УДК 004.9

Т.М. Майба, УАД, м.Львів

МЕТОД ВИЗНАЧЕННЯ ВЕЛИЧИНИ РИЗИКУ, ЩО ГРУНТУЄТЬСЯ НА ВИКОРИСТАННІ РЕЗУЛЬТАТІВ АНАЛІЗУ НЕГАТИВНИХ ПРОЦЕСІВ

Вступ

Модель ризику, яка оцінює рівень бепеки інформаційної системи управління (ISU), будується на основі цілого ряду даних про процеси, які відбуваються в ISU. Одним з ключових процесів, в цьому випадку, є процеси, що здійснюють негативний впл ив на систему. Оскільки приймається, що негативний вплив на ISU може виникати не залежно від системи, під лією зовнішніх факторів, то, для побудови моделі ризику, є важливими всі аспекти, що відображають здатність засобів захисту протидіяти відповідним негативним діям. Оскільки, будь які негативні дії на ISU проявляються у вигляді атак, то модель ризику повинна враховувати методи і засоби протидії атакам, які виявлені в середовищі ISU.

Мета роботи.

Розробка методів протидії, зокрема методом протидії блокуванням модифікованих фрагментів процесів управління, що були змінені внвслідок дії на них атак.

Виклад основного матеріалу

Безпосереднє блокування активного фрагменту системи управління, без проведення аналізу впливу такого фрагмента на можливість досягнення підцілі c_i, або цілі C в цілому, є не допустимим. Реалізація блокування $\varphi_i(U)$, де U є система управління, може здіснюватися в рамках комплексу наступних заходів, або з використанням наступних методів:

- Блокування в $\varphi_i(U)$ окремих елементів представляє собою елімінацію окремих елементів $\varphi_i(U)$ і тому, необхідно проводити аналіз впливу цих змін на ціль c_i, яка визначає необхідність використання відповідного $\varphi_i(U)$,
- Блокування $\varphi_i(U)$, при умові, що відповідна підціль c_i, яка повязана з $\varphi_i(U)$, або $\varphi_i(U) \to c_i$, може бути елімінована з C,
- Активізація аналогічного фрагменту $\varphi_j(U)$, що можна описати у вигляді $\varphi_j(U) \propto \varphi_i(U)$ та вплив такої підміни на кінцеву ціль C, яка описує виріб, що продукується TPP.

В більшості випадків, при розробці програмних засобів деякої системи управління, останні будуються таким чином, щоб, при необхідності розширення їх функціональних можливостей, можна було додати новий фрагмент без переробки уже спроектованої і працюючої версії $\varphi_i(U)$. Одним із способів забезпечення таких можливостей є реалізація можливих розгалужень, які в початковій версії не використовуються. Атаки, які

формуються небезпеками Nb_i, у відповідності до стратегії St_i реалізації атак,орієнтовані на такі способи модифікації окремих елементів u_i, фрагментів $\varphi_i \subset U$, які не приводять до їх прояву відразуж в процесі реалізації чергового циклу ΔT_i функціонування ISU. Це дозволяє атаці впливати на роботу ISU на протязі тривалого часу, не приводячи до явно виражених змін в цілі C функціонування TPP. Тому, атаки, для реалізації впливу на процеси функціонування TPP, використовують для модифікації u_{ij} фрагменти, що носять характер функціональної надмірності. В цьому випадку, безпосередній вплив модифікації u_{ij} на ціль може виникати в окремо вибрані моменти часу, що явним чином не повязані з реалізацією атаки, або можуть використовуватися інші умови активізації модифікованих фрагментів $\varphi_i(u) \subset U$. В цьому випадку, Za_i виявляють розширення, які не реалізовувались в рамках працюючої версії $U \subset (ISU)$ та реалізує їх блокування.

Якщо стратегія $St_i(A)$ формування та функціонування A_i передбачає модифікацію $\varphi_i(u)$, яка при першій активізації одразу проявиться, то засоби Za_i повинні реалізувати наступні функції:

- Провести аналіх міри допустимостимості змін в c_i, де $\varphi_i(u) \to c_i$, по відношенню до загальної цілі C,
- У випадку допустимості таких змін, Za_i реалізує блокування можливості актуалізації $\varphi_i(u)$ та реєструється атака,
- Якщо блокування $\varphi_i(u)$, з точки зору його впливу на c_i є не доустимим, то проводиться аналіз можливості модифікації $c_i \in \mathrm{C}$, або самої цілі, і тоді система функціонує у відповідності з $C^* = C/c_i$.

Важливим способом протидії атаці є використання виявленої атаки, для імітації її дії. Цей підхід є особливо важливим у випадках, коли атака складається з ряду окремих процесів дії на обєкт атаки. Досить часто використовуються атаки, які складаються з ряду втручань в систему зі сторони Nb_i. Очевидно, що реалізація оберненого звязку між атакою, яка в середовищі ISU називається інтузом, та Nb_i в явній формі мало ймовірна. Це потребувало би несанкціонованої активності зі сторони ISU по відношенню до Nb_i. Оскільки, Nb_i є зовнішнім процесом, або обєктом, то така активізація була би відразу виявлена. Реалізація опосередненого звязку між інтрузом і Nb_i грунтується на реалізації змін в ISU, які проявляються на засобах звязку ISU, що призначені для звязку ISU з зовнішнім оточенням. Прикладом таких засобів може служити Internet вітрини, що обслуговують ISU та інші інформаційні канали. Очевидно, що для виявлення інтрузів методом імітації не можуть використовуватися зміни в продукті, що виробляється в рамках TPP. Імітація дії атаки на ISU, по своїй суті, є протидією відповідному інтрузу на рівні Nb_i, яка відповідний інтруз впровадила у обєкт у вигляді атаки. В цьому випадку, інформаційна система безпеки (SUB), яка входить в склад ISU, забезпечує протидію Nb_i на рівні реалізації стратегії впливу Nb_i на ISU. Такий спосіб протидії є найбільш ефективний для ISU.

Модифікація виявленої атаки або інтруза типу β може слуєити складовою частиною методики імітації інтруза, яка коротко представлена вище. Модифікація атаки, як і імітація атаки використовується для реалізації протидії Za_i атакам на стратегічному рівні їх реалізації. Переважна більшвсть Nb_i, що орієнтовані на реалізацію впливу на ISU, в свою чергу, є відповідними інформаційними системами, або їх компонентами. Тому, модифікація A_i в ISU може реалізовуватися для здійснення контроверсійниї атакуючих дій зі сторони ISU. Контроверсійну атаку будемо називати к-атакою будемо позначати ka_i. Реалізація дій, що відповідають створенню ka_i атак, потребує додаткову інформацію про $Nb_i(IS)$, яка дозволила би виявити необхідні дані про відповідні IS. Переважно, такого типу діяльність реалізується зі сторони спеціалізованих засобів захисту, які, в силу свєї функціональної орієнтації, використовуються для захисту цілих локальних мереж. Прикладом такої системи може служити система IDS [1].

В результаті виявлення деякої атаки та нейтралізації дії такої атаки на ISU в рамках ISB реалізуються засоби, що здатні виявляти відповідні атаки. Було би доцільно розвязувати задачу не допущення можливості повторення такої ж атаки, або атаки, яка по своїх параметрах є досить близькою до виявленою раніше атаки. Повторяти всі процеси, що повязані з виявленням та протидією системи по відношенню до атаки A_j, що є близькою до раніше виявленої атаки A_i, було би не доцільно. Як відомо, передача інтруза від Nb_i до ISU реалізується по каналах звязку між Nb_i та ISU. Фізично, ця передача потребує легалізованого каналу звязку. Тому, Nb_i використовує легальні ознаки активізації звязку і по відповідних каналах може передавати інтрузи. Такий інтуз представляє собою програмний засіб, який додається до системних, чи прикладних програм і у відповідності з вибраними методами, активізується в середині ISU. Така активізація може полягати у перехопленні адрес активізації легальних програм. Очевидно, що в ідеальному випадку, система ISU повинна протидіяти впровадженню програми типу β середовище ISU. Практично, це є не можливим, оскільки будь яка ISU характеризуєтьсяч певною піддатністю, яка в рамках роботи називається загрозою. Називати властивість обєкту, яка може бути використана для реалізації негативної дії на обєкт атаки загрозою є в повній мірі обгрунтовано.Прикладом зменшення рівня загрози, для випадку проникнення інтруза в програмне середовище, є введення ідентифікаторів для програм, які можна розміщати в памяті системи ISU. Це означає, що кожна нова програма, яка передається в систему, повинна ідентифікуватися спеціальним ідентифікатором.

У звязку з виділенням параметру загрози, що характеризує обєкт, який необхідно захищати, виникає задача виявлення відповідних загроз. На сьогоднішній день, виявлення загроз реалізується, в основному, експериментальними методами, шляхом реалізації атак різних типів на досліджуваний обєкт та проведенням аналізу результату таких атак з ціллю виявлення характеристик обєкта, які використовувались відповідними

атаками [2,3]. Для того, щоб можна було виявляти загрози в обєктах не чисто експериментальним шляхом, необхідно побудувати модель відповідної системи. Для цього, необхідно виділити типові комоненти системи ISU. До таких компонент можна віднести наступні:

- База даних (BD),
- Операційна система (OS),
- Система прикладних задач (PS),
- Система доступу (SD),
- Інтерактивна система користувача (SK),
- Система відображенся співвідношення процесу управління (SV),
- обєкт управління (OU).

Систему типу ISU можна формально описати наступним співвідношенням:

$$ISU = F[OS, SD, SR, BD, SV, PS, OU], \quad (1)$$

де F – функція взаємозвязку між компонентами ISU. Для того, щоб можна було обгрунтувати можливість визначення такого параметру як загроза та можна було оцінити його початкове значення, необхідно впорядкувати структуру, що описується співвідношенням (1). Розглянемо таке впорядкування, яке можна задати аналітично. Впорядкування структури полягає у встановленні взаємозвязків між окремими компонентами. Такі функціональні взаємозвязки можна представити у вигляді наступних співвідношень:

$$OS = F_{OS}[SD, PS, SK]$$
$$PS = F_{PS}[OS, OU, BD]$$
$$BD = F_{BD}[OS, PS, SK]$$
$$SV = F_{SV}[PS, BD]$$
$$SK = F_{SK}[PS]$$
$$OU = F_{OU}[PS]$$
$$SD = F_{SD}[ZF],$$

де ZF – зовнішні фактори. Приведена система функцій описує базові залежності між компонентами і не відображає ситуації, при якій в рамках ISU була би відображена повна система можливих залежностей. У випадку відображення повної системи залежностей, всі компоненти могли б між собою комунікуватися. В функціонально орієнтованій системі така структура є не ефективна, тому доцільно оптимізувати, що передбачає зменшення кількості взаємозвязків між компонентами.

В термінології теорії графів, якщо структуру інтерпретувати як певний граф, то випадок, коли між всіма компонентами існують безпосередні звязки, відповідає уявленню про повний граф [4]. Тому, будемо говорити по зменшення міри повноти графу G структури ISU.

При побудові моделі загроз, важливим аспектом є встановлення факторів, від яких може залежати параметр загрози. До таких факторів можна віднести наступні:

- інтенсивністю обміну між компонентами (Jn),

- функціональне навантаження компоненти (Fn),
- віддаль між точкою доступу та компонентою, як параметр, що описує загрозу (Vd),
- час існування в компоненті укритого інтруза в неактивному стані (Tu),
- міра контрольованості окремої компоненти, з точки зору її захищеності (Zk).

Інтенсивність обміну між компонентами системи суттєво впливає на величину міри загрози, оскільки значна кількість типів інтрузів, для своєго переміщення в середину системи, використовує легальні пакети даних, чи програм. Наприклад, відомі віруси, які підєднуються до легальних файлів і як складові цих файлів переносяться по системі в процесі передачі заражених файлів [5]. Інтенсивність обміну між парою комнет системи будемо позначати $Jn(x_i, x_j)$, де x_i, x_j ідентифікатори відповідних компонент. Величина $Jn(x_i, x_j)$ буде вимірюватися в кількості пакетів pa_i, які передаються на протязі вибраного інтервалу часу $\Delta\tau_i$.

Функціональна навантажуваність компонент є параметром, який впливає на величину значення параметру загрози, оскільки величина завантаженості характеризує важливість відповідної компоненти для процесу розвязку задачі. Приймемо, що в системі в цілому і в кожній компоненті системи ідентифіковані окремі задачі. Кількість окремих задач, що розвязуються в одній компоненті, з точки зору функціональної характеристики, в цілому, означає, що відповідна компонента є в певній мірі важливою для всього процесу. В даному випадку, функціональність визначаємо кількістю окремих задач, оскільки інтрузу простіше укриватися в середовищі, яке є більш різнорідним, або більш активним. Кількість задач будемо позначати символом Fn. Очевидно, що в деякій компоненті може розміщатися менша кількість задач, але з точки зору їх важливості, для рішення загальної задачі, вони можуть мати більше значення, що визначає їх функціональну значимість і, відповідно, функціональну навантаженість. Але цей аспект, в даному випадку не буде прийматися до уваги, оскільки його можна враховувати використовуючи для кожної задачі коефіцієнт, що визначає міру її значимості. Вимірюватися ця складова величини загрози буде у кількості окремо ідентифікованих задач.

Очевидно, що не всі компоненти, які складають систему, можуть характеризуватися в рамках всієї системи таким параметром як загроза. Наприклад, якщо компонента, яка по своїх функціональних параметрах та функціональному призначенню не може вплинути безпосередньо на обєкт управління, не може характеризуватися таким параметром як загроза. Прикладом такої компоненти може служити компонента, що реалізує візуальне відображення технологічного процесу, або його параметрів. Тому, приймемо, що коли деяка компонента має параметр загрози Zg, то вона повинна вміщати елемент, який є програмною реалізацією, що може взаємодіяти з окремим кроком довільної, або певної атаки. Природно

припустити, що завдяки такому елементу інтруз, або його частина можуть бути доправлені не тільки в середовище ISU, а і може бути доставлений до вибраної небезпекою компоненти ISU, при цьому інші елементи, які не є загрозами, можуть приймати в цьому участь. Якщо ISU має доступ до зовнішнього середовища тільки через систему доступу SD, то відповідно компонента SD буде першим елементом, який визначає віддаль між точкою входу інтруза і компонентою, в якій інтруз планує активізувати рішення своєї основної задачі. Всі інші компоненти, чез які, з допомогою загрози з першої компоненти, інтруз буде проходити, будуть визначати віддаль, через яку повинен пройти інтруз. Очевидно, що в залежності від перетворень, які інтруз може ініціювати в кожній проміжній компоненті, віддаль проходження інтрузом через середовище ISU буде збільшуватися. Чим більша віддаль, яку інтруз мусить пройти, щоб попасти в компоненту, яка є ціллю, тим легше його виявити і, відповідно, знешкодити. Час перебування інтруза в середовищі деякої компоненти визначається цілим рядом факторів, що є характерними, для неї. До таких факторів належать:

- кількість засобів захисту, що використовуються в компоненті k_i,
- параметри середовища, що сприяють існуванню нелегальної компоненти, наприклад, наявність не контрольованих областей памяті, чи не контрольованих функціональних фрагментів і т.д.,
- зручність доступу до компоненти k_i та зручність у ідентифікації окремих елементів компоненти.

Ці параметри можна визначати для кожної компоненти окремо, не залежно від того, чи є в ній інтруз, чи ні. Але остаточна верифікація цього параметру реалізується у випадку виявлення інтуза, який активізував своє функціонування.

Міра захищеності окремих компонент є природою характеристикою, яка повязується з параметром загрози $Zg_i(k_i)$. Цей параметр можна вимірювати різними способами в залежності від різних факторів. Найбільш простий спосіб полягає у вимірюванні цього параметру шляхом підрахунку кількості засобів захисту, які використовуються в рамках цієї компоненти. Необхідність використання персональних засобів захисту в окремих компонентах обумовлюється специфікою використання цих компонент.

Величина параметру загрози, яким характеризується компонента системи ISU, визначається сумою окремих складових:

$$P\big(Zg_i(k_i)\big) = Fn_i + Jn_i - Vd_i + Tu_i - Zk_i. \qquad (2)$$

Всі значення приведених величин є цілими числами, що задаються на множині $\{0,1\}$. Міра Fn_i визначається експертом, Jn_i визначається кількістю пакетів, що передається за одиницю часу з вибраної компоненти $Jn_i\big(k_i \to k_j\big) = m/\Delta\tau$, де m кількість пакетів, $\Delta\tau$ – одиниця часу, що для всієї системи. Парметр Vd_i визначається числом компонент, через які необхідно пройти

інтрузу ($Intr_i$) від SD до $k_i(Intr_i)$, Tu_i вимірюється числом кількості одиниць елементарного інтервалу часу $\Delta\tau_i$, який прийнято єдиним для всієї системи, Zk_i вимірюється кількістю засобів захисту в компрненті k_i системи ISU. Таким чином, величина параметру загрози $P\big(Zg_i(k_i)\big)$ вимірюється цілим числом рівним алгебраічній сумі всіх складових чисел.

Приведені фактори, що впливають на величину параметра загрози, що має місце в окремій компоненті $(k_i) \in ISU$, ілюструють той факт, що повністю ліквідувати загрозу в окремому k_i не можливо. Значення цього параметру необхідно тримати на певному рівні, який є оптимальним, з точки зору рівня безпеки всієї системи.

На рівень безпеки всієї системи $ISU(TPP)$ впливають не тільки параметри такі як рівень загрози кожної окремої компоненти $(k_i) \in ISU$, але і ряд інших факторів, які також впливають на рівень безпеки системи в цілому. До таких факторів можна віднести наступне:

- загальний рівень загрози системі ISU, в цілому (Zs),
- активність небезпеки Nb_i (ISU) (An),
- методи захисту та методи забезпечення і визначення загального рівня безпеки (Vb),
- міра управляємості рівнем безпеки (Ub),
- міра узгодженості процесів в ISU з процесами в SUB, що означає можливість в SUB реалізувати процеси захисту таким чином, щоб не довести процеси виробництва до рівня, коли ці процеси не ефективні (Up).

Перш за все, розглянемо підходи до визначення загального рівня загрози, яка характеризує всю систему в цілому. Цю величину будемо визначати, як величину ризику втрат через не виконання процесу продукування замовлених виробів, або через неякісне їх виробництво. Величину ризику $R(t)$, в рамках даної роботи, використовується для визначення того, чи зміниться значення рівня безпеки функціонування системи ISU на величину ΔBz_i, яка є більша від допустимої величини зміни рівня безпеки. Перш за все, розглянемо функціональну блок схему ISU технологічного процесу, яка приведена на рис. 1. На приведеному рисунку використовуються наступні позначення:

- SD – система доступу до ISU,
- OS – операційна система управління програмними засобами,
- BD – база даних,
- SPZ – система прикладних задач управління технологічним процесом,
- VTP – система відображення текучого стану процесу управління TPP,
- TPP – технологічний поліграфічний процес,
- USO – система звязку засобів управління з обєктом,

- AOU – адміністратор оперативного управління TPP, яке реалізується у випадку виникнення нештатної ситуації.

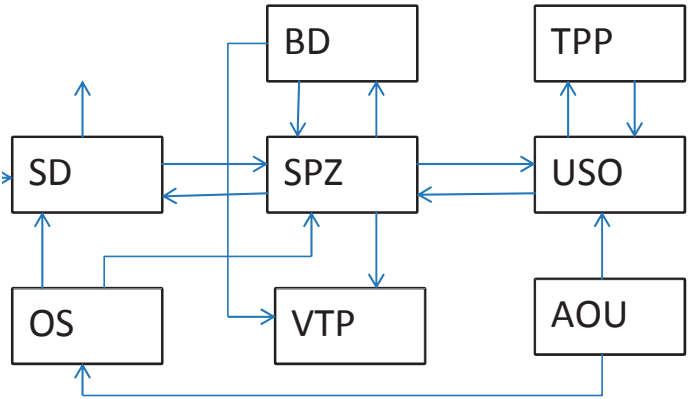

Рис. 1. Функціональна блок схема ISU.

Початковим критерієм для оцінки ризику $R_i(t)$ зміни величини Bz_i на $\Delta Bz_i > \delta^{\beta}$, де δ^{β} – поріг допустимого зменшення рівня безпеки, визначає допустимий рівень ефективності технологічного прцесу, що визначається рівнем безпеки. З одного боку, цей рівень визначається необхідними параметрами виробів, що виробляються в TPP. З другого боку, такі параметри визначають вимоги до параметрів TPP, наприклад, параметри, що забезпечують задану якість друкарського відбитку, параметри швидкості друкування і т.д. Всі параметри, що характеризують TPP, фахівці переносять на вимоги і, відповідно, параметри ISU. Тому, будемо говорити, що підтримання необхідних значень параметрів ISU, з точки зору несанкціонованого втручання в роботу ISU зовнішніх факторів, буде забезпечувати система управління захистом SUB. Відповідні задачі захисту, що розвязуються системою SUB, будуть орієнтуватися на використання засобів, що знаходяться в SUB і наявність яких обумовлюється всіма факторами, які створюють небезпеки. Такі небезпеки є причинами виникненням негативного впливу на ISU. Розглянемо наступну схему можливої негативної дії на ISU:

$$Nb_i\ (ISU) \rightarrow A_i(Zg_i) \rightarrow Jntr(Sp_i) \rightarrow H(Bz) \rightarrow H(R(t)), \qquad (3)$$

де $Nb_i\ (ISU)$ –небезпека для системи ISU, $A_i(Za_i)$ - атака, що формується Nb_i , а сама атака A_i використовує загрозу Za_i, що характеризує ISU, $Jntr(Sp_i)$ – інтруз, що сформований з допомогою атаки, який представляє собою програмного носія орієнтованого на реалізацію негативного впливу на вибрану атакою підсистему ISU , $H(Bz)$ – текуче значення рівня безпеки, до якого привела негативна дія інтруза $Jntr$, $R(t)$ – текуче значення величини

ризику, що позначається $H(R(t))$, яке сформовано на основі рівня безпеки $H(Bz)$.

Висновки

Виходячи з співвідношення (3), необхідно проаналізувати всі компоненти, що приймають участь в процесі зміни ризику і обумовлюють в кінцевому випадку збільшення величини ризику функціонування обєкту, що захищається. Загроза $g_i(k_i)$, в певній мірі, проаналізована вище і встановлено основні фактори, що на неї впливають. Тому хх розглядати не будемо. Розглянемо таку компоненту, як система управління рівнем безпеки SUB, що орієнтована на організацію захисту ISU. Оскільки, функціональні характеристики такої системи повинні відповідати задачам захисту, то коротко їх проаналізуємо. До таких характеристик можна віднести наступну:

- Здатність протидіяти відомим типам атак $\{A_{i1}, \dots, A_{in}\}$,
- Управління рівнем загроз, що характеризують ISU,
- Виявляти інтрузи, які попали в середовище ISU і знаходяться в режимі очікування своєї ініціації,
- По слідах дії атаки A_i на ISU, система SUB повинна виявляти причини відповіднизмін і елімінувати їх в рамках системи ISU,
- Передбачати можливість виникнення деякої атаки, з ціллю упередження її дії на ISU та недопущення негативних змін в системі ISU,
- Забезпечувати неможливість повторення виявленої атаки в наступні моменти часу функціонування ISU,
- Забезпечувати можливість управління величиною безпеки $H(Bz)$ в процесі функціонування $ISU(TPP)$,
- Забезпечувати можливість визначення величини ризику на основі даних про рівень $H(Bz)$,
- Розвязувати обернену задачу, яка полягає у тому, що на основі заданої величини ризику $R(t)$ визначати необхідну величину безпеки системи Bz та реалізовувати перетворення в системі ISU, які забезпечували би відповідний рівень безпеки функціонування системи.

1. *Расторгуев С.* Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993. -188 с.
2. *Феденко Б.А., Макаров И.В.* Безопасность сетевых ЩС. М.: ЭКОТРЕНДЗ. 1999.
3. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. СПб.: БХВ – Петербург, 2000. -320 с.
4. *Tamm У.* Теория графов. М.: Мир, 1988. – 424 с.
5. *Касперски К.* Записки исследователя компьютерных вирусов. СПб.: Питер, 2005. – 316 с.

Поступила 28.9.2015р.