак-Элиса на ЕС. Данный механизм аутентичности сообщений возможно использовать не только на эллиптических кодах, но и модифицированных (укороченных, и/или удлиненных) эллиптических кодах, а также на ущербных кодах с использованием гибридных крипто-кодовых конструкций. Такой подход позволяет практическую реализацию быстрого алгоритма хеширования с уровнем стойкости в постквантовой криптографии.

Single-factor model of information security threats of the automated management system of production of high-speed telecommunication distributed data transfer systems

UDC 004.056.53

Yurii Balaniuk[1], Ivan Yakoviv[2], Svitlana Kovtun[3]
The National Aviation University, [2]theivasyl@gmail.com, [3]svt.kovtun@gmail.com

When developing information security systems of the automated control system (ACS) by the production of high-speed distributed data transmission paths, it is necessary to take into account the complex technological process of the whole life cycle of production, which, first of all, includes: software products of information technology supporting the adoption of operational decisions at various stages of the technological cycle, differences between the permittivity of distributed paths and the required values, which caused by technological instability of the manufacturing process, range of geometric dimensions of hard-shaped conductors, deviation of load parameters from nominal values etc. Management of such a complex production process requires enhanced information security of the automated control system: its protection against accidental and deliberate impacts of different nature.

Analysis of the characteristics of automated control systems for the production of high-speed distributed paths and the opinions of experts in this field showed that the dominant mathematical model of risk (risk factor) and threat can be represented in the form of stochastic equations

$$\tilde{N}(y) = N(y) + \Delta_1(y), \tag{1}$$

$$\tilde{N}(y) = \frac{\tilde{W}'(y)}{2\tilde{W}(y)}, \qquad N(y) = \frac{W(y)}{2W'(y)}, \tag{2}$$

where is a variable that has the meaning of the current geometric coordinate of the information channel or another entity – a deterministic function that characterizes the parameters of the distributed path in the absence of an ASM threat – the random function of the distributed path (risk factor) when the threat is applied to the control system. Function

$$\Delta_1(y) = g(y)\Delta(y), \tag{3}$$

determines the random process caused by the impact of the threat on the control system. At the same time, based on the technology of production and the opinions of experts, we can assume that the component of the threat $\Delta(y)$ is normal stationary white noise with a correlation function $K_\Delta(y_1, y_2) = \frac{N_0}{2}\delta(y_2 - y_1)$, and zero mathematical expectation $m\{\Delta\} = 0$, $g(y)$ – deterministic function determined by the production process, $g(y) \geq 0$.

From (2) and (3) we find the parameters of the distributed path in case of absence of an ASC threat

$$W(y) = A(y)X, \qquad A(y) = \exp\left\{2\int_0^y N(y)dy\right\}. \quad (4)$$

$$X = \tilde{W}(0)\exp\left\{2\int_0^y \Delta_1(y)dy\right\}. \quad (5)$$

We represent the process X in the form

$$X = \exp\{2V\}. \quad (6)$$

Where

$$V = \int_0^y \Delta_1(y)dy + \frac{1}{2}\ln\tilde{W}(0). \quad (7)$$

From the foregoing we see that V is a Markov process with a diffusion coefficient

$$b(y) = \frac{N_0 g^2(y)}{2}, \quad (8)$$

and zero drift coefficient. Instead of the expression (7), we use another form of the notation

$$\frac{dV}{dy} = \Delta_1(y), \qquad V(0) = \lambda_0 = \frac{1}{2}\ln\tilde{W}(0), \quad (9)$$

$V(0) = \lambda_0$ – initial random value.

It follows from the relations (4), (6) that the statistical characteristics of the risk factor $\tilde{W}(y) = A(y)e^{2V}$ are completely determined by the Markov process V with some flow function $G(v, y)$.

Determining the level of information security

First, we consider the threat in which the characteristics of the ACS are limiting and with further strengthening of the destructive effect, the parameters of the control system do not change. In this case, we can assume that the process V is between fixed boundaries. Without loss of generality, we assume that the boundaries are located in the cross sections $V = 0$ and $V = 2h$.

The probability density $P(v, y)$ of a random process $V(y)$ is found from the Fokker-Planck-Kolmogorov solution:

$$\frac{\partial}{\partial y}P(v, y) = \frac{1}{2}b(y)\frac{\partial^2}{\partial V^2}P(v, y). \quad (10)$$

Separating the variables in this equation $P(v, y) = V(v)Y(y)$, we find,

$$\frac{1}{b(y)Y(y)}\frac{\partial Y}{\partial y} = \frac{1}{2}\frac{1}{V(v)}\frac{\partial^2 V(v)}{\partial V^2} = -\lambda^2, \quad (11)$$

where λ^2 is a positive number. As a result, we get

$$V'' + \lambda^2 V = 0, \quad (12)$$

$$Y' + \frac{\lambda^2}{2}b(y)Y = 0. \quad (13)$$

From this we find the function

$$Y(y) = Y(0)\exp\left\{-\frac{1}{2}\lambda^2\int_0^y b(y)dy\right\}. \quad (14)$$

Suppose that the boundaries from which the process V is reflected are in sections $V=0$, $V=2h$. In these sections, the flow $G(v,y)$ must be zero.

Since the flow $G(v,y) = -\frac{1}{2}\frac{d}{dV}\left[b(y)P(v,y)\right]$, then for the probability density $P(v,y)$ the boundary conditions are satisfied

$$\frac{\partial}{\partial V}P(v,y)\Big|_{v=0} = \frac{\partial}{\partial V}P(v,y)\Big|_{v=2h} = 0. \quad (15)$$

Consequently

$$V'(0) = V'(2h) = 0. \quad (16)$$

Taking into account conditions (16), the solution of equation (12) can be written as a set of orthogonal normalized functions ϕ_k:

$$\phi_0(V) = \frac{1}{\sqrt{2h}},\ \phi_k(V) = \frac{1}{\sqrt{h}}\cos\lambda_k V,\ \lambda_k = \frac{k\pi}{2h}. \quad (17)$$

Hence we find the general solution

$$P(v,y) = \sum_{k=0}^{\infty} C_k e^{-\frac{1}{2}\lambda_k^2\int_0^y b(y)dy}\cos\lambda_k V. \quad (18)$$

The constants C_k are found from the initial conditions. In particular, for a deterministic process V at the initial point $V(0)=\lambda_0$, we have $P(V,0)=\delta(V-\lambda_0)$, where $\delta(v)$ is the Dirac delta function. Then, $\delta(V-\lambda_0) = \sum_{k=0}\phi_k(V)\phi_k(0)$, we find

$$C_0 = \frac{1}{2h},\quad C_k = \frac{1}{h}\cos k\pi\frac{\lambda_0}{2h}. \quad (19)$$

Consequently,

$$P(v,y,\lambda_0) = \frac{1}{2h} + \frac{1}{h}\sum_{k=1}^{\infty}\cos\left[\frac{k\pi}{2h}\lambda_0\right]\cdot\cos\left[\frac{k\pi}{2h}v\right]\exp\left\{-\frac{k^2\pi^2}{8h^2}\int_0^y b(y)dy\right\}, \quad (20)$$

$$0<\lambda_0<2h,\ 0<v<2h.$$

When considering the process in the region -*h*, *h*, we get

$$P_{-h,h}(v,y,\lambda_0) = \frac{1}{2h} + \frac{1}{h}\sum_{k=1}^{\infty}\cos\left[\frac{k\pi}{2h}(\lambda_0+h)\right]\cos\left[\frac{k\pi}{2h}(v+h)\right]\exp\left\{-\frac{k^2\pi^2}{8h^2}\int_0^y b(y)dy\right\}, \quad (21)$$

$$-h<\lambda_0<h,\ -h<v<h.$$

If we consider the process between arbitrary boundaries *c*, *d*, *c*<*d*, in the above expression it is necessary to go to the new variable:

$$P_{c,d}(v,y,\lambda_0) = P_{-\frac{d-c}{2},\frac{d-c}{2}}(v,y,\lambda_0-\frac{c+d}{2}), \quad (22)$$

$$c < \lambda_0 < d \ , \ c < v < d \ .$$

If the initial condition $\lambda_0 = \mathrm{V}(0)$ is a random variable, then according to the method of separation of variables the general solution is:

$$P_{c,d}(v,y) = \int_c^d P_{c,d}(v,y,\lambda_0) P_0(\lambda_0) d\lambda_0 \ , \tag{23}$$

$c < v < d$, where $P_0(\lambda)$ is the probability density of the quantity λ_0 .

Now consider the threat in which the characteristics of the control system change over time and lead to a temporary change in the process of managing the production of information transmission channels. In this case, the level of information security will be determined by the probability $q_{c,d}$ with which the process V does not exceed the limits of acceptable limits.

The probability density of a given process is determined by the direct Fokker-Planck-Kolmogorov equation $\frac{\partial}{\partial y}\tilde{P}(v,y,\lambda_0) = \frac{1}{2} b(y) \frac{\partial^2}{\partial V^2} \tilde{P}(v,y,\lambda_0)$, and the following condition $\tilde{P}(c,y,\lambda_0) = \tilde{P}(d,y,\lambda_0) = 0$.

It is easy to see that this condition is equivalent to observing equality on the boundaries of the domain c, d: $V(c) = V(d) = 0$.

Separating the variables and assuming $c = -h$, $d = h$ for a nonrandom (deterministic) initial condition, we find the level of information security of the ACS:

$$q_{-h,h}(y,\lambda_0) = \frac{4}{\pi} \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \cos\left[\frac{(2n+1)\pi\lambda_0}{2h}\right] \exp\left\{-\frac{(2n+1)^2\pi^2}{8h^2} \int_0^y b(y)dy\right\} \ , \tag{24}$$

$$-h < \lambda_0 < h \ .$$

For an arbitrary region of boundaries c, d, we have

$$q_{c,d}(y,\lambda_0) = q_{-\frac{d-c}{2},\frac{d-c}{2}}(y, \lambda_0 - \frac{c+d}{2}) \ . \tag{25}$$

With a statistical initial condition with a probability density $P_0(\lambda_0)$, the level of information security is carried out taking into account (25). In this case, according to the theory of random processes

$$q_{c,d}(y) = \int_c^d q_{c,d}(y,\lambda_0) P_0(\lambda_0) d\lambda_0 \ . \tag{26}$$

Example. Suppose that the threat to information security λ_0 in the interval c, d is evenly distributed $P_0(\lambda_0) = \frac{1}{d-c}$. From (24) – (26) we find the level of information security of the ACS:

$$q_{c,d}(y) = \frac{8}{\pi^2} \sum_{n=0}^{\infty} \frac{1}{2n+1} \exp\left\{-\frac{(2n+1)^2\pi^2}{2(d-c)^2} \int_0^y b(y)dy\right\} \ . \tag{27}$$

Thus, the obtained results allow to estimate the level of information security of the automated production management system for high-speed distributed data transmission paths.

Анализ методов цифровой аутентификации

УДК 004.056.53

Юрий Журов

Национальный авиационный университет, iurii.zhurov@gmail.com

В течение первых двух десятилетий XXI века количество информационных систем (ИС) увеличилось на несколько порядков, также увеличилось количество субъектов ИС, а также плотность использования ИС одним субъектом. Особо стоит отметить возросшее количество взаимодействий объектов ИС. Данный тренд имеет резко положительную динамику и, так как, каждое взаимодействие субъектов/объектов ИС должно быть аутентифицировано, удерживается постоянный высокий запрос на: 1) эффективные экономически; 2) имеющие высокую степень надежности с точки зрения информационной безопасности; 3) эффективные с точки зрения внедрения; 4) производительные – методы или системы цифровой аутентификации.

Цель данной работы заключается в анализе существующих методов цифровой аутентификации для определения возможных направлений развития научного и практического поиска.

Рассмотрим классические методы аутентификации – методы, основанные на использовании, так называемых, факторов аутентификации. Выделяют следующие факторы – 1) знания; 2) владения; 3) свойства. Эмпирически все доступные варианты верификации аутентифицируемого субъекта/объекта можно отнести к одной из этих категорий, поэтому текущие методы базируются либо на использование этих факторов, либо на мультипликации факторов или вариативности их использования. Такими методами являются 1) однофакторная аутентификация (SFA); 2) двухфакторная аутентификация (2FA); 3) многофакторная аутентификация (MFA).

В 2005 году Shintaro Mizuno, Kohji Yamada, Kenji Takahashi на конференции Proceedings of the 2005 Workshop on Digital Identity Management в докладе «Authentication using multiple communication channels» предложили метод аутентификации с использованием нескольких коммуникационных каналов (МСА), однако общее состояние развития ИС и коммуникационных каналов на 2005 год не позволило выделить данный метод в отдельный подход цифровой аутентификации и МСА принято рассматривать как фактор владения. МСА - интересен с точки зрения повышения степени надежности информационной безопасности. На данный момент метод представлен в виде использования вторичного канала связи для проведения цифровой аутентификации одним из выше перечисленных классических методов аутентификации. Такой подход называется внеполосным (Out-Of-Band).

Также стоит отметить частный вариант фактора владения – так называемые «magic links» (ML) - аутентификация субъекта/объекта ИС при

помощи верификации доступности ему заранее указанного некоего объекта владения.

После анализа различных систем, используемых в ИС для цифровой аутентификации субъектов/объектов ИС, были выделены некоторые критерии и свойства этих систем – результаты представлены в таблице 1.

Таблица 1

		Стоимость внедрения	Стоимость обслуживания	Степень надежности ИБ	Сложность внедрения	Производительность использования
SFA	знание	9	2	1	9	9
	владение	3	3	6	1	7
	свойство	4	8	7	5	6
2FA		4	5	8	7	6
MFA		3	3	9	2	3
OOB		4	4	8	5	7
ML		8	8	2	8	7

Оценка от 1 до 10 (где 1 – хуже, 10 – лучше)

Ввиду того, что критерии не являются взаимозаменяемыми, данный анализ не позволяет сделать выбор наилучшего метода или дать абсолютную оценку той или иной системы цифровой аутентификации, используемой в ИС, однако приведенная таблица позволяет сделать предположение о существующих запросах к системам, использующим методы цифровой аутентификации.

По итогам проведенного анализа можно сделать следующие выводы: 1) наиболее эффективными являются методы, использующие комбинацию факторов, наиболее экономически выгодными являются методы не использующие внешнее программное обеспечение или оборудование, существует высокая потребность в методах имеющих высокую производительность и высокую степень надежности; 2) недостаточность вариантов комбинирования факторов аутентификации не позволяет существующим методам значительно улучшить экономическую эффективность, повысить степень надежности с точки зрения информационной безопасности, удешевить/ускорить внедрение, разработать производительные решения для высоконагруженных ИС; 3) интересным, с точки зрения систематизации подхода к данному вопросу как предмета научного исследования, является тот факт, что все методы используют коммуникационные каналы в том или ином виде или в той или иной комбинации, и это позволяет сделать предположение о том, что, возможно, неверно использовать термин «фактор» по отношению к коммуникационным каналам. Данное предположение, а также значительный положительный тренд развития ИС, коммуникационных каналов и способов их взаимодействия и

использования позволяет нам попробовать рассмотреть МСА более углубленно.

Научный руководитель д.т.н, проф. Корченко А.Г.

Обеспечение функциональной устойчивости и кибербезопасности виртуальных облачных ресурсов систем дистанционного обучения университета

УДК 621.39:004

Б.Б.Ахметов[1],А.Б.Адранова[2]

[1]*Университет Есенова**, Актау**, Казахстан, berik.akhmetov@yu.edu.kz*

[2]*Казахский национальный педагогический университет имени Абая, Алматы, Казахстан, assel.adranova@gmail.com*

Введение. Современное развитие информационных технологий (ИТ), в учебном процессе многих крупных университетов), характеризуется широким использованием облачных ресурсов, находящихся в центрах обработки данных (ЦОД). Такие центры представляют собой совокупность серверов, располагающихся на одной площадке с целью повышения их функциональной устойчивости (ФУ) и кибернетической безопасности (КБ). В авторы так определяют облачные вычисления (ОбВ). «Это модель обеспечения повсеместного и удобного доступа посредством сети к общему пулу, включающему вычислительные ресурсы, которые подлежат настройке. К таким ресурсам можно отнести: коммуникационные сети, серверы, средства хранения данных, приложений и сервисы. Ресурсы могут быть оперативно предоставляться освобождаться с минимальными эксплуатационными затратами или обращением к провайдеру».

К облачным технологиям активно проявили интерес как крупные холдинги, которые пытаются оптимизировать свои расходы на IT-инфраструктуру предприятия, так и малые компании, или учебные заведения, которые не имеют возможности сразу развернуть свою собственную инфраструктуру. Также в качестве заинтересованных лиц выступают обычные пользователи. При этом рядовых пользователей, прежде всего, интересует возможность хранения данных, и использование программ. В ходе эксплуатации облачных ресурсов потребители заинтересованы в существенном снижении капитальных затрат на построение ЦОД, закупку серверных и сетевых компонентов оборудования, обеспечении непрерывности и работоспособности ИТ инфраструктуры своих предприятий. Все эти ресурсоёмкие и сложные вопросы при использовании облака переводятся от пользователей на провайдеров облачных услуг. Пользователь лишь оплачивает фактические услуги. Также облачные сервисы предоставляют пользователям гибкость в настройке. Например, можно самостоятельно регулировать такие параметры, как вычислительная мощность, объемы файловых хранилищ, состав программного обеспечения (ПО) и тому подобное. Несмотря на явные преимущества ОбВ возникают и проблемные вопросы. Основными из них являются следующие: недостаточное доверие к поставщику сервиса; необходимость надежно обеспечить конфиденциальность, целостность,

подлинность информации в облаке; функциональную устойчивость информации на всех этапах ее существования; гарантировать бесперебойную работу и защиту от несанкционированного доступа (НСД); сохранения личных данных пользователей, которые передаются и обрабатываются в облаке.

Конфиденциальность при работе с облачными ИТ – это не только задача поставщиков, которые должны обеспечивать как физическую, так и программную неприкосновенность хранимых данных со стороны третьих лиц. Современные «облачные» ЦОД, как правило, проектируют опираясь на самые современные стандарты в области КБ (включая вопросы антивирусной защиты, шифрования, системы обнаружения вторжений (СОВ) и др.).

Функциональная устойчивость серверов в ЦОД обеспечивается сетевой и физической защитой, а также средствами обеспечения отказоустойчивости и надежным электропитанием. Сегодня на рынке представлен широкий спектр аппаратно-программных решений для обеспечения ФУ и КБ серверов, ориентированных на узкий круг задач. Однако вследствие постепенной замены классических аппаратных и программных систем виртуальными платформами, количество подобных задач существенно увеличилось и продолжает расти.

К известным типам угроз для целостности ФУ и КБ (сетевые атаки, уязвимости в приложениях операционных систем (ОС), вредоносное программное обеспечение) за последние годы добавились новые. К таким новым угрозам можно отнести такие – организация контроля среды (гипервизор), контроль за трафиком между гостевыми машинами и сложности с разграничением прав доступа. Поэтому работа современных ЦОД в ряде отраслей требует повышения уровня технических требований для обеспечения их ФУ. Причем это в полной мере относиться не только к облачным технологиям в образовании, но к более серьезной облачной архитектуре, которая, например, может использоваться в банках, промышленности на транспорте, словом в инфраструктуре критически важных компьютерных систем.

Появление и развитие технологий виртуализации вызвало масштабную миграцию большинства систем на виртуальные машины (ВМ). При этом решение задач обеспечения ФУ и КБ, связанные с эксплуатацией ПО в новой среде, требует иного подхода. Многие типы киберугроз достаточно изучены и для них разработаны соответствующие средства и методы противодействия. Однако такие методы необходимо адаптировать для использования в облаке. Проникновение платформ, базирующихся на технологиях виртуализации, достигло уровня, когда практически все компании, использующие эти системы, достаточно серьезно стали заниматься вопросами ФУ и КБ облака.

На сегодняшний день многие вопросы по повышению ФУ и КБ виртуальных облачных ресурсов полностью не исследованы. В существующих разработках решения такого типа задач имеют существенные недостатки. В частности, ряд исследователей констатируют отсутствие универсального метода для обеспечения ФУ и КБ облачных ресурсов из-за:

1) постоянных изменений возможностей, существующих ВМ в облачных информационных системах;

2) использования незащищенных интерфейсов приложений;

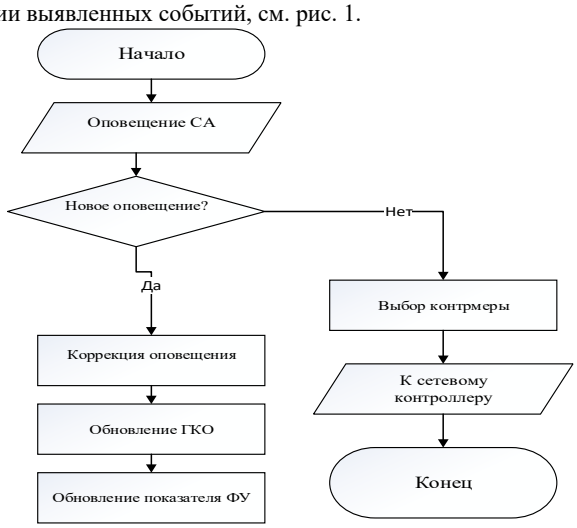
3) высокой ресурсоемкости существующих систем.

Поэтому, тема статьи, которая посвящена решению научно-прикладной задачи по разработке ИТ для обеспечения функциональной устойчивости и кибербезопасности виртуальных облачных ресурсов на основе программно-конфигурируемых сетей, является актуальной.

Современные методы обеспечения ФУ виртуальных облачных ресурсов на основе программно-конфигурируемых сетей неразрывно связаны с работами.

Основной материал.

В процессе исследований была усовершенствована модель, описывающая влияния кибератаки на ВОР. Модель отличается от существующих тем, что для построения ребер в графе корреляции оповещения (ГКО) используется функция, в которой учитывается разница во времени между поступлениями оповещений от соседних узлов ($D(Alert)$ и $Alert$) в системе: $T = D(Alert) \bigcup Alert.$ Был разработан граф атак на ВОС, который позволяет получить информацию обо всех известных уязвимости системы, а также в режиме реального времени показывает состояние ФУ и КБ системы. Это дает возможность спрогнозировать возможные угрозы и атаки путем корреляции выявленных событий, см. рис. 1.



Принятые сокращения: СА – сетевой анализатор; ГКО – граф корреляции сообщения

Рис. 1. Алгоритм обеспечения ФУ и КБ ВОС на основе ПКС

Сценарий графа так (далее СГА) можно подать в формате кортежа: $SC_{ga} = \langle VR, ED \rangle$, где $VR-$ множество вершин графа атак (ГА); $ED-$ множество направленных ребер, соединяющих вершины ГА. Вершины ГА могут быть трех типов: $NO_{co}-$ узлы конъюнкции (для отображения уязвимости); $NO_{di}-$ узлы дизъюнкции (для обозначения результата использования злоумышленником уязвимости); корневой узел $NO_{ro}-$ (для обозначения начальной стадии сценария атаки).

Множество вершин ГА VR определим так: $VR = NO_{co} \cup NO_{dt} \cup NO_{ro}$.

Множество ребер $ed \in ED_{pre} \subseteq NO_{dt} \times NO_{co}$ отражает то, какие NO_{dt} должны быть выполнены, чтобы достичь NO_{co} . Ребро $ed \in ED_{post} \subseteq NO_{co} \times NO_{dt}$ означает, что узлы NO_{dt} должны быть получены, для того чтобы узлы NO_{co} были выполнены.

Тогда, справедливо $ED = ED_{pre} \cup ED_{post}$, где $ED_{pre}-$ ребра ГА, которые отражают взаимосвязь между результатом использования уязвимости в предыдущем узле с самой уязвимостью в следующем узле; $ED_{post}-$ ребра, которые отражают взаимосвязь между уязвимостями в предыдущем узле с возможными результатами использования уязвимостей в следующем узле.

Граф корреляции оповещения (ГКО) подадим как кортеж вида: $G_{cev} = \langle AL, ED, SR \rangle$, где $\{AL\}-$ множество, содержащее все оповещения $(Alert)$. Оповещение $al \in AL$ является структурой данных, которые включают IP-адреса источника и получателя, тип оповещения, а также временные метки; $SR-$ набор маршрутов прохождения атаки в ГКО.

Выводы.

Таким образом, новизна проведенных исследований заключается в том, что усовершенствованы модели:

влияния атаки на ВОР. Предложенная модель отличается от существующих тем, что для построения ребер в графе корреляции оповещения применена функция, учитывающая разницу во времени между поступлениями оповещений от соседних узлов в системе.

оценки состояния ВОР. Модель отличается от существующих тем, что для выбора контрмеры используются показатель оценки влияния

контрмеры на договор об уровне обслуживания BOP и показатель затрат, необходимых для применения контрмер с точки зрения ресурсов и операционной сложности.

Система генерації надійних паролів

УДК 004.056

Анна Кемпф[1], Юрій Хлапонін[2]

Київський національний університет будівництва і архітектури,
[1]hrust666@ukr.net, [2]y.khlaponin@gmail.com

Система генерації надійних паролів розроблена з метою підбору надійного та стійкого паролю на основі запиту користувача. Проект містить у собі елементи запитів штучного інтелекту, ця технологія є визначаючою при створенні системи генерації надійних паролів.

На сьогоднішній день існує така загроза безпеці користувача як використання ненадійних паролів.

Ненадійні паролі можуть бути звичайними словами або фразами, буквами або цифрами, що йдуть підряд. Люди часто використовують їх, коли не замислюються про безпеку або просто хочуть швидше закінчити реєстрацію. Пароль є ненадійним, якщо:

Його довжина менше, ніж 12 символів

Він складається з:

- Легкої послідовності цифр: 12345, 228228, 10011001
- Дати народження або пам'ятної дати: 13051998, 19900513, 0151
- Номера телефону: 380996668849, 0958378769
- Поширених слів: password, qwerty, administrator, user, student
- Імені користувача, імен родичів або домашніх тварин: lisa, alex, oleg, barsik, vasya
- Відомої географічної назви: ukraine, kyiv, dnipro
- Юзернейму або його частини: username_example, oleg99
- Електронної пошти або іншого ресурсу: example@ukr.net, pochta@gmail.com

Такі паролі легко підібрати. Наприклад, хакеру знадобиться менше доби, щоб підібрати пароль «iryna20041998» і всього 13 секунд для пароля «qwerty12345».

При виборі пароля у людей виникають складності, тому що більшість з них не вміє створювати випадкові і сильні паролі. Якщо у вас є така проблема, щоб виправити її, можете спробувати метод, що описаний далі, або спеціальні додатки, що допоможуть із генерацією.

Що допоможе у створенні надійного паролю?

Для того, щоб легко створити надійний пароль та не бути у зоні небезпеки можна спробувати такий спосіб:

- обрати випадкову фразу або слово зі словника, написати її транслітом.
- замінити частину на спеціальні випадкові символи, але потрібно буде тримати пароль у пам'яті, тому ця заміна може створюватися за принципом схожості.
- у кінці або на початку кожного слова додати цифри та символи, аби довжина паролю була достатньою.

У вирішенні питання безпеки власного паролю авторами запропоновано власний мобільний додаток, що має назву «Система генерації надійних паролів». Усі паролі є випадковими та одноразовими, система не запам'ятовує жоден із них, а отже ніхто не може перехопити ваш пароль через додаток. Також визначним є те, що система працює без використання мережі Інтернет.

Розроблена система призначена для використання в смартфонах.

Додаток може бути встановлений власноруч користувачем, бо є програмою для пристроїв з операційною системою Android. Додаток повністю реалізований мовою C#, перші версії та діюча версія були розроблені у GeneratorAlpha, - це дозволило відстежувати побудову додатку на кожному кроці та прискорило його написання.

Дизайн додатку був розроблений у середовищі Figma, а окремі елементи за допомоги AdobeIllustrator.

Використання такого додатку - це відмінний спосіб згенерувати послідовність, тому що такий метод дійсно гарантує вам випадкову комбінацію слів у поєднанні із іншими символами. До того ж, утворену фразу буде легко запам'ятати.

Згенерований системою пароль є завжди доцільним, його довжина є ідеальною для дотримання безпеки користувача.

На рисунках бачимо готовий прототип додатку системи генерації надійних паролів з реальним паролем, що був згенерований системою із початковим словом «knuba».

Додаток змодельовано на мобільному пристрої під назвою «googlepixel 2 xl».

На Рис.1 пароль створено із використанням найбільшого словника (500 тис. англійських випадкових слів), до слова додано комбінацію із восьми довільних чисел від 0 до 9.

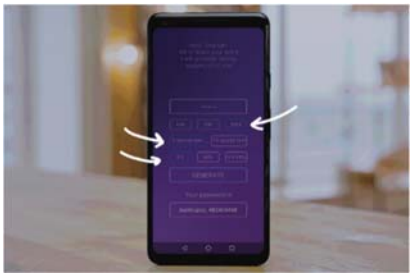


Рис. 1 – Прототип мобільного додатку для генерації надійних паролів

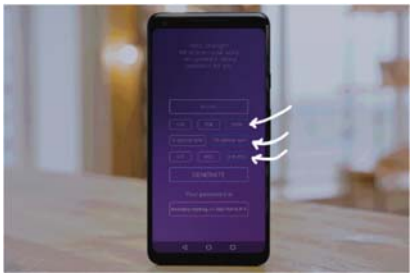


Рис. 2 - Прототип мобільного додатку для генерації надійних паролів із складнішим паролем більшої довжини

Результат генерації задовольняє усім вимогам у рамках надійності та стійкості. Слово є ассоціативним, робота додатку – коректною. На Рис. 2 змодельований пароль відрізняється тим, що додаткова комбінація складається із шістнадцяти спеціальних символів та чисел у поєднанні із словом.

Обидва паролі є стійкими, та відповідають вимогам щодо складності.

Розроблений мобільний додаток легко встановлюється та зручний у використанні.

Управління компетенціями працівників на підприємствах смарт індустрій

УДК 331.108.48

Олена Рудніцька[1], Дмитро Хлапонін[2], Віктор Сухомлін[3]

Київський національний університет будівництва і архітектури, [1]olena.rudnitska@gmail.com, Державний університет телекомунікацій, [2]kmld.85@gmail.com, Інститут підготовки кадрів Державної служби зайнятості України, [3]Suhomlin63@ukr.net

Спроби впровадження рішень, що ґрунтуються на підходах концепції Індустрії 4.0, а також впровадженні рішень у таких напрямках як «розумне виробництво», «розумне\безпечне місто», «розумне сільське господарство», Інтернет речей тощо, виявила гостру нестача фахівців, які можуть працювати на стику декількох спеціальностей. Поняття професії – застаріло. На перший план виходить набір компетенцій, як соціальних так і професійних. що часто є симбіозом компетенцій декількох професій.

Для соціального та економічного прогресу освіта та знання є ключовими ресурсами. Так, у звіті Європейської комісії наголошується, що підтримка зростання потребує кращого використання наявних трудових резервів. Для цього пропонується постійно збільшувати інвестиції в розвиток персоналу для підвищення їх продуктивності та працездатності.

Зокрема, вирішальне значення для процвітання країни має дефіцит знаннєвих ресурсів та, як наслідок, інноваційних чинників. В цьому контексті можна виділити такі аспекти:

- Ускладнення виробничих умов за рахунок ускладнення виробничих технологій.
- Скорочення життєвого циклу продукції для покращення фінансових показників підприємства.
- staffturnover (плинність кадрів).

Для адаптації до цих нових обставин важливо удосконалювати підхід до процесу управління компетенціями та знаннями. Завдяки все більш складним технологіям формувати компетенції стає складніше, але при цьому процес має відбуватися швидше. Зрозуміло, що підприємствам важливо забезпечити швидкий розвиток компетенцій фахівців в різних сферах. Це потребуватиме нових способів навчання та управління швидким зростанням знань. Таким чином, слід вирішувати наступні проблеми:

- Розвиток навчальних організацій для підтримки конкурентоспроможності
- Нові навчальні системи та методи
- Вдосконалення інтеграції науки та практики з метою забезпечення передачі знань з наукових установ до промисловості та навпаки

- Поліпшення інноваційної діяльності та інноваційної здатності організацій.

За даними NationMaster (база даних статистики, яка пропонує великий каталог змінних для цілей порівняння) в Україні на 2018 рік з усього працездатного населення 15.8% було задіяно в сільському господарстві (порівняно з 25% у 1996 році), 18.5% у промисловості (порівняно з 20% у 1996 році) та 65.7% у секторі послуг (порівняно з 55% у 1996 році).

В Україні, як і в багатьох європейських країнах вікова структура населення кардинально зміниться в найближчі роки. Ця тенденція сягає корінням в основному у скорочення народжуваності у поєднанні зі незначним збільшенням тривалості життя. До 2030 року населення світу у віці старше 65 років подвоїться і досягне 1 мільярда, збільшуючи питому вагу людей у віці 65 років та більше.

Щоб забезпечити універсальність виробничої системи, швидке, дешеве виробництво товарів без помилок, а також стійкість та орієнтацію на ресурси, потрібні працівники, яких можна «розгорнути» гнучко. Гнучкість повинна, крім часової гнучкості щодо робочого часу, стосуватися і здібностей персоналу.

Це призводить до різнобічного набору вимог до працівників. Різноманітність компетенцій повинна базуватися на знаннях та кваліфікації з різних сфер діяльності. Важливим фактором ефективного управління компетенціями є вибір методу опису компетенцій на підприємствах смарт індустрій. З цією метою можуть використовуватись такі методи:

- Метод аналізу робіт
- Метод прогностичного інтерв'ю (проводиться з керівниками, як в індивідуальному так і в груповому форматі)
- Метод критичних інцидентів (дозволяє зібрати інформацію про події, що вже відбувалися в компанії, як правило про кращі та гірші способи вирішення стандартних задач та співставлення їх)
- Метод аналізу задач
- Метод включеного спостереження
- Аналіз документів
- Метод аналізу діяльності, що орієнтований на властивості особистості

Для ефективного управління компетенціями на підприємствах смарт індустрій пропонується наступний процес:

- Створення профілю компетенцій працівника на основі моделі компетенцій підприємства
- Створення профілю компетенцій посади
- Порівняння профілю компетенцій працівника та профілю компетенцій посади
- Побудова плану навчання на основі різниці профілейкомпетенцій працівника та посади
- Навчанняпрацівника та оцінка отриманих компетенцій.
- Оновлення профілю компетенцій працівника

Цей процес за потреби може повторюватись, наприклад, при створенні нових посад, при зміні умов чи технологій виробництва тощо.

Дослідження стандартів забезпечення кібербезпеки хмарних технологій як сервісів

УДК 004.738.5

Тетяна Смірнова[1], Євгеній Солових, Олексій Смірнов[2]

Центральноукраїнський національний технічний університет,
[1]sm.tetyana@gmail.com, [2]dr.smirnovoa@gmail.com

Сучасний стан розвитку технологій визначає, що більшість інформаційних систем можливо представити у вигляді хмарних технологій як сервісів. Перед авторами поставлено завдання створення інформаційної системи інженерних розрахунків для оптимізації технологічних процесів відновлення поверхонь деталей у вигляді відповідного хмарного сервісу.

Метою даної роботи є дослідження існуючих хмарних технологій як сервісів та стандартів забезпечення кібербезпеки.

Для досягнення мети, у даній роботі проводиться аналіз існуючих хмарних платформ як сервісів, визначення типу хмарної платформи, як сервісу, яку можливо використовувати для вирішення поставленого завдання, й виявлення стандартів та механізмів забезпечення кібербезпеки хмарних технологій та сервісів.

Будь-яку послугу, що надається користувачеві за запитом через Інтернет із серверів постачальників хмарних обчислень будемо називати *хмарним сервісом* (as a Service, aaS). Таким чином хмарні сервіси саме і створені для того, щоб забезпечити простий, масштабований доступ і повністю керуються постачальником хмарних послуг.

Першим етапом було проведення дослідження існуючих хмарних платформ як сервісів. Були досліджені наступні платформи:

– Content as a service (CaaS) – або managed content as a service (MCaaS) – (керований контент як сервіс).
– Data as a service (DaaS) – дані як сервіс.
– Desktop as a service (теж DaaS) – робочий стіл як сервіс.
– Function as a service (FaaS) – функція як сервіс.
– Infrastructure as a service (IaaS) – інфраструктура як сервіс.
– Integration platform as a service (IPaaS) – інтеграційна платформа як сервіс.
– Mobile backend as a service (MBaaS) – мобільний сервіс як послуга або Backend as a Service (BaaS) – бекенд як сервіс.
– Network as a service (NaaS) – мережа як сервіс .
– Platform as a service (PaaS) – платформа як сервіс або application platform as a service (aPaaS) – платформа застосунків як послуга або послуга на основі платформи.
– Security as a service (SECaaS або SaaS) – безпека як сервіс.
– Software as a Service (SaaS) – програмне забезпечення як сервіс.
– Data Base as a Service (DBaaS) – база даних як сервіс.

– Information as a Service (теж IaaS) – інформація як сервіс.
– Integration as a Service (теж IaaS) – інтеграція як сервіс.
– Management або Governance as a Service (MaaS або GaaS) – адміністрування або керування як сервіс.
– Process as a Service (теж PaaS) – процес як сервіс.
– Storage as a Service (STaaS) – зберігання як сервіс.
– Testing as a Service (TaaS) – тестування як сервіс.
– Disaster Recovery as a Service (DRaaS) – аварійне відновлення як сервіс.
– Backup as a Service (BaaS) – резервне копіювання як сервіс.
– Monitoring as a Service (MaaS) – моніторинг як сервіс.
– Hardware as a Service (HaaS) – устаткування як сервіс.
– Communications as a Service (CaaS) – комунікація як сервіс.
– Container as a Service (CaaS) – контейнер як сервіс.
– Resourse as a Service (RaaS) – ресурс як послуга.
– Customer Relationship Management as a Service (CRMaaS) – керування взаємовідносинами з клієнтами як сервіс.
– Bookkeeping as a Service (BaaS) – бухгалтерський облік як сервіс.

На другому етапі було виявлено, що хмарною платформою, яка підходить для вирішення поставленого перед авторами завдання є сервіс CAEaaS (Computer Aided Engineering as a Service) – комп'ютерні системи інженерного аналізу як сервіс, який покликаний перенести роботу систем інженерних розрахунків та систем автоматизованого проектування (САПР) на хмарну платформу.

На третьому етапі, проведені дослідження та аналіз існуючих робіт у цій області дозволив виявити наступні стандарти та механізми забезпечення кібербезпеки хмарних технологій та сервісів:

1. Криптографічні методи: ISO/IEC 18033, IEEE 1363, ISO/IEC 29192.
2. Управління інцидентами: ISO/IEC 27035, ITU-T X.1056.
3. Управління ідентифікацією
4. Системи управління інформаційною безпекою: ISO/IEC 27000.
5. Оцінка інформаційної безпеки IT-систем: ISO/IEC 19790:2015, ISO/IEC 24759:2014, ISO/IEC TR 30104:2015, ISO/IEC 15408-3.
6. Мережева інформаційна безпека: ISA/IEC-62443.
7. Автоматизований та неперевний моніторинг інформаційної безпеки.
8. Гарантований супровід ПЗ: ISO/IEC 19770-2.
9. Управління ризиками/ланцюгами ризиків.
10. Система інженерії інформаційної безпеки: ISO/IEC 21827:2008, ISA/IEC 62443.

Таким чином, у подальшому потребує необхідності вирішення задача визначення загроз кібербезпеки для CAEaaS, яке призначено для реалізації інформаційної технології відновлення поверхонь деталей, та методів протидії загрозам кібербезпеки даного хмарного сервісу. з використанням розглянутих вище стандартів.

Інноваційне управління рухом суден

УДК 53.043

Геннадій Вільський
Миколаївський науково-навчальний центр освіти дорослих,
g.vilsky@gmail.com

Підтримка безпеки судноводіння в районах з лоцманським проведенням морських суден, біля берегів, у вузкостях і на акваторіях портів виконується завдяки засобів радіозв'язку, радіолокаційних станцій, пристроїв оцінки небезпеки зіткнення суден та автоматичних інформаційних систем [1]. Таке управління не включає встановлення і врахування інформаційної безпеки руху суден та унеможливлює швидке відбиття динаміки змін загроз і ризиків судноплавству.

Метою даної роботи є висвітлення інноваційних пропозицій з інформаційної безпеки управління рухом морських суден для підвищення безпеки судноплавства. Прийняття рішень з управління рухом суден в особливих умовах плавання базується на інформації отриманої, як правило, від станцій радіозв'язку і радарів, яку обробляють і аналізують тільки лоцмани-оператори координаційних центрів та постів регулювання рухом суден. Такий процес пов'язаний з небезпекою існуючої інформації, яка призводить до помилок в прийнятті команд на містках суден та до ризиків аварійності.

Інноваційне рішення з управління рухом суден відображено в [2]. Воно включає отримання даних про координати рухомих об'єктів і параметрах їх руху, їх вторинну обробку в обчислювальному комплексі та відображення на екрані індикатора обстановки інформації про рух рухомих об'єктів. Обов’язково встановлюються поворотні точки які кодуються і представляються графами кодових перетинів. При цьому здійснюється тільки загальний візуальний огляд навігаційної обстановки на підконтрольній території.

Найбільше оригінальна інноваційна пропозиція з управління рухом морських суден включає обробку інформації про поточні координати суден з встановленням конкретного фактору небезпеки. Для зон точок поворотів, маневрувань і розбіжностей, формується статистична база інцидентів з даними про загрози і ризики інформаційної безпеки судна (ІБС), яким при електронній обробці надають іменні категорії. До переліку таких категорій з ризиками належать: "Посадка на ґрунт"; "Зіткнення"; "Навал"; "Льодова"; "Техногенний"; "Тероризм". Іменні категорії загроз і ризиків зазначених морських інцидентів представляють у вигляді динамічних статистичних усвідомлюваних діаграм, за якими кількісно оцінюють поточні зміни загроз і ризиків аварійності мореплавання. Представлення на екрані навігаційної обстановки автоматизованого робочого місця судноводія зазначених загроз і ризиків дозволяє: швидке отримання рішень про насування та подолання небезпек аварійності на ділянках поворотних точок; досягнути

зниження інформаційної небезпеки судна за допомогою мінімального складу технічного ресурсу суднового навігаційного комплексу; підвищити якість прогнозування та оцінки терміну рейсу. Процес визначення динаміки змін проявлення та спаду ризиків інформаційної безпеки судна ілюстровано надає рішення у вигляду усвідомлюваним імовірних діаграмам [3]. Практика представлення розрахованих і побудованих усвідомлюваних імовірнісних поверхневих і лінійно-стовпчастих діаграмам ризиків інформаційної безпеки судна на підконтрольних ділянках водного шляху базується також показом відповідних графіків. Пропонована інновація ілюструється щільністю імовірності «Посадка на грунт» від передумови виникнення загрози "Втрата орієнтації в навігаційних обставинах" представлена у вигляді нормального розподілу Гауса кресленням на рис. 1. На рис. 2. показана поверхнева імовірнісна діаграма ризиків ІБС щодо аварійності морських суден, яка створюється за допомогою даних бортових систем і засобів телекомунікації (радіозв'язок,

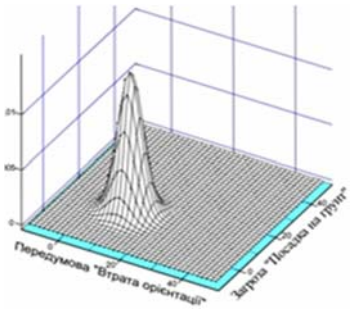


Рис.1. Щільність імовірності «Посадка на грунт»

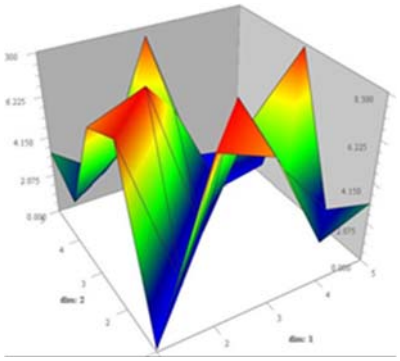


Рис. 2. Діаграма

ризиків ІБС

стільниковий зв'язок, глобальна морська система зв'язку при лихі) і за запитами від вахтової команди на містках суден. Для отриманого пакету усвідомлюваних імовірнісних діаграм, за розрахунковим алгоритмом, здійснюється кількісна оцінка параметрів ризиків і загроз аварійності. Таким чином з урахуванням плану руху і особливостей лоції маршруту водного шляху та згідно з даною інновацією встановлюються точки поворотів, в яких судна виконують безпечно маневрування і розбіжність. До переваг інновації відносяться: 1) Застосування комплексу дій своєчасно виявляється й ідентифікується корекція траєкторії руху; 2) Формалізація процедур звільняє лоцмана-оператора координаційного центру управління рухом суден, або поста регулювання рухом суден від півдговки рішень, а тільки зобов'язує його здійснювати постійний штатний контроль за відправленням електронних рекомендацій для команд на містках суден. Застосування зазначених інновацій забезпечує підвищення безпеки руху суден в районах з інтенсивним судноплавством.

Література

1. Вильский Г.Б. Информационная безопасность судовождения: монография.

// Г.Б Вильский// – Миколаїв: Видавництво ФОП Швець В.Д., 2014. – 336 с. ISBN 978-966-97563-2-1.

2. Патент 2395122 RU. Способ управления движением подвижных объектов

/ Борисова Л.Ф. // опубл. 20.07.2010.

3. Патент 131848 UA, Спосіб управління рухом морських суден / Вільський Г.Б.; Бень А.П.; Ходаковський В.Ф.// Дата чинного праву: 11.02.2019.

Аналіз криптографічного шифру ГОСТ 28147-89

УДК 621.391.25

Аліна Лапушинська[1], Роман Корольов[2]

Харківський національний економічний університет ім. С. Кузнеця,
[1]alapushinskaia@gmail.com, [2]korolovrv01@ukr.net

Інформація має цінність – це люди усвідомили дуже давно. З метою забезпечення конфіденційності інформації використовують особливий вид перетворень, який має назву «шифрування». Шифрування має на меті приховати змістовну та статистичну залежність між частинами вхідного повідомлення. Шифрувати можна будь-які повідомлення, що мають цінність для відправника або одержувача і можуть бути перехоплені третьою стороною з метою подальшого використання у своїх інтересах.

Саме тому з розвитком електронних обчислювальних машин та засобів їх взаємодії також розвивалися методи та засоби збереження конфіденційності інформації, які мають вигляд криптографічних програм та різноманітних шифрувальних пристроїв, які шифрують пакети або потоки даних, що використовуються для обміну інформацією між станціями локальних чи глобальних мереж та периферійними пристроями.

Серед усього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. Одним з таких методів є шифр ГОСТ 28147-89. Це один з найпростіших для розуміння та програмної реалізації шифр.

Сьогодні алгоритм залишається стійким для відомих атак, таким чином роблячи перспективним використання алгоритму у майбутньому. Цей стандарт визначає поблокове шифрування даних, з розміром блока 64 біти та довжиною ключа 256 біт. Алгоритм криптографічного перетворення має структуру мережі Фейстеля з 32-ма раундами та використовує операції додавання за модулем 2^{32}, додавання за модулем 2, нелінійної заміни S та циклічного зсуву. В роботі запропоновано удосконалений алгоритм ГОСТ 28147-89.

Метою даної роботи є розробка методу вдосконалення криптоперетворення в алгоритмі блочно-симетричного шифрування ГОСТ 28147-89 за рахунок збільшення довжини підблоків з 32 біт до 64 біт, що дає змогу обробляти вхідні блоки довжиною 128 біт та збільшити ключову послідовність з 256 біт до 512 біт без суттєвих змін основних кроків алгоритму ГОСТ 28147-89.

Структурна схема основного кроку удосконаленого криптоперетворення ГОСТ 28147-89 представлена на рисунку 1.

Рис.1. Схема основного кроку удосконаленого криптоперетворення ГОСТ 28147-89

Запропоновані рішення представлені в змінах основного кроку криптоперетворення ГОСТ 28147-89 дають змогу збільшити довжину ключової послідовності з 256 біт до 512 біт та збільшити довжину S блоку, не змінюючи основні кроки які використовуються в ГОСТ 28147-89, що ускладнює криптоаналіз.

Формування критеріїв для функціонального профілю захисту

УДК 004.056:004.75

Олександр Корченко[2], Анатолій Давиденко[3], Максим Шабан[1]

Інститут проблем моделювання в енергетиці[1,3], Національний авіаційний університет[2] , agkorchenko@gmail.com[2], davidenkoan@gmail.com[3], maximsaban@gmail.com[1]

Для вирішення задачі ідентифікації функціонального профіля захисту (ФПЗ) необхідно здійснити: визначення рівнів функціональних послуг безпеки (ФПБ), реалізованих в комплексних систем захисту інформації (КСЗІ) об'єкта експертизи; визначення повноти та несуперечності профілю; ідентифікацію опису ФПБ у вихідних документах. З урахуванням цього пропонується модель параметрів для ідентифікації ФПЗ в комп'ютерних системах (КС) [1].

Визначення множини критеріїв

Сформуємо множину усіх критеріїв захищеності інформації

$$\mathbf{МК} = \left\{ \bigcup_{q=1}^{w} \mathbf{МК}_{q} \right\} = \left\{ \mathbf{МК}_{1},\ \mathbf{МК}_{2},\ ...,\ \mathbf{МК}_{w} \right\}, \quad (1)$$

Визначення елементів множин критеріїв

Далі, на основі (1) визначимо елементи $\mathbf{МК}_{q}$ -ї множини критеріїв

$$\mathbf{МК}_{q} = \left\{ \bigcup_{e=1}^{w_q} \mathbf{МК}_{q,e} \right\} = \left\{ \mathbf{МК}_{q,1},\ \mathbf{МК}_{q,2},...,\ \mathbf{МК}_{q,w_q} \right\}, \quad (2)$$

де $\mathbf{МК}_{q,e} \subseteq \mathbf{МК}_{q}$ $(e = \overline{1, w_q})$ – e-й елемент $\mathbf{МК}_{q}$ -ї множини критеріїв, а w_q їх кількість.

Таким чином, (1) з урахуванням (2) представимо в наступному вигляді:

$$\mathbf{МК} = \left\{ \bigcup_{q=1}^{w} \mathbf{МК}_{q} \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \mathbf{МК}_{q,e} \right\} \right\} = \left\{ \left\{ \mathbf{МК}_{1,1},\ \mathbf{МК}_{1,2},\ ,\ ...,\ \mathbf{МК}_{1,w_1} \right\}, \right. \quad (3)$$

$$\left. \left\{ \mathbf{МК}_{2,1},\ \mathbf{МК}_{2,2},\ ,\ ...,\ \mathbf{МК}_{2,w_2} \right\},\ ...,\left\{ \mathbf{МК}_{w,1},\ \mathbf{МК}_{w,2},\ ,\ ...,\ \mathbf{МК}_{w,w_w} \right\} \right\}.$$

Визначення рівнів елементів множин критеріїв

Далі, на основі (3) визначимо рівень кожного елементи $\mathbf{МК}_{q,e}$ -го елемента $\mathbf{МК}_{q}$ -ї множини критеріїв

$$\mathbf{МК}_{\mathbf{q,e}} = \left\{ \bigcup_{\mathbf{y=1}}^{\mathbf{w_{q,e}}} \mathbf{МК}_{\mathbf{q,e,y}} \right\} = \left\{ \mathbf{МК}_{\mathbf{q,e,1}}, \mathbf{МК}_{\mathbf{q,e,2}}, .., \mathbf{МК}_{\mathbf{q,e,w_{q,e}}} \right\}. \quad (4)$$

де $\mathbf{МК_{q,e,y}} \subseteq \mathbf{МК_{q,e}}$ ($y = \overline{1, w_{q,e}}$) – y -й рівень $\mathbf{МК_{q,e}}$ -го елемента $\mathbf{МК}_q$ -ї множини критеріїв, а $w_{q,e}$ їх максимальний рівень.

Таким чином, (3) з урахуванням (4) має вигляд:

$$\mathbf{МК} = \left\{ \bigcup_{\mathbf{q=1}}^{\mathbf{w}} \mathbf{МК_q} \right\} = \left\{ \bigcup_{\mathbf{q=1}}^{\mathbf{w}} \left\{ \bigcup_{\mathbf{e=1}}^{\mathbf{w_q}} \mathbf{МК_{q,e}} \right\} \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \left\{ \bigcup_{y=1}^{w_{q,e}} МК_{q,e,y} \right\} \right\} \right\} =$$

$$\left\{ \bigcup_{q=1}^{w} \left\{ \bigcup_{e=1}^{w_q} \left\{ МК_{q,e,1}, МК_{q,e,2}, ..., МК_{q,e,w_{q,e}} \right\} \right\} \right\} = \left\{ \bigcup_{q=1}^{w} \left\{ \left\{ МК_{q,1,1}, МК_{q,1,2}, ..., МК_{q,1,w_{q,1}} \right\} \right\} \right.$$

$$\left. \left\{ МК_{q,2,1}, МК_{q,2,2}, ..., МК_{q,2,w_{q,2}} \right\}, ..., \left\{ МК_{q,w_q,1}, МК_{q,w_q,2}, ..., МК_{q,w_q,w_{q,w_q}} \right\} \right\} \right\} =$$

$$\left\{ \left\{ \left\{ МК_{1,1,1}, МК_{1,1,2}, ..., МК_{1,1,w_{1,1}} \right\}, \left\{ МК_{1,2,1}, МК_{1,2,2}, ..., МК_{1,2,w_{1,2}} \right\}, ..., \right.\right.$$

$$\left. \left\{ МК_{1,w_1,1}, МК_{1,w_1,2}, ..., МК_{1,w_1,w_{1,w_1}} \right\} \right\}, \left\{ \left\{ МК_{2,1,1}, МК_{2,1,2}, ..., МК_{2,1,w_{2,1}} \right\}, \right.$$

$$\left. \left\{ МК_{2,2,1}, МК_{2,2,2}, ..., МК_{2,2,w_{2,2}} \right\}, ..., \left\{ МК_{2,w_2,1}, МК_{2,w_2,2}, ..., МК_{2,w_2,w_{2,w_2}} \right\} \right\}, ...,$$

$$\left\{ \left\{ МК_{w,1,1}, МК_{w,1,2}, ..., МК_{w,1,w_{w,1}} \right\}, \left\{ МК_{w,2,1}, МК_{w,2,2}, ..., МК_{w,2,w_{w,2}} \right\}, ..., \right.$$

$$\left. \left. \left. МК_{w,w_w,1}, МК_{w,w_w,2}, ..., МК_{w,w_w,w_{w,w_w}} \right\} \right\} \right\}. \quad (5)$$

Висновок. Таким чином, в роботі запропонована модель параметрів, яка за рахунок теоретико-множинного представлення визначених множин критеріїв захищеності інформації, їх елементів та відповідних рівнів, дозволила у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації ФПЗ в КС. Далі, потрібно розробити метод ідентифікації ФПЗ, що дозволить автоматизувати процес визначення вимог щодо функцій захисту (послуг безпеки) та гарантій.

ЛІТЕРАТУРА

[1]. Vysotska O., Davydenko A.: Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. In: Hu Z., Petoukhov S., Dychka I., He M. (eds). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol. 938, pp. 356-368 (2019). DOI: https://doi.org/10.1007/978-3-030-16621-2_33

Модель смислових констант та змінних для експертиз ТЗІ

УДК 004.056:004.75

Юлія Гончаренко[2], Ольга Чолишкіна[3], Максим Шабан[1]

Інститут проблем моделювання в енергетиці[1], Національний авіаційний університет, greenhelga5@gmail.com[3], maximsaban@gmail.com[1]

Вступ. Проведення державних експертиз – це процес довготривалий і пов'язан з можливими помилками як на етапі проведення проектних робіт, так і під час проведення самої експертизи. Експерт повинен опрацювати усі документи, які були розроблені на етапі проектних робіт і виходячи з отриманої інформації розробити групу вихідних документів, а саме: «**Програма та методика проведення експертизи**», «**Перелік тестів**», «**Протокол випробувань**», «**Експертний висновок**». Час проведення державних експертиз різний, в залежності від обставин, але у середньому експертиза проводиться від 6 місяців до року. Це створює передумови для можливих помилок з боку експерта. Тому актуальним науковим завданням є створення інформаційної системи, яка б допомагала експерту при побудові вихідних документів, а також дозволяла б експерту перевірити функціональний профіль захисту (ФПЗ) [4] на предмет відповідності його нормативному документу НД ТЗІ 2.5.004-99 за формальними ознаками відповідності ФПЗ нормативному документу. Розглянемо більш детально проблеми з якими стикається експерт, а також шляхи їх вирішення. Досвід проведення державних експертиз КСЗІ [2] висвітлює проблему втрати часу на обробку великих масивів даних, звірку інформації на предмет її достовірності та, загалом, обробки великої кількості документів, які були створені на етапі предпроектних робіт. Таким чином, існує необхідність у створені моделі представлення документів для системи підтримки прийняття рішень (СППР) [1] при проведенні, наприклад, експертиз грід-засобів.

Далі, розглянемо модель декомпозиції вихідних документів, яка описує спосіб формування відповідних шаблонів документів. Вона складається з базових множин проектів документів експертизи технічного захисту інформації (ТЗІ) [3], множин смислових блоків (СБ) вихідних документів та структури взаємозв'язку змісту шаблона з множинами смислових змінних.

Базові множини проектів документів експертизи ТЗІ

Введемо множину всіх можливих документів

$$\mathbf{Doc}=\left\{\bigcup_{\mathbf{p=1}}^{\mathbf{m}}\mathbf{Doc_p}\right\}=\{\mathbf{Doc_1},\mathbf{Doc_2},...,\mathbf{Doc_m}\},(1)$$

де $\mathbf{Doc_p}$ – підмножина вхідних та вихідних документів *p*-го ($p=\overline{1,m}$) проекту, а

m –кількість можливих проектів.

Далі, використовуючи (1) визначимо

$$\mathbf{Doc_p} = \left\{\mathbf{Doc_p^{out}}, \mathbf{Doc_p^{in}}\right\}, \quad (3)$$

де $\mathbf{Doc_p^{out}}$, $\mathbf{Doc_p^{in}}$ – відповідно множини вихідних та вхідних документів p -го проекту підмножини $\mathbf{Doc_p}$.

З урахуванням (3) визначимо

$$\mathbf{Doc}_{\mathbf{p}}^{\mathbf{out}} = \left\{ \bigcup_{\mathbf{i=1}}^{\mathbf{z}} \mathbf{Doc}_{\mathbf{p,i}}^{\mathbf{SBout}} \right\} = \left\{ \mathbf{Doc}_{\mathbf{p,1}}^{\mathbf{out}}, \mathbf{Doc}_{\mathbf{p,2}}^{\mathbf{out}}, ..., \mathbf{Doc}_{\mathbf{p,z}}^{\mathbf{out}} \right\}, \quad (4)$$

де $\mathbf{Doc_{pi}^{out}}$ – підмножина СБ i -го ($\mathrm{i} = \overline{1,\mathrm{z}}$) вихідного документа p -го проекту, а z – кількість вихідних документів.

Використовуючи (3) сформуємо множину вхідних документів

$$\mathbf{Doc}_{\mathbf{p}}^{\mathbf{in}} = \left\{ \bigcup_{\mathbf{l=1}}^{\mathbf{v}} \mathbf{Doc}_{\mathbf{p,l}}^{\mathbf{in}} \right\} = \left\{ \mathbf{Doc}_{\mathbf{p,1}}^{\mathbf{in}}, \mathbf{Doc}_{\mathbf{p,2}}^{\mathbf{in}}, ..., \mathbf{Doc}_{\mathbf{p,v}}^{\mathbf{in}} \right\}, \quad (6)$$

де $\mathbf{Doc_{p,l}^{in}}$ – підмножина СБ l -го ($\mathrm{l}=\overline{1,\mathrm{v}}$) вхідного документа p -го проекту, а v – кількість вхідних документів.

Далі, використовуючи (4) визначимо підмножину СБ i -го ($\mathrm{i} = \overline{1,\mathrm{z}}$) вихідного документу p -го ($p = \overline{1,m}$) проекту

$$\mathbf{Doc}_{\mathbf{p,i}}^{\mathbf{out}} = \left\{ \bigcup_{\mathbf{i=1}}^{\mathbf{z}} \left\{ \bigcup_{\mathbf{j=1}}^{\mathbf{S_i}} \mathbf{SB}_{\mathbf{p,i,j}}^{\mathbf{out}} \right\} \right\} = \bigcup_{\mathbf{i=1}}^{\mathbf{z}} \left\{ \mathbf{SB}_{\mathbf{p,i,1}}^{\mathbf{out}}, \mathbf{SB}_{\mathbf{p,i,2}}^{\mathbf{out}}, ..., \mathbf{SB}_{\mathbf{p,i,S_z}}^{\mathbf{out}} \right\} = \left\{ \left\{ \mathbf{SB}_{\mathbf{P,1,1}}^{\mathbf{out}}, \mathbf{SB}_{\mathbf{P,1,2}}^{\mathbf{out}}, ..., \mathbf{SB}_{\mathbf{P,1,S_1}}^{\mathbf{out}} \right\}, \right.$$

$$\left. \left\{ \mathbf{SB}_{\mathbf{P,2,1}}^{\mathbf{out}}, \mathbf{SB}_{\mathbf{P,2,2}}^{\mathbf{out}}, ..., \mathbf{SB}_{\mathbf{P,2,S_2}}^{\mathbf{out}} \right\}, ..., \left\{ \mathbf{SB}_{\mathbf{P,z,1}}^{\mathbf{out}}, \mathbf{SB}_{\mathbf{P,z,2}}^{\mathbf{out}}, ..., \mathbf{SB}_{\mathbf{P,z,S_z}}^{\mathbf{out}} \right\} \right\},$$

(8)

де S_i – кількість СБ i -го ($\mathrm{i}=\overline{1,\mathrm{z}}$) вихідного документу.

Множини СБ вихідних документів).

Визначамо принцип формування змісту СБ. Кожен СБ складається з множини смислових змінних (СЗ) і констант (СК), де СК – це стійка смислова конструкція, час існування якої виходить за межі проведення державної експертизи КСЗІ. В свою чергу, СЗ – це смислова конструкція, час існування якої відбувається протягом державної експертизи КСЗІ.

Побудова моделі передбачає проведення ручного аналізу кожного вихідного документу на предмет виявлення стійких семантичних конструкції для подальшої побудови типового шаблона документа.

Розпишемо кожен СБ як об’єднання множин СК та СЗ.

Тоді, вираз (8) для СБ вихідного документу $\mathbf{SB}_{\mathbf{pij}}^{\mathbf{out}}$ має вигляд

$$\mathbf{SB}_{\mathbf{p,i,j}}^{\mathbf{out}}=\left\{\bigcup_{i=1}^{z}\left\{\bigcup_{j=1}^{S_i}\left\{\left\{\bigcup_{a=1}^{t_{i,j}}SC_{p,i,j,a}^{out}\right\},\left\{\bigcup_{b=1}^{r_{i,j}}SV_{p,i,j,b}^{out}\right\}\right\}\right\}\right\}=$$

$$\bigcup_{i=1}^{z}\bigcup_{j=1}^{S_i}\left\{\left\{SC_{p,i,j,1}^{out},SC_{p,i,j,2}^{out},...,SC_{p,i,j,t_{i,j}}^{out}\right\},\left\{SV_{p,i,j,1}^{out},SV_{p,i,j,2}^{out},...,SV_{p,i,j,r_{i,j}}^{out}\right\}\right\}=$$

$$\bigcup_{i=1}^{z}\left\{\left\{\left\{SC_{p,i,1,1}^{out},SC_{p,i,1,2}^{out},...,SC_{p,i,1,t_{i,1}}^{out}\right\},\left\{SV_{p,i,1,1}^{out},SV_{p,i,1,2}^{out},...,SV_{p,i,1,r_{i,1}}^{out}\right\}\right\},\right.$$

$$\left\{\left\{SC_{p,i,2,1}^{out},SC_{p,i,2,2}^{out},...,SC_{p,i,2,t_{i,2}}^{out}\right\},\left\{SV_{p,i,2,1}^{out},SV_{p,i,2,2}^{out},...,SV_{p,i,2,r_{i,2}}^{out}\right\}\right\},...,$$

$$\left.\left\{\left\{SC_{p,i,S_i,t_{i,1}}^{out},SC_{p,i,S_i,t_{i,2}}^{out},...,SC_{p,i,S_i,t_{i,S_i}}^{out}\right\},\left\{SV_{p,i,S_i,r_{i,1}}^{out},SV_{p,i,S_i,r_{i,2}}^{out},...,SV_{p,i,S_i,r_{i,S_i}}^{out}\right\}\right\}\right\}=$$

$$\left\{\left\{\left\{SC_{p,1,1,1}^{out},SC_{p,1,1,2}^{out},...,SC_{p,1,1,t_{1,1}}^{out}\right\},\left\{SV_{p,1,1,1}^{out},SV_{p,1,1,2}^{out},...,SV_{p,1,1,r_{1,1}}^{out}\right\}\right\},\right.$$

$$\left\{\left\{SC_{p,1,2,1}^{out},SC_{p,1,2,2}^{out},...,SC_{p,1,2,t_{1,2}}^{out}\right\},\left\{SV_{p,1,2,1}^{out},SV_{p,1,2,2}^{out},...,SV_{p,1,S_1,r_{1,2}}^{out}\right\}\right\},...,$$

$$\left\{\left\{SC_{p,1,S_1,t_{1,1}}^{out},SC_{p,1,S_1,t_{1,2}}^{out},...,SC_{p,1,S_1,t_{1,S_1}}^{out}\right\},\left\{SV_{p,1,S_1,r_{1,1}}^{out},SV_{p,1,S_1,r_{1,2}}^{out},...,SV_{p,1,S_1,r_{1,S_1}}^{out}\right\}\right\},$$

$$\left\{\left\{SC_{p,2,1,1}^{out},SC_{p,2,1,2}^{out},...,SC_{p,2,1,t_{2,1}}^{out}\right\},\left\{SV_{p,2,1,1}^{out},SV_{p,2,1,2}^{out},...,SV_{p,2,1,r_{2,1}}^{out}\right\}\right\},$$

$$\left\{\left\{SC_{p,2,2,1}^{out},SC_{p,2,2,2}^{out},...,SC_{p,2,2,t_{2,2}}^{out}\right\},\left\{SV_{p,2,2,1}^{out},SV_{p,2,2,2}^{out},...,SV_{p,2,2,r_{2,2}}^{out}\right\}\right\},...,\qquad(9)$$

$$,...,\left\{\left\{SC_{p,2,S_2,t_{2,1}}^{out},SC_{p,2,S_2,t_{2,2}}^{out},...,SC_{p,2,S_2,t_{2,S_2}}^{out}\right\},\left\{SV_{p,2,S_2,r_{2,1}}^{out},SV_{p,2,S_2,r_{2,2}}^{out},...,SV_{p,2,S_2,r_{2,S_2}}^{out}\right\}\right\},...,$$

$$,...,\left\{\left\{SC_{p,z,1,1}^{out},SC_{p,z,1,2}^{out},...,SC_{p,z,1,t_{z,1}}^{out}\right\},\left\{SV_{p,z,1,1}^{out},SV_{p,z,1,2}^{out},...,SV_{p,z,1,r_{z,1}}^{out}\right\}\right\},$$

$$\left\{\left\{SC_{p,z,2,1}^{out},SC_{p,z,2,2}^{out},...,SC_{p,z,2,t_{z,2}}^{out}\right\},\left\{SV_{p,z,2,1}^{out},SV_{p,z,2,2}^{out},...,SV_{p,z,2,r_{z,2}}^{out}\right\}\right\},...,$$

$$\left.,...,\left\{\left\{SC_{p,z,S_z,t_{z,1}}^{out},SC_{p,z,S_z,t_{z,2}}^{out},...,SC_{p,z,S_z,t_{z,S_z}}^{out}\right\},\left\{SV_{p,z,S_z,r_{z,1}}^{out},SV_{p,z,S_z,r_{z,2}}^{out},...,SV_{p,z,S_z,r_{z,Sz}}^{out}\right\}\right\}\right\},$$

де $t_{i,j}$ – ідентифікатор СК j -го смислового блоку S_i -ої кількості СБ i -го ($i=\overline{1,z}$) вихідного документу p -го проекту, а $r_{i,j}$ – ідентифікатор СЗ j -го смислового блоку S_i -ої кількості СБ i-го ($i=\overline{1,z}$) вихідного документу p -го проекту.

Структура взаємозв'язків змісту шаблона з множинами смислових змінних.

Таким чином, розглянувши декомпозиційну модель представлення СК та СЗ, з'являється можливість побудови шаблонів вихідних документів, якими є відформатований певним чином документ-заготовка, що зберігається в

окремому файлі та використовується як основа для створення документів. В шаблоні зберігаються різноманітні елементи, які становлять основу документа: СБ, графіка документа разом з призначеними ним атрибутами формату; параметри друкованої сторінки документа; список доступних стилів; макроси (послідовність дій, що автоматизують роботу з документом); елементи автотексту для вставки в документ текстових або графічних фрагментів; призначені для користувача панелі інструментів, меню та поєднання клавіш.

При створенні нового документа деякі з цих елементів (наприклад, СБ і стилі) копіюються в нього з обраного шаблону.

Побудова такого шаблону здійснюється при проведенні першої експертизи. При другій та наступних експертизах, у випадку повної або часткової зміни структури документу,. відбувається корегування шаблону.

Висновки. В роботі запропонована декомпозиційна модель, яка за рахунок сформованих множин вхідних та вихідних документів р-го проекту, а також множини смислових блоків, смислових констант та змінних р-го проекту дозволяє автоматизувати процес ідентифікації функціонального профілю захисту.

Модель процесса автоматизированного принятия решений при анализе чрезвычайных ситуаций на железнодорожном транспорте

УДК 614.86

Абуова А.К.
Казахский университет путей сообщения, akbala86@gmail.com

Введение. Подготовка, принятие и реализация управленческих решений по ликвидации чрезвычайных ситуаций (ЧС) и техногенных аварий (ТГА) на железнодорожном транспорте (ЖДТ) в максимально возможные короткие сроки является первостепенной задачей для управления ЖДТ. В целях сокращения времени на выработку и принятие обоснованного решения обоснована необходимость применения интеллектуальных компьютерных технологий для автоматизации процесса анализа ЧС на ЖДТ с автоматической генерацией рекомендаций руководителям по их ликвидации.

Основной материал. Для анализа возможностей выполнения СППР задач, стоящих перед руководителями служб, занимающихся ликвидацией ЧС на ЖДТ, они были формализованы для последующего синтеза моделей. Информационная модель ситуации представлена на рисунке 1.

Рис. 1. – Информационная модель оценки ситуации, связанной с ликвидацией последствий аварии или ЧС на ж.д.

Место ситуации V характеризуется следующими параметрами: v_1 – показатель, определяющий плотность заселенности района (местности) в котором произошло ЧС на ЖДТ. Чем более людно место ЧП, тем большее значение имеет v_1; v_2 – показатель, определяющий наличие на месте ЧП зданий, сооружений, учреждений с повышенным уровнем опасности. Значение v_2 зависит от уровня опасности сооружений и их количества; v_3 – географическое расположение места ЧП. В итоге получим: $V = \{v_1, v_2, v_3\}$.

Множество событий, описывающих ЧС на ЖДТ обозначим p: $p = \{p_1, ..., p_a\}, a = \overline{1,o}$, где p_a – отдельное событие, которое характеризует ЧС; o – общее возможное количество событий в процессе развития ЧС.

Время возникновения ЧС состоит из двух величин: $C = \{c_1, c_2\},$ где c_1 – абсолютное время возникновения ЧС, которое определяется датой и временем начала ЧС; c_2 – относительное время ЧС, т.е. промежуток времени который прошел от начала ЧС до момента поступления сообщения о ней.

Абсолютное время ситуации имеет отношение к количеству лиц, которые могут быть участниками или свидетелями ЧС и описывается двумя параметрами: время года ($c_{1,1}$) и время суток ($c_{1,2}$). Таким образом: $c_1 = \{c_{1,1}, c_{1,2}\}.$

Количество лиц, которые могут быть свидетелями ЧС, характеризуется показателем K, который зависит от показателей $V, C.$ Значение K возрастает с увеличением возможного количества человек. Статус ситуации S зависит от ее развития, если $S \to \min$, то ситуация является штатной, и, если $S \to \max$, то ситуация является чрезвычайной.

Множество типов ситуации обозначим T, $T = \{t_1, t_2, t_3, t_4\}$, где t_1 – показатель ситуации, который определяет необходимость привлечения

аварийных бригад ЖД; $t_2 -$ военнослужащих $t_3 -$ групп немедленного реагирования (ГНР) или следственно-оперативной группы (СОГ); $t_4 -$ применение других действий, не связанных с привлечением вышеупомянутых сил и средств.

В случае необходимости привлечения определенного вида сил, значение соответствующего показателя увеличивается, в противном случае – уменьшается.

Множество возможных решений для ликвидации ЧС обозначим как R, $R = \{r_j\}, j = \overline{1,q},$ где $r_j -$ одно из возможных решений конкретной ситуации; $q -$ общее возможное количество решений.

Формализованное представление модели для задач распознавания ситуаций и принятия первичных решений опишем так:

$$
\begin{aligned}
& r_j \in R_1, if \quad S \to \max \\
& r_j \in R_2, if \quad t_1 \to \max, \quad S, t_2, t_3, t_4 \to \min \\
& r_j \in R_2 \cup R_3, if \quad t_1, t_2 \to \max, \quad S, t_3, t_4 \to \min \\
& r_j \in R_2 \cup R_4, if \quad t_1, t_3 \to \max, \quad S, t_2, t_4 \to \min \\
& r_j \in R_2 \cup R_3 \cup R_4, if \quad t_1, t_2, t_3 \to \max, \quad S, t_4 \to \min \\
& r_j \in R_5, if \quad t_4 \to \max
\end{aligned}
\tag{1}
$$

где $R_1 -$ множество решений о признании ситуации чрезвычайной; $R_2 -$ множество решений о привлечении аварийных бригад ЖД $R_2 = \{r_{2,1}, ..., r_{2,f}\}, f = \overline{1,h}$; $r_{2,f} -$ решение о привлечении соответствующих аварийных бригад ЖД; $h -$ максимальное количество аварийных бригад ЖД на участке, где работает ЛПР; $R_3 -$ множество решений о привлечении военнослужащих для ликвидации ЧС на ЖД ; $R_3 = \{r_{3,1}, ..., r_{3,e}\}, e = \overline{1,g}$; $r_{3,e} -$ решение о привлечении соответствующего отряда (группы отрядов) военнослужащих для ликвидации ЧС на ЖД; $g -$ максимальное количество военнослужащих для ликвидации ЧС на ЖД на участке, где работает ЛПР; $R_4 -$ решение о привлечении ГНР или СОГ $R_4 = \{r_{4,1}, r_{4,2}\}$; $r_{4,1} -$ решение о

привлечении ГНР; $r_{4,2}$ – решение о привлечении СОГ; R_5 – множество решений о признании ситуацию такой, что не требует привлечения дополнительных сил и средств, $R_5 = \{r_5\}$.

Прогнозированием развития ситуации будем считать определение развития оперативной обстановки во времени, а именно, как изменятся место ЧС и события, ее характеризующие.

Множество последствий принятого решения N выглядит так: $N = \{n_1, n_2, n_3, n_4, n_5, n_6\}$, где n_1 – успешное завершение ситуации ($n_1 \to \max$) или наоборот ($n_1 \to \min$); n_2 – переход ситуации в чрезвычайное положение ($n_2 \to \max$) или наоборот ($n_2 \to \min$); n_3 – достаточность задействованных сил и средств, если задействованных сил и средств достаточно, то $n_3 \to \max$, если необходимо привлечь еще дополнительные силы $n_3 \to \min$; n_4 – убытки от ЧС на ЖД и людские жертвы $n_4 = [n_{4,1}, n_{4,2}, n_{4,3}]$; $n_{4,1}$ – количество физических потерь, $n_{4,2}$ – количество материальных убытков; $n_{4,3}$ – количество морального ущерба, с ростом количества соответствующих потерь $n_{4,1}, n_{4,2}, n_{4,3} \to \max$, с уменьшением $n_{4,1}, n_{4,2}, n_{4,3} \to \min$; n_5 – возможное количество потерь для стороны ликвидирующей ЧС на ЖД $n_5 = [n_{5,1}, n_{5,2}]$; $n_{5,1}$ – количество физических потерь среди личного состава стороны ликвидирующей ЧС; $n_{5,2}$ – количество материальных убытков, с ростом количества соответствующих потерь $n_{5,1}, n_{5,2} \to \max$, с уменьшением $n_{5,1}, n_{5,2} \to \min$; n_6 – время, за которое ситуация может быть решена. Чем быстрее будет решена ситуация, тем меньшее значение имеет n_6. В случае, если ситуация не может быть решена успешно или она переходит в чрезвычайное положение, $n_6 \to \max$

Формализованное представление модели в задачах прогнозирования развития ситуаций и определения последствий первоначальных решений представлено ниже.

$$n_1 = ((((\ p_{n_1 w} \setminus p_{n_1 u}) \setminus p_{sw}),\ (v_{3\ n_1 w} \setminus v_{3\ n_1 u}),\ v_1, v_2, c_{1,1}, c_{1,2}, c_2),\ r_j);$$

$$n_2 = ((\ p_{sw}, v_2, v_1, c_{1,1}, c_{1,2}),\ r_j);$$

$$n_3 = (((\ p_{n_3 w} \setminus p_{n_3 u}),\ (v_{3\ n_3 w} \setminus v_{3\ n_3 u})),\ r_j);$$

$$n_4 = (((\ p_{n_4 w} \setminus p_{n_4 u}),\ v_1, c_{1,1}, c_{1,2}),\ r_j);$$

$$n_5 = ((\ p_{n_5 w} \setminus p_{n_5 u}),\ r_j);$$

$$n_6 = ((\ p_{sw}, v_2, v_1, c_{1,1}, c_{1,2}),\ r_j),\ if\quad v_2, v_1, c_{1,1}, c_{1,2} \rightarrow$$

$$\rightarrow \max,\quad c_2 \rightarrow \min,\quad p`_{s\,w} \neq 0;$$

$$n_6 = (((\ p_{n_1 u} \setminus p_{n_1 w}),\ (v_{3\ n_1 u} \setminus v_{3\ n_1 w}),\ c_2),\ r_j),\ if\quad c_2 \rightarrow$$

$$\rightarrow \max;\quad p_{n_1 u} \neq 0, v_{3\ n_1 u} \neq 0;$$

(2)

где "\" - разность множеств; $p_{n_1 w}, p_{n_3 w}, p_{n_4 w}, p_{n_5 w}$ – события, которые при применении решения r_j способствуют высокому значению соответствующего последствия; $p_{n_1 u}, p_{n_3 u}, p_{n_4 u}, p_{n_5 u}$ – события, которые при применении решения r_j не способствуют высокому значению соответствующего последствия; $p_{s,w}$ – события, которые при применении решения r_j способствуют переходу ситуации в чрезвычайную; $v_{3\ n_1 w}, v_{3\ n_3 w}$ – места ситуации, которые при применении решения r_j способствуют высокому значению соответствующего последствия; $v_{3\ n_1 u}, v_{3\ n_3 u}$ – места ситуации, которые при применении решения r_j не способствуют высокому значению соответствующего последствия.

Для решения задач распознавания и оценивания ситуации на ЖДТ и принятия первичных решений по прогнозированию развития ситуации и определения последствий первичных решений предложено использовать аппарат искусственных нейронных сетей. Выбор этого аппарата мотивирован тем, что рассмотренные задачи относятся к слабо формализуемым. Таким задачам присуще большое количество возможных решений, а их исходные данные могут быть неточными, ошибочными или противоречивыми.

Выводы: обоснована необходимость применения интеллектуальных компьютерных технологий для автоматизации процесса анализа ЧС на ЖДТ с

автоматической генерацией рекомендаций руководителям (лицам, принимающим решение – ЛПР) по их ликвидации в целях сокращения времени на выработку и принятие обоснованного решения и проведена детализация задач, выполняемых ЛПР после поступления информации о ситуации. На основе детализированных задач, предложена концептуальную модель процесса принятия решения о ликвидации последствий ЧС на ЖД;

разработано новое формализованное описание модели для задач распознавания ситуации и принятия первоначальных решений. Модель отличается от известных тем, что в ней учитываются информационные зависимости параметров ситуации, которые доступны ЛПР. Это дает возможность формализовать процесс принятия решений по распознаванию и прогнозированию ситуации.

Научный руководитель – д.т.н., профессор, Лахно Валерий Анатольевич
д.т.н., профессор, Ахметов Бахытжан Сражатдинович

Теоретико-множинне представлення параметру «Рівень порушення» для кортежної GDPR-моделі

УДК 004.056.5

Ірина Лозова[1], Євгеній Педченко[2], Анастасія Баланда[3]

Національний авіаційний університет, [1]illozovaya@gmail.com, [2]ypedchenko@intrasystems.ua, [3]anasteisha.b.a@gmail.com

Для організацій, які здійснюють діяльність у просторі ЄС актуальним є питання відповідності нормам положень Регламенту GDPR, можливості оцінити власні масштаби збитку у разі його порушення та існуючі заходи забезпечення безпеки, щодо попередження витоку персональних даних.

Отже, постає задача розробки моделі, що дозволяє відповідно до положень Регламенту GDPR визначити множини вхідних та вихідних параметрів для формалізації процесу оцінювання збитків від втрати персональних даних.

Метою даної роботи є представлення параметру «Рівень порушення» з використанням теоретико-множинних підходів для побудови кортежної GDPR-моделі, що дозволить формалізувати процес оцінювання збитків від втрати персональних даних.

Один з параметрів кортежної GDPR-моделі є L – «Рівень порушення», що визначаємо виразом:

$$\mathbf{L} = \{\bigcup_{i=1}^{n_l} \mathbf{L_i}\} = \{\mathbf{L_1}, \mathbf{L_2}, ..., \mathbf{L_{n_l}}\}, \quad (1)$$

де: $\mathbf{L}$ – множина усіх можливих рівнів порушень, $\mathbf{L_i} \subseteq \mathbf{L}$ $(i = \overline{1,n_l})$ – i-та підмножина рівнів порушення, а n_l кількість таких підмножин.

Наприклад, при $n_l = 2$ $(i = \overline{1,2})$ формулу (1) можна представити як:

$$\mathbf{L} = \{\bigcup_{i=1}^{2} \mathbf{L_i}\} = \{\mathbf{L_1}, \mathbf{L_2}\} = \{\mathbf{"Ст.83, п.4", "Ст.83, п.5"}\},$$

де відповідно до Регламенту GDPR: $\mathbf{L_1} = \{\mathbf{"Ст.83, п.4"}\}$ та $\mathbf{L_2} = \{\mathbf{"Ст.83, п.5"}\}$, що відповідно трактується як: «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 10 000 000 євро або, у випадку підприємства, до 2% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою» та «На порушення таких положень, згідно з параграфом 2, поширюється застосування адміністративних штрафів сумою до 20 000 000 євро або, у випадку підприємства, до 4% від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою».

Далі, підмножину $\mathbf{L_i}$ визначимо як:

$$\mathbf{L_i} = \{\bigcup_{j=1}^{n_{li}} L_{ij}\} = \{L_{i1}, L_{i2}, ..., L_{in_{li}}\}, \quad (2)$$

де $L_{ij} \subseteq \mathbf{L_i}$ $(i = \overline{1,2}$, $j = \overline{1,n_{1i}})$ – j-а підмножина груп рівнів порушення споріднених за певною темою чи близьких за певними характеристиками у межах i-ї підмножини, а n_{1i} кількість груп i-ї підмножини.

Відповідно до статті 83 (п.4, п.5) та, з урахуванням (2) вираз (1) можна представити у такому вигляді:

$$\mathbf{L} = \{\bigcup_{i=1}^{n_1} \mathbf{L_i}\} = \{\bigcup_{i=1}^{n_1} \{\bigcup_{j=1}^{n_{1i}} L_{ij}\}\} = \{\{L_{11}, L_{12}, ..., L_{1n_{1i}}\}, \{L_{21}, L_{22}, ..., L_{2n_{1i}}\}, ..., \{L_{n_1 1}, L_{n_1 2}, ..., L_{n_1 n_{1i}}\}\}, \quad (3)$$

Тоді, наприклад, при $n_1 = 2$ $(i = \overline{1,2})$, $n_{11} = 3$ $(j = \overline{1,3})$, $n_{12} = 5$ $(j = \overline{1,5})$, формула (3) матиме вигляд:

$$\mathbf{L} = \{\bigcup_{i=1}^{2} \{\bigcup_{j=1}^{n_{1i}} L_{ij}\}\} = \{\{L_{11}, L_{12}, L_{13}\}, \{L_{21}, L_{22}, L_{23}, L_{24}, L_{25}\}\} =$$

$$\{\{\text{"Cm.83,n.4,nn.a"}, \text{"Cm.83,n.4,nn.b"}, \text{"Cm.83,n.4,nn.c"}\},$$

$$\{\text{"Cm.83,n.5,nn.a"}, \text{"Cm.83,n.5,nn.b"}, \text{"Cm.83,n.5,nn.c"}, \text{Cm.83,n.5,nn.d"}, \text{"Cm.83,n.5,nn.e"}\}\}$$

де: $L_{11} = \{\text{"Cm.83,n.4,nn.a"}\}$, $L_{12} = \{\text{"Cm.83,n.4,nn.b"}\}$, $L_{13} = \{\text{"Cm.83,n.4,nn.c"}\}$, $L_{21} = \{\text{"Cm.83,n.5,nn.a"}\}$, $L_{22} = \{\text{"Cm.83,n.4,nn.b"}\}$, $L_{23} = \{\text{"Cm.83,n.4,nn.c"}\}$, $L_{24} = \{\text{"Cm.83,n.4,nn.d"}\}$ та $L_{25} = \{\text{"Cm.83,n.4,nn.e"}\}$, що трактується як: «Обов'язки контролера і оператора відповідно до статей 8, 11, 25–39, і 42, і 43», «Обов'язки органу з сертифікації відповідно до статей 42 і 43», «Обов'язки органу з моніторингу відповідно до статті 41 (п.4)», «Основні принципи опрацювання, в тому числі умови надання згоди, відповідно до статей 5, 6, 7 і 9», «Права суб'єктів даних відповідно до статей 12–22», «Акти передавання персональних даних до одержувача в третій країні чи до міжнародної організації відповідно до статей 44–49», «Будь-які обов'язки відповідно до закону держави-члена, ухваленого згідно з главою IX» та «Невідповідність постанові або тимчасовому чи остаточному обмеженню на опрацювання чи призупинення потоків даних наглядового органу відповідно до статті 58 (п.2) або ненадання доступу як порушення статті 58 (п.1)».

Ієрархічну структуру параметра **L** можна представити у вигляді схеми на рис.

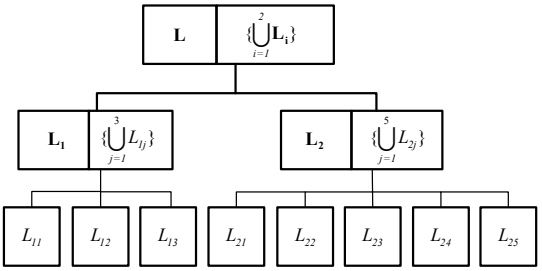


Рис. Ієрархічна структура параметра **L**

Отже, розроблено ієрархічну структуру та теоретико-множинне представлення параметра «Рівень порушення», що дозволить побудувати кортежну GDPR-модель, яка формалізує процес оцінювання збитків від втрати персональних даних.

Для фіналізації процесу створення GDPR-моделі в подальшому необхідно здійснити аналогічне представлення інших параметрів, що є складовими зазначеної моделі.

З історії створення вітчизняної системи охорони державної таємниці. Травень 1993 – січень 1994 рр.

УДК 35.078.3:342.738(091)(02)

Валерій Ворожко

Національний авіаційний університет, ГДА СБУ, wp06vv@gmail.com

Нині Україна протистоїть потужним зусиллям своїх зовнішніх і внутрішніх ворогів, мета яких – ліквідація української незалежної державності, знищення української нації та України як суб'єкта міжнародного права і геополітичної реальності. Сучасні суспільно-політичні виклики зумовлюють необхідність об'єктивного аналізу всіх складових функціонування «державного організму» України та його трансформації в сучасну демократичну країну.

Метою даної роботи є підвищення ефективності вітчизняної системи охорони державної таємниці с урахуванням існуючого досвіду.

В перші роки існування національної незалежної держави існувала думка, що формування системи охорони державної таємниці, аналогічної радянському режиму, могло б створити передумови для зловживань щодо застосування секретної інформації, порушень прав і свобод людини.

Демократизація правовідносин у сфері, пов'язаній з державною таємницею, повинна була передбачати розширення прав і, водночас, підвищення відповідальності керівників усіх рівнів за режим секретності та персоніфікацію питань щодо віднесення відомостей до державної таємниці та їхнє засекречування. Тому було прийнято рішення про створення окремого спеціального уповноваженого органу державної влади з питань охорони державної таємниці.

Верховна Рада України вже на етапі прийняття законів, які регламентували діяльність СБ України, залишила за цим державним органом лише функції спеціальної компетенції як правоохоронного органу. Організаційно-правові функції СБ України щодо охорони державної таємниці були вилучені зі сфери її компетенції.

Визначений ВР України політичний курс щодо формування системи охорони державної таємниці був реалізований відповідними рішеннями уряду держави. Постановою КМУ від 4 травня 1993 р. № 327 було створено Державній комітет України з питань державних секретів (Держкомсекретів України).

Постановою КМУ 16 червня 1993 р. було затверджено положення про Держкомсекретів України, яким було встановлено, що Держкомсекретів України є центральним органом державної виконавчої влади, підвідомчим КМУ, який «... забезпечує у межах своїх повноважень проведення державної політики з питань захисту державних секретів, реєструє відомості, що становлять державну таємницю або є таємними, організує, координує і контролює режимно-секретну діяльність державних органів, підприємств, установ і організацій незалежно від

форм власності, дипломатичних представництв та інших об'єктів України за кордоном».

21 січня 1994 р. постановою Верховної Ради України № 3855-12 було введено в дію Закон України «Про державну таємницю». Правові норми Закону України «Про державну таємницю» передбачали створення системи охорони державної таємниці з урахуванням досвіду розвинених демократичних країн. Звичайно було використано і радянський досвід охорони державної таємниці.

Спеціально уповноваженим центральним органом державної виконавчої влади у сфері забезпечення охорони державної таємниці був визначений Держкомсекретів України. Було також встановлено, що окремі функції у цій сфері, у тому числі щодо технічного захисту інформації, оперативних заходів охорони державної таємниці, фельд'єгерського зв'язку, охорони державної таємниці у засобах масової інформації виконують відповідні державні органи в межах повноважень, передбачених законодавством.

Закон України «Про державну таємницю» вперше в нашій країні на підставі базового Закону України «Про інформацію» встановив правовий режим інформації, що містить державну таємницю.

Закон, єдиний в СНД, передбачав створення інституту державних експертів з питань таємниць, тільки рішеннями яких інформація могла бути віднесена до державної таємниці (ст. 7–9, 11, 12). На підставі мотивованих рішень державних експертів з питань таємниць формувався «Звід відомостей, що становлять державну таємницю» (ст. 10). Інститут державних експертів не існував в СРСР і не існує в інших країнах на пострадянському просторі. Щось досить подібне є в США – це так звані класифікатори 1 рангу. Закон встановлював дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, лише після отримання дозволу (ліцензії) Держкомсекретів України на цей вид діяльності (ст. 19).

Закон України «Про державну таємницю» виводив з обігу поняття «державні секрети» та розподілив інформацію, що віднесена до державної таємниці, на три ступеня – «особливої важливості», «цілком таємно» та «таємно». Поняття «службова таємниця» та «державні секрети» в Законі не використовувалися. За замовчанням всі носії інформації з грифом обмеження доступу «таємно», засекречені в СРСР та в незалежній Україні до прийняття 21 січня 1994 р. Закону України «Про державну таємницю» з грифами «секретно» і «таємно», перетворилися на носії секретної інформації, що створило певні проблеми під час їхнього розсекречування.

У досліджуваний період в Україні система охорони державної таємниці формувалася з урахуванням досвіду розвинених країн світу та традиційних засобів і методів, що в цілому виправдали себе у вітчизняній практиці, збільшилася відкритість держави перед суспільством, скоротилася чисельність відомостей, що належать до державної таємниці, відкритими стали загальні переліки такої інформації, механізми засекречування та умови розсекречування. Вжиті заходи в

складних умовах початкового етапу державного будівництва дозволили створити логічну завершену організаційну структуру державних органів, діяльність яких була спрямована на формування і вдосконалення інституту охорони державної таємниці України.

Функції системи управління інформаційною безпекою

УДК 004[056.53+413.4]

Володимир Мохор[1], Василь Цуркан[2]

ІПМЕ ім. Г.Є. Пухова НАН України, [1]v.mokhor@gmail.com,
КПІ ім. Ігоря Сікорського,[2]v.v.tsurkan@gmail.com

Забезпечення конфіденційності, цілісності та доступності інформації в організації досягається завдяки реалізуванню функцій системою управління інформаційною безпекою. Вони реалізуються з огляду на наявність вхідних і вихідних даних, обмежень і механізмів. Тому для формалізування її функцій використано графічну нотацію функціонального моделювання IDEF0 (Integrated Computer Aided Manufacturing Definition).

Метою даної роботи є формалізування функцій системи управління інформаційною безпекою в організації.

Функції системи управління інформаційною безпекою формалізуються функціональним блоком. Кожна сторона такого блоку характеризується своїм призначенням: ліва – вхідні дані, права – вихідні дані, верхня – обмеження, нижня – механізми, виклики. Водночас визначається мета та точка зору функціонального моделювання системи управління інформаційною безпекою. Зокрема, метою є забезпечення конфіденційності, цілісності та доступності інформації. Тоді як точкою зору визначаються організація, а також внутрішні (вище керівництво, персонал) та зовнішні зацікавлені сторони. Важливість виокремлення зацікавлених сторін обумовлена тим, що з їхнього боку можливе встановлення важливих вимог для забезпечення інформаційної безпеки.

При розгляданні діяльності управління інформаційною безпекою як функції верхнього рівня виокремлюються такі вхідні дані: інформаційні активи, відомості про інформаційні активи, відомості про організацію. За результатами зазначеної діяльності отримуємо збереженість властивостей інформаційних активів (конфіденційність, цілісність, доступність) з прийнятним рівнем ризику. Управління інформаційною безпекою обмежується зовнішніми та внутрішніми обставинами організації; вимогами зацікавлених сторін до забезпечення інформаційної безпеки, а також інтерфейсами та залежностями між діями в організації. Цей перелік уточняється виокремленням критеріїв оцінювання і прийняття ризику інформаційної безпеки. Як механізми розглядаються внутрішні та зовнішні зацікавлені сторони, метод оцінювання ризику інформаційної безпеки; виклик – загальна система управління організацією. Декомпозиція діяльності управління інформаційною безпекою відображена, наприклад, такими функціями: встановлення обставин діяльності організації, встановлення зобов'язань вищого керівництва організації, планування, функціонування, оцінювання ефективності, вдосконалювання системи управління інформаційною безпекою.

Отже, такий підхід дозволяє, по-перше, формалізувати функції системи управління інформаційною безпекою у графічній нотації IDEF0. По-друге, серед них виокремити функцію верхнього рівня як діяльність з управління інформаційною безпекою. По-третє, для кожної них задати вхідні та вихідні дані, обмеження, механізми та виклики. Як наслідок, по-четверте, встановити функціональні межі системи управління інформаційною безпекою.

Підсилення практичної ролі та відповідальності експертних комісій при державних експертах з питань таємниць

УДК 004.056.5

Олена Азаренко[1],
Юрій Дрейс[2], Володимир Щербина[3]
[1]Національний авіаційний університет, ,
icaocentre@nau.edu.ua[1], smya@nau.edu.ua[3], dreisyuri@gmail.com[2]

Відомо, що державний експерт з питань таємниць – це посадова особа, уповноважена Указом Президента України здійснювати відповідно до вимог заонодавства віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування [1]. Тому з метою сприяння виконанню державними експертами з питань таємниць (ДЕТ) покладених на них завдань у сфері охорони державної таємниці (ОДТ), у т.ч. запобігання розголошенню відомостей, що становлять державну таємницю, створюються експертні комісії [2]. Наразі, окремі особи, що є ДЕТ мають скоріш політичний, а ніж практичний досвіт виконання функцій пов'язаних з ОДТ [3], тому підвищення ролі та відповідальності експертних комісій при ДЕТ є актуальним науково-прктичним завданням.

Метою даної роботи є надання методичних рекомендацій та окремих пропозицій щодо змін в організаційный роботі експертної комісії при ДЕТ з метою підвищення їх ролі та відповідальності у сфері забезпечення ОДТ.

Пропонуємо створювати експертні комісій (ЕК) ДЕТ у відповідних сферах основної діяльності очолюваного ним органу державної влади, міністерства, установи, підприємства, що пов'язана з обробкою службової інформації та/або державної таємниці (тобто суб'єкта режимно-секретної діяльності (СРСД)). Перелік таких відповідних сфер має визначається ДЕТ на підставі затвердженої організаційної структури СРСД. Зміна організаційної структури СРСД повина вести до зіміни переліку цих відповідних сфер. При формуванні переліку службової інформації та/чи розгорнутого переліку відомостей, що становлять державну таємницю СРСД, визначені відповідні сфери зазначаються у них в якості окремих розділів.

Створення ЕК та формування її складу повинно відбувається на основі рішення ДЕТ по кожній відповідній сфері згідно до визначеного їх переліку. До складу ЕК має увійти не менше шести її членів, ДЕТ у якості голови комісії та її секретар. Компетенція кожного члена ЕК повинна відповідати сфері у якій вона створюється, що підтверджується посадою, кваліфікацією, освітою, досвідом тощо. Секретар не може бути членом ЕК. Секретар ЕК за дорученням ДЕТ організовує роботу членів комісії, визначає перелік питань необхідних

для опрацювання членами комісії, узагальнює рішення членів комісії, формує порядок денний та веде протокол засідання ЕК, розробляє проект остаточного для затвердження ДЕТ рішення ЕК. Робота ЕК має відбувається у формі індивідуального (самостійного) прийняття рішень кожним членом комісії персонально та, за рішенням ДЕТ у разі необхідності, коллективного у формі засідання ЕК. Індивідуальні (самостійні) рішення кожного члена комісії повинні узагальнюватися секретарем комісії та на їх основі готується проект остаточного рішення ЕК. Проект остаточного рішення ЕК приймається більшістю прийнятих індивідуальних рішень членів комісії. У разі відсутності такої більшості, ДЕТ повинен скликати ЕК для формування проекту остаточного рішення на її засіданні. Проект остаточного рішення затверджує ДЕТ як рішення ЕК, який підписують члени комісії. Індивідуальні рішення прийняті членами ЕК є невідємними складовими частинами затвердженого ДЕТ рішення ЕК, які оформлюються у якості його додатків. У разі наявності іншої (окремої) думки, член ЕК оформлює свої доводи письмово та подає їх у якості додатку до затвердженого ДЕТ рішення ЕК, де напроти прізвища такого члена комісії замість підпису ставиться напис «окрема думка». Відповідальність за прийняте рішення ЕК несуть її члени персонально. На членів ЕК мають поширюватися усі преференції ДЕТ, окрім політичних.

Висновок. З метою підвищення ефективності виконання покладених завдань на ДЕТ пропонується посилити практичну роль та відповідальність експертних комісій у сфері ОДТ.

Література

1. Ю. Дрейс, "Функціонування системи охорони державної таємниці в Україні: організаційно-правова структура, принципи та завдання", Безпека інформації, Т. 20. – № 2. – 2014. – С.176-184.

2. О. Корченко, О. Архипов, Ю. Дрейс, "Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія", К.: Наук.-вид. центр НА СБ України. – 332 с. – 2014. – ISBN 978-617-7092-26-0.

3. О. Корченко, Ю. Дрейс "Удосконалення інституту державних експертів з питань таємниць", Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). [Електронне видання]. – Київ : Нац. акад. СБУ, 2019. – С.168-169.

Програмний модуль виявлення аномалій в соціотехнічних системах

УДК 004.056.53

Тарас Паращук[1], Анна Корченко[2],
Марина Коломієць[3]

Національний авіаційний університет,

[1]taras1039@gmail.com,[2]annakor@ukr.net, [3]m.kolomiiets@nau.edu.ua

На сьогодні більшість систем виявлення вторгнень стають невід'ємною частиною захисту будь-якої соціотехнічної системи, вони використовуються для моніторингу підозрілої активності в системі та виявлення атакуючих дій неавторизованої сторони.

Останні дослідження, які проведені фахівцями в відповідних галузях за останні роки показали, що корпоративні мережі переважної більшості організацій не здатні забезпечити належний захист від існуючих кіберзагроз на рівні персоналу так і системи. Відзначені дві масштабні кібератаки, які потрясли світову спільноту – віруси WannaCry та NotPetya інфікували сотні тисяч комп'ютерів в різних країнах. Також, користувачі зіткнулися і з низкою інших, менш значних атак, що пов'язані з вірусами-вимагачами, DDoS-атаками, викраданням персональних даних.

Активізація таких кібератак ініціює створення спеціальних технічних рішень, засобів та систем протидії, здатних залишатись ефективними при появі нових або модифікованих видів кіберзагроз з невстановленими або нечітко визначеними властивостями. Загалом такі системи направлені на виявлення підозрілої активності чи втручання в мережу для прийняття адекватних заходів щодо запобігання кібератакам. Ці системи, як правило, достатньо дорогі, мають закритий код та вимагають періодичної підтримки висококваліфікованих фахівців для налаштування до умов конкретних підприємств. Достатньо актуальними і необхідними систем виявлення вторгнень є ті, які орієнтовані на виявлення аномальних станів. Основними їх недоліками є, наприклад, надлишок помилкових спрацювань, складність процесу налаштування, тривалий процес навчання та створення відповідного профілю нормального стану системи. Більш ефективними в цьому є експертні підходи, засновані на використанні знань і досвіду фахівців відповідної предметної галузі.

Виходячи з цього, побудова технічних рішень і створення спеціальних засобів, що дозволяють детектувати раніше невідомі кібератаки шляхом контролю поточного стану нечітко визначених параметрів в слабоформалізованому середовищі оточення, заснованих на експертних підходах, є актуальною задачею.

Метою роботи є розробка програмного модуля формування еталонів параметрів для систем виявлення аномалій в соціотехнічних системах.

В запропонованому модулі формування еталонів параметрів за основу вибрано два параметра: кількість одночасних підключень (КОП) та кількість пакетів з однаковою адресою відправника і одержувача (КПОА), це дозволяє

ефективно виявляти аномалії двох основних видів Spoofing IP, ARP-spoofing та на базовому рівні відслідковувати початок процесу DoS/DDoS-атак. Його можна структурно розділити на такі основні алгоритмічні елементи:

1. ServicesSensors – даний клас відповідає за організацію ефективної роботи сенсорів програмної моделі, які орієнтовані на визначення кількості підключених клієнтів та аналізу пакетів, що надходять до системи.
2. ManagerSensors – даний клас відповідає за отримання та первину обробку даних з сенсорів системи відносно двох основних параметрів аналізу КОП і КПОА.
3. ConstantCoordinates – даний клас відповідає за отримання експертних оцінок відносно параметрів КОП і КПОА, що характеризують основні стани системи в залежності від виникнення критичних чи аномальних ситуацій.
4. CurrentCoordinates – даний клас відповідає за процес конвертації та обробки вхідних даних за допомогою математичних методів (метод лінійної апроксисмації локальними максимумами, базові правила роботи з нечіткими множинами).
5. ParameterSensors – даний клас відповідає за отримання налаштувань «сенсорів» та експертних оцінок за допомогою обміну даними з вище описаними класами та методами.

Таким чином, розроблений програмний модуль, який, за рахунок базового алгоритму та низки розроблених процедур (конструювання координатної сітки; ініціалізації величин на основі набору баз даних та модулів; графічного формування параметрів; пошуку спільних точок відповідно базових правил та графічної інтерпретації результату), дозволяє виявляти аномалії в соціотехнічних системах.

Method of neural networks utilization for malware recognition

UDC 004.056.5 Volodymyr Pogorelov[1], Mykolay Karpinski[2],

Evheniia Ivanchenko[3]

National Aviation University[1,3], Akademia Techniczno-Humanistyczna

w Bielsku-Białej[2], [1]volodymyr.pogorleov@gmail.com, [2]mpkarpinski@gmail.com, [3]evivancenko@gmail.com

An important way to improve the recognition of computer viruses is the "intellectualization" of recognition methods through the use of the theory of artificial neural networks (NN). The prospects of this area are confirmed by some successful applications of NN in the detection of computer viruses (antivirus with open source ClamAV, startup Deep Instinct) and a large number of relevant theoretical and practical work. However, insufficient recognition accuracy and insufficient adaptability to operating conditions, the secrecy of the solutions used significantly limit their scope. At the same time, constant progress in the field of neural network theory indicates the possibility of significant improvement of the tested recognition methods.

In such a setting, the scientific and applied task of developing an effective neural network method for recognizing computer viruses, adapted to the conditions of domestic anti-virus protection systems, is relevant.

The proposed method consists of the following steps:

Stage 1 - determining the conditions for the creation and use of NN.

Stage 2 - the formation of portraits of viruses and secure programs.

Stage 3 - determination of architectural parameters of DNN.

Stage 4 - verification of NN.

Stage 5 - evaluation of the effectiveness of NN.

The computer virus database BIG-2015, published by Microsoft, is used for training and testing of DNN (table 1).

Table 1

Database BIG-2015

Name	*Number of examples*
Ramnit	1541
Lollipop	2478
Kelihos_v3	2942
Vundo	475
Simda	420
Tracur	751

Note that due to the use of the proposed design method GNM architecture managed to avoid long-term numerical experiments, aimed at determining the appropriateness of its use and to determine it structural parameters, and approximately 1.5 times to reduce computational costs, related to the definition of the specified architectural parameters.

Thus, the results studies confirm the possibility of improving the efficiency of recognition computer viruses through the application of the developed method.

Supervisor — doctor of science, prof., Terejkowskyi I.A

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ

X міжнародної науково-технічної конференції «ITSec»

19-24 березня 2020 року

м. Київ (Україна), м. Шарм-ель-Шейх (Египет),
Національний авіаційний університет

Оригінал-макет підготовлено на кафедрі
безпеки інформаційних технологій
Національного авіаційного університету