Действительно:

$$\upsilon(x) = \frac{ds}{d\tau} = \frac{dx}{d\tau(x)}; \quad \frac{1}{\upsilon(x)} = \frac{d\tau}{dx} = \frac{T}{p^*}\overline{F}^*(x).$$

Тогда величина $\frac{1}{\upsilon_i(x)}$, обратная скорости и кусочно-линейная функция, обратная закону движения источника на интервале (x_{i-1}, x_i), определятся по формулам:

$$\frac{1}{\upsilon_i(x)} = \frac{T}{p^*}\overline{F}_c^*(x); \quad \tau_c^* = \frac{T}{p^*}\overline{F}_c^*(x)x + \tau(x^{j-1}); \quad x^{j-1} < x \le x^i; \quad i = 1,2,...,n.$$

Далее рассчитывается закон движения источника $s^*(t)$.

Следовательно, в модели невозможно учесть все факторы, влияющие на температурное поле воздействующее на защищаемые объекты, поэтому программный закон движения корректируется экспериментально по показаниям пирометра или визуально. Величину $\frac{1}{\upsilon_i(x)}$ следует уменьшить, если на данном участке температура превышает заданную, и увеличить в противном случае. Аналогично корректируется программная мощность подвижного источника p^*. Неконтролируемые возмущения температурного поля можно компенсировать двумя способами: человеком-оператором или автоматически в соответствии с разработанным алгоритмом управления, например, непрерывным или разрывным в скользящем режиме.

ЛИТЕРАТУРА

1. Введение в математическое моделирование: [учеб. пособ.] / Под ред. П.В. Трусова. – М.: Логос, 2004. – 440 с.

2. Электронный журнал, № 2, февраль 2011 г. – Http://technomag.edu.ru/ Страница 28.

3. Зарубин В.С. Математическое моделирование в технике: [учеб. для вузов] / Под ред. В.С. Зарубина, А.П. Крищенко. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. – 496 с.

4. Строгалев В.П. Имитационное моделирование: [учеб. пособ.] / В.П. Строгалев, И.О. Толкачева. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 280 с.

5. Васильев К.К. Математическое моделирование систем связи: [учеб. пособ.] / К.К. Васильев, М.Н. Служивый. – Ульяновск: УлГТУ, 2008. – 170 с.

6. Барышников Н.В. Использование методов полунатурного моделирования для исследования характеристик системы автоюстировки / Н.В. Барышников, В.В. Карачунский, В.И. Козинцев, А.С. Румянцев, Д.В. Худяков // Тезисы докладов IV НТК «Радиооптические технологии в приборостроении». – Сочи, 2006. – С.105-108.

Надійшла: 30.07.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 004.621.3

Хорошко В.О., Іванченко І.С.

БАГАТОРІВНЕВИЙ ЗАХИСТ ІНФОРМАЦІЇ

У даній статі досліджено організацію багаторівневого захисту інформації із використанням поняття атома захисту. Розглянуто класифікаційні рівні степенів захисту елементів інформації та досліджено метод, що дозволяє диференційовано підійти до питання побудови багаторівневої системи захисту інформації із використанням інформаційної бази.

Ключові слова: атом захисту, безпека інформації, рівень секретності, гриф секретності, молекули захисту.

Вступ

У літературі [1, 2] показано, що для характеристики безпеки інформації (БІ) поділ рівнів чутливості інформації на «чутливі» та «нечутливі» не є адекватним. У багатьох випадках необхідна диференціація засобів захисту в залежності від рівня чутливості окремих

елементів інформації, іншими словами, для організації її з різними грифами секретності є проблема багаторівневого захисту.

Поділ інформації на групи створює передумови для зберігання інформації із різними рівнями секретності у різних групах. Крім того, такий розподіл повинен передбачати різні степені безпосереднього захисту в залежності від рівня секретності інформації. Наприклад, інформація із грифом «цілком таємно» повинна мати більш надійний захист безпосередній захист, ніж інформація із грифом «таємно».

Організація багаторівневого захисту суттєво полегшується з використанням поняття атома захисту. Оскільки елементи, що належать до одного атома, вимагають застосування однакових засобів захисту, їх необхідно виділяти до одного рівня класифікації, тобто самі рівні класифікації можуть розглядатися в якості атрибутів захисту.

Основна частина

Нехай, сегменти під файлів БІ, що містять елементи з різними рівнями класифікації, попарно не перетинались, тобто не мали спільних елементів. У такому випадку доступ до елементів одного рівня класифікації не буде пов'язаний з доступом до елементів, що належать до інших рівнів. Об'єднуючи атоми захисту в один сегмент під файлу, можна отримати молекулу захисту [3]. З врахуванням того, що кожен атом захисту входить в одну молекулу, будь-які дві молекули захисту не містять спільних елементів.

Розв'язання проблеми багаторівневого захисту для інформаційної бази, зображеної на рис. 1, ілюструється за допомогою табл. 1, 2 та рис. 3.

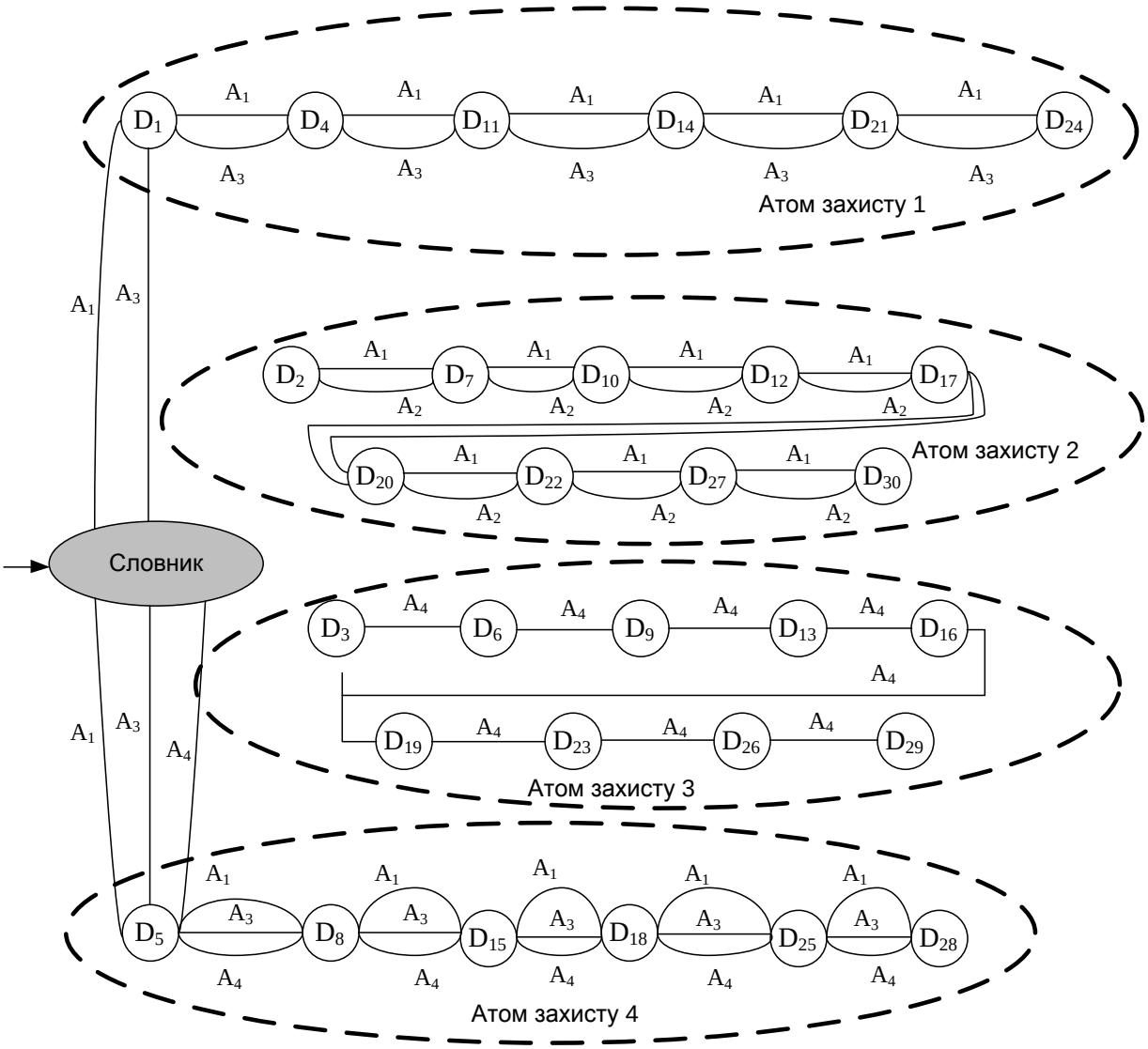

Рис.1. структура бази даних із розбиття елементів даних по атомам захисту

Слід враховувати, що атрибут A_1 – це процес розробки автоматизованої системи керування інформаційними базами (АСКІБ); A_2 – механічні характеристики АСКІБ; A_3 – факт належності до колективу розробників; A_3 – факт належності до групи розробників секретних елементів АСКІБ; A_4 – факт належності до колективу розробників підприємства; A_4 – співробітники співвиконавців, які беруть участь у розробці АСКІБ; ??? – елементи групи БІ.

На фізичному рівні захист може бути реалізований за допомогою розміщення елементів, що належать до різних рівнів класифікації, на фізично розподілених пристроях зовнішньої пам'яті. Це можливе тому, що розподіл елементів БІ на атоми та молекули захисту дає можливість логічного (на основі вимог захисту) розділення елементів на групи, доступ до яких не передбачає потреби додаткового доступу до іншої інформації, а, відтак, розміщення окремих груп може бути здійснене на пристроях пам'яті, що характеризуються незалежним звертанням.

Таким чином, логічне розділення реалізується і на фізичному рівні. Відповідно цьому, на рис. 2 наведена інтерпретація в контексті застосування атомарної концепції захисту.

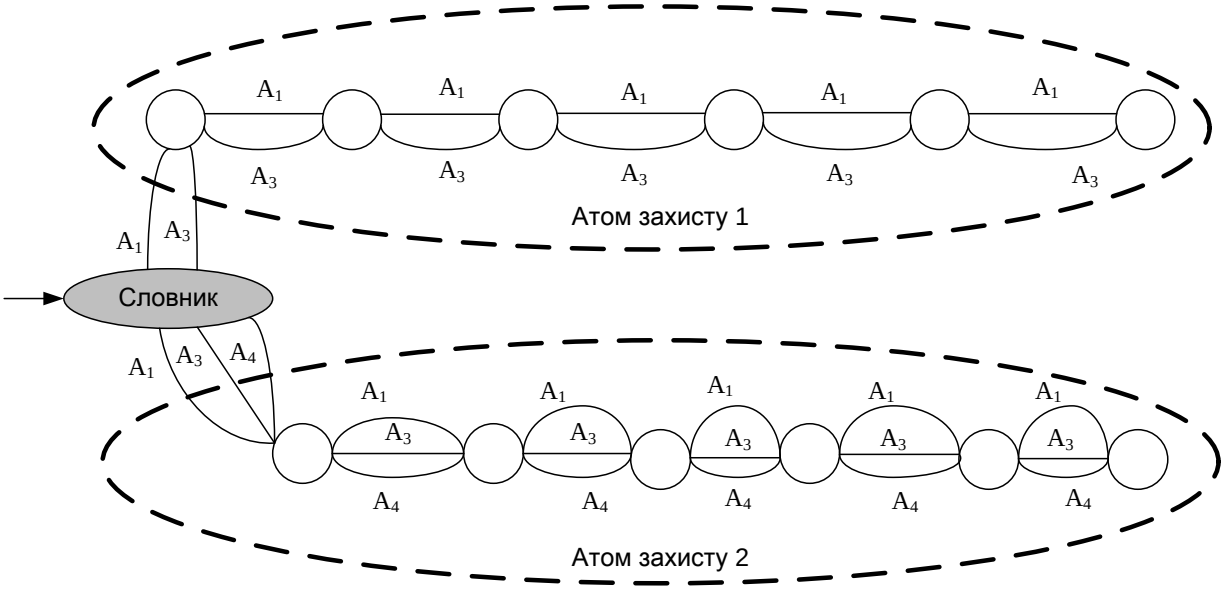

Рис. 2. Образ інформаційної бази при запиті $Q=A_2 \wedge [(A_1 \wedge A_4) \vee (A_3 \wedge A_4)]$

Зокрема, на рис. 3 елементи, що належать до атомів (1 і 4), (2), (3) та молекул 1, 2 і 3 відповідно, відносяться до різних рівнів класифікації.

Таблиця 1

Класифікаційні рівні сегментів захисту елементів інформації БІ

Класифікаційний рівень	Специфікація захисту
Цілком таємно	$A_1 \wedge A2 \wedge A3$
Таємно	$A_1 \wedge A_2 \wedge A_3 \wedge A_4$
Для службового користування	$A_1 \wedge A_2 \wedge A_3 \wedge A_4$

Доступ до атомів молекул 1, 2 і 3 є незалежним, отже з розміщенням їх на окремих пристроях із незалежним звертанням, на фізичному рівні відтворюється схема класифікації та логічного розподілення елементів БІ за рівнями секретності.

Розподіл елементів інформаційної бази на атоми та молекули захисту так, як це описано, приводить, по суті, до утворення ієрархії моделей БІ.

Порівняно із ситуацією, коли користувач має вичерпні відомості про весь склад елементів усієї БІ та перелік взаємозв'язків між цими елементами, наявність ієрархії моделей БІ створює ряд переваг, а саме:

1) користувачеві достатньо мати спрощене уявлення про структуру БІ, із якою він працює, що, звужуючи діапазон відомої інформації до окремої молекули чи атома захисту, значно спрощує виконання його безпосередніх завдань;

2) процес управління доступом набуває більшої надійності; користувач не може звертатися до інформації, що належить до області поза межами визначеної для нього моделі БІ. В ідеальному випадку ця модель повинна бути максимально обмеженою за принципом «необхідності знання», тобто доступною є лише інформація, потрібна користувачеві для виконання його безпосередніх робочих завдань;

Таблиця 2

Організація багаторівневого захисту в інформаційній базі, що відповідає рис. 3

Елементи підфайлу	Рівень захисту	Адреси елементів інформації в елементі підфайлу
Молекула 1	цілком таємно	1, 4, 11, 14, 21, 24, 5, 8, 15, 18, 25
Молекула 2	таємно	2, 7, 10, 12, 17, 20, 22, 27, 30
Молекула 3	для службового користування	3, 6, 9, 13, 16, 19, 23, 26, 29
Атом 1	цілком таємно	1, 4, 11, 14, 21, 24
Атом 2	таємно	2, 7, 10, 12, 17, 20, 22, 27, 30
Атом 3	для службового користування	3, 6, 9, 13, 16, 19, 23, 26, 29
Атом 4	цілком таємно	5, 8, 15, 18, 25, 28

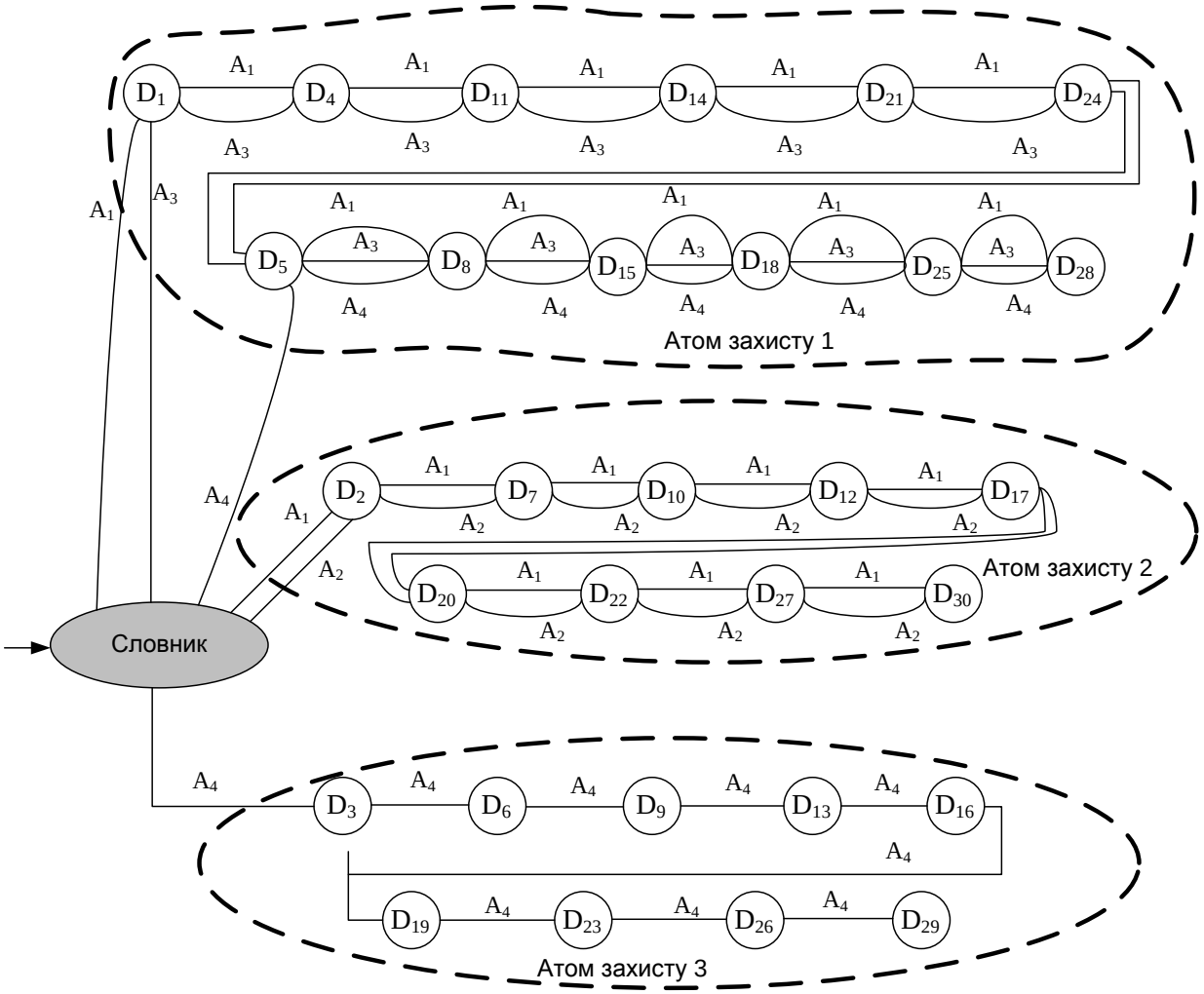

Рис. 3. Структура інформаційної бази із розбиття елементів інформації по молекулах захисті

3) модель БІ для користувача може залишатись незмінною, тоді як схема БІ в цілому піддається реструктуризації, наприклад, із метою виточення нових або модифікації вже існуючих систем, прав доступу або предикатів; у моделі не відбувається змін і в тих випадках, коли необхідні об’єкти, права доступу або предикати зі схеми БІ видаляються;

4) певна ізоляція користувача від змін, що відбуваються у структурі інформаційної бази, може розглядатися як один із проявів незалежності інформаційної бази від прикладних засобів автоматизованої обробки інформації, що її використовує користувач;

5) можливість роздільного та фізичного рівні зберігання груп елементів (атомів, молекул), що дозволяє не лише блокувати обхідні шляхи доступу, а й покращує його характеристики. При цьому процедура виділення окремих пристроїв пам'яті для зберігання окремих атомів та молекул БІ повинна завершувати процес проектування фізичної структури БІ. Тут можна одержати додатковий виграш, якщо розподілити згруповані елементи БІ по окремих пристроях пам'яті таким чином, щоб забезпечити пріоритет доступу найбільш часто використовуваною інформацією , або максимізувати степінь близькості розміщення даних, що зберігаються.

Зокрема, якщо прийняти, то до різних елементів, об'єднаних в атоми чи молекули, звертання ймовірно будуть здійснюватися одночасно, то їх групове зберігання в одній і тій же фізичній області сприятиме підвищенню продуктивності системи обробки даних у цілому [4].

Висновки

Описаний метод дозволяє побудувати багаторівневу систему захисту інформації із використанням інформаційної бази та розбиття елементів по молекулах та атомах захисту. Це дозволяє створити модель безпеки інформації більш гнучкою та трансформуватися під конкретний об'єкт.

ЛІТЕРАТУРА

1. Лимов С.В. методы с средства защиты информации в 2х томах./Лимов С.В., Перегудов Д.А., Хорошко В.А.-К.:Арий, 2008.

2. Невойт Я.В. Исследование потоков информации на выходе имитационной модели / Невойт Я.В., Мазуренко А.Н., Хорошко В.А.//збірник наук. праць СНУЯЕтаП,№1(37), 2011.-с.191-196.

3. Сяо Д. Защита ЭВМ./Сяо Д.,Керр Д.,Медтси С.- М.:Мир,1982.-263с.

4. Уелдон Дж.Л. Администрирование и статистика, 1984.-207с.

Надійшла: 29.07.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.

УДК 004.43(031):681.3.01(02)

Кущ С.М., Луценко В.М., Прогонов Д.О.

ВИЯВЛЕННЯ ПРИХОВАНИХ ПОВІДОМЛЕНЬ ЯК СКЛАДОВА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглянутою є проблема використання криптографічних методів захисту інформації при проектуванні комплексних систем захисту інформації (КСЗІ). Головна увага приділяється методам виявлення прихованих повідомлень, котрі є вбудованими у 2D-контейнери на основі LSB-методів. Розглядається випадок слабкого заповнення, а процедура виявлення передбачає використання Вейвлет аналіз.

Ключові слова: системи захисту інформації; стеганографія; проект захисту; криптографія; образ.

Постановка проблеми. Забезпечення надійного захисту інформації з обмеженим доступом, що циркулює у системах електронного документообігу об'єкта інформаційної діяльності (ОІД) від витоку до глобальної мережі Інтернет, є особливо актуальною задачею, зважаючи на активність використання глобальної сіті [1-3].

Методи вирішення такої задачі представляють неабиякий інтерес як для приватних організації (захист баз даних клієнтів, конструкторської документації тощо), так і для державних структур (захист інформації, що становить державну таємницю).

Найбільш перспективними напрямками прихованої передачі даних сьогодні є крипто-графічні та стеганографічні методи [4]. Використання лише криптографічних методів має суттєвий недолік.