УДК 378.147:004.9
© Чуприна Г. П.

ФОРМУВАННЯ ЗНАНЬ ІЗ ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПСИХІЧНИХ МОДЕЛЕЙ РЕПРЕЗЕНТАЦІЇ ПОНЯТЬ

Постановка проблеми. Програмні засоби захисту інформації є однією з найважливіших частин механізму захисту сучасних інформаційних систем. Вони вирішують такі задачі, як захист від:

– несанкціонованого доступу до ресурсів ПК;
– несанкціонованого використання і копіювання інформації;
– комп'ютерних вірусів та шкідливого програмного забезпечення;
– хакерських атак тощо.

Крім того, більшість користувачів застосовують саме програмні засоби захисту інформації, тому що вони мають ряд переваг перед іншими засобами захисту. По-перше, вони легко встановлюються на комп'ютері та дають можливість настроювати їх для різних умов використання, враховуючи специфіку загроз інформаційної безпеки конкретних комп'ютерних систем. По-друге, прості в застосуванні, що не вимагає від користувача ніяких нових навиків та мають непомітний режим роботи. По-третє, вони не обмежені можливостями свого вдосконалення для захисту від нових загроз [6]. Поряд із перевагами програмних засобів захисту інформації є й недоліки: зниження ефективності комп'ютерних систем, нижча продуктивність та ін. Але ми вважаємо найголовнішим недоліком програмних засобів захисту інформації – їх численність та різноманітність. На сьогодні нараховують близько п'ятисот таких програм.

Досить велика кількість програм, різноплановість їх призначення, складу, принципів дії та характеристик, а також неструктуроване дидактичне подання в літературі обумовлюють проблему навчання студентів їхнього ефективного використання.

Аналіз останніх досліджень і публікацій. Процес засвоєння навчального матеріалу в значній мірі визначається психічними процесами ментальної репрезентації цієї інформації в пам'яті людини. Психологами розроблена досить велика кількість різноманітних моделей ментальної репрезентації понять людини [5; 7], моделей у вигляді структури понять.

Важливо знати, як правильно організувати відображення та закріплення в пам'яті студента великої кількості понять та логічних відношень між ними, щоб у будь-який момент можна було їх відтворити і при необхідності використати в діяльності.

Постановка завдання – визначення психічної моделі ментальної репрезентації понять для формування знань із програмних засобів захисту інформації.

Виклад основного матеріалу. Формування знань – це не будь-яке подання інформації або відомостей, «знання» необхідно розглядати через призму таких термінів, як «мислення», «розуміння», «дія» [4]. Знання відображають наше уявлення про предметну галузь і є системою понять, відношень та залежностей між ними [1].

Визначення поняття «знання» можна подати такою формулою [3]:

Знання = Поняття + Відношення.

Таким чином, для того, щоб засвоїти знання з програмних засобів захисту інформації, потрібно усвідомити систему понять із цієї дисципліни і побудувати логічні відношення між ними.

Як було визначено в попередніх дослідженнях, зміст навчання дисципліни «Програмні засоби захисту інформації» повинен бути структурованим і мати можливість узагальнення як для експрес-ідентифікації програмного продукту, так і для повного вивчення програмних засобів захисту інформації – подвійне, діалектично протилежне узагальнення.

Тому структурування змісту навчання дисципліни ПЗЗІ повинно дати змогу проводити два діалектично протилежних узагальнення понять із цієї дисципліни.

Також було визначено, що основою для побудови змісту навчання ПЗЗІ виступають знання, які в свою чергу складаються з понять та логічних відношень між ними [4].

Процес формування будь-яких понять виходить із визначення понять за допомогою ознак [7]. Але коли множина опису ознак хаотична, не структурована, як, наприклад, первинно-інформаційний матеріал із програмних засобів захисту інформації, то він не може бути придатним для якісного вивчення.

Проведемо аналіз моделей репрезентації понять у пам'яті людини за І. Хофманом, Дж. Андерсоном, Р. Солсо [5; 7] і визначимо ті моделі, на основі яких будуватимемо дидактичні моделі подання навчального матеріалу з програмних засобів захисту інформації.

Першою розглянемо модель множинної репрезентації понять. За цією моделлю поняття предсталяє собою упорядковану множину об'єктів (сукупність прикладів), яку можна подати у вигляді структури (рис. 1)

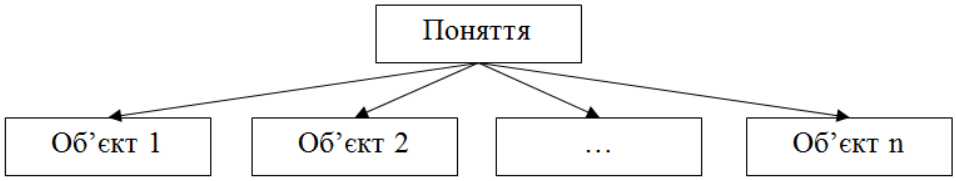

Рис. 1. Модель множинної репрезентації понять

де (об'єкт 1), (об'єкт 2),...,(об'єкт n) – елементи множини.

Розглянемо моделі множинної репрезентації поняття на конкретних прикладах.

Множина «програмні засоби захисту інформації» складається з таких об'єктів: антивірусні програми, міжмережні екрани, засоби ідентифікації та автентифікації користувача, засоби управління доступом до ресурсів ПК, протоколювання й аудит, криптографічні засоби; і має певну структуру (рис. 2).

Рис. 2. Модель множинної репрезентації поняття «ПЗЗІ»

Множина MALWARE (шкідливі програми) складається з таких об'єктів: Adware (реклама), Spyware (шпигунський софт), віруси, черв'яки, трояни, rootkit, …, і має відповідну структуру (рис. 3).

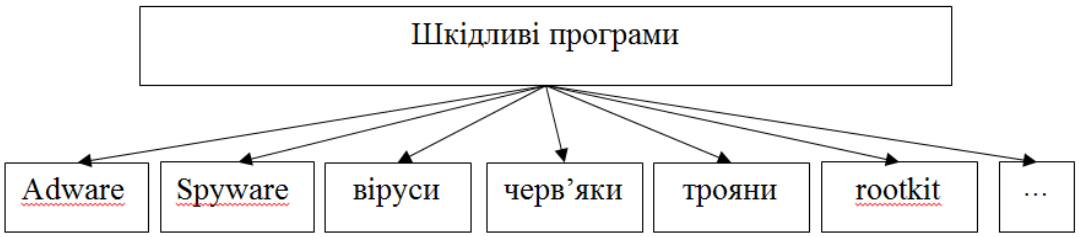

Рис. 3. Модель множинної репрезентації поняття «Шкідливі програми»

Модель множинної репрезентації поняття належить до образних моделей. Вона складається тільки зі списку елементів цього поняття і являє собою його цілісним представленням. Інформації про характеристики всіх об'єктів загалом ця модель не містить. Необхідність використання її в навчанні виникає при початковому формуванні поняття. Але в подальшому навчанні ця модель стає малоефективною. Обумовлено це тим, що із збільшенням об'єму множини зростає і час для ідентифікації об'єкта як елемента цієї множини [5; 7].

У програмних засобах захисту інформації кількість об'єктів із часом тільки збільшується, тому, використовуючи модель множинної репрезентації, дуже швидко відбувається накопичення майже однорідних об'єктів. Вони мають незначну кількість розпізнавальних ознак, що призводить до їх усереднення. При цьому з'являється образ (прототип), який характеризує всю множину об'єктів у цілому.

З цієї причини наступною розглянемо модель репрезентації понять за допомогою прототипів. Ця модель теж належить до образних моделей, але ідентифікація об'єкта за її допомогою відбувається значно швидше [7]. Обумовлено це тим, що, чим більше об'єкт схожий на прототип, тим швидше відбудеться розпізнавання об'єкта, що належить до відповідної множини. На перший погляд, ця модель могла бути корисною в таких випадках:

– при орієнтації у різноманітті об'єктів;

– при ідентифікації нових об'єктів, які раніше були невідомі, тобто для вирішення проблеми з першим видом узагальнення – експрес-ідентифікацією.

Розглянемо перше припущення щодо використання моделі репрезентації понять за допомогою прототипу при орієнтації в різноманітті об'єктів програмних засобів захисту інформації.

Як було зазначено в попередніх дослідженнях, кожен із видів програмних засобів захисту інформації має велику кількість програмних продуктів. Наприклад, засоби ідентифікації й автентифікації користувача, яких налічується близько п'ятдесяти об'єктів. Вони можуть бути між собою однотипні, однорідні і розрізнятися лише способом дії або незначними функціями. Але усереднення розпізнавальних ознак відбувається не з усіма об'єктами засобів ідентифікації й автентифікації користувача, а лише з майже однаковими програмними продуктами, які відрізняються несуттєвими ознаками. Тому в цьому випадку з'являється прототип (образ), який характеризує не всю множину об'єктів в цілому (рис. 4), а лише її частку або частки (рис. 5).

Отже, припущення щодо використання моделі репрезентації понять за допомогою прототипу при орієнтації в різноманітті об'єктів програмних засобів захисту інформації не підтвердилось.

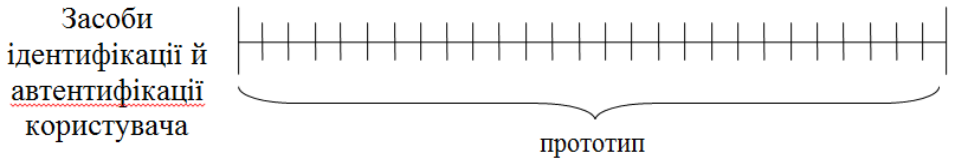

Рис. 4. Репрезентація поняття за допомогою прототипу

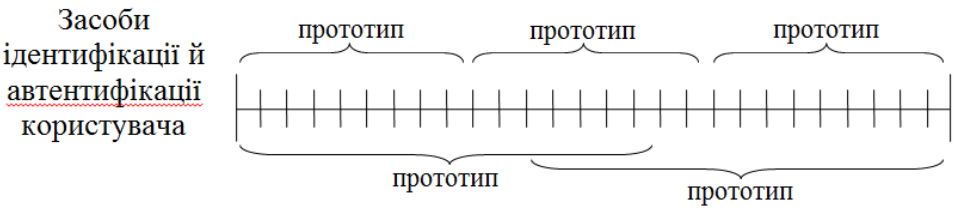

Рис. 5. Репрезентація поняття за допомогою прототипів

Розглянемо наступне припущення щодо використання моделі репрезентації понять за допомогою прототипу при ідентифікації нових об'єктів, які раніше були невідомі.

Репрезентації понять за допомогою прототипу починається з відношення його до відповідного первинного поняття і тільки після цього відбувається ідентифікація його як елемента більш загального або більш конкретного класу. Якщо відбувається ідентифікація нового об'єкта, то елемент відноситься тільки до більш загального класу [7].

Первинним поняттям, за дослідженнями Е. Рош [7], виступає поняття середнього рівня абстракції. Розглянемо рівні абстракції для програмних засобів захисту інформації на такому прикладі (рис. 6):

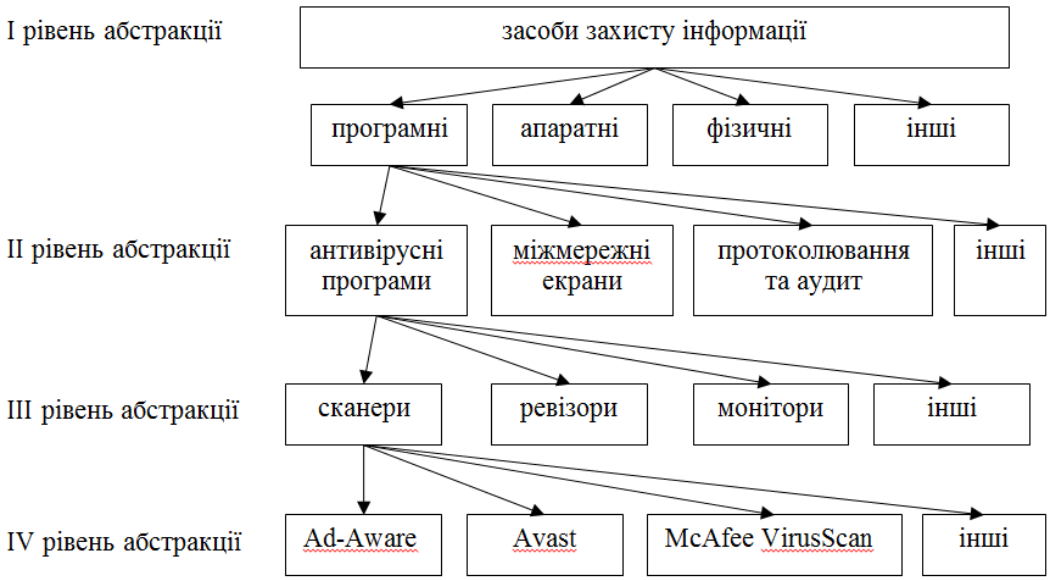

Рис. 6. Рівні абстракції для програмних засобів захисту інформації

– I рівень абстракції – засоби захисту інформації (програмні, апаратні, фізичні, організаційні та інші);

– II рівень абстракції – програмні засоби захисту інформації (антивірусні програми, міжмережні екрани, засоби ідентифікації і автентифікації користувача, засоби керування доступом до ресурсів ПК, протоколювання та аудит, криптографічні засоби захисту інформації);

– III рівень абстракції – види програмних засобів захисту інформації (сканери, ревізори, монітори, пакетні фільтри, прикладні шлюзи, засоби ідентифікації і автентифікації користувача на основі багаторазових паролів, дискреційні моделі засобів управління доступом до ресурсів ПК, засоби протоколювання на основі статистичного методу, електронний цифровий підпис та інші);

–IV рівень абстракції – конкретні програмні продукти (Ad-Aware, Avast Home Edition, AVG Internet Security, ESET NOD32 Antivirus, Kaspersky Internet Security, Symantec Norton AntiVirus, Spyware Doctor, Trojan Remover, Agnitum Outpost Firewall Pro, Folder Guard Pro, Windows Security Officer, Security Administrator, Program Lock Pro, ActiveExit, AccessEnum і багато інших).

Для цього прикладу середнім рівнем абстракції виступає II рівень і відповідно більш загальним класом – I рівень абстракції. Отже, при ідентифікації нового конкретного програмного продукту за допомогою прототипу його можна буде віднести до II рівня абстракції, тобто до одного з видів програмного засобу захисту інформації, або до I рівня абстракції, тобто до одного з засобу захисту інформації. Для віднесення програмного продукту до третього рівня абстракції необхідно порівняти його ознаки з ознаками відповідного виду програмного засобу захисту інформації, а це вже репрезентація поняття не за допомогою прототипу.

Отже, припущення щодо використання моделі репрезентації понять за допомогою прототипу при ідентифікації нових об’єктів, які раніше були невідомі, теж не підтвердилось.

Крім цього, прототип не дає можливості структурувати матеріал з програмних засобів захисту. Тому для вирішення проблеми з першим видом узагальнення – експрес-ідентифікації – репрезентація понять за допомогою прототипу не підходить.

Проблема забезпечення ефективного навчання студентів програмним засобам захисту інформації обумовлена наявністю не тільки досить великої кількість цих програм, але й ще більшої кількості ознак, які їх описують. Звичайно, якщо ознаки об’єктів будуть майже однорідними, то тут можна використовувати репрезентацію понять за допомогою прототипу, проте найчастіше в програмних засобах захисту інформації зустрічаються об’єкти з різноманітними розпізнавальними ознаками, у такому випадку механізм і модель прототипу стає малоефективною [7].

Із цієї причини наступними проаналізуємо моделі репрезентації понять за допомогою ознак. В загальному вигляді вони мають таку структуру (рис. 7):

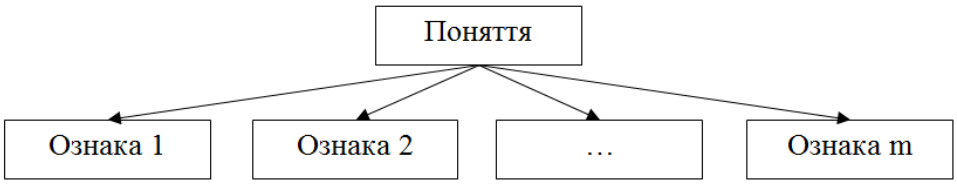

Рис. 7. Модель репрезентації понять за допомогою ознак

де (ознака 1), …, (ознака m) – множини ознак опису об’єкта.

Однією з перших моделей репрезентації ознак є модель Н. Аха й С. Хала (Ach, Hull) [7]. У цій моделі поняття являє собою множину об’єктів із чітко розпізнавальними ознаками. Об’єкти групуються в підмножини за допомогою різних алгоритмів розпізнавання ознак, наприклад: відношення якості, відношення контрастності, відношення порівняння. Таке групування в нашому випадку тільки ускладнює процес психічної репрезентації понять програмних засобів захисту інформації, оскільки нами зафіксовано наявність різних алгоритмів розпізнавання.

Наступною розглянемо модель Л. Ріпса, Е. Шобена і Е. Смітта [7]. У цій моделі ознаки понять зберігаються у формі упорядкованого списку й діляться на характерні й означальні. Характерні ознаки виділяють різні підкласи в межах цього поняття, означальні виражають властивості об'єктів, які специфічні для поняття й дозволяють відрізняти приналежні до нього об'єкти від об'єктів будь-якого іншого класу. Але для великої кількості ознак програмних засобів захисту інформації двох груп буде недостатньо.

Розглянемо більш складну модель B. Hayes-Roth, F. Hayes-Roth [7], згідно з якою для кожного об’єкта, що репрезентується в пам’яті, фіксується багатомірний набір ознак і відповідне правило, яке визначає приналежність до класу. Поняття репрезентується і класифікується в пам'яті впорядкованою множиною ознак, що характеризуються різними критеріями: класифікація нового об'єкта визначається тим набором ознак, зв'язок якого з одним із понять має найбільшу вагу.

Для ідентифікації понять цієї моделі, як і попередньої, не залучаються стійкі набори ознак. При зміні цілей діяльності виникає необхідність у використанні інших ознак об'єкта, що призводить до значних когнітивних зусиль.

Якщо ознаки понять не дані свідомості людини, вони не можуть слугувати для понятійної репрезентації й ідентифікації об'єктів. Крім того, необхідно всю досить велику множину ознак, якими характеризуються програмні засоби захисту інформації, представити у вигляді підмножин ознак, які будуть відрізнятися між собою принципами відображення певних функцій [7].

Тому розглянемо наступну ознакову модель – модель Ф. Клікса, яка має структуру подану на рис. 8:

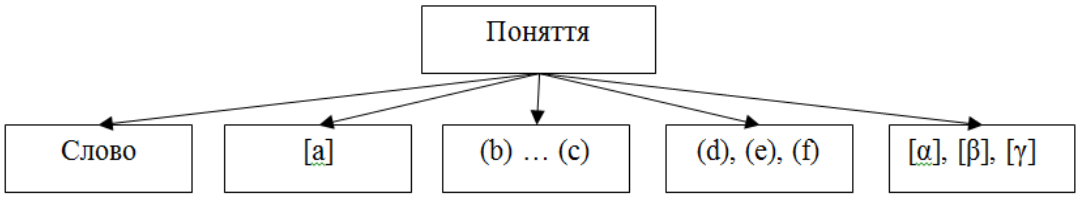

Рис. 8. Ознакова модель репрезентації понять Ф. Клікса

де (слово) – слово або словосполучення, яке позначає поняття;
[a] – підмножина комплексних ознак;
(b) … (c) – підмножина необхідних ознак;
(d), (e), (f) – підмножина випадкових ознак;
[α], [β], [γ] – підмножина характерних відношень.

У цій моделі поняття «ознака» розуміється як узагальнення всіх одиниць пам'яті, які дозволяють відрізняти між собою репрезентації понять; розглядаються складні ознаки і комплексні відношення між одиницями пам'яті [7].

Розглянемо репрезентацію понять у пам'яті людини за допомогою моделі Ф. Клікса на прикладі загальної антивірусної програми (рис. 9). Уся множина ознак загальної антивірусної програми буде поділятися на підмножини ознак, які складатимуться з:

– комплексних ознак (інтерфейс програми, алгоритм та інші);

– необхідних ознак (алгоритм для пошуку вірусів, алгоритм для видалення вірусів, резидентна, автооновлення через Інтернет, наявність бази сигнатур вірусів та інші);

– випадкових ознак (пошук троянських програм, блокування руткітів, скриптів, сканування електронної пошти, безкоштовна, простий інтерфейс та інші);

– характерних відношень (комп'ютер, інформація, захист та інші).

Ця модель, серед розглянутих ознакових моделей, є найбільш універсальною, оскільки вона має чітку структуру, дає можливість покроково, послідовно, детально вивчати програмні засоби захисту інформації. Тому модель Ф. Клікса можна обрати за основу для репрезентації понять у пам'яті студента для повного вивчення програмних засобів захисту інформації (рис. 9).

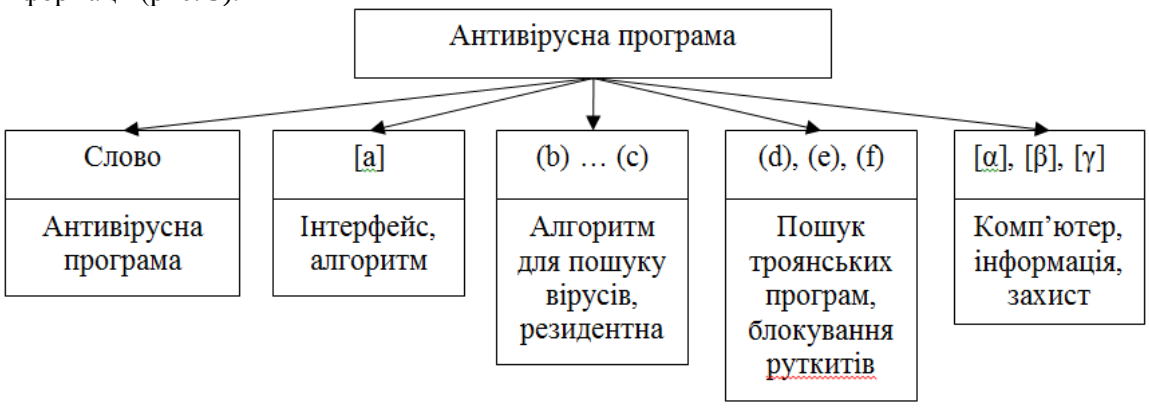

Рис. 9. Структура антивірусної програми за ознаковою моделлю Клікса

Якщо уважно подивитися на рис. 9, то можна помітити, що ця модель має підмножини ознак, які при експрес-ідентифікації будуть зайвими. Наприклад, помітка «Слово», яке відноситься до фонетико-графемних ознак, у нашому випадку практично не спрацьовує. Пояснюється це тим, що назви більшості програм подаються англійською мовою, за допомогою скорочень. Наприклад, програма з назвою Avast! Professional Edition не дає

можливості віднести її до антивірусної програми, якщо заздалегідь про це невідомо, або програма BlackICE PC Protection нічим не видає себе за міжмережний екран. Отже, ця підмножина ознак при експрес-ідентифікації може не фіксуватися.

Далі розглянемо підмножину комплексних ознак. Вона складається із загальних ознак, які можуть відповідати багатьом програмам, тому її теж не можна враховувати при експрес-ідентифікації програмного продукту.

Наступна підмножина називається «необхідні ознаки». Вона складається з найнеобхідніших ознак, за якими можна одразу ідентифікувати програмний продукт, причому дуже швидко. Отже, для експрес-ідентифікації програмного продукту її можна взяти за основу.

Далі розглянемо підмножину випадкових ознак. Ця підмножина складається з ознак, які будуть не тільки зайвими при експрес-ідентифікації, але й заважатимуть цьому процесу. Тому при репрезентації понять для моделі експрес-ідентифікації цю підмножину ознак ураховувати не будемо.

Розглянемо останню підмножину ознак, яка складається з характерних відношень. У цій підмножині встановлюються загальні відношення між поняттями, які можуть підходити до багатьох програм, і тому вони є несуттєвими для експрес-ідентифікації програмного продукту.

Таким чином, у моделі Ф. Клікса залишилася мінімальна кількість суттєвих ознак, які і будуть основою для репрезентації понять у напрямку експрес-ідентифікації програмного продукту, а діаметрально протилежний набір із максимальної кількості ознак стане основою для репрезентації понять у напрямку повного вивчення програмного засобу захисту інформації.

Крім репрезентації понять, існує репрезентація семантичних відношень (процесуальні та декларативні). Репрезентація семантичних відношень теж представлена багатьма моделями, до них відносяться моделі Дж. Андерсона, Д. Румельхарта, П. Ліндсєя, Д. Нормана [7]. Для нашого дослідження вони не актуальні, тому що моделюють семантичні структури (висловлення, логічні структури), а не окремі (одиночні) поняття.

Висновки. Отже, з проведеного аналізу моделей репрезентації понять за основу для двох видів узагальнення оберемо ознакову модель Ф. Клікса. Для моделі експрес-ідентифікації програмного продукту модель Ф. Клікса складатиметься із мінімально достатньої кількості суттєвих ознак, для моделі повного вивчення програмного засобу захисту інформації – з максимальної кількості суттєвих ознак (її ще можна назвати повноознаковою моделлю).

Перспективи подальших досліджень. Але ці моделі залишаються невизначеними з точки зору специфіки їх змістовного наповнення для використання в технічних дисциплінах. Тому в подальшому дослідженні розглянемо змістовне наповнення цих психічних моделей конкретною технічною інформацією предметної галузі програмних засобів захисту інформації.

Список використаних джерел

1. Ващенко Г. Загальні методи навчання / Г. Ващенко. – К. : Українська Видавнича спілка, 1997. – 196 с.
2. Кокорева Л .В. Диалоговые системы и представление знаний / Л. В. Кокорева, О. Л. Перевозчикова, Е. Л. Ющенко. – К. : Наук. думка, 1993. – 448 с.
3. Лазарєв М. І. Полісистемне моделювання змісту технологій навчання загальноінженерних дисциплін : [монографія] / М. І. Лазарєв. – Х. : Вид-во НФаУ, 2003. – 356 с.
4. Педагогика и психология высшей школы / под ред. М. В. Булановой-Топорковой. – Ростов н/Д, 2002. – 544 с.
5. Солсо Р. Л. Экспериментальная психология / Р. Л. Солсо, Х. Х. Джонсон, М. К. Бил. – СПб. : Прайм-ЕВРОЗНАК, 2001. – 528 с.

6. Хорев. П. Б. Методы и средства защиты информации в компьютерных системах : [учеб. пособие] / П. Б. Хорев. – М. : Академия, 2005. – 256 с.
7. Хофман И. Активная память: Эксперимент. исслед. и теории человеч. памяти / И. Хофман. ; пер. с нем. [под. ред. и предисл. Б. М. Величковского и Н. К. Корсаковой]. – М. : Прогресс, 1986. – 312 с. – (Обществ. науки за рубежом: Психология).

Чуприна Г. П.

Формування знань із програмних засобів захисту інформації на основі психічних моделей репрезентації понять

Проаналізовано моделі репрезентації понять у пам'яті людини з метою визначення найбільш універсальної, адекватної моделі структурування і узагальнення великої кількості різнорідної інформації з програмних засобів захисту інформації.

Ключові слова: психічні моделі, репрезентації понять, програмні засоби, захист інформації.

Чуприна А. П.

Формирование знаний программных средств защиты информации на основе психических моделей репрезентации понятий

Проанализированы модели репрезентации понятий в памяти человека с целью определения наиболее универсальной, адекватной модели структурирования и обобщения большого количества разнородной информации программных средств защиты информации.

Ключевые слова: психические модели, репрезентации понятий, программные средства, защита информации.

A. Chuprina

Formation of Knowledge of Information Security Software in the Basis of Mental Models Representations of Concepts

This paper analyzes a representation model of concepts in human memory with purpose to determine the most universal, adequate structure model and synthesis of a large number of heterogeneous data protection software information.

***Key words*:** mental models, representation of concepts, programs` facilities, information security.

Стаття надійшла до редакції 08.05.2012 р.