При $R/\lambda<200$ возможности оптимальных и неоптимальных алгоритмов практически совпадают. Помимо этого использование оптимальных алгоритмов обработки сигналов протяженных объектов открывает широкие возможности для идентификации объектов и построения адаптивных систем пространственно-временной обработки сигналов.

1. Пространственно-временная обработка сигналов / Под ред. *И.Я.Кремера*. - М.: Радио и связь, 1984. - 224с.
2. Радиоэлектронные системы: основы построения и теория. / Справочник. Под ред. *Я. Д. Ширмана*. - М.: Радиотехника, 2007. - 512 с.
3. Оптическая обработка, информации. Применения /Под ред. *Д.Кейсесента*. Пер. с англ. - М.: Мир, 1980.-352с.
4. *Олянюк Я.В.* Оптимальный прием сигналов и оценка потенциальной точности космических измерительных комплексов. - М.: Сов. радио, 1973. – 182 с.

*Поступила 12.02.2010р.*

УДК 685.03

О.Ф.Нікулін, С.О. Нікулін

## МОДЕЛЮВАННЯ ОКРЕМИХ НЕБЕЗПЕК СПЕЦІАЛІЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ

Асортимент засобів захисту системи захисту в цілому визначається цілим рядом факторів, до яких відносяться наступі вимоги:

1. вимоги по забезпеченню заданої величини ризику роботи системи управління,
2. особливості реалізації об’єкту управління (OU), для якого створюється спеціалізована система управління,
3. вимоги до міри універсальності та структурної простоти організації системи захисту, що дозволяє забезпечити необхідну простоту її експлуатації.
4. Загальна структура SZ буде складатися з наступних логічних і фізичних компонент. До фізичних компонент відносяться:
5. загальна система управління SZ (USZ)
6. універсальні локальні засоби захисту Zhi, кількість яких може бути різною, що залежить від загальних вимог до системи захисту.

До логічних компонентів будуть відноситися компоненти, що реалізуються в рамках системи USZ на окремих засобів, до яких відносяться наступні:

 

1. в рамках USZ реалізуються логічні компоненти, що представляють собою окремі функціональні блоки, які орієнтовані на виконання наступних функцій:
2. формування моделей небезпек, що активізують виникнення атак,
3. оцінка величини ризику функціонування системи OU в поточний момент часу,
4. управління зміною локалізації в середовищі Zhi системи управління (SU),
5. в рамках окремих Zhi реалізуються логічні компоненти, асортимент яких може мінятися в залежності від особливостей розв'язку задачі забезпечення безпеки функціонування SU, яка визначається в рамках логічних компонент (USZ). До таких компонент відносяться наступні:
6. визначення типу атаки та її виявлення на ранніх стадіях її зародження,
7. визначення загроз, які можуть бути використаними певними небезпеками для реалізації атаки,
8. формування заходів по активній протидії виявленому типу атаки та нейтралізація загроз, що використовуються відповідною атакою.

Приведені типи логічних компонент являються базовими і можуть розширятися в рамках USZ чи Zhi. Таке розширення реалізується в рамках загальної для двох фізичних компонент функціональної можливості, яка в рівних мірах реалізується в USZ і окремих Zhi і полягає у придатності останніх до адаптації по відношенню до критеріїв, що є спільними для USZ та Zhi та твердження, що приймаються по відношенню до небезпек та їх взаємозв'язку. Для зручності використані технології будемо називати та твердження, що стосуються небезпек, будемо називати аксіомами, або положеннями, оскільки останні приймаються без доведення.

Положення 3.1 по відношенню до будь-якої деякої інформаційної системи існують небезпеки, що на інтервалі функціонування останньої активізують по відношенню до неї атаки.

У відповідності з цим положенням не існує абсолютно безпечних інформаційних систем. Будь-яка небезпека ініціює атаки на інформаційні системи лише в тому випадку, коли мають місце наступні умови:
1. якщо небезпека зацікавлена у втратах, до яких можуть привезти ініційовані нею атаки, у відповідних системах, що атакуються,
2. якщо інформаційна система має загрози,
3. якщо інформація про об'єкт можливої атаки є доступною для зовнішнього оточення, і така доступна інформація відображає дані про об'єкт, які знаходяться у певних межах.

Перша умова дозволяє сформувати принципи визначення небезпек як певних об'єктів, в рамках яких можуть ініціюватися атаки. До таких принципів відносяться наступні:

1. небезпека може бути характерна для цих об’єктів, які по певних ознаках у першу чергу, по ознаках цілі функціонування об’єктів, можуть бути визначені як споріднені об’єкти,
2. оскільки небезпека як фактор мусить мати фізичне відображення в оточуючому середовищі, то таким відображенням будемо вважати ті чи інші об’єкти з оточуючого середовища, які можна віднести до класу об’єктів, стосовно яких розглядається проблема забезпечення безпеки,
3. оскільки небезпеки й відповідні атаки розглядаються як такі, що реалізуються в інформаційному середовищі засобів, що його реалізують, то в даному випадку будемо говорити про небезпеки, які проявляються у вигляді атак виключно на основі використання інформаційних засобів. А це означає, що відповідні атаки будуть носити інформаційний характер.

Приведені принципи дозволяють сформувати методи визначення небезпек для відповідної системи, яку передбачається захищати. Один з таких методів може ґрунтуватися на наступному узагальненому алгоритмі визначення небезпеки.

Алгоритм А1

1. Визначити всі об’єкти, що використовують інформаційні засоби та являються спорідненими в рамках цілей функціонування до системи, що охороняється.
2. Проаналізувати функціональні можливості об’єктів, що вибрані в п.1, по проведенню аналізу санкціонованої інформації, що доступна зовнішньому середовищу і може бути використана для несанкціонованого втручання в процес функціонування об’єкту ,що охороняється.
3. Оцінити потенціальні можливості в досягненні цілей об’єктами, що віднесені до потенціальних небезпек та порівняти відповідні можливості з можливостями досягнення цілей об’єктів, що охороняються.

Приведений алгоритм описує певні зональні дії, що пов’язані з визначенням небезпек, і дозволяє отримати лише наближені оцінки того, що відповідний об’єкт являється небезпекою для системи, що охороняється. Таким чином, у результаті виконання алгоритму А1 можна отримати ряд оцінок, які дозволяють в певному наближенні виявити потенційні небезпеки для об’єкту охорони. Для більш точного кількісного аналізу потенційних небезпек розглянемо параметри небезпек, які їх характеризують з різною мірою адекватності. Першим таким параметром являється мірі спорідненості. Будь-яка ціль функціонування інформаційної системи як ключової системи, що забезпечує той чи інший технологічний процес в системі, що охороняється, незалежно від того, чи вона представляє собою продукт чи послугу, описується певною системою параметрів, що мають визначені діапазони значень. Формально це можна представити співвідношенням $ci(xi)=fi[(Pij, ..., Pim)]$ де Pij — параметр, що описує ціль ci(xi), ΔPij – діапазон значень, які може приймати відповідний параметр в рамках цілі ci(xi), xi — об’єкт охорони, φi — функція, що описує структуру цілі ci(xi), що

формується з параметрів Pij. Приймемо, що зовнішніми об'єктами по відношенню до xi є об'єкти {x1, .., xi+1, .., xn}. Тоді міра спорідненості між xi та xj визначається по наступних аспектах:

1. по кількості спільних параметрів для xi та xj,
2. по кількості однакових ? для xi та xj і однакових Pij,
3. по структурній відмінності φi і φj для xi та xj.

Позначимо міру спорідненості між xi і xj символом η. Міра спорідненості є максимальною, якщо має місце співвідношення {[(Pi1= Pj1), .., (Pim= Pjm)]&[(ΔPi1= ΔPj1), .., (ΔPim= ΔPjm)]&(φi=φj)}→(η= max). Розглянемо можливі способи вимірювання цієї величини, оскільки оцінка величини η дає можливість серед можливих небезпек ввести впорядкованість. Величина кількості співпадаючих параметрів, що описують ціль, описується співвідношенням:

$$\eta(Pik)= \Sigma mj,i=1\delta(Pik, Pjk).$$

При однакових параметрах Ci і Cj у останніх можуть відрізнятися діапазони допустимих значень. У цьому випадку складова параметра ? визначається у відповідності з наступним співвідношенням:

$$\eta(\Delta Pik)= [\Sigma mj,i=1(|\Delta Pik- \Delta Pjk |)]/m. \quad (1)$$

Така оцінка величини відповідає величині середнього значення різниць між діапазонами допустимих значень та параметрів, що описують цілі ci і cj. Оскільки різні параметри можуть вирівнюватися в різних одиницях, тому числові значення можуть мати різну величину, що може приводити до спотворення результатів для η(ΔPik).

У формулі (1) використовується відносне значення величини різниці між діапазонами, допустимих значень параметрів, яке вимірюється процентах як безмірна величина. У цьому випадку визначимо приведений масштаб вимірювання параметра, який буде рівним: m(ΔPik)= ΔPik/100, m(ΔPjk)= ΔPjk/100. Верхня і нижня границя приведених діапазонів для Pik і Pjk визначається по виразах:

$$[Pvik/[\ m(\Delta Pik)]]= Pvpik,\ [Pnik/[\ m(\Delta Pik)]]= Pnpik,\ \Delta pPik= |Pvpik- Pnpik|.$$

У цьому випадку вираз (1) запишеться у вигляді:

$$\eta(\Delta Pik)= [\Sigma mj,i=1(|\Delta pPik- \Delta pPjk |)]/m.$$

Може мати місце ситуація, що не для всіх Pik і Pjk буде виконуватися умова Pik=Pjk. У цьому випадку η(ΔPik) визначається тільки для тих Pik, які є однаковими. Це означає, що для визначення η вага складової η(Pik) є більша від складової η(ΔPik). Виходячи з приведених формул, max η(ci, cj)=0. Із зменшенням η його величина в абсолютних числових величинах збільшується.

Розглянемо спосіб визначення складової η(φi, φj). При цьому можливі випадки, коли φi має різний вигляд. Вони можуть представляти собою аналітичні залежності, структурні зв'язки або логічні залежності. В останньому випадку параметри Pij повинні допускати інтерпретацію на множині {0,1}, що малоймовірно, оскільки для Pij задаються величини діапазонів допустимих значень. Тому останній випадок розглядати не

будемо. Аналітичне представлення φі для сі малоймовірне, оскільки кількість параметрів, що описують сі, як правило велика. Якщо при цьому прийняти, що φі — аналітична функція, то остання являється параметричною.

Практично сі може представляти собою деякий продукт, послугу або довільний об'єкт. Переважно в таких об'єктах окремі параметри пов'язані між собою у відповідності з тією чи іншою структурою, що характерна для окремої цілі. Звичайно, що між окремими параметрами в рамках такої структуру можуть існувати аналітичні залежності. Тоді таку структуру можна відобразити у вигляді графіка Gi, вершини якого відповідають параметрам Pik, а ребра відображають взаємозв'язки між параметрами або υi= φii(Pik, Pir). У цьому випадку φii можна розглядати як деяку аналітичну функцію, або функцію, що задана будь-яким іншим способом, що можна записати υi= [[(Pik= φiik(Pir)]V[(Pir= φiir(Pik)].. Зрозуміло, що між параметрами Pik і Pjk можуть бути залежності, що безпосередньо не відображаються одним ребром. У цьому випадку будемо говорити про опосереднені залежності. Обмежитися випадками графітової структури для φі доцільно і обґрунтовано тим, що функцію для одного аргументу значно простіше описувати деякою кривою, ніж функцією двох або більшої кількості аргументів. У загальному випадку для опису сі у вигляді аналітичної функції від великої кількості аргументів необхідно для характеристики сі вибрати певний інтегральний параметр, що в більшості випадків суттєво понижує точність вираховування окремих компонент, які впливають на параметр η(φі). Тому приймемо, що залежності між параметрами Pik і Pjk, як складові структури, сі та сj. Для вибору пари параметрів, що формують залежність φі будемо вибирати ті чи інші параметри, які являються або можуть бути більш активними. Активність визначається величиною співвідношення:

$$\{(\Delta Pi>\Delta Pj)\rightarrow (\Delta Pi/\Delta Pj)\geq \delta i]\}V\{(\Delta Pi<\Delta Pj)\rightarrow (\Delta Pj/\Delta Pi)\geq \delta i]\},$$

де δі — поріг активності взаємозв'язку між параметрами Pі і Pj. Таким чином, φі будемо розглядати як графік Gi. Завдяки тому, що Gi може характеризуватися цілим рядом інваріантів, то приймемо, що φі і φj визначають міру спорідненості η(φі, φj) на основі обчислення відповідних інваріантів та порівнянні їх значень. Наприклад, якщо серед вибраних інваріантів використовуються такі як кількість ребер Gi, то міра спорідненості в частині складової η(φі, φj) буде тим більша, тим менша різниця між значеннями відповідних інваріантів. У випадку, коли таким інваріантом являється кількість вершин Pі і Pj, то останній співпадає з компонентою η(Pik).

Наступним важливим параметром небезпеки, яка асоціюється з певною системою, є міра спорідненості з об'єктом, що охороняється не менше ніж δі, є параметр, що характеризує функціональні можливості небезпеки в інформаційному середовищі, що її оточує. Цей параметр будемо називати зовнішньою активністю небезпеки і будемо його позначати символом μ. Функціональна зовнішня активність небезпеки πі або μ(πі) визначається наступними параметрами:

- комунікаційними можливостями πі,
- мережевими повноваженнями πі,
- інтенсивністю співпраці πі з зовнішнім середовищем,
- функціональними особливостями πі,

Комунікаційні можливості πі визначаються внутрішніми характеристиками πі, до яких відносяться такі як кількість портів, що є для реалізації транзакцій, кількість IP-адрес, що дозволені в рамках πі для реалізації комунікацій, інтенсивність потоків обміну між πі і зовнішнім середовищем та цілий ряд інших параметрів, якими характеризується πі. Функціональна зовнішня активність використовується для того, щоб можна було оцінити можливі стратегії реалізації небезпекою πі атак. Оскільки для різного типу πі параметри, що формують характеристику зовнішньої активності, є різними, то обмежимося тільки μ(πі) як параметром, що характеризує πі.

Відомо [2], що більшість інформаційних систем, у тому числі систем спеціального призначення, орієнтовані, крім роботи з мережею, на роботу з користувачами. У цих випадках до складу інформаційної системи захисту об'єкта включаються системи доступу (SD), які виконують наступні задачі:

- забезпечення доступу до системи користувача, або ряду користувачів, що обслуговують систему управління,
- захист системи управління від несанкціонованого доступу до системи,
- реалізація зв'язку між системою управління об'єктом та системою управління в частині її реалізації у вигляді інформаційної системи.

Як правило, значна частина атак, що можуть здійснюватися по відношенню до об'єкту, який охороняється, може реалізуватися на основі використання SD. У цьому випадку небезпеку для системи представляє собою користувач, що користується системою або пробує скористуватися нею, виходячи за межі своїх повноважень. Оскільки ідентифікувати користувача з небезпекою, що існує по відношенню до об'єкту охорони, досить складно, то останню в даному випадку будемо ідентифікувати з певною частиною або підсистемою SD, яка реалізує функцію захисту доступу. Таким чином, SD буде складатися з наступних окремих компонент:

- підсистеми управління доступом (UD),
- підсистеми захисту (ZD),
- підсистеми організації доступу, яка являється частиною SD, що пов'язує між собою UD і ZD та реалізує загальне управління SD.

У даному випадку підсистему ZD будемо ідентифікувати з небезпекою, що пов'язана з користувачами. Така ідентифікація обумовлюється тим, що ZD повинна в певній мірі виявляти можливі негативні наміри по відношенню до системи управління зі сторони користувача, якщо останній ініціює спробу несанкціонованого доступу до системи. В цьому сенсі ZD відображає ті чи інші негативні прояви, що ініціюються користувачем по відношенню до системи, що охороняється, оскільки уявлення про небезпеку являється уявленням про можливі негативні дії зі сторони об'єкту, який їх ініціює, то

ZD повинна бути здатною розпізнавати відповідні дії зі сторони споживача і нейтралізувати можливість їх виконання. Тому небезпека зі сторони ZD виникає у тому випадку, якщо виникає ситуація, що створюється користувачем у відповідності з намірами останнього, є негативною для об'єкта охорони, а ZD не в стані таку ситуацію розпізнати. Якщо виходити з класичних уявлень про розпізнавання образів, то в їх основі лежить використання еталонів, з якими порівнюється те, що треба розпізнати [3]. Тому можна стверджувати, що у випадку, коли ZD не вміщає необхідної інформації про можливі негативні наміри або їх опис, то ця обставина визначає небезпеку, що пов'язана з використанням в системі управління з об'єктом SD. Існує підхід до організації ZD в SD, який гуртується на розпізнавання та ідентифікації користувача, який реалізує спробу співпраці з системою. Але більшість атак, що реалізуються на певну систему управління (SU) і ініціатором яких може бути несанкціонований користувач, здійснюється на основі використання санкціонованих способів співпраці з системою. Негативні аспекти такої співпраці виникають або використовуються тільки за межами умов реалізації несанкціонованого доступу до системи. Тому ZD при такому підході може допустити несанкціонованого користувача в систему, оскільки вона не може передбачити можливість цих подій, що ініціюються за межами контролю, який реалізується в SD при такому підході [4]. Тому в рамках даної роботи розподіляються функції управління доступом, які полягають і реалізуються підсистемою UD:

- ідентифікація та аутентифікація користувача,
- перевірка та надання повноважень,
- загальний контроль за використанням відповідних повноважень користувачем, переважно, контроль часу доступу до системи.

Підсистема ZD не повинна дублювати функцій UD та не повинна в тій чи іншій формі функціонувати з точки зору виявлення недовіри до UD. Тому ZD функціонує у відповідності з наступними умовами:

- у відповідності із стратегією забезпечення безпеки підсистема ZD здійснює додаткову перевірку стану безпеки доступу, яка полягає в аналізі динамічних параметрів доступу, наприклад, частоти доступу окремого користувача, характеру зміни параметрів доступу споживачів та інших динамічних параметрів, які перевіряються з інтервалом, що суттєво перебільшує інтервал між двома послідовними доступами,
- система захисту перевіряє ресурси, якими користувалися користувачі, якщо параметри сеансу доступу в поточному зверненні користувача були модифіковані,
- система захисту контролює стратегію реалізації доступу кожним окремим користувачем на предмет виявлення аномалій у профілі споживача. Приведені умови відображають тільки частину особливостей роботи ZD в рамках SD.

1. *Зима В. М., Молдовсян А. А., Молдовсян Н. А*. Безопасность глобальных сетевых технологий. – СПб.: БХВ — Петербург, 2000.
2. *Соколов А. В., Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002.
3. *Пентлод А.* Распознавание лиц для интеллектуальных сред/Открытие системы. — 2000, № 3, — ст. 17–20.
4. *Кухарев Г. А*. Биометрические системы. Методы и средства идентификации личности человека. – СПб.: Политехника, 2001.

*Поступила 11.02.2010р.*

УДК 654.07:517.9

О.А.Машков, В.Р.Косенко

## ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ В СКЛАДНИХ ОРГАНІЗАЦІЙНИХ СИСТЕМАХ З ПОГЛЯДУ СИСТЕМНОГО ПІДХОДУ (частина 2) (ПРИНЦИПИ ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ)

Під принципами управління при управлінні організаційними системами доцільно розуміти основні правила, положення та норми поведінки, за якими діють учасники організаційного управління за умов, що склалися в суспільстві. Принципи організаційного управління синтезують та відображають об'єктивність законів суспільної формації, характерні риси практики організаційного управління. Принципи управління визначають вимоги до системи, структури, організації і процесу організаційного управління. У принципах організаційного управління знаходять свій вияв основні вимоги, що ставляться до побудови органів управління та методів здійснення функцій управління, доцільний характер взаємовідносин учасників управлінських відносин. Таким чином, принципи управління являють собою результат узагальнення людьми об'єктивно діючих законів та закономірностей, притаманних їм загальних рис, характерних фактів та ознак, які стають загальною підставою їх діяльності. Водночас науково-теоретичне узагальнення та напрацювання людьми принципів не означає, що вони мають суто суб'єктивний характер. Принципи управління відображають сутність явищ та реальних процесів управління, що підпорядковуються певним законам і закономірностям. Вони об'єктивні гак само, як закони і закономірності. Тобто принципи управління - це керівні ідеї, основоположні засади, що відображають закономірності розвитку відносин управління. На практиці важливе значення має зв'язок принципів управління з методами управління, що не можна розглядати без цілеспрямованого впливу. Ціль

 