УДК 683.05

О.В. Шевченко

РОШИРЕННЯ ЛОГІКО-ГРАФОВОЇ МОДЕЛІ ІНФОРМАЦІЙНИМИ КОМПОНЕНТАМИ

Розширенням логіко-графової моделі Н^{LG} являється опис залежностей виникнення тих, чи інших подій x_{ij} від різних причин $\{\xi_{i1}, \ldots, \xi_{ik}\}$. Відповідні причини виникнення окремої події являються наслідком існування загроз $\{\zeta_1, \ldots, \zeta_k\}$. Оскільки загроза являється властивістю об'єкта захисту, то вона сама по собі не може бути причиною виникнення x_i. Це можливо тільки у тому випадку, коли загроза являється критичною $\left(\zeta_i = \zeta_i^k\right) \to \left(\xi_i = \zeta_i\right)$. Прикладом критичної загрози являється ситуація, коли відповідна загроза безпосередньо впливає на процес функціонування об`єкту. У випадку, коли загроза характеризує апаратну частину реалізації об`єкту, то загрозою може бути використання електронного елементу у схемі параметр потужності якого недостатньо великий. Через це час, функціонування елемента є значно меншим від величини часу нормального функціонування, що визначений у документації. Коли відповідний елемент відмовляє, то це приводить до порушення у роботі об`єкту. У даному випадку, причини виникнення тих, чи інших подій x_i обумовлюються загрозою, або рядом загроз, використання яких деяким чинником, у ролі якого виступає атака, приводить до можливості виникнення певної події. Формально, це записується у вигляді наступного співвідношення:

$$x_i = \psi\left(\zeta_1, \ldots, \zeta_m\right) \qquad (1)$$

Прикладом, що ілюструє таку можливість, по відношенню до апаратних засобів деякого об`єкту, може бути наступне. Нехай, атака на об`єкт представляє собою послідовність дій, що полягають у реалізації перепадів напруги живлення деякої компоненти апаратної частини об`єкту. Тоді, якщо у відповідній частині апаратних засобів використовуються елементи, які можуть витримати тільки обмежену кількість таких перепадів напруги кожний з яких визначається зміною величини напруги, або струму не більше ніж на деяку задану величину, то такий елемент представляє собою загрозу, яка характеризується у рамках даного прикладу, двома параметрами - інтервалом часу дії таких сачків ζ_1, та величиною зміни значення напруги у момент такого її перепаду напруги ζ_2. Очевидно, що така загроза ζ_i сама по собі, без дії зовнішніх чинників (атаки), якщо об`єкт працює у штатному режимі, з заданою величиною стабільності напруги живлення, не приведе до

© О.В. Шевченко

виникнення деякої події x_i. Таким чином, можна написати наступне співвідношення:

$$\zeta_i = \varphi(\zeta_1, \ldots, \zeta_m) \tag{2}$$

Слід зауважити, що описана ситуація стосовно загроз ζ_i, може мати місце і по відношенню до програмних засобів реалізації компонент об`єкту, що захищається. Необхідність розподілу фактору події на два класи: самої події та причини виникнення певної події, що можна описати залежністю у вигляді:

$$(\xi_{i1}, \ldots, \xi_{ik}) \to x_{ij} \tag{3}$$

обумовлюється тим, що атаки наряду з іншими подіями, які можуть виникнути в об`єкті, мають свою визначену послідовність. Ці події обумовлюються, а також мають інтерпретаційні описи у предметній області W_i, або

$$x_i = [\beta_{i1} * \ldots x_{im} \mid \ldots \mid \beta_{ik} * \ldots \beta_{in}], \tag{4}$$

де β_{ij} - слова природної мови, які описують відповідні події, серед яких є окремі події, що визначаються як ціль атаки, яка позначається як x_{ij}^c. Така подія може бути однією з цілого ряду можливих подій, що мають, або можуть мати місце в об`єкті.

Другою причиною такого поділу є те, що одні і ті ж самі причини $\xi_{i1}, \ldots, \xi_{im}$, але в іншій комбінації можуть спричиняти іншу подію x_{ik}. Суміщення множини подій $x_1, \ldots, x_m$, з причинами їх виникнення привело б не тільки до необґрунтованого ускладнення описів, але й до того, що причина деякої події, як певний фактор відповідних подій x_i, інтерпретувалась би як сама подія. Якщо звернутися до приведеного вище прикладу з електронним елементом, на якій діють перепади напруги, то при певних структурних, або схемних розв`язаннях у проекті апаратних засобів, вихід з ладу такого елементу може не привести до події, яка полягає у відмові об`єкту у виконати деякі функції, або у її виконанні способом, що непередбачений технічними умовами. Також це може мати місце, якщо відповідний фрагмент схеми є резервований у вигляді гарячого резерву, або його функціонування не має відношення до реалізації поточного алгоритму функціонування. Це може мати місце завдяки тому, що живлення на цей фрагмент подається незалежно від того, чи він приймає участь у реалізації поточного алгоритму функціонування, чи ні, наприклад, якщо цей елемент пов`язаний з реалізацією виводу на друкування деякої поточної інформації, але ця функція не використовується для виконання процесів встановлення з`єднання між абонентами і т.д. Тому, можна говорити про певну ієрархію, яка існує у рамках загальної моделі забезпечення безпечного функціонування об`єкту, між різними компонентами такої логіко-ймовірнісної моделі. Таку ієрархію

можна записати у вигляді деякого списку, в якому спочатку описуються параметри, або фактори, що мають найвищій рівень в ієрархічний структурі. Такий список можна представити наступним чином:

- фактори $\{x_{i1}, \ldots, x_{ij}, \ldots, x_{mk}\}$, що описують події, які впливають на штатні режими роботи об`єкту;

- фактори $\{\xi_1, \ldots, \xi_n\}$, що описують причини виникнення подій x_{ij} і зв`язані з подіями, у рамках даної роботи логічними залежностями;

$$x_{ij} = L(\xi_{i1}, \ldots, \xi_{im}) \tag{5}$$

- фактори, що можуть викликати виникнення інших факторів ξ_i, які обумовлюються загрозами ζ_i;

- фактори ζ_{ij}, які представляють собою параметри, що описують, або визначають загрози ζ_i.

Формально, така ієрархічна структура може бути у загальному вигляді, записана у вигляді наступного виразу:

$$\begin{aligned}&\left[(\xi_{i1}, \ldots, \xi_{ik}) \to \zeta_i\right] \Rightarrow \left[(\zeta_{i1}, \ldots, \zeta_{im}) \to \xi_i\right] \Rightarrow \\ &\Rightarrow \left[(\xi_{i1}, \ldots, \xi_n) \to x_i\right] \Rightarrow \left[\left(x_{i1,\ldots}, x_{ig}\right) \to x_{ik}^C\right]\end{aligned} \tag{6}$$

На рисунку 3.2. приведено фрагменти ієрархічної системи зв`язків між основними факторами, за допомогою яких реалізуються атаки.

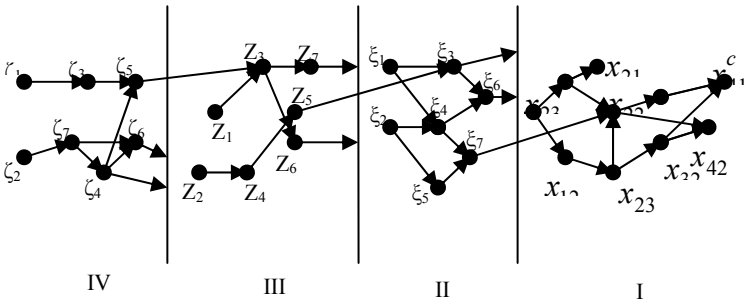

Рис. 1. Схема фрагментів та поділи цих фрагментів загальної системи H^{LG} на рівні ієрархії

Загрози ζ_{ij}, що являються характеристиками об`єкту, визначається параметрами $\zeta_{ij}$, які існують в об`єкті захисту, як результат того чи іншого способу проектування системи. Крім того, загрози в об`єкті захисту можуть формуватися або зароджуватися у процесі функціонування об`єкту під дією фізичних процесів, що є природними для елементів даного об`єкту, чи компонент об`єкту у цілому. Прикладом таких процесів можуть бути процеси

фізичних змін, які у діагностиці прийнято називати процесами старіння. У програмних компонентах, незалежно від того, що останні являються описом алгоритмів функціонування фізичних елементів і компонент, також можуть відбуватися зміни, які обумовлюються основними причинами процесів змін, що називаються старінням. До таких причин відносяться наступні.

- час функціонування системи;

- режими роботи системи, що можуть змінюватися непередбачуваними способами;

- зовнішні фактори, що не приводять до явно виражених наслідків свого впливу на процес функціонування об`єкту, який охороняється.

Прикладом процесів зміни у програмних компонентах можуть служити наступні фактори, які можна вважати залежними від приведених вище причин. Наприклад, у результаті зміни режимів роботи ініціювалась програма алгоритм дії якої привів до зміни деякої константи, чи даних, що використовуються у інших випадках функціонування об`єкту. Такий випадок настає лише через досить великі інтервали часу. Тоді, цю зміну можна розглядати як таку, що залежна від часу функціонування об`єкту, що відповідає першій з наведених причин. Оскільки відповідна зміна може привести до впливу на процес функціонування у майбутньому, то вона може бути віднесена до класу загроз, що виникають у процесі функціонування ТКС і відносяться до програмних компонент. Зрозуміло, що більшість загроз у програмній компоненті виникає на етапах проектування програмних частин системи ТКС і тоді під дією причин, що приведені вище можуть мінятися параметри відповідних загроз.

Розглянемо приклад взаємодії всіх процесів і факторів, що реалізуються у випадку, коли ціль є визначеною у відповідної атаки. Наприклад, деяка подія, яка є ціллю x_i^c полягає у заміні адреси абонента, при реалізації процесу надання послуги зв`язку. Причиною, що спричинила підміну адреси може бути деяка програма, якщо розглядати цю процедуру у межах програмних засобів, яка приводить до модифікації відповідної адреси. Можливість такої несанкціонованої модифікації може мати наступну природу:

- програма яка здійснює цільову модифікацію адреси, може бути впроваджена несанкціонована, у склад програмних засобів, і тоді процес такого впровадження відповідає стадії розвитку атаки;

- програмне забезпечення, може мати фрагменти або один фрагмент алгоритму, який таку заміну реалізує у силу неоднозначності функціонування програмної компоненти, яка займається формуванням адрес у системі ТКС.

У першому випадку існує зовнішня небезпека, яка ініціює завантаження, необхідного фрагменту в систему програмного забезпечення, використовуючи комп’ютерну мережу, або інші канали зв`язку системи з зовнішнім середовищем. У рамках програмної компоненти, що орієнтована на формування адрес абонентів, існує можливість докомпонувати її

додатковими фрагментами, які допускають активну взаємодію з оригінальною частиною програмних засобів. Така взаємодія може активізуватися на основі аналізу адрес, які необхідно модифікувати, якщо такий аналіз проводить несанкціонована програма. У даному прикладі, стадією зародження атаки являється процес завантаження необхідної програми у програмну складову ТКС. У цьому випадку, загрозою для відповідної програмної компоненти є відсутність у рамках її алгоритму функції аналізу, або контролю відповідності всіх активних компонент програми, що передбачені технічними вимогами. Наявність такого контролю дозволила би виявити завантажений фрагмент програми, яка перед процесом формування адреси абонента здійснює її контроль. Параметром такого типу загрози може бути кількість умов, при яких такий контроль передбачено, наприклад, контроль того чи здійснюється перевірка на вихід її частини за допустимі границі окремі складові адресного поля пам'яті, в якій розміщається відповідна складова. Якщо, при цьому виконується умова перевірки того, чи не порівнюється поточний адрес, що формується, з конкретним значенням цієї адреси, то нештатний фрагмент може виконати свою функцію підміни окремого номера. Другою компонентою відповідної загрози, являється відсутність блокування можливості довантаження до комплекту функціонально визначених програм нових фрагментів у процесі роботи системи ТКС. Стандартним засобом захисту проти таких довантажень являється реалізація основних програм у постійній пам`яті, в якій деяка програма записується на основі реалізації незворотних процесів.

При визначенні параметрів загрози, виходячи з графової структури, що зображена на рис. 1, може мати місце ситуація, коли деяка загроза, наприклад ζ_3, характеризується одночасно параметрами ζ_3 і ζ_{41}, які у залежності від використання у вузлі графа ζ_5 операції & чи V характеризують ζ_3. У випадку використання & два параметри одночасно характеризують ζ_3, а при використанні V, ζ_3 може характеризуватись параметром ζ_3 або ζ_{41}, або одночасно обома параметрами. У відповідності з прикладом структури H^{LG} на IV рівні ієрархії, параметр ζ_3 виникає з параметру ζ_1, а параметр ζ_4 виникає на основі більш складної залежності між ζ_7 і ζ_2, яку можна описати у вигляді $\zeta_2 \to \zeta_7 \to \zeta_4$. Хоча параметри ζ_1 і ζ_3 та параметри ζ_2, ζ_7 і ζ_4 безпосередньо не визначають несправність ζ_3, ми все одно їх відносимо до параметрів, що характеризують загрозу ζ_3. Це дозволяє розширити можливості засобів захисту, що орієнтовані на усунення загроз. Наприклад, якщо усунути або певним чином змінити значення параметру ζ_2, то це може привести до елімінації параметрів ζ_4 і ζ_6, які згідно з приведеним фрагментом структури моделі, являються безпосередніми

параметрами окремих загроз на третьому рівні H^{LG}. Прикладів таких залежностей можна приводити досить багато на основі аналізу предметної області W_i, що описує ТКС.

Важливою задачею для системи забезпечення безпечного функціонування ТКС являється задача визначення, чи не приведе використання деякого засобу захисту у довільному місці довільного фрагменту моделі H^{LG} до появи нових параметрів загроз і відповідно, до виникнення нових загроз у рамках H^{LG}. Ця проблема, або задача безпосередньо зв`язана з задачею суперечності моделі H^{LG}.

Суперечність у рамках даної моделі, має дещо ширше значення ніж суперечність у математичній логіці. Якщо у математичній логіці уявлення про суперечність означає можливість виводу двох суперечних співвідношень з деякої логічної системи, причому під суперечністю розуміються такі значення результатів обрахунку цих двох співвідношень, які допускають їх суперечну інтерпретацію. Наприклад, для математичної логіки така інтерпретація визначається на множині 0,1. У рамках моделі H^{LG} існує декілька типів суперечностей, які описуються наступними визначеннями.

Визначення 3.2. Локальна суперечність η^L має місце у тому випадку, коли у системі захисту реалізується такий засіб захисту λ_i, який елімінує загрозу ζ_i, але приводить до появи загрози ζ_j, якої у H^{LG} не було.

Формально це записується наступним співвідношенням:

$$\eta^L = \left\{ \forall \mathrm{H}^{LG} \exists\, \zeta_i \neg \exists\, \zeta_j \left[\left(\lambda_i \to \neg\, \zeta_i \right) \to \zeta_j \right] \right\} \tag{7}$$

Визначення 3.3. Розширена суперечність η^R має місце у тому випадку, коли один, або кілька засобів захисту $\lambda_1, \ldots, \lambda_k$ приводять до елімінації загроз $\zeta_{i1}, \ldots, \zeta_{im}$, але спричиняють до появи нових загроз $\zeta_{i1}, \ldots, \zeta_{in}$, і при цьому має місце нерівність $\eta < m$.

Формально така суперечність описується наступним співвідношенням:

$$\begin{aligned} \eta^R = \Big\{ \forall \mathrm{H}^{LG} \exists \left(\zeta_{i1}, \ldots, \zeta_{ik} \right) \neg \exists \left(\zeta_{j1,\ldots,} \zeta_{jm} \right) \Big[\left(\lambda_1, \ldots, \zeta_{i1} \right) \& \left(\lambda_2 \to \neg \zeta_{i2} \right) \& \ldots \\ \ldots \& \left(\lambda_k \to \neg \zeta_{ik} \right) \Big] \to \Big[\left(\zeta_{j1}, \ldots, \zeta_{jm} \right) \& \left(k < m \right) \Big] \Big\} \end{aligned} \tag{8}$$

Визначення 3.4. Допустима суперечність η^D має місце у тому випадку, коли один, або кілька засобів захисту $\lambda_{1\ldots} \lambda_k$ приводить до елімінації не всіх існуючих у системі H^{HG} загроз.

Формально, це можна описати наступним співвідношенням у вигляді:

$$\eta^D = \left\{\forall \mathrm{H}^{LG} \exists(\zeta_1, \ldots, \zeta_n) \left[\left[\lambda_1 \to \neg\zeta_1\right] \& \left(k < m\right)\right]\right\} \qquad (9)$$

Розглянемо наступне твердження.

Твердження 3.1. Довільна система захисту S^{λ} є неповною, або не забезпечує захисту від всіх можливих атак на систему, що захищається S^{TL}.

Перш ніж доводити це твердження, розглянемо наступне визначення стратегії протидії атакам системи захисту S^{λ}.

Визначення 3.5. Стратегія протидії Ω^{P} атакам A_i є допустимою, якщо процес збільшення у S^{λ} засобів захисту λ_i у системі захисту є збіжним, або якщо кожний крок розширення S^{λ} хоча би одним λ_i приводить до того, що виконується співвідношення:

$$\lambda_i(\zeta_1, \ldots, \zeta_n) \to \left[(\zeta_1, \ldots, \zeta_k) \& \left(k < m\right)\right] \qquad (10)$$

Приведене вище твердження означає, що для $\lambda = \lambda_1, \ldots, \lambda_n$ у S^{λ} завжди існує така $\zeta_{i \in} \zeta$ і для якої у S^{λ} не існує засобу λ_i який протидіяв би атаці, що використовує загрозу ζ_i, або має місце співвідношення:

$$\forall\left(\lambda_i \in S^{\lambda}\right) \exists \left(\zeta_i \in \mathrm{H}^{LG}\right)\left[\neg\left(\lambda_i \to \neg\zeta_i\right)\right] \qquad (11)$$

Система захисту S^{λ} деякого об`єкту S^{TL} є повною, якщо виконуються наступні умови:

- якщо у S^{TL} і відповідно у H^{LG} системи S^{TL} не існує такої загрози, для якої б у S^{λ}, що входить у склад S^{TL} не існувало би відповідного засобу захисту, щоб формально записується у вигляді співвідношення:

$$\left[\forall\left(\zeta_i \in \mathrm{H}^{LG}\right) \exists \left(\lambda_i \in S^{\lambda}\right)\right] \to \left[\neg\exists\zeta_j\left[\neg\left(\lambda_i \to \neg\zeta_j\right)\right]\right] \qquad (12)$$

Система захисту S^{λ} об`єкту S^{TL} є достатньою, якщо при виникненні довільної атаки $\alpha_i \in \mathrm{A}$ на S^{TL} система H^{LG} виявить загрозу ζ_i, якою скористалась атака, і формує такий засіб λ_i, який елімінує загрозу ζ_i і зупинить розвиток відповідної атаки α_i.

Твердження 3.1. можна довести спираючись на приведенні уявлення про повноту та достатність $S^{\lambda} \subset S^{TL}$.

Припустимо, що існує деяка система захисту S^{λ}, яка є повна. У цьому випадку, це означало би, що у системі S^{TL} у рамках H^{LG} не існує загроз ζ_i по визначенню, або для всіх існуючих загроз у $S^{\lambda} \subset S^{TL}$ існують такі λ_i, що

має місце $\forall\zeta_i\forall\lambda_i\left[\left(\lambda_i \to \neg\zeta_i\right)\right]$. Оскільки небезпека, яку будемо позначати, як деяку зовнішню системи S^N по відношенню до S^{TL}, по визначенню не має у S^{TL} повної інтерпретації, то це означає, що у S^N має місце $\left(\mathrm{A} \in S^N\right) \to \alpha_i$ така, що $\left[\alpha_i\left(\zeta_i^*\right) \& \neg\left(\lambda_i \to \zeta_i\right)\right]$. У протилежному випадку у S^{TL} існувала б повна інтерпретація S^N, або $J\left(S^N\right) \in J\left(S^{TL}\right)$. По визначенню, така ситуація не можлива, по крайній мірі, на момент t_0, який визначає початок функціонування S^{TL}. З другого боку, якщо у $J\left(S^N\right)$ не існує x_J^c, такої яка б співпадала з x_J^C і з H^{LG}, то у S^N не появиться α_i, для якої мало б місце $\alpha_{i=}x_{i1} \to \ldots \to \left(x_{jk}^C = x_i^C\right)$. У цьому випадку α_i не буде виведена у S^N. Більш того, має місце, співвідношення:

$$\left[\forall\left(x_{ij}^C \in S^N\right)\forall\left(x_{ji}^C \in S^{TL}\right)\neg\exists\left(x_{ij}^C = x_{ji}^C\right)\right] \to \neg\left(S^N \to S^{TL}\right), \qquad (13)$$

де співвідношення $S^N \to S^{TL}$ означає, що S^N може бути небезпекою для S^{TL}. Але по визначенню для S^{TL} існує хоча би одна небезпека S_i^N, тому останнє співвідношення не можливе, що і доводить твердження.

Розглянемо твердження, про несуперечність системи захисту S^λ, яке ґрунтується на використанні моделі H^{LG}, що описує загрози ζ_i, їх параметри ζ_i, та умови виникнення відповідних загроз, а також описує події, що можуть мати місце у системі S^{TL} і пов`язані з виникненням недопустимих, або несанкціонованих ситуацій у системі, що охороняється. Відмітимо, що всі події, що описуються у H^{LG} відносяться до таких подій, які можуть представляти собою ціль атаки, або можуть представляти собою події, які сприяють досягненню або переходу до подій, що являються ціллю. Обмежимося твердженням про локальну несуперечність моделі H^{LG}.

Твердження 3.2. Система H^{LG} локально не суперечна.

Приведене твердження означає, що має місце наступне:

$$\left[\left(\zeta_i \in S^{HL}\right)\&\left(\zeta_i \notin S^{HL}\right)\&\left(\lambda_i \notin S^\lambda\right)\&\left(S^\lambda \to \lambda_i\right)\right] \to \left(\lambda_i \to \neg\zeta_i\right)\&\left(S^{HL}\ \&\ \lambda_i\right) \to \neg\,\zeta_i\big) \qquad (14)$$

Кожен λ_i являється деякою функцією ζ_i і тоді можна записати, що $\left(\zeta_i \to \lambda_i\right) \to \left[\lambda_i = \psi\left(\zeta_{i1}, \ldots, \zeta_m\right)\right]$, оскільки ζ_{ij} визначають, або описують ζ_i, у відповідності з $\zeta_I = \varphi_1\left(\zeta_1, \ldots, \zeta_m\right)$. Тоді достатньо показати, що $\neg\left[\left(S^{HL}\ \&\ \lambda_i\right) \to x_j\right]$. Розглянемо випадок коли $\zeta_i = \&_{i=1}^k\,\zeta_i$. Тоді достатньо,

щоб $\left[\lambda_i = \psi^*(\zeta_i)\right] \to \neg\zeta_i$. Поява нового ζ_i може мати місце тільки у тому випадку, коли у S^N і існує $x_i^C = x_i^C$ і x_i^* є виводимим у S^{HL}. Оскільки у S^{TL} немає повної інтерпретації S^N, то припустимо, що у S^N існує $x_i^C = x_i^C *$. Тоді, досить показати, що S^{HL} не виводиме з $\left(\lambda_i \,\&\, S^{HL}\right)$. Якби $\left(\lambda_i \,\&\, S^{HL}\right) \to x_i^C *$, то мало би місце співвідношення $J\left(x_i^C *\right) \to J\left(\zeta_i^*\right) \to J\left[\zeta_i^* = \varphi(\zeta_{i1}, \ldots, \zeta_{im})\right]$. Але λ_i виводимо з S^λ і S^{HL} завдяки тому, що у S^{HL} існує вивід $J(x_i) \to J(\zeta_i)$. Це означає, що $\forall\left[\xi_i \in \varphi(\zeta_1, \ldots, \zeta_n)\right]$ існує хоча би один ζ_i такий, що $\lambda_i = \psi^*(\zeta_i)$. Вивід у S^{HL} ζ_j був би можливим, якщо б існувала залежність $J(\neg\zeta_i) \to j\left(\zeta_j^*\right) \to j\left(x_j^C *\right)$. Але, по визначенню, має місце співвідношення:

$$J\left(S^N\right) \neq J\left(S^{HL}\right) \tag{15}$$

Тому приведена залежність не можлива і $\left(S^{HL} \,\&\, \lambda_i\right) \to \zeta_j$ не виведення.

Як видно з доведення відсутності локальної суперечності η^L, останнє ґрунтується на тому, що інтерпретація всіх цілей, які можуть існувати у S^N не може бути повністю відображена у S^{HL}, оскільки у цьому випадку, система S^{TL} буде повною, що суперечить твердженню 3.1. Якщо твердження 3.1 було би невірне , то це означало би, що система S^{TL} реалізована таким чином, що всі можливі цілі S^N враховані у S^λ, а у S^{HL} описані всі можливі загрози та події, що відвідають несанкціонованим ситуаціям. Це, у свою чергу, означало би, що система S^{TL} є повністю безпечна. Якщо б така можливість існувала би по відношенню до однієї системи ТКС то можна було би стверджувати, що можна створити повністю безпечні системи ТКС при інших варіантах їх реалізації. Це суперечить тезі про те, що повністю безпечних систем типу ТКС не існує. Додатковим аргументом справедливості такої тези є те, що технічна система на протязі свого часу функціонування, як і кожна фізична система попадає під дію цілого ряду чинників, які незалежно від їх початкового стану призводять до змін в її компонентах, серед яких можуть мати місце зміни негативного характеру.

1. *Биргер И.А*. Техническая диагностика. М.: Машиностроение, 1978.
2. *Непомнящий В.А., Рякин О.М*. Прикладные методы верификации программ. - М.: Радио и связь, 1988.

Поступила 2.02.2009р.