Document Analysis and Recognition (ICDAR-2005), 2005, Seoul, South Korea, pp. 192-196.124
5. *Xu-Cheng Yin, Jun Sun, Satoshi Naoi*, "Perspective rectification for mobile phone camera-based documents using a hybrid approach to vanishing point detection", Proceedings of the Second International Workshop on Camera-Based Document Analysis and Recognition (CBDAR-2007), 2007, Curitiba, Brazil, pp. 37-44.
A. *Ulges, C. Lampert, and T. M. Breuel*. Document capture using stereo vision. In Proceedings of the ACM Symposium on Document Engineering, pages 198–200. ACM, 2004.
6. *Yamashita, A. Kawarago, T. Kaneko, and K.T. Miura*. Shape reconstruction and image restoration for non-flat surfaces of documents with a stereo vision system. In Proceedings of 17th International Conference on Pattern Recognition (ICPR2004), Vol.1, pages 482–485, 2004.
7. *M.S. Brown and W.B. Seales*. Document restoration using 3d shape: A general deskewing algorithm for arbitrarily warped documents. In International Conference on Computer Vision (ICCV01), volume 2, pages 367–374, July 2001.
8. *Кульчицька І.О., Тимченко О.В.* Особливості алгоритмів бінаризації зображень документів // Зб. наук. пр. ІПМЕ НАН України. – Вип.68. – К.: 2013. – С.141-149.
9. *Линник Ю. В.* Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений / Юрий Владимирович Линник. – Государственное издательство Физико-математической литературы. – 1958
10. *Тимченко О.В., Кульчицька І.О., Тимченко О.О.* Відновлення геометрії довільно спотворених зображень документів шляхом сегментації // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.70. – К.: 2013. – С.171-176.
11. *Кульчицька І.О.* Метод корекції переспективних спотворень на зображеннях текстових документів // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ НАН України. – Вип.71. – К.: 2014. – С. 153-159

Поступила 7.9.2015р.

УДК 004.9

Б.В.Дурняк, М.М. Кляп, УАД, м.Львів

ОРГАНІЗАЦІЯ СИСТЕМИ ПРОГНОЗУВАННЯ, ПРИ ВИНИКНЕННІ НЕОЧІКУВАНИХ НЕГАТИВНИХ ФАКТОРІВ

Вступ

В рамках загальної організації системи управління DTP, при виникненні негативних зовнішніх факторів, що орієнтовані на реалізацію впливу на технологічний процес, необхідно більш детально зупинитися на компоненті, що представляє собою модель зовнішніх процесів $Z\,\mathrm{Pr}_i$. Цю компоненту необхідно розглянути з точки зору наступних аспектів її функціонування:

- з точки зору аспектів взаємозв'язку $M(Z\,\mathrm{Pr}_i)$ з модулями $M(PR_i)$ та $M(O\,\mathrm{Pr}_i)$,

- з точки зору аспектів використання Vp_i, для реалізації функцій захисту від негативного впливу,

- з точки зору функціонування системи безпеки, або засобів безпеки системи управління технологічним процесом.

В даному випадку, розглядаються процеси прогнозування не з загальної точки зору цих процесів, а з точки зору захисту системи управління від негативного впливу випадкових подій Vp_i на систему управління.

Мета роботи - розглянути процеси прогнозування з точки зору захисту системи управління від негативного впливу випадкових подій.

Виклад основного матеріалу

Приймається, що негативні фактори будуть існувати постійно по відношенню до технологічного процесу типу DTP. Це означає, що їх поява буде випадковою в часі та, практично, відповідні події, що є носіями цих негативних факторів, будуть характеризуватися різними складно передбачуваними значеннями параметрів, що характеризують Vp_i. Невизначеність Vp_i буде обумовлюватися не тільки приведеними вище характеристиками, а і не визначеністю типів подій, що прогнозуються системою $S(\mathrm{Pr}_i)$. Слід відмітити, що $S(PR_i)$ складається, щонайменше, з двох моделей $M(O\,\mathrm{Pr}_i)$ та моделі $M(PR_i)$. В процесі детального аналізу $S(PR_i)$ буде показано, що в склад $S(PR_i)$ можуть входити і інші компоненти, в тому числі, і модель $M(Z\,\mathrm{Pr}_i)$. Функціонування $M(Z\,\mathrm{Pr}_i)$ з точки зору її взаємодії з моделями $M(PR_i)$ та $M(O\,\mathrm{Pr}_i)$ є досить важливим, оскільки останні дві моделі є постачальниками вхідних даних для $M(Z\,\mathrm{Pr}_i)$ і, відповідно, системи безпеки ISU, яка позначається символами SB. Розглядати всі аспекти функціонування $M(Z\,\mathrm{Pr}_i)$ та $M(PR_i)$ і $M(O\,\mathrm{Pr}_i)$ в комплексі необхідно, оскільки робота $M(Z\,\mathrm{Pr}_i)$ безпосередньо залежить від цих компонент. В прийнятій інтерпретації, що характерна для систем безпеки, Vp_i можна розглядати як деяку атаку, кінцевою ціллю якої є система ISU, що, в цілому, виходить за рамки $M(Z\,\mathrm{Pr}_i)$ оскільки SB розв'язує задачі виявлення атак At_i, розв'язує задачі реалізації протидії атакам, визначає величину текучого значення рівня безпеки та цілий ряд інших задач, які відображають особливості предметної області інтерпретації задач безпеки

системи управління. Оскільки прогнозування виникнення Vp_i обумовлюється необхідністю забезпечення заданого рівня безпеки, який при адекватній інтерпретації, може задаватися у вигляді вимог до системи захисту, то завдяки прогнозу у системи безпеки SB виникає можливість не тільки оперативно і адекватно реагувати на At_i, а і упереджувати виникнення відповідних атак. Це є можливим завдяки тому, що в рамках $M(O\,\mathrm{Pr}_i)$ реалізуються не тільки процеси попереднього аналізу вхідних даних, а і процеси виявлення загроз (Zg_i) які існують в ISU, для відповідних атак At_i.

Для того, щоб розглядати $M(Z\,\mathrm{Pr}_i)$ з точки зору її зв'язку з моделями $M(O\,\mathrm{Pr}_i)$ та $M(PR_i)$ необхідно визначитися з особливостями інтерпретації цих моделей в предметній області задач захисту системи ISU та системи SB в цілому. Як уже зазначалось, додатковими функціями $M(O\,\mathrm{Pr}_i)$ є наступні можливості моделі:

- аналіз загроз Zg_i, що існують в рамках системи ISU,
- елімінація активних загроз,
- розпізнавання передумов можливих атак.

Уявлення про загрози є специфічним, оскільки до останньої можна віднести деяку характеристику системи тільки в тому випадку, якщо така характеристика буде використана можливою атакою. У випадку, коли системі SB відома деяка атака, то відповідно, відома Zg_i, яку така атака використовує. Елімінація такої загрози може реалізуватися лише в тому випадку, коли атаки, що її використовують активізуються небезпеками. Тому, навіть по відношенню до відомих загроз, останні не елімінуються, оскільки елімінація загроз передбачає розширення відповідної моделі.

У відповідності з функціональною орієнтацією окремих компонент функціонування системи прогнозування, будемо формувати інтерпретацію для моделі $M(O\,\mathrm{Pr}_i)$, яка ґрунтується на специфіці задач, для розвитку яких система прогнозування орієнтована, тому, приймемо, що на вхід моделі $M(O\,\mathrm{Pr}_i)$ будуть подаватися не просто деякі сигнали зовнішніх негативних факторів, а будуть подаватися дані, що пов'язані з активізацією атак. Оскільки $M(O\,\mathrm{Pr}_i)$ є компонента, що структурно в $S(PR_i)$ розміщається першою, а фізично, у системи SB і, відповідно, ISU входом є точка підключення до мережі, то $M(O\,\mathrm{Pr}_i)$, при такому уточненні, є моделлю, яка проводить попередній аналіз даних з пакетів, які пропущені в системі через Firewall [1]. Firewall будемо розглядати в рамках стандартного засобу захисту, який, як мінімум реалізує фільтрацію пакетів на основі аналізу, в першу чергу адрес. Щоб можна було, в даному випадку, вхідні дані розглядати як вхідні сигнали, що допускають інтерпретацію їх послідовностей, як марковські

процеси, то семантично повні фрагменти таких даних, або фрагменти інформації будемо розглядати, як такі, що можуть, в більшій мірі, або меншій мірі мати відношення до початкових фрагментів атак. Переважно, атака представляє собою деяку програмну реалізацію алгоритму, що сформований відповідною небезпекою. З фізичної точки зору, однією з функцій попереднього аналізу, який проводить $M\left(O\,\mathrm{Pr}_i\right)$, є розпізнавання інформації в чергових пакетах, що приходять в систему. Якщо аналізована інформація представляє собою програму, яка може бути реалізацією атаки, то міра відповідальності цієї програми відомим сигнатурам визначає міру близькості відповідних даних тій чи іншій атаці. В $M\left(O\,\mathrm{Pr}_i\right)$ відповідна міра інтерпретується, як сигнал, параметри якого мають виходити за задані границі. Такі сигнали можна аналізувати як послідовності, що відповідають, або можуть відповідати рядам маркова. В цьому випадку, прогнозування виникнення Vp_i, що ґрунтується на використанні приведених вище сигналів, буде означати, що міра подібності вхідної інформації до реалізації атаки є достатньо висока і у відповідності з прогнозом, атака може бути здійснена через певний інтервал часу Δt_i, якщо базовим параметром прогнозування є параметр часу. Таким чином, модель $M\left(O\,\mathrm{Pr}_i\right)$ формує ряд виборок, що представляють собою міру близькості відповідної послідовності елементів програми до сигнатури, що відповідає програмі, яка представляє собою атаку. Приведений алгоритм функціонування $M\left(O\,\mathrm{Pr}_i\right)$ ґрунтується на тому, що, в переважній більшості, атаки, що активізуються в середовищі об'єкту, час від часу модифікуються, що реалізуються небезпекою з ціллю, яка полягає у тому, щоб система захисту, в цілому, які по своїй суті, представляють собою еталони профілів атак, не могли розпізнати чергову атаку. Оскільки небезпека Nb, не може мати повної інформації про об'єкт атаки, то вона повинна формувати послідовність атак, кожний раз наближаючи її до атаки, яка враховує більшість характеристик та можливостей засобів захисту, які виявляють та протидіють можливим атакам. Це обґрунтовує положення про те, що атака, яка на виході системи $S\left(PR_i\right)$ інтерпретується, як подія Vp_i, виникає на фоні послідовних втручань, що активізуються Nb_i.

Розглянемо більш детально особливості інтерпретації процесу функціонування моделі $M\left(PR_i\right)$ з точку зору фізичної реальності, на яку відповідна модель орієнтована в предметній області, що стосується проблем захисту системи ISU. Модель $M\left(PR_i\right)$ отримує на вході інформацію з $M\left(O\,\mathrm{Pr}_i\right)$ наступних типів:

- параметри сигналу, що відображають міру близькості інформації, що приходить в пакетах, до відомих образів, або профілів атак, які описуються у вигляді відповідних сигнатур,

- крім параметрів сигналу, у випадку необхідності, модель $M(PR_i)$ може отримати з $M(O\,\mathrm{Pr}_i)$ текстовий опис інтерпретації атаки, якщо остання реалізується,
- модель $M(PR_i)$ може отримувати з $M(O\,\mathrm{Pr}_i)$ дані про загрози, які були використані передумовами атаки, або могли бути використані передумовами атаки, що поступали на вхід моделі $M(O\,\mathrm{Pr}_i)$.

Прогноз, який реалізується в $M(PR_i)$ реалізується на основі даних про сигнали, які інтерпретують міру близькості відповідних даних, що поступили в систему до атак, які можуть реалізовуватися зовнішніми факторами, що представляють собою небезпеку Nb_i. Якщо $M(PR_i)$ встановила можливість виникнення атаки, яка визначається базовим параметром прогнозування, то опис випадкової події Vp_i, який передається в модель $M(Z\,\mathrm{Pr}_i)$, доповнюється інтерпретаційним описом $j(At_i)$ відповідної атаки. Цей опис разом з параметрами At_i, або Vp_i використовується для адекватного вибору засобів захисту системи ISU від передбачуваної атаки. Оскільки атака ініціюється на основі використання загрози Zg_i, яка характеризує об'єкт захисту, то одним із способів протидії відповідній атаці може служити елімінація відповідної Zg_i. Цей спосіб протидії можливій атаці є одним з найбільш поширених та найбільш ефективним. Елімінація загрози, практично, полягає у модифікації засобів захисту системи, завдяки якій вторгнення атаки в систему було б не можливим. Така модифікація полягає:

- у розширенні можливостей існуючих засобів захисту, наприклад, розширення функціональних можливостей існуючих Firewall-ів,
- у створенні нових засобів захисту, наприклад, використання систем типу $IDS[2]$.

Інший підхід до реалізації протидії атакам полягає у реалізації впливу на активізовану в середовищі ISU атаку таким чином, щоб остання не могла виконати поставлену ціль. Такий підхід передбачає можливість активізації самої атаки, а, за рахунок того, що вона була спрогнозована моделлю $M(PR_i)$, то система безпеки може бути заздалегідь підготовлена до знищення відповідної атаки. Прикладом такого способу протидії системою захисту атакам може служити антивірусна система, яка передбачає можливість активізувати атаку, або допустити її в середовище об'єкту нападу і тільки після того її елімінувати. Сучасні антивірусні системи, при цьому, розв'язують задачі розпізнавання окремих вірусів, а після розпізнавання реалізується їх усунення. Основними недоліками цього підходу є наступні фактори:

- атака, яка проникла в систему може встигнути частково здійснити

свій негативний вплив,

- при виділенні віруса з системи немає гарантії того, що цей самий вірус знову не попаде в систему,
- відомі віруси при їх повторних використаннях можуть самомодифікуватися, що може призвести до того, що відповідний вірус не зможе бути розпізнаним.

Оскільки в рамках досліджуваного підходу обов'язковою функцією процесів захисту системи є функція прогнозування події Vp_i, то необхідно визначити склад всієї системи захисту, або системи безпеки SB, та роль додаткових компонент в SB, яку вони виконують, при розв'язуванні задач захисту системи управління.

Модель $M(Z\,\mathrm{Pr}_i)$ орієнтована на виконання наступних функцій, які логічно доповнюють функції моделей $M(O\,\mathrm{Pr}_i)$ та $M(PR_i)$, з ціллю завершення розвязку задачі захисту. Для того, щоб такі функції окреслити, розглянемо вхідні дані, які подаються до моделі $M(Z\,\mathrm{Pr}_i)$:

- інформація про прогнозовану подію Vp, або атаку At_i,
- інтерпретаційний опис відповідної події $j(At_i)$,
- Інформація про загрозу Zg_i, яка може бути використана для активізації атаки At_i.

Виходячи з цих даних, модель $M(Z\,\mathrm{Pr}_i)$ може розв'язувати наступні задачі захисту:

- елімінацію загроз Zg_i, що можуть використовуватися прогнозованими атаками,
- упередження негативних впливів атак на компоненти системи управління,
- формування розширеного інтерпретаційного опису потенціальної атаки,
- дослідження додаткових можливостей атаки, якщо прогнозована атака не відноситься до атак, що є уже відомими системами безпеки.

Елімінація загроз уже розглядалась, тому, більш детально зупинимось на упередженні негативних впливів атак на компоненти системи управління. Такого типу протидія атакам використовується в тому випадку, коли є неможливою елімінація загрози. Не можливість елімінації загрози може обумовлюватися різними причинами, до яких можна віднести наступні:

- коли загроза відноситься до компонент, в які вносити зміни не дозволено, наприклад, коли зміни пов'язані з втручанням в сертифікати системи, наприклад, в операційну систему і. т.д.,
- коли усунення однієї загрози може привести до виникнення іншої загрози,
- коли усунення деякої загрози є значно дорожче від захисту

відповідної компоненти системи, на яку орієнтована дія прогнозованої атаки.

Для того, щоб вибрати один з приведених способів протидії атаці, в рамках $M(Z\,\mathrm{Pr}_i)$ використовується компонента, що аналізує відповідні дані та вибирає оптимальне рішення по реалізації протидії. Таку компоненту в моделі $M(Z\,\mathrm{Pr}_i)$ будемо позначати (KPR). З приведеного вище виходить, що наступною компонентою моделі $M(Z\,\mathrm{Pr}_i)$ є компонента, що реалізує процес протидії атаці (RPA). В рамках системи $S(PR_i)$ може мати ситуація, коли $M(PR_i)$ сформувала прогноз про можливу атаку Vp_i, а сама атака в $M(O\,\mathrm{Pr}_i)$ не може бути розпізнана. Це означає, що інформація про Vp_i передається у $M(Z\,\mathrm{Pr}_i)$, але даних, що супроводжують інформацію про Vp_i є недостатньо, щоб можна було розпізнати тип атаки. Відсутність даних про тип атаки не дозволяє коректно прийняти рішення про спосіб протидії її негативного впливу на компоненти системи ISU. В цьому випадку, в рамках $M(Z\,\mathrm{Pr}_i)$ розв'язується задача виводу розширеного інтерпретаційного опису потенціальної атаки. Для цього, в склад $M(Z\,\mathrm{Pr}_i)$ вводиться компонента виводу розширень інтерпретаційних описів (VIO). Крім зазначених функцій, в моделі $M(Z\,\mathrm{Pr}_i)$ повинні виконуватися функції, що реалізують управління моделями $M(PR_i)$ та $M(O\,\mathrm{Pr}_i)$. Таке управління полягає у формуванні нових вимог до функціонування зазначених компонент і, в першу чергу, вимоги до моделі $M(PR_i)$. До таких вимог по модифікації процесів функціонування можна віднести наступні:

- вимога по зміні базового параметру прогнозування, наприклад, в більшості випадків, таким параметром є час, в цих випадках прогноз полягає у визначенні моменту часу t_{i+1}, по відношенню до t_i, коли відповідна Vp_i може відбутися, прикладом іншого параметру може служити параметр, що характеризує міру небезпеки деякої події, це означає, що $M(Z\,\mathrm{Pr}_i)$ повинно отримувати інформацію про Vp_i, яка визначає міру небезпеки Vp_i для об'єкту, що охороняється,
- вимога по прогнозуванню зміні рівня безпеки системи,
- вимоги по виключенню з процесу прогнозування атак заданого типу.

Вимога по прогнозуванню зміни рівня безпеки, для моделі $M(PR_i)$ означає, що ця модель повинна з заданою періодичністю реалізувати прогноз

рівня безпеки, що може здійснюватися лише у випадку, коли відповідні вхідні дані в модель подаються з системи SB. Вимога по виключенню атак з процесу прогнозування обумовлюється наступним. Необхідність в цьому може виникнути в тому випадку, коли можливість негативного впливу атаки на вибрану компоненту ISU блокується засобами захисту на певний період. Такий період може визначатися повним циклом виробництва певного продукту, а блокування реалізується безпосередньо на об'єкті атаки.

Оскільки $M(Z\,\mathrm{Pr}_i)$ є моделлю, яка використовує для свого функціонування дані про результати прогнозу, то така модель може формувати розширення інформаційного опису у випадках, коли модель $M(PR_i)$ не надає повної інформації про прогнозовану подію Vp_i. Таке розширення реалізується з допомогою процесів виводу, які ґрунтуються на використанні наступних засобів:

- засобів перетворення текстових описів в логічні формули, які, представляють собою певним чином реалізовану інтерполяцію логіки, що відображається у відповідному текстовому описі,
- засобів виводу логічних формул, які представляють собою розширені системи виводу, які є відомими в математичній логіці [4],
- опис цілі перетворення, яка обумовлюється задачею захисту системи від події Vp_i, яка в неповній формі представляє собою результат прогнозування,
- засоби переходу від логічної інтерполяції текстових описів, що отримані в результаті прогнозування, до текстової форми опису виведених розширень.

Процеси $Z\,\mathrm{Pr}_i$, що описуються в $M(Z\,\mathrm{Pr}_i)$, тісно пов'язані не стільки з самою системою управління ISU, скільки з системою безпеки SB. Тому, необхідно коротко зупинитися на задачах, які розв'язуються системою SB. До таких задач відносяться наступні:

- ┐ изначення текучого рівня безпеки системи ISU,
- інтерпретація подій, що відбуваються в ISU, які допускають можливість здійснення негативного впливу на процес управління,
- виявлення успішних атак на систему управління,
- аналіз результатів негативного впливу атак на ISU,
- визначення необхідного, або достатнього рівня безпеки системи управління.

Визначення текучого рівня безпеки системи ISU ґрунтується на аналізі атак дія яких на ISU була блокована, або виявлених атак, на основі аналізу успішних атак, які здійснили негативний вплив на ISU і тільки після того були виявлені та, на основі прогнозування змін рівня безпеки системи. Рівень

безпеки будемо інтерпретувати, як оцінку здатності технологічного процесу реалізовувати процес функціонування таким чином, щоб продукція, що виробляється відповідала заданим вимогам. Таке визначення рівня безпеки дозволяє пов'язати функціональні характеристики атак із змінами та втратами, до яких може привести та, чи інша атака. Тому, кожна атака буде характеризуватися деяким коефіцієнтом, який характеризує міру небезпеки окремої атаки для DTP, що описується співвідношенням $Ub_i(At_i) = \alpha_i At_i$, де Ub_i - міра зменшення рівня безпеки, при дії атаки At_i на DTP. Практично, кожний засіб захисту Za_i може співставлятися з певним типом атак. Це означає, що At_i визначає, які Za_i будуть використовуватися, або $At_i \to Zg_i$. Приймемо, що рівень безпеки RB, завжди є більший від рівня небезпек, або має місце співвідношення:

$$SB(DTP) = \sum_{i=1}^{n} RB_i(Za_i) - \sum_{i=1}^{m} Ub_i(At_i).$$

Приведена рівність відображає текучий стан $SB(DTP)$, коли враховуються всі атаки, що є відомими. Якщо $SB > 0$, то це означає, що всі атаки можуть бути розпізнані і їм в рамках системи може здійснюватися протидія засобами Za_i. Практично, засоби Za_i інтегруються в одну систему. Очевидно, що в SB повинен виконуватися певний баланс між кількістю та атаками At_i. Для цього, приймається, що $SB(DTP) \geq \delta(Ub_i)$, де $\delta(Ub_i)$ деяка порогова надмірність показника безпеки по відношенню до небезпек. Величина $\delta(Ub_i)$ необхідна для того, щоб система не виявилась вразливою у випадку, коли в ISU прийшла At_i^*, яку система захисту $S(Za)$ не розпізнала або не змогла протидіяти цій атаці. В цьому випадку, виникає питання про те, як забезпечується $\delta(Ub_i)$ в рамках SB на практиці.Очевидно, що в основі такого забезпечення лежить можливість прогнозування виникнення тих, чи інших атак. При цьому, прогнозується не можливість виникнення атаки певного типу, а можливість виникнення атаки деякого нового типу. Реалізація такого прогнозування суттєво відрізняється від прогнозування виникнення відомих атак. Відповідна функція реалізується в рамках системи SB. Прогнозування цього типу проводиться на основі наступних принципів:

- на основі аналізу даних про кількість різних атак, що відрізняються від атаки, що була виявлена в текучий момент появи атаки нового типу (At_i^R),
- на основі аналізу успішних атак, що були виявлені в системі (At_i^U),
- на основі аналізу можливих модифікацій відомих атак, яка може приводити до уникнення активізації відповідного засобу Za_i, (At_i^M).

Встановити залежності між появою атаки нового типу та атаками At_i^R, At_i^U та At_i^M в явній формі досить складно. Тому, опис функції такого типу заміняється моделлю прогнозування нової атаки $M(PAt)$. В неявній формі така атака записується у вигляді співвідношення:

$$\delta(Ub_i) = F[\varphi^R(At_i^R), \varphi^M(At_i^M), \varphi^U(At_i^U)]\,. \quad (1)$$

Перш за все, розглянемо можливість явного опису функцій φ^R, φ^M, φ^U. Функція $\varphi^R(At_i^R)$ може представляти собою вираз для підрахунку кількості атак різного типу за вибраний перід часу функціонування ΔT_i. В явному вигляді цю функцію можна записати:

$$\varphi^R(At_i^R) = \sum_{i=1}^{m} At_i^R,$$

де R – означає, що чергова складова суми представляє собою атаку нового типу. Більш повно цю функцію можна записати у наступному вигляді:

$$\varphi^R(At_i^R) = \sum_{i=1}^{m}\{\forall(At_{i-1})\exists\, At_i[At_i = At_i^R] \rightarrow (At_i = 1)\}.$$

Це співвідношення означає, що якщо для всіх атак в межах інтервалу ΔT_i має місце атака така, що At_i є атакою нового типу At_i^R, то до отриманої суми додаємо одиницю. Фактично, $\varphi^R(At_i^R)$ означає загальну кількість атак нового типу.

Функція $\varphi^M(At_i^M)$ описується наступним чином:

$$\varphi^M(At_i^M) = \sum_{i=1}^{k}\{\forall At_{i-1}\exists\, At_i[(At_1 * \ldots * At_{i-1}) \rightarrow At_i] \rightarrow \\ \rightarrow [(At_i = At_i^M)\&(At_i^M = 1)]\}\,.$$

Функція $\varphi^U(At_i^U)$ описується наступним співвідношенням:

$$\varphi^U(At_i^U) = \sum_{i=1}^{k}\{\forall At_{i-1}\exists\, At_i[(At_i \rightarrow Za_i) \rightarrow (At_i = At_i^U)\&(At_i^M = 1)]\}.$$

Приведені формули описують способи обчислення складових функцій, що входять у формулу (1). Тоді функція F представляє собою опис моделі прогнозування виникнення вибраного типу атаки. В цьому випадку модель може бути описана у вигляді:

$$\delta(Ub) = \left\{M\left[PR_i\left(\varphi^R(At_i^R)\right)\right]\&M\left[PR_i\left(\varphi^M(At_i^M)\right)\right]\&M\left[PR_i\left(\varphi^U(At_i^U)\right)\right]\right\}. \quad (2)$$

Висновок

Співвідношення (2) описує випадок, коли прогнозування виникнення атаки типів At_i^R, At_i^M, At_i^U реалізується незалежно відповідними моделями $M(PR_i)$. Очевидно, що на основі інтерпретації даних про атаки різних типів, моделі прогнозування $M(PR_i)$ можуть бути звязаними між собою. Це грунтується на можливості існування зв'язків між атаками, що на практиці досить часто має місце [5].

1. *Столлинг В*. Основы защиты сетей. Приложения и стандарты. Киев: ВХБ, 2000.
2. *Романцов Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
3. *Тимофеев П.А*. Принципы защиты информации в компьютерных системах. // Конфидент, 1998, N3.
4. *Расева Е., Сикорский Р*. Математика метаматематики. М.: Наука, 1972.
5. *Касперски К.* Техника сетевых атак. М.: «Солон-Р», 2001.

Поступила 5.10.2015р.