УДК 004.9

МЕТОДИ ДИНАМІЧНОЇ МОДИФІКАЦІЇ ПРОГНОЗУВАННЯ

М. М. Кляп

ДВНЗ "Ужгородський національний університет"
пл. Народна, 3, Ужгород, 88000, Україна

Проаналізовано Vp_i та встановлено слабкі місця в інформаційній системі управління ISU(DTP). Визначено потребу зміни рівня захисту, який відповідав би реальним небезпекам, що їх ініціюють атаки, та необхідній мірі захисту DTP. Сформульовано визначення таких понять: небезпека та атака. Розглянуто тримірну систему координат.

Ключові слова: *апроксимувальна функція, захист, незебпека, атака, загроза.*

Динамічна реалізація модифікації системи прогнозування дає можливість підвищити ефективність адаптації відповідних змін до поточних ситуацій, які виникають в *DTP*. Це досягається завдяки тому, що відповідні зміни в системі прогнозування *S(PR)* реалізуються безпосередньо перед тим, коли їх необхідно використовувати. Така часова синхронізація дозволяє точніше визначати значення параметрів тих факторів, які протидіють атакам на об'єкт захисту, що дає змогу ефективніше забезпечувати елімінацію негативного впливу випадкових подій Vp_i.

Однією з основних функціональних компонент системи прогнозування є компонента ZPr_i, що розв'язує задачі, які зумовлюють необхідність використання всієї *S(PR)*. Для того щоб можна було конструктивно проводити аналіз $M(ZPr_i)$, вважатимемо, що ZPr_i представляє процеси, які розв'язують задачі захисту *DTP* від зовнішніх факторів, вплив яких проявляється через використання подій Vp_i. За такої інтерпретації ZPr_i має розв'язувати такі задачі:

– аналізувати Vp_i та ідентифікувати тип загрози, яку може завдати відповідна випадкова подія;
– визначати слабкі місця в інформаційній системі управління *ISU(DTP),* використавши які, Vp_i може реалізовувати загрозу;
– визначати необхідні методи протидії загрозам та реалізовувати їх в режимі реального часу, що є процесом реалізації негативного впливу, який здійснює Vp_i;
– визначати рівень безпеки, що забезпечується для *ISU(DTP)* процесами ZPr_i;
– визначати потребу зміни рівня безпеки, що відповідав би реальним небезпекам, які ініціюють атаки, та необхідній мірі захисту *DTP*.

Визначимо термінологію, пов'язану з безпекою *DTP*, яку використовуватимемо в цій роботі.

Визначення 1. Небезпекою називатимемо зовнішні щодо *DTP* об'єкти чи процеси, які можуть виникати, а також функціонувати незалежно від об'єкта захисту.

Визначення 2. Загрозою будемо називати процес, який може призвести до негативного впливу на *ISU(DTP)* і на *DTP* та використовує слабкі місця в *ISU* чи інших підсистемах *DTP*. Наприклад, підсистеми, які характеризуються людськими факторами, для реалізації послідовних дій, орієнтованих на здійснення негативного впливу на об'єкт захисту.

З цього визначення бачимо, що загроза являє собою деяку стратегію, що породжується небезпекою і взаємодіє з усіма компонентами та чинниками, які можуть сприяти її успішній реалізації.

Визначення 3. Атака — це така послідовність дій, що ініціюється небезпекою відповідно до вибраної стратегії реалізації атаки.

Такі поняття, як слабке місце в інформаційній системі та аналогічне йому поняття піддатливості системи на певні дії, що призводять до негативних наслідків, визначені у відповідних стандартах, які стосуються безпеки інформаційних систем [1–2].

Аналіз випадкових подій Vp_i враховує такі особливості цих подій. Випадкова подія Vp_i не обов'язково повинна бути такою, що може створювати загрозу для об'єкта, оскільки може активізуватися зовнішніми процесами, які через свою природу не можуть впливати на рівень безпеки *ISU(DTP)*. Найпростіший спосіб розпізнавання Vp_i полягає у порівнянні поточної Vp_i з усіма відомими негативними подіями. Такий спосіб розпізнавання є найгромізкішим. Тому в межах ZPr_i реалізуються процеси імітації стежки реалізації процесу активізації можливої атаки. Під стежкою атаки будемо розуміти місця апаратних та програмних засобів, які могла б використати певна загроза. Реалізація різних атак може потребувати різних місць у середовищі *ISU*. Тому одним із способів виявлення небезпеки та її ідентифікації може бути спосіб, який ґрунтується на використанні фальшивих стежок здійснення атаки. Приймемо, що одна з таких стежок $h(a_i)$ відповідає загрозі A_i, яка реалізується атакою a_i. Оскільки Vp_i надходить у модель $M(ZPr_i)$ з випередженням у часі, то є достатньо часу для імітації реалізації атаки a_i на основі загрози A_i. Розподіл атак на різні типи реалізовуватимемо відповідно до змін рівня безпеки BS_i, до якого призводить відповідна атака, та міри складності її реалізації. Остання буде вимірюватися кількістю точок взаємодії атаки з системою захисту, якою є $M(ZPr_i)$, та кількістю точок системи управління, з якими a_i взаємодіє. Отже, можна формально записати міру загрози, яку становить певна небезпека, за допомогою співвідношення:

$$Bs(a_i)=\alpha\{[\sum_{i=1}^{k}(a_i\&b_i)+\sum_{j=1}^{m}(a_j\&u_j)]/[\sum_{i=1}^{k}b_i+\sum_{j=1}^{m}u_j]\}, \qquad (1)$$

де α — коефіцієнт приведення міри безпеки Bs_i до шкали вимірювання, a_i — кроки атаки, b_i — точки в системі безпеки *BS*, які використовує атака, u_j — точки системи управління, які використовуються в *SU*.

Прийнявши інтерпретацію $M(ZPr_i)$, яка відповідає моделі, що реалізує захист *ISU*, доцільно розглянути окремі складові зовнішнього процесу. При

традиційному підході профіль системи безпеки формується на основі аналізу *ISU*, який полягає у виявленні слабких точок системи, визначення необхідного захисту, що залежить від задач, які система розв'язує, та інших чинників, які необхідно враховувати відповідно до політики безпеки [3–4]. Профіль системи безпеки є сукупністю засобів, які зорієнтовані на реалізацію процесів захисту *ISU*. Такі засоби здебільшого являють собою програмну реалізацію, що дає можливість робити їх достатньо мобільними. Однією з головних особливостей небезпеки, яка являє собою є зумовлюючі процеси OPr_i, є її здатність враховувати певну інформацію про активізовані шляхи породження Vp_i, атаки та здатність визначати їх успішність чи неуспішність. Наявність в OPr_i процесів аналізу даних про зовнішні атаки, забезпечує можливість вводити певні корективи у разі реалізації подальших загроз з метою збільшення ймовірності успішної реалізації атаки.

Розглянемо основні функції, які реалізуються в межах ZPr_i системи *S(PR)* у тому випадку, коли інтерпретація цих процесів відповідає задачам захисту інформаційних компонент об'єкта управління. До таких задач належать:

– задачі аналізу параметрів Vp_i з метою виявлення можливого способу реалізації загроз Vp_i відповідної атаки на *ISU*;
– задачі вибору й активізації протидії загрозі, зумовленій подією Vp_i з урахуванням інтервалу і часу, через який ця подія відбудеться;
– розширення опису загрози й імітація атаки, яка може реалізуватися загрозою, що відповідає події Vp_i;
– простежування всього процесу реалізації загрози, яка може являти собою деяку сукупність атак;
– задача аналізу зміни рівня безпеки, яка реалізується залежно від впливу загрози на об'єкт захисту.

Випадкова подія Vp_i, яка інтерпретується як виникнення атаки щодо *ISU*, може містити інформацію про відповідну небезпеку Nb_i. Обов'язковими даними такої інформації є:

– період, через який відбувається подія Vp_i з моменту передання інформації про Vp_i до ZPr_i або моделі $M(ZPr_i)$;
– параметр або ідентифікатор типу небезпеки $Nb_i(Ф)$;
– хоча б один параметр, який характеризує відповідну небезпеку.

Формально це можна описати співвідношенням:

$$Vpi=f\{[\Delta t,Nb(\omega),P_{i1}(Nb)],P_{i2}(Nb),\ldots,P_{ik}(Nb)\}, \qquad (2)$$

де Δt — час, через який може появитися Vp_i на вході $M(ZPr_i)$, $Nb(\omega)$ — ідентифікатор типу *Nb*, переважно як ідентифікатор використовують базовий параметр, характерний для окремого типу $Nb: P_{ij}(Nb)$ параметр, який характеризує *Nb* і не є ідентифікатором *Nb*. Vp_i містить щонайменше два параметри, один з яких орієнтований на ідентифікацію $Nb(\omega)$, а інший — належить до базових параметрів *Nb*. Приймемо, що $Vp_i=f\{[\Delta t,Nb(\omega),P_i(Nb)]$. Прогнозування в цьому

випадку здійснюється за всіма трьома параметрами. Якщо за базовий параметр обрано Δt, то це означає, що існує наближена залежність:

$$Nb(\omega)=\varphi_1 [P_i (Nb),\Delta t]; \quad P_i (Nb)=\varphi_2^* [Nb(\omega),\Delta t]. \tag{3}$$

Ці рівняння можна записати так:

$$Nb(\omega)=\varphi_1^* (\Delta t); \quad P_i (Nb)=\varphi_2^*(\Delta t). \tag{4}$$

Такі функції можна розглядати як апроксимувальні. Параметри $P_i (Nb)$ і Δt приймемо за координати відповідних змінних. Аналогічно можна вчинити з параметрами $Nb(\omega)$ і Δt. Розглянемо тримірну систему координат, яка складається із $Nb(\omega)$, $P_i (Nb)$ та Δt. Параметр Δt має інтерпретацію часу, тому його масштаб можна описувати лінійною функцією незалежно від інших параметрів. У цьому випадку значення параметрів $Nb(\omega)$ та $P_i (Nb)$ можна розглядати як траєкторію на відповідній площині. Параметри загроз, про які йдеться, відрізняються від традиційної інтерпретації параметрів. Звичайна інтерпретація параметра передбачає існування його ідентифікатора у формі деякої величини, яка має певне фізичне трактування, наприклад, температуру, та прийняту в предметній галузі шкалу або одиницю вимірювань. У системі *ISU* подія Vp_i характеризується параметром, який ідентифікує спосіб здійснення атаки відповідною загрозою. Наприклад, якщо атака типу *DOS*, то параметр $Nb(\omega)$ буде відповідати прийнятому в системі оцінювання різних типів атак значенню β_i. Параметром $P_i (Nb)$ може бути параметр, що визначає величину інтервалу часу τ_i, і на який діє відповідна атака протягом часу її реалізації. Прикладом іншого параметра може слугувати певний тип адреси, за яким здійснюється атака. Формування відповідних шкал для відомих атак є прерогативою авторів розробки системи захисту окремо взятого об'єкта. Предметна галузь інтерпретації об'єкта захисту є однією з основних при виборі інтерпретації для параметрів Vp_i та способів вимірювання їхніх значень. Якщо наявні різні типи загроз, то кожен із них інтерпретується за такими характеристиками:

– вартістю реалізації атаки відповідною загрозою α^a;

– вартістю втрат, до яких може призвести успішна атака α^z.

У такому разі величина значення відповідного параметра $\rho_i(\alpha)$ вимірюється співвідношенням $\rho_i (\alpha)=\alpha^a-\alpha^z$. Це означає, що коли вартість втрат перевищує вартість мети атаки, то $\rho_i (\alpha)$ має додатнє значення і, відповідно, $Nb(P_i(\alpha))$ зростає. Коли $P_i(\alpha)=0$, то атака збалансована із захистом. Якщо $P_i(\alpha)<0$, то параметр атаки відносно рівня захисту не потребує збільшення $\rho_i (\alpha)$ або $Nb(\alpha)$, а навпаки, може зменшуватися. Зрозуміло, що всі ці інтерпретації є індивідуальними для кожної системи захисту.

Очевидно, що в межах Nb_i повинні наводитися дані, що їх використовує небезпека і які необхідні для того, щоб можна було зреалізувати атаку. Фрагмент атаки може відповідати одній події Vp_i, але найчастіше виникає ситуація,

коли одна подія спричиняє реалізацію всієї атаки. Це дає можливість розпізнати тип атаки, адже тоді система захисту *ISU* використовує дані про відомі атаки. Завдяки тому, що Vp_i має параметр Δt, існує можливість здійснити імітацію формування атаки на основі наявних у Vp_i даних про типи атак та даних, що розміщені у системі захисту *Z(ISU)*.

Використання та реалізація процесів імітації дії атак ґрунтується на відомих технологіях Honeypot [5]. Кожна небезпека використовує обернений зв'язок і від атакованого об'єкта отримує дані про результат дії загрози, яку сформувала відповідна небезпека. Обернений зв'язок може бути таких типів:

– короткотерміновий — реалізується у режимі реального часу;
– довготерміновий — використовує дані про зміни, які відбулися в *ISU*, в результаті атаки, ініційованої відповідною небезпекою;
– природний обернений зв'язок.

Перший тип оберненого зв'язку здійснюється, якщо ефект дії атаки на об'єкт виникає безпосередньо у процесі її реалізації. Це актуально тоді, коли в результаті атаки дані з атакованої системи передаються у несанкціоновану систему. Наприклад, коли кошти з рахунку атакованої системи пересилаються у систему, визначену небезпекою.

Довготерміновий обернений зв'язок відповідає ситуації, коли в результаті атаки атакований об'єкт виробляє подукцію, яка не відповідає умовам чи вимогам, що обумовлюються системою.

Природний обернений зв'язок відбувається тоді, коли результат дії атаки на *ISU* проявляється в результаті функціонування системи, у якій відбулися зміни, зумовлені проведеною атакою. В цьому випадку зміни у системі не призводять одразу до змін у продуктах, які виробляються атакованим технічним об'єктом. Зміни в *SU*, зумовлені атакою, можуть полягати у негативних змінах параметрів, що характеризують сам об'єкт. Наприклад, зменшення продуктивності виробництва, використання неоптимальних режимів управління та інші.

Система захисту може бути розширена засобами перевірки результатів дії атак на *ISU* з метою виявлення успішно проведених атак. Такі перевірки дають змогу використовувати засоби протидії наслідкам дії атак, які в межах такого підходу розширюють можливості засобів захисту та системи безпеки загалом.

Для того щоб можна було автоматизувати процеси функціонування системи захисту, або системи безпеки *SU*, яка в цьому випадку є зовнішньою системою процесів ZPr_i, що використовують у своєму функціонуванні результати прогнозування Vp_i, необхідно формалізувати опис усієї системи процесів та опис кожного з процесів, що відповідають окремим задачам. Вони розв'язуються в ZPr_i або в $M(ZPr_i)$, яка є моделлю ZPr_i. Передусім необхідно сформулювати прикладні задачі, розв'язання яких реалізується в межах $M(ZPr_i)$. До них належать:

– протидія атакам у точках послідовності їх дій, що є спільними для багатьох атак різних типів;

– формування схем відтворення процесу реалізації відомих атак;
– формування методів адаптації засобів протидії до модифікованих фрагментів атаки, яку реалізує загроза;
– моніторування стану об'єкта захисту;
– синхронізація процесу функціонування моделі $M(ZPr_i)$ з моделями $M(OPr_i)$, $M(PR)$;
– обчислення поточного рівня захищеності об'єкта на основі використання поняття про міру захисту;
– управління рівнем захищеності об'єкта.

Процес імітації складається з таких компонент:
– створення псевдоідентифікаторів реалізації окремих кроків;
– імітація перетворень, які здійснюють очікувані атаки;
– формування псевдоефекту реалізації атаки.

Під час здійснення процесів імітації обмежимося послідовними процедурами її реалізації. Припустимо, що кожен наступний етап імітації залежить від результату попереднього. Початкові дані, якими є значення параметрів P_i *(Nb)* події Vp_i, є величинами, які характеризуються ймовірністю того, що відповідні величини можуть зумовлювати активізацію необхідних процесів. Приймемо, що активізація процесу, яка призводить до змін у процесі ZPr_i, є можливою тільки після реалізації деякої послідовності подій, пов'язаних з окремою небезпекою *Nb*. Характерним для взаємодії між певними кроками реалізації атаки a_i є те, що розподіл ймовірностей відповідного переходу, який відображає зміну, має експоненціальний характер. Це дає змогу використовувати ланцюги Маркова для моделювання відповідних процесів здійснення атак [6]. У цьому випадку запишемо загальний процес реалізації атаки у вигляді співвідношення:

$$Vp_i \rightarrow A_i\ (a_{i1} \rightarrow a_{i2} \rightarrow \cdots \rightarrow a_{in}). \tag{5}$$

У результаті використання ланцюгів Маркова існує можливість визначити ймовірність настання кожної з послідовних подій, що ідентифікують окремий крок атаки A_i. Початкова ймовірність визначається на основі ймовірності появи Vp_i, яка активізує виникнення атаки. Наприклад, успішність реалізації другого кроку можна подати у вигляді співвідношення:

$$\frac{dP_i}{dt} = -\lambda_{ij}P_i - \lambda_{ji}P_j + \lambda_{ki}P_k + \lambda_{ri}P_r, \tag{6}$$

де λ_{ij} — умовна ймовірність того, що перехід у a_2 не відбудеться, P_i — початкова ймовірність i — того стану системи. Після інтегрування цього рівняння отримуємо ймовірність переходу системи із стану a_{i1} до a_{i2} протягом часу Δt. В цьому випадку ситуація є загрозою для Nb, що реалізує атаку A_i, яка ідентифікується в процесі розвитку переходами в стани $a_2, a_3, ..., a_n$. У разі переходу зі стану a_{i2} у стан a_3, а не в стан a_2, описується ймовірністю P_3 і т. д. Процес реалізації не

повинен бути послідовним, наперед визначеним процесом, а може являти собою процес з розгалуженням відносно нумерації можливих станів. На підставі таких структур переходу небезпеки *Nb* зі стану a_i до стану a_j реалізуються схеми імітації здійснення атаки, що є кінцевою ціллю в межах задач імітації атак.

На основі отриманої структури атаки A_i $(a_{i1}\rightarrow\cdots\rightarrow a_{in})$ формуються процеси протидії, які в загальному вигляді входять до складу ZP_{ri} і відображені в $M(ZPr_i)$. Ці функції позначатимемо:

$$Nb_i=[M(ZP_{i1}),\ldots,M(ZP_{i,(i+n)})]. \quad (7)$$

Оскільки в $M(ZP_i)$ процеси є визначеними, а серед них існують процеси, які реалізують протидію впливу відомих атак, то на основі даних про імітацію здійснення атаки відповідні процеси $P_i(Za)$ модифікуються таким чином, щоб не допустити можливості реалізації взаємодії Nb_i, яка використовує $(a_{i1}\rightarrow a_{i2}\rightarrow\cdots\rightarrow a_{in})$ з елементами системи $SU(DTP)$. Така взаємодія, коли йдеться про програмні засоби, може полягати у заміні команд у відповідній програмі на команди з Nb_i, у доповненні програми $m_i\in M(SU)$ фрагментами $m^*\in Nb_i$ і т. д.

Використання ZPr_i як зовнішньої відносно *SU* системи дає змогу реалізувати в межах $M(ZPr_i)$ функції виведення нових засобів захисту. Припустимо, що з часом можуть появлятися Nb_i, які не були передбачені на етапі початкового формування ZPr_i. Тому в ZPr_i відсутні процеси, які реалізують відповідну протидію. Розв'язання цієї проблеми ґрунтується на таких положеннях та вимогах:

– нова атака A_i^*, що ініціюється засобами Nb_i, має спільні властивості чи спільні фрагменти реалізації з тими атаками, які уже були відомими;
– існує можливість у межах системи $M(RP)$ формувати додаткові вимоги до $M(RP)$, завдяки яким можна було б отримати додаткову інформацію про можливу подію Vp_i.

Це дає змогу ефективніше розширювати склад процесів у ZPr_i. Відповідна модифікація ZPr_i ґрунтується на процесах виведення нових стежок $h(A_i)$ в $M(ZPr_i)$ для формування процесу дії і, відповідно, протидії нових Nb_i^*.

Приймемо, що нові Nb_i^* матимуть такі самі цілі, як і відомі реалізації Nb_i. Завдяки цьому стає можливо побудувати систему виведення нових процесів реалізації атак A_i^* де $Nb_i^*\rightarrow A_i^*$. Така можливість ґрунтується на тому, що логіка реалізації A_i^* у вигляді $a_{i1}^*,\ldots,a_{in}^*$ та правила реалізації кроків атаки є однаковими для всіх можливих атак A_i^*. Виведення нового засобу Nb_i (A_i^*) ґрунтується на таких вимогах до всієї ZPr_i:

– усі засоби захисту $P_i(Za)$, які реалізуються в $M(ZPr_i)$, формуються у вигляді окремих функціональних фрагментів завдяки $m_i(ZPr_i)$;
– фрагменти $m_i(ZPr_i)$ можуть створити нові $h(A_i)$;
– нові атаки здебільшого є модифікаціями відомих атак;
– модифікація відомих атак реалізується шляхом зміни логіки функціонування атак.

Кожен функціонально-орієнтований фрагмент $m_i(ZA_i)$, де ZA_i — реалізація одного засобу захисту проти атаки типу A_i, має власну функціональну орієнтацію, яка стосується можливостей реалізації окремих задач протидії. Прикладом може слугувати функція відновлення фрагмента тексту програми, яка була модифікована атакою, функція маскування окремих фрагментів даних для охорони від несанкціонованого доступу до них, модифікація фрагментів програми або окремих команд, які реалізують активізовані атаки і т. д. Функціональність фрагментів і їх можливості $(m_i(ZA_i)) \in ZA_i \in M(ZPr_i)$ зв'язані з особливостями об'єкта захисту та задачами захисту, які передбачається виконувати. Відповідні засоби орієнтовані на типи атак, що можуть активізуватися відносно відповідних об'єктів захисту та систем управління ними. Ці особливості становлять систему умов $U=\{u_1,...,u_2\}$, на основі використання яких визначаються типи окремих $m_i(ZA_i)$ та ZA_i загалом. Оскільки модифікація ZA_i здійснюється з урахуванням логічних взаємозв'язків між $m_j(ZA_i)$ і $m_i(ZA_i)$, то перетворення, які реалізуються під час виведення нових ZA_i*, ґрунтуються на використанні логічних правил виведення. При їх використанні проводиться аналіз u_i, який є певним обмеженням для логічних правил виведення $L(PV)$. Оскільки $m_i(ZA_i)$ являють собою тексти програм, що написані на обраній мові програмування, то, крім логічних правил виведення $L(PV)$, використовують правила виведення, які враховують текстові особливості відображення $m_i(ZA_i)$. Прикладом таких правил можуть бути: конкатенація фрагментів або $m_i(ZA_i) \| m_j(ZA_i)$; правило перестановки фрагментів, або $\{m_i(ZA_i) * m_j(ZA_i) * ... \rightarrow ... * m_j(ZA_i) * m_i(ZA_i) * ...\}$ та інші правила.

Активізація процесу модифікації $Z(A_i) \in M(ZPr_i)$ реалізується в тому випадку, коли в процесі імітації атаки виявилося, що засоби протидії $Z(A_i)$, які існують в $M(ZPr_i)$, не забезпечують можливості реалізації такої протидії. Наприклад, коли атака орієнтована на впровадження троянського коня в середовище SU, а в $M(ZPri)$ не існує $Z(A_i)$ такого, який міг би його елімінувати, то необхідно проводити модифікацію $M(ZPr_i)$. Така ситуація може виникнути через те, що троянський кінь після впровадження не активізується або безпосередньо, в розвитку дії атаки, не активізується в середовищі, в яке він був впроваджений.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ГОСТ 34.10-94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электрической цифровой подписи на базе асимметричного криптографического алгоритма. Функция хеширования. — 1994.
2. Гостехкомисия Россия: Руководящий документ. Концепция защиты СВТ и АС от НДС к информации. — М., 1992.
3. Столлин В. Основы защиты сетей. Приложения и стандарты / В. Столлин. — М. : Издательский дом «Вильямс», 2002.
4. Владимиров А. А. WI-FOO: «Боевые приёмы» взлома и защиты безпроводных сетей / А. А. Владимиров, Л. В. Гавриленко, А. А. Михайловский. — М. : НТ Пресс, 2005.
5. Piotrowski Michal Krolicza nora. Ochrona sieci komputerowych za pomocą technologii honey-pot / Michal Piotrowski. — Warszawa : PWN, 2007.

6. В. И. Тихонов Марковские процессы / В. И. Тихонов, М. А. Миронов. — М. : «Сов. Радио», 1977.

METHODS OF DYNAMIC MODIFICATION OF FORECASTING

M. M. Kliap

SHEE "Uzhgorod National University"
3, Narodna Square, Uzhgorod, 88000, Ukraine

The article analyses Vp_i and defines weak points in management of information system ISU(DTP). It shows the necessity of change of protection level which would conform to the real dangers which are initiators of attacks and would correspond to the necessary protection measure of DTP. It determines such concepts as threat, danger and attack. The three-dimensional system of coordinates has been considered.

Keywords: *approximation function, protection, danger, attack, threat.*

Стаття надійшла до редакції 26.08.2015.