УДК 004.68

Мелкумян К.В.

СУЧАСНИЙ ПІДХІД ДО СТВОРЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Актуальність застосування методів штучного інтелекту з метою захисту інформаційних ресурсів у комп'ютерних системах на теперішній час є очевидною. Зокрема у [1] наведено перелік загроз конфіденційності, цілісності і доступності інформації, що обробляється у комп'ютерній мережі, у співвідношенні до рівня складності щодо їх виявлення і класифікації, рівня складності запобігання цим загрозам та вибору заходів безпеки, а також наслідків їх реалізації. З представленого робиться висновок, що відношення кількості загроз, які мають досить складний рівень виявлення до запобігання їм, та їх реалізація становить 48% (тобто майже половину) у відношенні до загальної кількості загроз. Досить складний рівень виявлення вказаних загроз є результатом невизначеності щодо всій множини їх проявів та ознак, а проблема запобігання даним загрозам значно ускладнюється відсутністю чітко детермінованих методів вибору заходів безпеки.

Зазначене також підтверджується у [2, 3], де наведено формалізований опис задачі захисту інформації, який полягає в тому, щоб будь-яка реальна траєкторія обчислювального процесу □ у фазовому просторі системи □ не потрапила до множини несприятливих траєкторій *N* або ділянок цих траєкторій. Для чого служба захисту інформації для утримання траєкторій обчислювального процесу від виходу в *N* керує виключно обмеженням на доступ в кожний момент часу. При цьому основна складність захисту інформації полягає в тому, що, маючи можливість використовувати набір локальних обмежень на доступ в кожний момент часу, потрібно вирішувати глобальну проблему недопущення виходу будь-якої траєкторії до множини N.

Вирішення саме такого класу задач є одним з основних напрямів досліджень з штучного інтелекту та створення інтелектуальних систем, які оперують не тільки даними, а й знаннями. В межах цього напрямку будуються способи поповнення знань на основі їх неповних описів, вивчаються системи класифікації знань, що зберігаються в інтелектуальній системі, розробляються процедури узагальнення знань і формування на їх основі абстрактних понять, створюються методи достовірного та правдоподібного висновку на основі знань, пропонуються моделі міркувань, що опираються на знання та імітують особливості міркувань людини.

В основі функціонування інтелектуальних систем лежить конкретне рішення проблеми представлення знань. В межах вказаної проблеми одне з основних місць посідає задача вибору моделі представлення знань, яка б дозволила автоматизувати процес виявлення великої кількості різноманітних загроз інформації, що обробляється, та мінімізації можливої шкоди.

На етапі вибору моделі представлення знань, згідно з якою інтелектуальна система здійснює процедуру висновку, беруться до уваги особливості прикладної галузі використання інтелектуальних систем. Водночас поширення сфери використання інтелектуальних систем на нові галузі захисту інформації та значне зростання складності задач обумовлюють потребу у більш універсальних методах побудови моделі представлення знань.

У даній статті запропоновано основи формальної моделі, яка може бути використана для представлення знань та забезпечення процедур висновків на знаннях в інтелектуальних системах. Зазначене викладено у вигляді таких визначень, наслідків та аксіом.

Визначення 1

Нехай існує деяка кінцева множина $T=\{t\}$, де t називається *термом*. Тоді T назвемо *множиною термів*.

Визначення 2

Нехай для деякої трійки термів t_i, t_k, t_n □T існує процедура

$$t_i \square t_k = t_n,$$

де оператор $\square$ називається *оператором синтезу*, процедура $t_i \square t_k$ називається *операцією синтезу* терму t_n з використанням термів t_i та t_k, а терм t_n є *результатом операції синтезу* з використанням термів t_i та t_k, або *результатом синтезу* з термів t_i та t_k.

Визначення 3

Якщо для деякої трійки термів $t_i, t_k, t_n \in T$ існує операція синтезу терму t_n: $t_i \square t_k = t_n$, то терми t_i та t_k називаються *близькими* для t_n.

Визначення 4

Якщо для деякої трійки термів $t_i, t_k, t_n \in T$ існує операція синтезу терму t_n: $t_i \square t_k = t_n$, то терм t_n називається *безпосередньо пов`язаним* з парою t_i та t_k.

Визначення 5

Множина $T_p = \{ t_i, t_k, t_n \}$, де терми $t_i, t_k, t_n \in T$, для яких визначена операція синтезу $t_i \square t_k = t_n$, називаються *трійкою синтезу* p.

$P = t_i, t_k, t_n \in T \mid t_i \square t_k = t_n$.

У разі, якщо для множини T_p не визначена операція синтезу, то T_p називається *виродженою ТС* та позначається – $\tilde{p}$.

Терми t_i, t_k називаються *основою трійки синтезу*, а t_n – *верхівкою трійки синтезу*.

Визначення 6

Нехай існує функція $s_i(t_k, t_l, t_m)$, яка ставить у відповідність кожній трійці термів $t_k, t_l, t_m \in T_i$, де $T_i \in T$, трійку синтезу $p_n \in P_i$, де P_i – деяка множина трійок синтезу, що включає в себе в тому числі вироджену трійку синтезу, тоді функція s_i називається *функцією сумісності* на множині T_i. При цьому T_i є областю визначення, а P_i є областю значень функції s_i.

T_i, на якій визначена функція сумісності s_i, називається *простором термів* S_{Ti}.

$S_{Ti} = (T_i, P_i, s_i)$.

Аксіома 1

Якщо S_{Ti} є простором термів $S_{Ti} = (T_i, P_i, s_i)$, то у S_{Ti} для будь-якої пари термів $t_j, t_k \in T_i$ існує не більше однієї трійки синтезу $p_n \in P_i$, для якої t_j, t_k є її основою.

Визначення 7

Нехай $A = \{ t_a, t_{a+1}, \ldots, t_{a+m} \}$ – підмножина термів T_i, де $T_i \in T$, і на T_i задана функція сумісності s_i, тобто існує простір термів $S_{Ti} = (T_i, P_i, s_i)$, тоді множина $T_A \in T_i$, елементи якої і тільки вони входять до трійок синтезу P_A, де $P_A \in P_i$, і до основи P_A входить хоча б один елемент A, називається *підпростором* простору термів S_{Ti} з *множиною визначення* A.

Визначення 8

Нехай $A = \{ t_a, t_{a+1}, \ldots, t_{a+m} \}$ – підмножина термів T_i, де $T_i \in T$, і на T_i задана функція сумісності s_i, тобто існує простір термів $S_{Ti} = (T_i, P_i, s_i)$, тоді множина $T_A \in T_i$, елементи якої і тільки вони входять до трійок синтезу P_A, де $P_A \in P_i$, і до основи P_A входять елементи A і тільки вони, називається *розрізом* простору термів S_{Ti} з *множиною визначення* A.

Визначення 9

Нехай існує підпростір S_{TA} з множиною визначення A у просторі термів $S_{Ti} = (T_i, P_i, s_i)$, де до A входить лише один елемент $A=\{t_a\}$, тоді підпростір S_{TA} називається *площиною* у просторі термів S_{Ti} з *елементом визначення* t_a.

Визначення 10

Нехай існує деяка послідовність термів $t_k, t_{k+1}, \ldots, t_{k+m} \in T_i$, де $T_i \in T$, у просторі термів S_{Ti}, де для кожної пари сусідніх термів терм t_{k+n} є близьким для терму t_{k+n+1}, тоді терм t_k називається *опосередковано близьким для терму* t_{k+m} *у просторі термів* S_{Ti}, а послідовність термів $t_{k+1}, t_{k+2}, \ldots, t_{k+m-1}$ називається *опосередкованим зв'язком між термом* t_k *та термом* t_{k+m}.

Визначення 11

Нехай для кожного терму $t_i \in T_i$, де $T_i \in T$, визначено показник його стану k_i, який може приймати значення {0, 1}, тоді будемо вважати, що терм знаходиться у стані *пасивному*, якщо $k_i = 0$, у стані *активному*, якщо $k_i = 1$.

Оператор, який вказує на показник стану терму, будемо називати *оператором визначення стану терму d()*. Тобто $k_i = d(t_i)$.

Визначення 12 *(Правило активізації термів)*

Процедура надання терму активного стану у просторі термів $S_{Ti}=(T_i, P_i, s_i)$ за результатами оцінки показників стану інших термів T_i називається *активізацією* терму.

Необхідною і достатньою умовою активізації терму $t_i \in T_i$, де $T_i \in T$, у просторі термів S_{Ti} є існування у вказаному просторі операції синтезу для терму $t_i : t_i = t_n \square t_k$ та за умови, що обидва терми t_n та t_k знаходяться в активному стані.

$$D(t_i) = \begin{cases} \square 1, \text{ якщо } t_i = t_n \square t_k \text{ та } d(t_n) = 1 \text{ та } d(t_k) = 1; \\ \square\ d(t_i), \text{ якщо } t_i = t_n \square t_k \text{ та } (\ d(t_n) = 0 \text{ або } d(t_k) = 0); \\ \square\ d(t_i), \text{ якщо } t_i = t_n \square t_k \text{ та } d(t_n) = 0 \text{ та } d(t_k) = 0. \end{cases}$$

Наслідок 1

Результатом активізації терму є надання йому активного стану незалежно від попереднього стану цього терму.

Визначення 13

Нехай існує функція $f_i\ (t_j, t_k)$, яка ставить у відповідність кожній парі термів $t_j, t_k \in T_i$, де $T_i \in T$, що являють собою основу трійок синтезу у просторі термів $S_{Ti}= (T_i, P_i, s_i)$, стан $d(t_n)$ терму t_n ($t_n \in T_i$), що є безпосередньо пов`язаний з t_j та t_k, згідно з правилом активізації у відповідність до показників стану $d(t_j)$ та $d(t_k)$, тоді функція $f_i(t_j, t_k)$ називається *функцією активізації* у просторі термів $\tilde{S_{Ti}}$

Визначення 14

Простір S_{Ti}, для якого визначено функцію активізації, називається *активним простором* $S^a_{Ti} = (S_{Ti}, f_i) = (T_i, P_i, s_i, f_i)$.

Визначення 15

Активний простір $S^a_{Ti}=(T_i, P_i, s_i, f_i)$ знаходиться *у стані змін*, якщо застосування функції активізації хоча б до однієї пари термів $t_j, t_k \in T_i$, що являють собою основу не виродженої тріади у просторі термів $S_{Ti}= (T_i, P_i, s_i)$, призведе до зміни показника стану безпосередньо пов'язаного з ними терму.

Визначення 16

Активний простір $S^a_{Ti} = (T_i, P_i, s_i, f_i)$ знаходиться *у стані спокою*, якщо застосування функції активізації до будь-якої пари термів $t_j, t_k \in T_i$, що являють собою основу не виродженої тріади у просторі термів $S_{Ti}= (T_i, P_i, s_i)$, не призведе до зміни показника стану безпосередньо пов'язаного з ними терму.

Визначення 17

Зміна показника терму в активному просторі S^a_{Ti} не у відповідності до правила активізації називається *зовнішнім втручанням*.

Встановлення відповідності між термами та поняттями певної прикладної області, а також між показником терму та фактом істинності відповідного поняття дозволить використовувати запропоновані визначення для створення моделей представлення знань із застосуванням трійок синтезу.

Видається досить вірогідним, що запропоновані основи побудови формальної моделі представлення знань є універсальними для будь-якої прикладної області.

У подальшому видається доцільним здійснення досліджень з метою позиціювання цієї моделі від таких моделей представлення знань, як логічні моделі, семантичні сітки, продукційні моделі, фреймові моделі, [4] нейронні сітки тощо.

Список літератури

1. *Мелкумян К.В.* Використання штучного інтелекту для захисту інформації в комп'ютерних мережах / Защита информации: Сборник научных трудов. – Киев: КМУГА,

2000. – 145 с. – С. 53 – 57.

2. *Мелкумян К.В., Вербицький М.А.* Узагальнений опис побудови інтелектуальної системи захисту інформації в розподілених автоматизованих системах / Захист інформації: Науково-технічний журнал. – Киев: КМУЦА, 2000, № 3. – 66 с. – С. 13 – 19.

3. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. – М: "Яхтсмен",1996.

4. *Искусственный интеллект:* Справочник/ Под ред. Д.А.Поспелова. – В 3-х кн. Кн. 2. Модели и методы. – М.: Радио и связь, 1990.

Надійшла 25.01.2006
Після доробки 16.05.2006

УДК 004.623 **Безмалый В.Ф.**

ПАРОЛЬНАЯ ЗАЩИТА: ПРОШЛОЕ, НАСТОЯЩЕЕ, БУДУЩЕЕ

Одним из важнейших процессов, создаваемых для соблюдения такого свойства информации, как конфиденциальность, является ограничение доступа. Наиболее распространен такой процесс аутентификации, как использование пароля. Практически с момента создания первых многопользовательских операционных систем для ограничения доступа используются пароли. Вспомним историю.

Операционные системы Windows 95/98 сохраняли пароль в PWL файле. PWL файлы хранились в каталоге Windows. Их имена, как правило, хранились как USERNAME.PWL. Вместе с тем стоит отметить, что PWL файл был зашифрован и извлечь из него пароли было не просто. Первый алгоритм шифрования версии Windows'95 был создан так, что позволял создать программы для расшифровки PWL файлов. Однако в версии OSR2 этот недостаток был устранен. Система защиты паролей в OSR2 была сделана профессионально и достоверно в терминах криптографии. Однако, несмотря на это, содержала несколько серьезных недостатков, а именно:

- все пароли преобразованы к верхнему регистру, это значительно уменьшает количество возможных паролей;
- используемые для шифрования алгоритмы MD5 и RC4 позволяют более быстрое шифрование пароля, но достоверный пароль Windows должен быть, по крайней мере, длиной в девять символов.

Система кэширования пароля по существу ненадежна. Пароль может быть сохранен только в том случае, если никакой персонал, не имеющий соответствующего разрешения, не может обращаться к вашему компьютеру.

В настоящее время рекомендуемая Microsoft длина пароля для рабочей станции Windows XP должна составлять не менее 8 символов, при этом в пароле должны встречаться большие и маленькие буквы, цифры и спецсимволы. При этом время жизни пароля должно составлять не более 42 дней. К тому же на пароль налагается требование неповторяемости. В дальнейшем эти требования будут только ужесточаться. К чему это приведет, вернее, увы, уже приводит? Чем сложнее пароли, чем больше приложений требуют ввод пароля, тем выше вероятность того, что ваши пользователи для всех приложений, в том числе и для аутентификации в ОС, будут использовать один и тот же пароль или они будут записывать его на бумагу. Хорошо это или плохо? Допустимо ли?

С одной стороны – явно не допустимо, так как резко вырастает риск компрометации пароля, с другой – слишком сложный пароль (типа PqSh*98+) весьма сложно удержать в голове, и пользователи явно будут либо выбирать простой пароль, либо постоянно забывать