*Література: **1**. NIST SP 800-53 Marianne Swanson, Nadya Bartol et al. Security Metrics Guide for Information Technology Systems. 2003. **2**. 2. Марка Д. А., МакГоуэл К. М. Методология структурного анализа и проектирования SADT. - М.: Метатехнология, 1993. - 240 с. **3**. A. Jøsang., S. J. Knapskog. A Metric for Trusted Systems. In Reinhard Posh, editor, Proceedings of the 15th IFIP/SEC International Information Security Conference. IFIP, 1998 **4**. A. Jøsang An Algebra for Assessing Trust in Certification Chains. In J. Kochmar, editor, Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999. **5**. Леншин А. В. Применение аппарата субъективной логики для оценки безопасности банковских ИТ-систем // Актуальні проблеми та перспективи розвитку фінансово-кредитної системи України: Збірник наукових статей. Харків: Фінарт, 2002, с. 410 – 412. **6**. Леншин А. В., Потий А. В. Применение оператора попарной усредненной конъюнкции для оценки уровня защищенности ИТ-систем // Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах", - Київ, 2003, с 57 – 58. 7. Потий А. В., Леншин А. В. Оценка защищенности информационно-телекоммуникационных систем с использованием математического аппарата субъективной логики //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р. **8**. Потій О.В., Лєншин А.В. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки //Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, Київ, 2004 р., с. 38-47. **9**. Потій О. В., Лєншин А. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації //Радиотехника. Тематический выпуск "Информационная безопасность", вып. 141, Харьков, 2005 г., с. 144-160. **10.** Потий А. В., Леншин А. В. Принципы построения системы экспертной оценки защищенности ИТ-систем «Советник» //Збірник наукових статей за матеріалами VI міжнародної науково практичної конференції "Безпека інформації в інформаційно-телекомунікаційних системах",.- Київ, 2003, с 25-26. **11.** Лєншин А. В., Потій О. В. Практичні рекомендації по використанню системи "Радник" при оцінці рівня організаційного захисту інформації в ІТС //VII Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р.*

УДК 681.3.06

СИСТЕМНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Олександр Архипов, Валерій Ворожко*

Національний технічний університет України „КПІ", Національна академія СЕ України

Анотація: **Розглядається застосування методології керування інформаційними ризиками для аналізу ефективності систем захисту державної таємниці.**

Summary: **Considered application of risk-management methodology for research on the state secret protection.**

Ключові слова: **Інформаційний ризик, державна таємниця, захист інформації.**

І Вступ

Державна таємниця (ДТ) - специфічна категорія таємних відомостей, умови віднесення інформації до якої та захист цієї інформації здійснюється відповідно до закону [1]. Процес глобальної інформатизації суспільства, що зараз триває, приніс для ДТ, як і для інших видів інформації з обмеженим доступом (ІзОД) певні проблеми, пов'язані із особливостями захисту ДТ в умовах нового інформаційного середовища. Вперше ці проблеми окреслилися наприкінці 60-х - на початку 70-х років двадцятого століття, а особливої актуальності набули в останні десять років через масоване впровадження в різних сферах діяльності сучасних інформаційних технологій.

За цей час техніка та методологія захисту інформації, пройшли довгий шлях розвитку – від окремих розрізнених нескладних механізмів захисту до системної концепції захисту, втіленням якої є цілеспрямоване використання комплексу організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів захисту інформації. Суть системної концепції - поєднання у найбільш раціональний спосіб усіх наведених вище заходів в певній організаційній формі - системі захисту інформації (СЗІ). Наскільки вдалим є це поєднання, як визначити рівень успішності функціонування СЗІ? Ці цілком природні в загальному випадку питання набувають особливої актуальності в разі, коли об'єктом захисту є ДТ, рівень важливості й,

відповідно, потрібний ступінь захисту якої є найвищим порівняно з іншими видами ІзОД.

Відповідь на зазначені вище питання стає можливою після введення системи певних формальних критеріїв якості (рівня) захисту, що його реалізує СЗІ, причому найбільш бажаною, універсальною й зручною формою цього критерію є кількісна, бо вона максимально спрощує аналіз та порівняння різних варіантів захисту, а в деяких випадках дозволяє оптимізувати вибір найкращого варіанту.

II Постановка задачі

Побудова СЗІ в загальному випадку являє послідовний розв'язок трьох задач: аналізу, синтезу та управління.

Зміст задачі аналізу - об'єктивне оцінювання загроз інформації й можливої шкоди від їх реалізації, задачі синтезу - визначення та використання найбільш ефективних механізмів захисту від загроз, що їх визнано значущими. Задача управління - забезпечення ефективного захисту інформації в часі і просторі на всіх етапах обробки та існування ІзОД в умовах змін оточуючого інформаційного середовища.

Втілення системної концепції захисту інформації на практиці стикається з рядом труднощів, головними з яких є потреба загальновизнаної єдиної базової методології узгодженого розв'язку задач аналізу, синтезу і управління, яка б забезпечила застосування для всіх цих задач єдиної системи критеріїв (показників), підпорядкованих спільній меті - досягненню потрібного рівня захисту ІзОД. Тут ми знов стикаємося з проблемою введення зазначених у Вступі формалізованих критеріїв якості СЗІ, універсальний характер яких має забезпечити проробку, співставлення, аналіз різних варіантів СЗІ та оптимізацію вибору кращого за умов визначеного рівня захисту.

Аналіз публікацій з питань захисту інформації, матеріалів науково-дослідних робіт та практичних розробок СЗІ, вивчення змісту міжнародних, регіональних, національних галузевих нормативних документів та стандартів [2 – 5] дозволяє стверджувати, що в якості подібної системної методології може бути використано підхід, відомий як оцінювання та керування інформаційними ризиками [6, 7]. Спираючись на цей підхід, можна визначити, що входить до складу ІзОД, яка потребує захисту, оцінити необхідний ступінь захисту ІзОД, обрати стратегію розвитку інформаційної структури організації й підтримувати на відповідному рівні її безпеку. Розглянемо можливість та перспективи застосування методології оцінювання та керування інформаційними ризиками для аналізу ефективності систем захисту ДТ.

III Основна частина

Суть методології оцінювання ризиків полягає в співставленні вихідного та залишкового ризиків для ІзОД, які розраховуються через оцінки можливих збитків, що можуть виникнути внаслідок ймовірної реалізації загроз ІзОД до (вихідний ризик R) або після (залишковий ризик *г*) впровадження СЗІ. За результатами співставлення робиться висновок щодо доцільності використання тих чи інших механізмів захисту ІзОД, їх ефективності та ефективності функціонування СЗІ в цілому.

В формальному представленні маємо:

$$R_i = P_i Q_i \qquad r_i = p_i P_i Q_i$$

де P_i - ймовірність реалізації /-ої загрози, Q_i - втрати (в грошових або умовних одиницях), обумовлені реалізацією /-тої загрози щодо ІзОД, p_i - ймовірність реалізації /-тої загрози після впровадження СЗІ через наявність вразливості в системі захисту щодо цієї загрози. Маючи ризики R_i *9* $г_i$, можна оцінити ефективність захисту ІзОД від і-тої загрози:

$$E_1 = (R_i - r_i)/R_i = 1 - p_i \tag{1}$$

де показник E_1 може змінюватися від 1 (випадок "абсолютної" захищеності від і-тої загрози, $r_i = 0$) до О (нульову ефективність захисту маємо у випадку $R_i = r_i$, тобто при абсолютній, стовідсотковій вразливості СЗІ щодо і-тої загрози). Ще одна форма функціоналу ефективності захисту має вираз

$$E_2 = R_i / r_i \tag{2}$$

Діапазон змін E_2 - від 1 (абсолютна неефективність) до нескінченності оо (абсолютно ефективний захист).

Показник ефективності захисту, який також має сенс показника доцільності введення механізму захисту, задається співвідношенням:

$$V_i = (R_i - r_i)/q_i = (1 - p_i)P_i Q_i / q_i \tag{3}$$

де q_i – оцінка вартості витрат на створення та впровадження механізму (механізмів) захисту проти ш-тої загрози.

Наведені вище вирази дають змогу оцінити ефективність фрагментарного захисту від окремої часткової

загрози. Однак інформація, що захищається, може зазнавати впливу ряду потенційних загроз, тому окрім аналізу часткових ризиків P_i, принциповим є визначення сукупної ймовірності P існуючої щодо ІзОД небезпеки й сукупного ризику R (відповідно значень p, r). Нарешті, якщо ІзОД складається з кількох окремих інформаційних ресурсів $\mathrm{IP}_1,...,\mathrm{IP}_m$, то об'єднання ризиків за всіма m складовими та розрахунок відповідного об'єднаного залишкового ризику дає змогу оцінити ефективність СЗІ за всім комплексом ІзОД. Визначивши загальносистемний ризик ідентифікаторами R_Σ, r_Σ, можна розраховувати за вже формулами (2), (3) показники $E_{\Sigma 1}, E_{\Sigma 2}$, що безпосередньо характеризують ефективність СЗІ. На жаль, проблема „згортання" часткових ризиків до загальносистемного на сьогодні математично строго не розв'язано. Для аналізу сукупних втрат від реалізації всієї множини загроз використовуються функціонали виду:

$$R_\Sigma = \sum_{i=1}^{n} P_i Q_i \tag{4}$$

де сума $\sum P_i Q_i$ може суттєво відрізнятися від 1, через що вони, на відміну від вживаного у математичній статистиці середнього ризику R, не мають прийнятної ймовірносної інтерпретації. Іноді, щоб формально наблизити R_Σ до R, суму у правій частині (4) домножують на множник $W = 1/\sum P_i$.

В практиці захисту ІзОД популярні системні показники ефективності СЗІ типу [12]

$$ROI = (R_\Sigma - r_\Sigma - q_\Sigma)/q_\Sigma \tag{5}$$

- показник повернення інвестицій (ROI – return on investment), q_Σ - загальні витрати на створення та обслуговування СЗІ, так звана сукупна вартість володіння (TCO - total cost of ownership), або

$$V_\Sigma = (R_\Sigma - r_\Sigma)/Q \tag{6}$$

де знаменник Q може бути вельми різним за змістом. Це, зокрема, загальна вартість певного об'єкту інформаційної діяльності (ОІД), де циркулює ІзОД, вартість ІзОД та інформаційних послуг з її обробки, загальна вартість інформаційних ресурсів, що їх задіяно в інформаційно-аналітичній системі, яку захищає СЗІ тощо.

Системні показники на зразок V_Σ дають змогу співставити витрати на створення СЗІ на ОІД (або інформаційно-аналітичній системі), яка забезпечує певні вимоги до рівня захисту ІзОД, із загальноекономічними характеристиками ОІД (чи показниками інформаційної діяльності, що ним забезпечується).

Можливість врахування аспекту економічної доцільності в задачі синтезу СЗІ є вельми привабливою й разом з тим актуальною особливістю аналізу та керування інформаційними ризиками, зокрема в умовах сучасної ринкової економіки. Тому цей підхід починають широко застосовувати як методологію побудови СЗІ різні бюджетні структури (в автоматизованих системах (АС), інформаційно-телекомунікаційних системах (ІТС), інформаційно-аналітичних системах тощо), а також структури, орієнтовані у своїй діяльності на міжнародні стандарти у сфері інформаційної безпеки, наприклад, заклади банківської галузі. Однак застосування методології інформаційних ресурсів для системи захисту ДТ суттєво обмежено.

Можливою причиною цього є існуюче уявлення про некоректність введення поняття залишкового ризику для СЗІ в сфері ДТ. Так в ДСТУ 3396.1-96. "Технічний захист інформації. Порядок проведення" робіт в розділі 3.2. постановка задачі захисту ІзОД, що складає ДТ, формулюється наступним чином: „досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності", що можна трактувати як гарантування $p_t = 0$ за будь-яку вартість q_i. Очевидно, така декларативна постановка задачі аж ніяк не відповідає сьогоднішній реальності і стимулює ситуацію, коли особа, відповідальна за захист інформації, може небезпідставно стверджувати, що ретельно відслідковуючи вимоги чинних нормативів та керівних документів, стовідсотково гарантує захист ДТ.

Наразі реальну ситуацію із рівнем захисту ІзОД можна, хоча, певно, дуже приблизно, оцінити, спираючись на наведені в чисельних літературних джерелах аналітичні відомості про залежність ефективності СЗІ від сумарних витрат на її функціонування. Так в [8] зазначається, що для досягнення ефективності захисту ІзОД в 50% витрати на захист повинні досягати 10% вартості інформаційної системи, а ефективність в 90% - 15-20% вартості. В [7, стор.18] наведено фактично аналогічні відомості: за твердженням експертів-практиків, оптимум в питанні захисту ІзОД, який дозволяє почувати себе в цьому аспекті достатньо впевнено, досягається при витратах на СЗІ в 10-20% від загальної вартості інформаційної

системи.Дещо іншу залежність наведено в [9]: витрати на захист інформаційних ресурсів в більшості випадків не повинні перевищувати 10% від їх вартості.

Крім того, в уже цитованому вище джерелі [7], але на стор. 87, йдеться про додаткові асигнування на безпеку інформації в розмірі 5-15% від суми коштів, що витрачаються на підтримку роботи інформаційної системи. Очевидно, що в наведених вище двох групах джерел мова йде про різні речі: в [8], [7, стор. 18] загальна сума, від якої нараховуються відсотки на СЗІ - це вартість основних засобів таких підприємств як АС, ІТС та їм подібних, які за своїм базовим, головним призначенням орієнтовані на обробку, передачу, накопичення та зберігання даних з ІзОД, а в [7, стор. 87], [9] нарахування відсотків йде на сумарний обсяг фінансування робіт, що проводяться на підприємстві, в науковому закладі, наприклад, науково-дослідних розробок, результатом яких буде створення певного інформаційного продукту (ресурсу).

В наведених джерелах мова йде про захист конфіденційної інформації, тому цитовані оцінки слід вважати нижньою межею витрат #Е на захист ДТ. Отже приблизна оцінка мінімально потрібних асигнувань на СЗІ для відомостей, що становлять ДТ, дорівнює $q_{\Sigma} = 20\%Q$.

Ще одним прикладом невідповідності практики захисту ДТ принципам системного аналізу є традиційне обмеження аналізу загроз ДТ тільки загрозами витоку секретної інформації або загрозами несанкціонованого доступу (НСД) до неї, тоді як загрози знищення, модифікації та немотивованого обмеження доступу фактично не оцінюються. Остання із зазначених загроз - це за своєю суттю загроза необгрунтованого віднесення інформації до ДТ. За оцінками, наведеними в [10], втрати через необгрунтоване закриття інформації в 70-80 рр. в колишньому СРСР доходили до кількох десятків мільярдів рублів. Ці збитки виникли через втрату вигоди від:

- нереалізованих впроваджень та нереалізованого продажу радянських технологій за кордон;
- заборони продажу промислових виробів, військової техніки та озброєння,
- а також через відсутність, внаслідок необгрунтованого віднесення відповідної інформації до ДТ, взаємодії та координації між підприємствами, що проводили розробку нових технологій.

Таким чином несистемне, звужене сприйняття загроз щодо ДТ призводить до однобічної, необ'єктивної оцінки відповідних інформаційних ризиків і далі трансформується у цілком реальні економічні збитки. Слід зауважити, що в законі України [1] у тексті ст. 9 серед завдань, покладених на державного експерта під п.1) записано: „визначає: ... доцільність віднесення до ДТ інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора;...". Однак в методичних рекомендаціях державним експертам [11] відсутні будь-які згадки про необхідність проведення порівняльного аналізу зокрема та аналізу збитків (інформаційних ризиків) через втрату вигод від відкритого використання інформації, що є предметом експертизи, а також внаслідок обмеження доступу до цієї інформації зацікавлених осіб або продажу відповідних інформаційних продуктів. Тобто в діючих методичних рекомендаціях [11] маємо редукцію системного аналізу інформаційного об'єкту, що експертується, до аналізу лише інформаційних ризиків внаслідок розголошення інформації про об'єкт експертизи.

IV Висновки

В середині 90-х 20-го сторіччя серед множини питань, пов'язаних із забезпеченням захисту ІзОД, найбільш пророблением та впорядкованим в плані нормативно-правового, організаційного та технічного забезпечення було питання захисту ДТ. На жаль, нині, на фоні загального динамічного розвитку систем захисту інформації, інтенсивної гармонізації національної нормативної бази із світовими та європейськими стандартами у галузі інформаційної безпеки, ситуація в сфері захисту ДТ виглядає стабільно консервативною, відстороненою щодо сприйняття і використання нових напрямів, технологій та ідей в галузі захисту ІзОД. Зокрема це стосується системного підходу до оцінювання ефективності функціонування систем захисту ДТ і в першу чергу питання введення формалізованих критеріїв та показників ефективності, відсутність яких виключає можливість об'єктивної оцінки рівня захисту ДТ, достатність залучених до захисту ДТ ресурсів.

*Література: **I.** Закон України „Про державну таємницю" (Відомості Верховної Ради (ВВР), 1994, № 16, ст. 93). **2.** 1nformation Technology - Practice for Information Security Management. International Standard ISO/IEC 17799:2000(E). **3.** Information Security Management. Part 2. Specification for Information Security Management systems. British Standard BS 7799, Part 2. 2000. **4.** CRAMM v. 4.0 User's Guide. **5.** Risk Management Guide for Information Technolog Systems, NIST, Special Publication 800-30. **б.** Симонов С. В. Методология анализа рисков в тформационньїх системах// Конфидент. Защита информации. - № 2. - 2001. - с. 48 - 53. **7.** Петренко С. А., Симонов С. В. Управление информационньши рисками. Зкономически оправданная безопасность. М.:*

Компания Ай Ти; ДМК Пресе, 2004. - 348с. ***8.*** *Андрощук Г. А., Крайнєє П.П. Зкономическая безопасность предприятия: защита коммерческой тайньї. - К: Изд. Дом «Ин Юре», 2000. – 400 с.* ***9.*** *Гринберг А. С., Горбачев Н. Н., Тетяков А. А. Защита информационньїх ресурсов государственного управлений. - М.: Юнити-ДАНА, 2003. – 327 с.* ***10.*** *Фатьянов А. А. Проблеми защитьг конфиденциальной информации, не составляющих государственную тайну//Информационное общество. - № 1. – 1997. - с. 49 - 56.* ***11.*** *Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності. Затверджено Держкомсекретів України, наказ №2 3 від 9. 02. 1998 р.* ***12.*** *Гостев И.М. Безопасность - бесполезная трата денег или их выгодное вложение?// Конфидент. Защита информации. - № 5. - 2003. - с. 16 - 18.*

УДК 65.012.8:330.131.5

МЕТОДИКА ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Светлана Гришко, Сергей Резников

Харьковский национальный университет радиоэлектроники

Аннотация: **Предлагается методика оценки экономической эффективности для комплексной системы защиты информации. Она позволяет определить ценность информации, находящейся в данной организации, оценить возможный ущерб от различных действий злоумышленника, сравнить разные варианты защиты и выбрать оптимальное соотношение по принципу «цена-качество».**

Summary: **The method of estimation of economic efficiency for the complex system of defence of information is offered. It allows to define the value of information being in this organization; to estimate possible harm from different actions of malefactor; to compare different variants of defence and choose optimum correlation on the principle «price-quality».**

Ключевые слова: **Эффективноссть защиты информации, стоимость защиты информации, информмационная ценность.**

Введение

Для функционирования любой структуры, будь то государственная, предпринимательская или общественная организация, необходимы разнообразные ресурсы: материальные, трудовые, финансовые. Но в современных условиях все большее значение приобретает еще один вид ресурсов – информационный. Специфика информации, как и любого другого нематериального актива, состоит в том, что она не имеет материальной формы и, как правило, жесткой привязки к носителю, а ее хищение может быть произведено путем простого копирования, т. е. без физического изъятия объекта.

Такие особые свойства, а также ценность информационного ресурса заставляет уделять все больше внимания вопросам защиты информации. Для их решения требуются значительные финансовые средства.

Поэтому в сфере обеспечения безопасности информации возникает классическая **проблема экономической эффективности –** поиск оптимального соотношения затрат и результатов. Здесь это означает, что нужно найти наилучшее сочетание организационно-технических решений по защите информации с затратами на их осуществление.

Вопросы экономической эффективности давно и детально исследовались как отечественными, таки и зарубежными специалистами. Можно выделить такие основные направления экономического обоснования:

- обоснование экономической эффективности некоммерческих инновационных проектов, которое проводится на основе сопоставления капитальных и эксплуатационных затрат, определения срока окупаемости; такая методика, в частности, рассматривается в [1, 2];

- обоснование экономической эффективности инвестиционных проектов, которое проводится на основе таких показателей: чистый приведенный доход, индекс доходности, индекс рентабельности; на наш взгляд, этот подход лучше всего рассмотрен в [3], кроме того, существует и нормативный документ для такого обоснования – методика [4].

Эти хорошо известные подходы не могут быть применены к оценке эффективности системы защиты информации. Они рассматривают в качестве результата от внедрения предлагаемых решений **изменение качества объекта** - например, улучшение технических характеристик, прирост дохода, экономию ресурсов. В нашем случае результатом будет **сохранение качества объекта**, отсутствие (или уменьшение)