УДК 004.056.7

А.М. Орєхов, В.О. Хорошко

КОНЦЕПЦІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

У статті розглядається підхід до розроблення системної концепції забезпечення безпеки інформаційного простору. Доведено, що для розв'язання цієї задачі необхідний аналіз дій зловмисника та розробка його моделі, а вже після цього розробляють тактику забезпечення безпеки інформаційного простору. Взаємопов'язане розв'язання задач системної концепції забезпечення безпеки інформації в інформаційному просторі, в кожному з яких існують свої підходи, методи та способи їхнього вирішення, засоби захисту повинні забезпечувати повністю.

Ключові слова: інформаційний простір,технічні засоби захисту, система безпеки інформаційного простору.

Вступ

Актуальність системного підходу до розв'язання задач охорони діяльності особливо зросла в останні роки. Саме в сучасних умовах України, коли відбувається становлення нових суспільних, економічних, політичних відносин, якщо недостатній механізм їхнього правового регулювання, спостерігається закономірний спалах криміногенних обставин. Різко активізується діяльність терористичних та злочинних угрупувань, зростає їхня кількість та якісне технічне і методичне забезпечення; вони проникають у інформаційний простір (ІП) [1-5].

За інформаційно-аналітичним оглядом експертів рівень злочинів щодо ІП у найближчі роки залишається незмінним. Злочинні дії організованих угрупувань будуть спрямовані на отримання таємної інформації про діяльність підприємства установ.

За оцінками експертів підготовка і реалізація злочинних акцій здебільшого здійснюється на високому професійному рівні, характеризується системним підходом (зокрема і в плані приховування втручання в ІП) і часто супроводжується жорстоких виконанням цих дій.

Тому, розробляючи систему концепції забезпечення безпеки ІП, необхідно врахувати як світовий, так і вітчизняний досвід, що стосується всієї багатогранної діяльності для захисту ІП.

Практика охорони ІП показує, що для вирішення проблем і задач охорони ІП потрібний науково обґрунтований підхід. Це стосується особливо важливої, особливо небезпечної інформації, інформації особливого ризику (інформації щодо керування повітряним рухом).

Мета роботи

Для розв'язання задач і проблем вибору структури та складу засобів захисту інформації необхідно, проаналізувати можливі варіанти дій зловмисника, тобто людини, яка несанкціоновано намагається отримати інформацію.

Основна частина

Слід врахувати, що зловмисником може виявитись людина, яка випадково отримала доступ до таємної інформації. Тобто, проаналізувавши можливі дії зловмисника, необхідно скласти варіанти його моделей, які сприймаються як основні чинники при виборі тактики захисту ІП, з урахуванням важливості та значущості цієї інформації.

Для правильної оцінки параметрів зловмисника треба зважити на його стартову позицію, а саме:

- зловмисник не має доступу до інформації, яка знаходиться у ІП, і йому треба подолати всі рубежі захисту;
- зловмисник має доступ до деякої інформації, але не має доступ до ІП;
- зловмисник має доступ до інформації та до ІП, але не має доступу до конкретних відомостей;
- зловмисник має доступ до інформації і до ІП та до конкретних відомостей.

Зрозуміло, що для першої групи ймовірність виявлення та складності отримання інформації для здійснення протиправних дій визначається комплексом засобів захисту, а для четвертої групи - рівнем всієї системи забезпечення безпеки, зокрема, і станом системи захисту.

Тому для вирішення цих питань необхідно розглянути модель зловмисника. У термінах вирішення задачі оцінки безпеки ІП опис зовнішньої середи повинно утримувати не тільки опис зовнішніх об'єктів, по опис можливого зловмисника.

У простому випадку зловмисник описується множиною зовнішніх впливів (загроз) $T = \{t_i\}$ з відповідними характеристиками $H(T) = \{h(t)\}$. У більш загальному випадку необхідно розглянути різні типи зовнішніх впливів $T_1, T_2, \ldots$. Це відповідає різним задачам зловмисника: отримання інформації, проникнення до неї, створення неї тощо. Таким чином у загальному випадку, маємо перелік множин: $T = \{T_i\}$ при *i=1,...,N,* опис яких відповідає опису характеристик $H(T)$.

Крім того в моделі також необхідно врахувати внутрішні взаємодії, відповідаючи, з одного боку, можливому впливу на інформації або на її елемент, а с другого - можливість елемента самому провести дії, які не передбачені технологією та можуть мати небажані наслідки.

Нехай різні можливі впливи на елементи і зв'язки об'єкта захисту (інформація) характеризуються відповідними множинами $U(0)$ і $U(c)$, де $U(0) = \{u(\text{i})\}$ і $U(c) = \{u(\text{i, j})\}$.

Аналогічно можливість елемента виявити активність, тобто виявити деякі впливи, не передбачені технологією обробки інформації з множини $V(0)$ і $V(c)$ відповідно, а множини $V(0) = \{\nu(\text{i})\}$ і $V(c) = \{\nu(\text{i, j})\}$ в свою чергу можуть об'єднуватися у список *V* як це вже наведено раніше.

Як складові опису об'єкта *U* і *V* щодо отримання оцінок повинні володіти відповідними наборами характеристик: $H(U)$ і $H(V)$.

Припускається, що загрози повинні утворювати пару з різними уразливостями - з множин $U(0)$ і $U(c)$, то є зовнішні впливи (загрози зі сторони зловмисника) повинна відповідати «можливості такого впливу» щодо створення пари *(t,u)* (якщо такий зовнішній вплив не конкретизований, крім того, для відповідного об'єкта, як $t = t(i)$ або $t = t(i, j)$. У результаті такої зовнішньої загроза може «розвинутись», як по відповідним технологічним зв'язкам моделі, так і по нетехнологічним, які у загальному випадку являється парами виду: *(V,U).*

Відповідно, у склад моделі, що описує зловмисника, крім безпосередніх загроз входять відзначені раніш множини уразливостей *U* та внутрішніх впливів *V*, по-перше, як фактори, що сприяють нападу, по-друге, як одиничне джерело впливів при відсутності зовнішніх зловмисників.

Тому, найнебезпечнішим, з погляду служби безпеки, є підготований і технічно забезпечений зловмисник, який може застосувати для вторгнення і обходу засобів охорони.

Отже, модель захисту ІП необхідно будувати з урахуванням моделювання всіх можливих дій зловмисника.

Для підвищення ймовірності виявлення підготовленого зловмисника комплексом технічних засобів охорони ІП можуть застосовуватися повністю приховані рубежі захисту.

Оскільки дії зловмисників мають системно продуманий професійний характер, то їм треба протиставити організацію і технічне забезпечення, що виконане на вищому щаблі професіоналізму. Саме цим і пояснюється необхідність розроблення узагальненої системної концепції із забезпеченням безпеки ІП, яка у кожному випадку повинна бути адаптована до конкретної ситуації з урахуванням умов функціонування, розміщення, особливостей довкілля тощо. Отже, для кожної конкретної інформації у ІП повинна розроблятися на базі загальної особиста концепція безпеки, з урахуванням якої розробляють проект забезпечення інформації засобами захисту. [4]

Технічні засоби захисту (ТЗЗ) повинні задовольняти сучасним вимогам із забезпечення безпеки, які підлягають охороні, від зазіхань потенційних зловмисників.

Програмні та криптографічні засоби захисту забезпечують визначений рівень захисту інформації.

Враховуючи вищевикладене, розробники засобів забезпечення безпеки інформації повинні розглядати під час аналізу вихідних положень безпеки для визначення «моделей зловмисника» і такі чинники як:

- наявність у вільному продажу закордонних та вітчизняних виробів спецтехніки;
- можливість організованими злочинними угрупуваннями людей, які були підготовані у силових структурах;
- наявність значних фінансових ресурсів у кримінальних структурах.

Тобто враховуючи ті чинники, які дають можливість злочинним формуванням організувати напад на інформацію, що охороняється, врахувати можливі злочинні дії з високим рівнем їхньої попередньої підготовки.

Центральною підсистемою в системі забезпечення безпеки інформації в ІП є узагальнена система охорони, за допомогою якої реалізуються практичні заходи із запобігання несанкціонованого доступу до інформаційних ресурсів ІП. Ця система забезпечує охорону ІП від несанкціонованих дій, пошкоджень, крадіжок та інших незаконних або злочинних дій.

На практиці для цієї системи складається з двох фаз: виявлення зловмисника або несанкціонованих дій та протидія цим діям.

Задачі виявлення зловмисника та визначення місця порушення можуть бути здійснені як за допомогою підрозділу служби забезпечення захисту ІП за допомогою ТЗЗ, ПКЗЗ. Треба відзначити,що задачі виявлення та контроль за станом безпеки ІП, що охороняється, розв’язують, як правило, за допомогою ТЗЗ і ПКЗЗ, а також за допомогою систем контролю. [3] Застосування цих засобів дає змогу в розумних межах зменшити кількісний склад підрозділу служби забезпечення захисту ІП, але водночас підвищити надійність захисту інформації, підвищити оперативність заходів протидії несанкціонованим діям зловмисника.

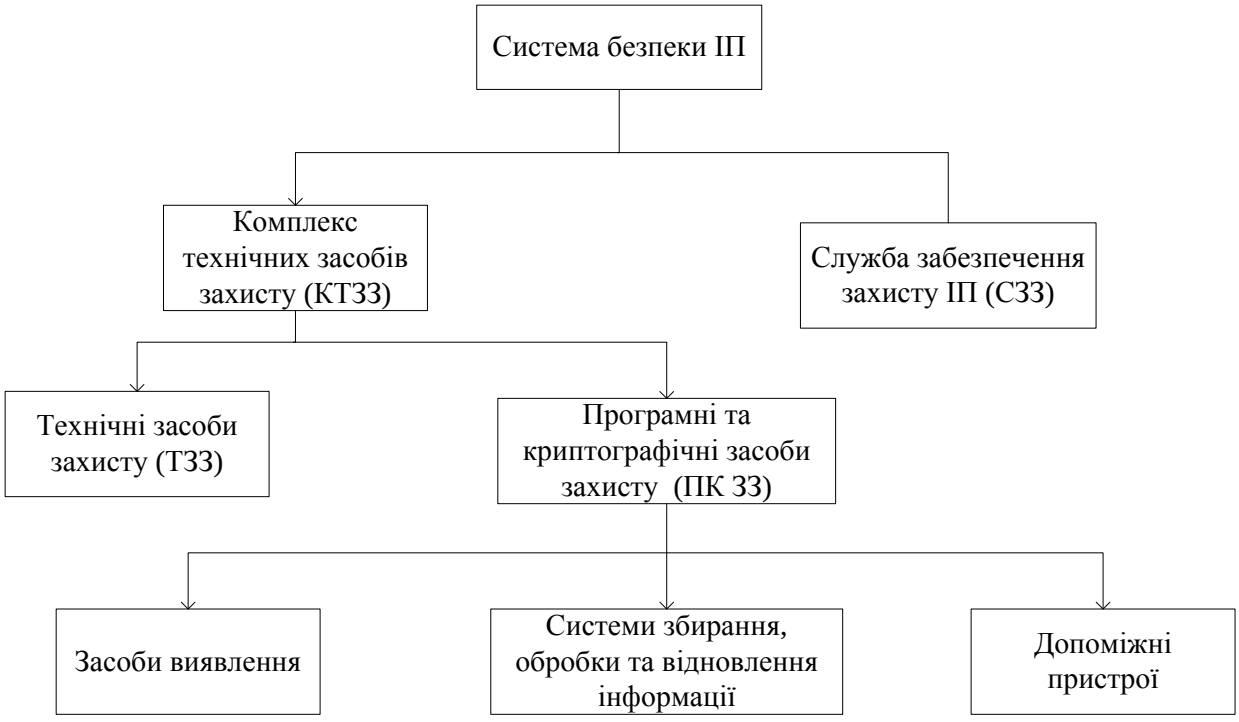

Рис. 1. Узагальнена структура системи безпеки ІП

На рисунку подана загальна система безпеки ІП, до складу якої входять: комплекс технічних засобів захисту (КТЗЗ) та служба забезпечення захисту ІП (СЗЗ). У свою чергу КТЗЗ складається з двох складових: технічні засоби захисту (ТЗЗ) та програмні та криптографічні засоби захисту (ПКЗЗ), вони у свою чергу поділяється на: засоби виявлення (ЗВ), системи збирання, обробки та відновлення інформації (СЗОВІ), а також допоміжні пристрої, такі, як джерела електроживлення, системи сигналізації, тощо.

Багаторічні дослідження систем забезпечення безпеки інформаційних ресурсів в ІП свідчать про необхідність розроблення системної концепції забезпечення безпеки кожного конкретного елемента ІП, що практично передбачає комплексне взаємопов'язане розв'язання службою забезпечення захисту ІП декількох блоків задач, а саме:

- визначення стратегії комплексної безпеки;
- забезпечення безпеки від несанкціонованого доступу до інформації;
- захист інформації;
- захист від прогнозованих до застосування засобів прихованого контролю;
- захист від диверсійно - терористичних дій;
- захист систем зв'язку;
- врахування людського чинника в системі забезпечення безпеки;
- можливість застосування зловмисником вітчизняної або закордонної апаратури, яка може бути застосована ним для несанкціонованого отримання інформації;
- організація системи контролю доступу.

Розглянемо ці блоки задач забезпечення захисту ІП детальніше.

При визначенні стратегії комплексної безпеки ІП вирішується проблеми класифікації, систематизації та диференціації можливих загроз для інформації, визначають структуру і задачі служби забезпечення захисту ІП, а з іншого боку, нормативно - правові документи, що регламентують діяльність з безпеки інформації з позиції юриспруденції. На основі аналізу ресурсів, техніко-економічних показників та соціальних аспектів безпеки розробляють заходи із забезпечення безпеки інформації.

Вирішення питання забезпечення безпеки від несанкціонованого доступу до інформації моделюють стратегію і тактику поведінки зловмисника на основі аналізу доступності до ІП та розглядають засоби його безпеки. На основі визначення життєво важливих елементів ІП розробляють принципи та схеми обладнання його технічних та програмно-криптографічних засобами забезпечення безпеки інформації. Після цього вибирають остаточний варіант системи забезпечення безпеки ІП.

Захист інформації забезпечуються спеціальними методами. Для цього розробляють концептуальну модель захисту, у якій розв'язують широке коло задач по всіх можливих каналах витоку інформації та каналах несанкціонованих дій. Здійснюють класифікацію каналів зв'язку і на її основі розробляють методи оптимального зв'язку, криптографічного захисту та захисту телефонних мереж зв'язку, оскільки канали зв'язку є найдоступнішими для дій зловмисників. А на основі моделювання можливих способів приймання інформації зловмисником за допомогою спеціальної техніки.

Що стосується захисту інформації в автоматизованих системах обробки інформації, то тут особливе місце займає розроблення та впровадження спеціальних математичних і програмних методів захисту операційних систем, баз даних та серверів, методів ідентифікації користувачів, введення паролів, ключів та антивірусних програм від несанкціонованого доступу і копіювання інформації та її спотворення.

Задачі захисту інформації від прогнозованих до застосування засобів прихованого контролю орієнтовані на модель зловмисника, яким може бути працівник одного з підрозділів забезпечення роботи ІП, або на здійснення контррозвідувальних заходів при одержанні оперативної інформації про зацікавленість злочинних угрупувань інформацією, що охороняється.

Задачі захисту ІП від диверсійно-терористичних дій розв'язуються спеціальними методами захисту - методами досліджень, класифікації та моделювання варіантів активних дій терористів, вивчаючи можливі способи та методи дій диверсійно-терористичних груп та їх технічних способів дій. На основі цих досліджень вибирають методи та засоби протидії, тощо.

Людський чинник в системі забезпечення безпеки інформації і ІП відіграє значну роль, оскільки саме тут розв'язують низку запобіжних задач, таких як:

- перевірка працівників, які влаштовуються на роботу;
- розроблення та реалізація заходів із вивчення особового складу обслуговуючого персоналу, особливо тих, в діях яких є загроза інформації, яка охороняється;
- розроблення та реалізація заходів із забезпечення операції «чисті руки».

Що стосується досліджень вітчизняних та закордонних засобів несанкціонованого отримання інформації, які можуть бути застосовані зловмисником щодо цих дій, то тут аналізують способи застосування злочинними угрупуваннями видів цих засобів.

Тому тут розробляють методи та засоби їхнього виявлення, локалізації та знешкодження, паралельно оцінюють ефективність системи безпеки інформації.

Організація системи контрою доступу до інформаційних ресурсів ІП спрямована на реалізацію процедур оцінки прав на доступ до інформації користувача. Тому тут розв'язують задачі ідентифікації за сукупністю її загальних та особистих ознак і аутентифікації.

Окрім цих перерахованих задач, існують і інші, які можуть бути як загальносистемними, так і спеціальними.

Висновки

Взаємопов'язане розв'язання перерахованих вище задач системної концепції забезпечення безпеки інформації в ІП, в кожному з яких існують свої підходи, методи та способи їхнього вирішення, засоби захисту повинні забезпечити повністю. Тільки у такому разі можна говорити про виконання необхідних та достатніх умов у справі забезпечення безпеки інформації від підготовленого та технічного забезпеченого зловмисника. Але, оскільки абсолютного захисту бути не може, то в кожному випадку необхідні порівняльні оцінки витрат на захист інформації та можливі втрати, у разі відмови від застосування методів захисту інформації в ІП, вартість яких висока.

ЛІТЕРАТУРА

1.Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К.: Изд. «Юниор», 2003. – 504 с.

2.Юдін О.К. Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид. ТОВ «НВП», «ІНТЕРСЕРВІС», 2009. – 716 с.

3.Бурячок В.Л. Основи формування державної системи кібернетичної безпеки / Бурячок В.А. – К.: Вид НАУ, 2013. – 432 с.

4.Лепков С.В. Методы и средства защиты информации. В 2-х томах. / Лепков С.В., Перегудов Д.А., Хорошко В.А. – К.: Арий, 2008.

5. Емельянов С.Л. Проблема защиты информации от утечки и пути ее решения / Емельянов С.Л. – Одесса: Феникс, 2011. – 624 с.

Надійшла: 24.02.2014 р. Рецензент: д.т.н., проф. ТолюпаС.В.