корреляционной обработки.

2 Увеличение постоянной составляющей в сигналах амплитудных спектров мощности формант после корреляционной обработки подтверждает выражение (6). Изменение постоянной составляющей спектров формант пропорционально дисперсии отфильтрованного некоррелированного шума $sh(t)$.

Проведенные эксперименты позволяют сделать вывод об увеличении точности представления сигналов фонем после корреляционной обработки.

Выводы

Полученные результаты позволяют сделать вывод о целесообразности применения предложенного корреляционного алгоритма анализа фрагментов речевого сигнала при идентификации абонента с целью увеличения точности и эффективности идентификации.

Повышение точности идентификации достигается за счет уменьшения стохастической шумовой составляющей $sh(t)$ исходного речевого сигнала $s(t)$ путем расчета его АКФ $Rss(\Delta t)$ на интервале идентификации. Эффективность обработки повышается в результате обработки массивов данных с половинной размерностью на времени Tr.

При расчете линии регрессии АКФ на интервалах идентификации можно, в дальнейшем, применять математический аппарат множественного корреляционного анализа.

Литература: ***1****. Михайлов В. Г., Златоустова Л. В. Измерение параметров речи /Под ред. М. А. Сапожкова.- М.: Радио и связь, 1987. – 168 с.* ***2****. Алдошина И. А. Основы психоакустики // Звукорежиссер. – 2000. - № 6. – С. 36 - 40.* ***3****. http://www.speechpro.com/.* ***4****. Новосельский А. Ф., Жариков Ю. Ф. Программный пакет VIS для идентификации по голосу //Тезисы докладов 8-й Международной конференции "Информатизация правоохранительных систем". – М.: 1999. – С. 323-324.* ***5****. Вокодерная телефония. Методы и проблемы. Под ред. А. А. Пирогова –М.: Связь, 1974. - 536 с.* ***6.*** *Цвикер Э., Фельдкеллер Р. Ухо как приемник информации. Пер. с нем. под ред. Б. Г. Белкина.- М.: Связь, 1971. – 225 с.* ***7****. Рабинер Л., Шафер Р. Цифровая обработка речевых сигналов. -М.: Радио и связь, 1981. – 496 с.* ***8****. Бабак В. П. та ін. Обробка сигналів – К.: Либідь, 1996. – 392 с.* ***9****. Липцер Р. Ш., Ширяев А. Н. Статистика случайных процессов. М.: Наука, 1974. – 386с.* ***10****. Гоноровский И. С. Радиотехнические цепи и сигналы: Учебник для вузов. -М.: Радио и связь, 1986. - 512 с.*

УДК 681.321;322:621.395

ФУНКЦІОНАЛЬНО-ВАРТІСНИЙ АНАЛІЗ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Володимир Кононович, Тетяна Тардаскіна*

Академія зв'язку України, Одеський регіональний центр ТЗІ ВАТ "Укртелеком",

**Одеська національна академія зв'язку*

Анотація: **Розглядаються моделі і задачі функціонально-вартісного аналізу системи забезпечення інформаційної безпеки телекомунікаційних мереж загального користування з урахуванням положень міжнародних стандартів МСЕ-Т Х.800, Х.805. Пропонуються оцінки економічної ефективності системи забезпечення інформаційної безпеки окремих об'єктів мережі.**

Summary: **In the article are considered models and tasks of functionally-value analysis of ensuring information security system of the telecommunication network which based on ITU-T Recommendation X.800, X.805, assessments of economic effectiveness ensuring information security system their separate objects are proposed.**

Ключові слова: **Інформаційна безпека, телекомунікаційні мережі, технічна і економічна ефективність, загрози, послуги, механізми безпеки.**

І Вступ

Забезпечення достатнього рівня інформаційної безпеки телекомунікаційних мереж загального користування (ТМЗК) можливе лише на основі комплексного підходу до побудови системи забезпечення інформаційної безпеки (СЗІБ) [1] на всіх стадіях і етапах життєвого циклу СЗІБ, включаючи її створення

та експлуатації. Процес забезпечення інформаційної безпеки споріднений процесам управління якістю телекомунікаційних послуг та економічною ефективністю. Цей процес включає такі етапи, як виявлення критеріїв захищеності від різного роду впливів, гарантій коректності реалізації послуг безпеки інформації, які реалізуються СЗІБ, показників якості, до яких входить інформаційна безпека телекомунікаційних послуг, та техніко-економічних показників. Вимоги до забезпечення інформаційної безпеки ТМЗК встановлені Законом України "Про телекомунікації" та іншими нормативно-правовими актами [2, 3], які передбачають створення перешкод для будь-якого несанкціонованого втручання у процес функціонування мереж, забезпечення захисту від спроб викрадення, модифікації, виведення з ладу або знищення компонентів мережі, а також забезпечення захисту від викрадення, знищення, перекручення, блокування, несанкціонованого витоку інформації та від порушення встановленого порядку її маршрутизації. Безпечна телекомунікаційна мережа має бути захищена від зловмисних й ненавмисних атак, бути надійною, масштабованою, забезпечувати гарантований час відповіді, доступність послуг та інформації, цілісність інформації та обладнання та точність білінгової інформації. Численність показників захищеності, гарантій коректності реалізації, якості, факторів телекомунікаційних технологій, складність взаємодії між ними та їх взаємовпливу, наявність обмежень технічного, технологічного, організаційного та економічного характеру, необхідність оцінки ступеня ризику реалізації загроз на етапі прийняття рішень визначають необхідність застосування методів системного і функціонально-вартісного аналізу. Задача такого аналізу та оцінки ефективності СЗІБ ТМЗК залишається поки що невирішеною [4 – 7] і є актуальною.

Метою даної роботи є аналіз застосування моделей функціонально-вартісного аналізу СЗІБ телекомунікаційних мереж загального користування з урахуванням рекомендацій стандартів міжнародного союзу електрозв'язку (МСЕ) та оцінки економічної ефективності СЗІБ окремих об'єктів ТМЗК.

II Моделі функціонально-вартісного аналізу системи забезпечення інформаційної безпеки телекомунікаційних мереж

Показники захищеності, гарантій, якості та взаємопов'язані з ними техніко-економічні показники формуються на різних стадіях життєвого циклу СЗІБ в різних етапах проектування, створення та експлуатації. Задачі функціонально-вартісного аналізу можна розділити на три класи: детерміновані задачі, коли вихідні дані моделі є повністю визначеними; стохастичні задачі, коли у вихідній інформації є елементи невизначеності, або деякі параметри носять випадковий характер з відомими імовірнісними характеристиками, або частина параметрів має якісний характер і оцінюється експертними методами за допомогою якісних шкал та методів нечіткої логіки; комбіновані детерміновано-нечіткі задачі, коли серед вхідних параметрів присутні як повністю визначені або стохастичні параметри, наприклад, параметри технічних каналів витоку, так і нечіткі параметри, наприклад, показники захищеності, які забезпечуються механізмами захисту від несанкціонованого доступу. Задачі функціонально-вартісного аналізу СЗІБ ТМЗК відносяться до третього класу. Складність їх вирішення полягає у труднощах виявлення та аналізу впливу різноманітних факторів. Телекомунікаційні мережі можна класифікувати як надскладні системи, що постійно розвиваються в напрямі мультисервісності та поліфункціональності. На даному етапі головним напрямом розвитку телекомунікацій є перебудова (шляхом поступового заміщення) традиційної телефонної мережі загального користування в мережі наступного покоління (Next Generation Network - NGN), для яких характерною є перевага пакетизації мереж, перш за все на магістральному рівні, над цифровізацією. Спостерігається припинення інвестування систем комутації каналів і перехід на комутацію пакетів. Інформаційна безпека телекомунікаційних мереж має забезпечуватись в умовах інтеграції інформаційних та телекомунікаційних технологій і застосовуватись до радіо, оптичних і металевих голосових ліній зв'язку та передачі даних, а також в умовах дії на мережах операторів різних форм власності. Захисту підлягають усі складові елементи телекомунікаційних мереж: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення інформаційної безпеки, оскільки вразливість будь-якої ланки мережі може створити проблеми для усіх її учасників – провайдерів, операторів і споживачів послуг.

Моделі функціонально-вартісного аналізу будуються за модульним принципом. В основі побудови моделі лежить поділ складного комплексу мережі між її кінцевими пунктами на окремі архітектурні компоненти інформаційної безпеки. МСЕ прийняв модель мережної безпеки, розроблену в Лабораторіях Белла, за основу нового стандарту забезпечення безпеки комп'ютерних та телекомунікаційних мереж, які передають інформацію за принципом "з кінця в кінець" – Рекомендація МСЕ X805 [8]. Ця Рекомендація являє собою повно функціональну багаторівневу наскрізну рамочну структуру. Основними її компонентами є: механізми захисту, які відносяться до конкретних аспектів забезпечення мережної безпеки, такі як автентифікація або цілісність даних, і охоплює ресурси, застосування мережі та інформацію користувачів; рівні захисту, які включають рівні інфраструктурний, послуг та застосувань, які

розрізняються з точки зору вразливостей, що мають блокуватись відповідно до вимог конкретного рівня; площини захисту, які охоплюють процеси менеджменту, мережного управління (сигналізації, контролю) з використанням різноманітних протоколів (наприклад, SIB та кінцевих користувачів, наприклад, організацію віртуальних приватних мереж). Рис. 1, який запозичено з [1, 8], ілюструє архітектуру інформаційної безпеки у телекомунікаційних мережах загального користування. Рисунок зображує концепцію захисту мережі механізмами захисту в кожній площині інформаційної безпеки з кожним рівнем забезпечення інформаційної безпеки, щоб протидіяти визначеним загрозам безпеці та щоб зменшити вразливості, які існують на кожному рівні та площині і, таким чином, послабити атаки на безпеку.

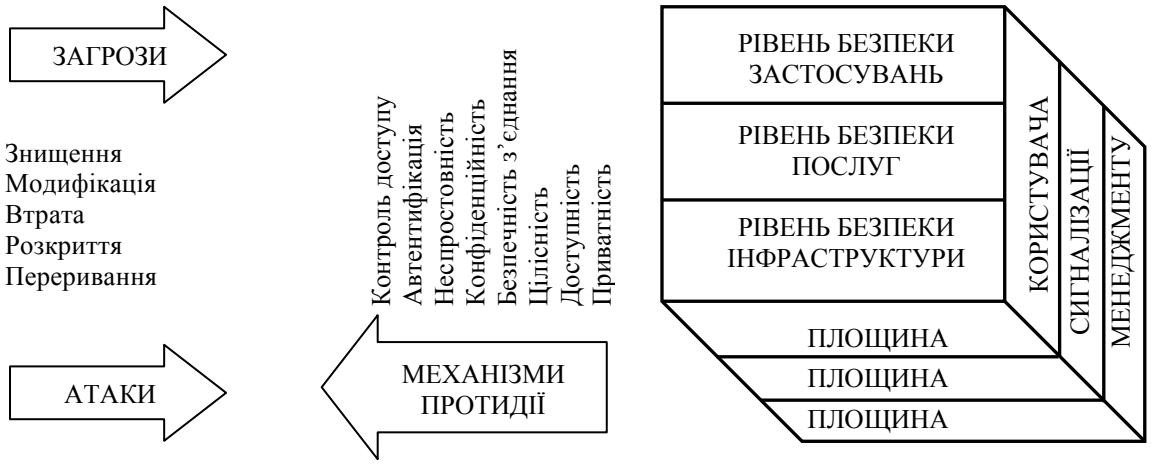

Рисунок 1 – Архітектура інформаційної безпеки телекомунікаційної мережі передачі інформації з кінця в кінець

Механізмами забезпечення інформаційної безпеки називають набір заходів безпеки, які захищають проти всіх головних загроз безпеки, підтримують політику безпеки, яка визначена для окремої мережі, і сприяють дотриманню набору правил менеджменту безпеки. Механізми інформаційної безпеки обмежуються мережею, а розповсюджуються на застосування, кінцевих користувачів та використовуються провайдерами служб або підприємствами, які надають послуги безпеки, маючи ліцензії на цей вид діяльності. Механізмами інформаційної безпеки є: керування доступом, автентифікація, неспростовність причетності до участі в обміні, конфіденційність даних, безпечність комунікацій (з'єднання), цілісність даних, доступність та приватність.

Механізми забезпечення інформаційної безпеки застосовуються для протидії певній множині загроз. У табл. 1 відображається низка загроз, яким протистоять кожен з механізмів інформаційної безпеки.

Таблиця1 – Матриця відповідності механізмів безпеки загрозам безпеки, яким вони протистоять

Механізми інформаційної безпеки	Загрози безпеці інформації та іншим ресурсам				
	Знищення	Спотворення чи модифікація	Крадіжка або втрата	Розкриття (компрометація)	Переривання послуг
Керування доступом	+	+	+	+	-
Автентифікація	-	-	+	+	-
Неспростовність	+	+	+	+	+
Конфіденційність	-	-	+	+	-
Безпечність з'єднання	-	-	+	+	-
Цілісність	+	+	-	-	-
Доступність	+	-	-	-	+
Приватність	-	-	-	+	-

Позначка "+" на перетині колонок та рядків таблиці позначає, що окремій загрозі безпеці протистоїть відповідний механізм інформаційної безпеки.

Механізми забезпечення контролю доступу захищають проти неавторизованого використання ресурсів мережі. Контроль доступу гарантує, що лише авторизованим суб'єктам або пристроям дозволений доступ до елементів мереж, інформації, інформаційних потоків, послуг та застосувань. Зокрема, роле-

орієнтований контроль доступу забезпечує різні рівні доступу, який гарантує, що суб'єкти можуть отримати доступ і виконувати дії з елементами мереж, інформацією і потоками інформації, щодо яких вони уповноважені.

Механізми забезпечення автентифікації служать для підтвердження ідентичності взаємодіючих суб'єктів. Автентифікація гарантує валідність та законність об'єктів та суб'єктів, які беруть участь у взаємодії (приміром, осіб, пристроїв, служб або застосувань) і забезпечує гарантію, що суб'єкт не робить спробу маскараду (маскування під авторизованого користувача) або неправомочного повтору попереднього зв'язку.

Механізми забезпечення неспростовності участі в обміні забезпечують засоби для попередження спроби відмови суб'єкта від виконаних специфічних дій відносно даних, а також доступності доказів різних дій, зв'язаних з телекомунікаційною мережею (таких, як доказ зобов'язання, намірів або вручення, доказів авторства (джерела) даних, володіння, використання ресурсу). Ці механізми гарантують доступність свідчень, які можуть бути подані третьою стороною і використані для доказу, що мав місце деякий випадок або деякий наслідок події.

Механізм забезпечення конфіденційності даних захищає дані від неавторизованого розкриття. Конфіденційність даних гарантує, що зміст даних не може бути зрозумілим неавторизованому суб'єкту. Для забезпечення конфіденційності даних часто використовуються методи шифрування, списки контролю доступу і допустимих файлів.

Механізми забезпечення безпечності зв'язку гарантують, що потоки інформації протікають лише між авторизованими кінцевими пунктами, що інформація не витікає або не перехоплюється із інформаційного потоку між цими кінцевими пунктами.

Механізми забезпечення цілісності даних гарантують коректність або точність даних. Дані захищені від неправомочної модифікації, видалення, створення та копіювання даних і, крім того, забезпечується індикація цих неправомочних дій.

Механізми забезпечення доступності гарантують, що події, які впливають на мережу, не призводять до відмови від авторизованого доступу до елементів мережі, інформації, інформаційних потоків, послуг і застосувань. У цю категорію включені засоби відновлення після катастроф, аварій та відмов обладнання телекомунікаційної мережі.

Механізми забезпечення приватності (Privacy) забезпечують захист інформації, яка може бути отримана від спостереження за функціонуванням мережі. Прикладом такої інформації можуть бути WEB-сторінки, які відвідав користувач, географічне місце розташування користувача, IP-адреси або DNS-імена пристроїв в телекомунікаційній мережі провайдера послуг. У вітчизняних нормативно-правових документах сфери ТЗІ механізми забезпечення приватності не визначаються, що певно є наслідком відсутності в Україні традицій недоторканості приватної власності. Але Конституцією України, Законом України "Про телекомунікації", (стаття 9), Ліцензійними умовами [9, 10] та іншими нормативними актами закріплена норма захисту таємниці зв'язку, "забезпечення конфіденційності інформації, яка стосується споживача, забезпечення і відповідальності за схоронність відомостей щодо споживача, отриманих при укладені договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, їх оплати, маршрутів передавання тощо" [9]. Механізми забезпечення приватності інформації щодо споживача мають застосовуватись навіть в тому випадку, коли договором не передбачається надавання послуги забезпечення конфіденційності інформації споживача.

III Методичний підхід до забезпечення інформаційної безпеки

Методичний підхід до інформаційної безпеки телекомунікаційної мережі полягає у розгляді кожного механізму безпеки на кожному рівні забезпечення інформаційної безпеки та в кожній площині інформаційної безпеки. Утворюється дев'ять модулів безпеки, кожен з яких комбінує вісім механізмів безпеки, які застосовуються до окремого рівня забезпечення безпеки в окремій площині інформаційної безпеки. При цьому ясно, що залежно від вимог до даної мережі, можливо не потрібно мати всі запроваджені архітектурні елементи, тобто інколи не потрібно мати повний набір механізмів безпеки, рівнів забезпечення інформаційної безпеки або площин забезпечення інформаційної безпеки. Сказане ілюструється розподілом механізмів безпеки за рівнями моделі архітектури взаємодії відкритих систем (ВВС) та площинами моделі мереж наступного покоління, який наведено в табл. 2.

Площини архітектури мережі наступного покоління NGN приведені відповідно до [11]. Площина абонентського доступу базується на трьох середовищах передачі: металевому кабелі, оптоволокні та радіоканалах. В площині комутації реалізується комутація пакетів та/або (на перших етапах) комутація каналів і знаходиться структура мультисервісних вузлів доступу. Площину програмного управління складають програмні комутатори (Softswitch). Верхня площина забезпечує реалізацію інтелектуальних

послуг та експлуатаційного управління.

Таблиця 2 – Розподіл механізмів безпеки за Рекомендаціями МСЕ X.800, X.805 та моделлю мереж наступного покоління

Механізми безпеки		Площини моделі мереж наступного покоління						
		Абонентського доступу		Комутації	Програмного управління		Інтелектуальних послуг та експлуатаційного управління	
Рекомендації МСЕ		Рівні моделі архітектури ВВС						
X.800	X.805	1	2	3	4	5	6	7
Керування доступом		Ні	Ні	Так	**Так**	Ні	Ні	**Так**
Обмін автентифікацією		Ні	Ні	**Так**	**Так**	Ні	Ні	**Так**
Цифровий підпис	Неспростовність	Ні	Ні	**Так**	**Так**	Ні	Ні	**Так**
Нотаріальне засвідчування		Ні	Ні	Ні	Ні	Ні	Ні	Так
Шифрування	Конфіденційність	**Так**	**Так**	**Так**	**Так**	Ні	**Так**	**Так**
Заповнення трафіка	Безпечність з'єднання	**Так**	Ні	**Так**	Ні	Ні	Ні	**Так**
Контроль маршрутизації		**Так**	**Так**	**Так**	**Так**	Ні	**Так**	**Так**
Цілісність (даних та ресурсів)		Ні	Ні	**Так**	**Так**	Ні	Ні	**Так**
-	Доступність	**Так**	**Так**	**Так**	**Так**	Ні	**Так**	**Так**
-	Приватність	Ні	Ні	**Так**	**Так**	Ні	Ні	**Так**

Розподіл послуг безпеки за рівнями моделі архітектури ВВС подано згідно з Рекомендаціями МСЕ X.200, X.800 [12, 13]. Інформаційна безпека будується на принципах ієрархічної безпеки. Безпека забезпечується на кожному з рівнів моделі ВВС і функціональні послуги безпеки розподілено за цими рівнями. У моделі ВВС виокремлюються сім рівнів опрацювання інформації: 1 – фізичний; 2 – канальний; 3 – мережний; 4 – транспортний; 5 – сеансовий; 6 – представний; 7 – прикладний. Кожен рівень виконує певні завдання та функції й забезпечує умови функціонування суміжних рівнів. Згідно з міжнародними рекомендаціями служби безпеки в мережі будуються за ієрархічним багаторівневим модульним принципом: служба безпеки – сервіси безпеки – функціональні послуги безпеки – механізми безпеки. Деталізація розподілу механізмів безпеки подається в Рекомендації МСЕ X805, у якій розглядаються архітектурні елементи, що можуть забезпечити інформаційну безпеку для систем передачі інформації з кінця в кінець.

Для забезпечення інформаційної безпеки телекомунікаційних мереж з кінця в кінець механізми безпеки повинні застосовуватись до ієрархії обладнання мережі з групуванням їх у сімейства засобів, які описуються як рівні забезпечення безпеки. У свою чергу, на кожному з рівнів функціонують деякі типи механізмів інформаційної безпеки, які кваліфікуються як площини інформаційної безпеки.

Визначено такі ієрархічні рівні мережно-орієнтованих засобів забезпечення інформаційної безпеки: рівень забезпечення інформаційної безпеки інфраструктури, рівень забезпечення безпеки послуг, рівень забезпечення безпеки застосувань. Рівні забезпечення інформаційної безпеки є послідовністю взаємозалежних засобів безпеки мереж: рівень забезпечення безпеки інфраструктури взаємозалежить від рівня забезпечення безпеки послуг, а рівень забезпечення безпеки послуг взаємозалежить від рівня забезпечення безпеки застосувань. Кожен рівень має різні уразливості безпеки. Механізми інформаційної безпеки застосовуються до рівнів забезпечення безпеки, щоб зменшити вразливості, які існують на кожному рівні та, таким чином, послабити атаки на безпеку. На кожному з рівнів пропонується така гнучкість механізмів протидії потенційним загрозам, яка найбільш придатна для окремого рівня інформаційної безпеки. В Рекомендації МСЕ X.805 підкреслюється, що всі три рівні забезпечення інформаційної безпеки можуть бути застосовані до кожного з семи рівнів моделі ВВС, оскільки кожен рівень моделі ВВС має свою інфраструктуру, надає свої послуги і має свої застосування.

Рівень забезпечення інформаційної безпеки інфраструктури телекомунікаційної мережі складається із засобів обслуговування передачі інформації мережею, а також індивідуальних елементів мережі, захищених за допомогою механізмів інформаційної безпеки. Рівень інфраструктури складається з основних блоків мереж, служб та застосувань. Прикладами компонентів, які належать до рівня

інфраструктури, є індивідуальні маршрутизатори, комутатори та служби, а також канали зв'язку між індивідуальними маршрутизаторами, комутаторами та серверами.

На рівні інфраструктури мережі можна виділити три типи концепцій побудови захисту: "бар'єрного" (захисту периметра), "лінійного" і "розподіленого". Вузли зв'язку, прикінцеві системи зосереджені на порівняно невеликій території і мають систему захисту, побудовану по принципу „кругової оборони" чи захисту периметра. Всі об'єкти, які захищаються, розташовані в захищеному фізичному середовищі на території, що охороняється. З теоретичних положень технічного захисту інформації відомо, що найслабша ланка, яка не блокована організаційними і/або організаційно-технічними чи криптографічними засобами, визначає результуючий рівень захищеності.

Систему "лінійного" захисту можна було б розглядати як крайній випадок сильно витягнутої "бар'єрної" системи захисту. Але "лінійний" захист має суттєву відмінність від "бар'єрного". Системи передавання, канали, магістральні лінії характеризуються своєю протяжністю і проходять незахищеним середовищем. Системи захисту в них або розподіляються вздовж лінії, або побудовані за принципом „компенсації". У останньому випадку засоби захисту сконцентровані на прикінцевих (або транзитних) пунктах і забезпечують, так би мовити „компенсацію" загроз у незахищених ланках тракту передавання інформації. Так, система передавання зі зворотним зв'язком має на прикінцевому пункті засоби прийняття рішення про втрату цілісності інформації та формування запиту на повторне передавання помилкового блоку. Не всі послуги безпеки можна здійснювати методом "компенсації". Приміром, порушення доступності при DoS-атаках не може бути компенсоване у прикінцевому обладнанні, якщо нема обхідних шляхів для встановлення з'єднання. Найчастіше захист за "компенсаційним" принципом використовується при забезпеченні конфіденційності.

Концепція "розподілених" систем захисту має застосовуватись в IP-мережах. Поняття каналу передавання в таких мережах розмите. Тракт передавання може не закріплюватись за одним повідомленням. Повідомлення поділяється на пакети, кожен з яких може передаватись довільним маршрутом. Віртуальні канали створюються не для всіх повідомлень. Рівень захищеності такої мережі буде визначатись захищеністю найбільш слабкого маршруту з усіх можливих маршрутів. А захищеність маршруту визначається його найслабкішою ланкою.

Рівень забезпечення інформаційної безпеки послуг відноситься до інформаційної безпеки служб, які провайдери послуг забезпечують їх клієнтам. Ці послуги надаються як транспортні функції та підключення до служб, які дають забезпечення доступу до телекомунікаційної мережі або до Інтернет (наприклад, сервіс автентифікації, авторизації та спостережності (AAA), сервіс динамічної конфігурації хоста, сервіс доменних імен тощо), до додаткових служб типу телефонної служби, служби якості сервісу (QoS), віртуальних приватних мереж (VPN), послугам місця розташування, термінового передавання повідомлень тощо. Рівень інформаційної безпеки послуг використовується для захисту провайдерів послуг та їх клієнтів, які є потенційними цілями загроз безпеки. Для прикладу, нападаючі можуть спробувати блокувати можливості провайдера послуг, або можуть спробувати переривати можливість обслуговування індивідуальних клієнтів.

Рівень забезпечення інформаційної безпеки застосувань зосереджений на безпеці мережне-базованих застосувань, доступних клієнтам провайдера послуг. Ці застосування дають змогу мережним службам та центрам даних виконувати функції транспорту (передачі) файлів (FTP) і застосувань web browsing, довідкові функції управління, передачі голосових повідомлень та e-mail, а також високо рівневі функції, такі як керування телекомунікаціями користувача, електронна комерція, дистанційне навчання, відео конференції тощо. На цьому рівні є такі потенційні цілі для атак на безпеку: застосування користувача, застосування провайдера та служба провайдера.

Площина інформаційної безпеки – це деякий тип механізмів інформаційної безпеки, що функціонують у захищеній мережі. Визначаються такі площини безпеки інформації для представлення трьох типів захищеного функціонування, яке має місце у мережі: площина безпеки менеджменту, площина безпеки сигналізації та контролю, площина безпеки кінцевого користувача. Ці площини безпеки характеризують специфічні потреби інформаційної безпеки, пов'язані з виконанням менеджменту мережі, організацією контролю і сигналізації мережі, та відповідними діями кінцевого користувача. Мережі повинні проектуватись таким чином, щоб події на одній площині безпеки були б повністю ізольовані від подій у інших площинах безпеки. Наприклад, потік запитів до служби доменних імен (DNS) у площині кінцевого користувача, ініційованих запитами кінцевого користувача, не повинні блокувати інтерфейс керування, адміністрування, технічного обслуговування та забезпечення (OAM&P) у площині менеджменту, який дозволяв би адміністратору виправляти проблему. Кожен тип описаних функцій мережі має свої власні специфічні потреби безпеки. Концепція площин інформаційної безпеки дозволяє диференціювати специфіку безпеки відносно пов'язаних з ними дій і можливістю розглядати їх незалежно. Наприклад, у

службі передачі голосу за допомогою IP (VoIP) послуги служби безпеки розподіляються за рівнями таким чином, що захист менеджменту служби VoIP (приміром обслуговування користувачів) повинен бути незалежним від захисту служби контролю та сигналізації (наприклад, протоколу типу SIP), а також бути незалежним від захисту даних (голосу) кінцевого користувача, які транспортуються мережею.

В *площині забезпечення безпеки менеджменту* розглядається захист функцій OAM&P у елементах мережі, засобах обслуговування передачі, системі надавання базових послуг (системі підтримки функціонування, системі підтримки бізнесу, системі піклування про клієнта тощо), та центрах даних. Площина менеджменту підтримує функції надійності, працездатності, адміністрування, постачання (забезпечення) та безпеки (FCAPS). Підмережа, яка передає трафік у інтересах менеджменту, може бути спільно канальною та зовнішньо канальною відносно трафіка користувача.

В *площині забезпечення безпеки контролю та сигналізації* розглядається захист функцій, які забезпечують ефективну доставку інформації, послуг та застосувань через мережу. Сюди включаються функції керування встановленням з'єднання, які дозволяють вузлам комутації (наприклад, комутаторам і маршрутизаторам) визначати найкращі маршрути для трафіка через основну транспортну мережу. Цей тип інформації називають контрольною або сигнальною інформацією. Підмережа, яка передає контрольно-сигнальну інформацію, також може бути спільно канальною або зовнішньо канальною відносно трафіка користувача. Для прикладу, IP мережі несуть керуючу інформацію в пакетах, тобто всередині каналу, тоді як у комутованих телефонних мережах загального користування (PSTN) керуюча інформація передається в окремих (зовнішньо канальних) системах сигналізації (SS7). Трафік такого типу включає протоколи маршрутизації DNS, SIP, SS7, Megaco/H.248, H.242 тощо.

Площина забезпечення безпеки кінцевого користувача направлена на забезпечення безпеки доступу та безпеки використання мережі провайдера послуг клієнтами. Ця площина також описує дійсні потоки даних кінцевого користувача. Кінцевий користувач може використовувати мережу, яка забезпечує тільки з'єднання (комутацію), або використовувати додатково служби типу VPNs, або може використовувати доступ до мережне-базованих застосувань.

Модульна структура інформаційної безпеки може застосовуватись до будь-якої мережі на будь-якому рівні протокольного стеку. Наприклад, в IP-мережі, яка реалізується на трьох рівнях протокольного стеку, рівень інфраструктури описує індивідуальні маршрутизатори, канали зв'язку типу "точка-точка" між маршрутизаторами і серверні платформи для забезпечення підтримки служб, необхідних у IP-мережі. Рівень послуг відноситься до основної служби безпосередньо (таких, як здатність підключення до Internet), IP підтримує служби (такі, як AAA, DNS тощо) та просунуті додаткові служби, які пропонує провайдер послуг (такі, як VoIP, QoS, VPN, тощо). Нарешті, рівень застосувань описує безпеку застосувань користувача, до яких надається доступ через IP-мережу типу e-mail.

Аналогічно, для мережі з асинхронним методом переносу (ATM), яка позиційована на двох рівнях протокольного стеку, рівень інфраструктури описує індивідуальні комутатори та канали зв'язку типу "точка-точка" між комутаторами. Рівень послуг описує різні класи пропонованих засобів транспорту (постійної швидкості передавання, змінної швидкості передавання в режимі реального часу, змінної швидкості передавання не в режимі реального часу, доступну швидкість передавання і не специфіковану швидкість передавання). Нарешті, рівень застосувань стосується використання кінцевим користувачем мережі ATM для доступу до застосування типу відео конференцій.

IV Методика функціонально-вартісного аналізу

Методика функціонально-вартісного аналізу забезпечує послідовне уточнення оцінок при переході від початкових стадій та етапів життєвого циклу до наступних: розробки та планування, реалізації та впровадження, техобслуговування та підтримки. Програма забезпечення інформаційної безпеки містить в собі політику безпеки, процедури реагування на інциденти, плани відновлення тощо, а також процедури реалізації технології інформаційної безпеки протягом стадій формування технічного завдання та проектування СЗІБ. Кінцевою метою є вибір ефективних засобів протидії загрозам при реалізації системи інформаційної безпеки, вартість витрат на яку не перевищує вартість втрат, очікуваних від реалізації загроз. На етапі реалізації функціонально-вартісний аналіз є основою для оцінки інформаційної безпеки. В продовж стадії експлуатації мереж реалізована програма забезпечення інформаційної безпеки має підтримувати поточну інформаційну безпеку при змінах навколишнього середовища, допомагати в керуванні політикою та процедурами безпеки, в реагуванні на інциденти та в планах відновлення системи інформаційної безпеки.

У склад функціонально-вартісного аналізу входять: оцінка захищеності ресурсів та гарантій, оцінка технічної і економічної ефективності та задачі підвищення рівня ефективності (рис. 2). Основними методами оцінки є розрахунково-аналітичний (інструментальний), експертний, імітаційний. Оцінка захищеності, техніко-економічної ефективності та підвищення рівня ефективності проводяться на основі

єдиної інформації, яка включає: результати стадій функціонально-вартісного аналізу, фактори ризику та фактори які впливають на показники, показники функціонально-вартісного аналізу, нормативно-правова база. Стадії функціонально-вартісного аналізу поділяються на проектні, реалізації та впровадження і експлуатаційні, що охоплює весь життєвий цикл СЗІБ до стадії утилізації включно.

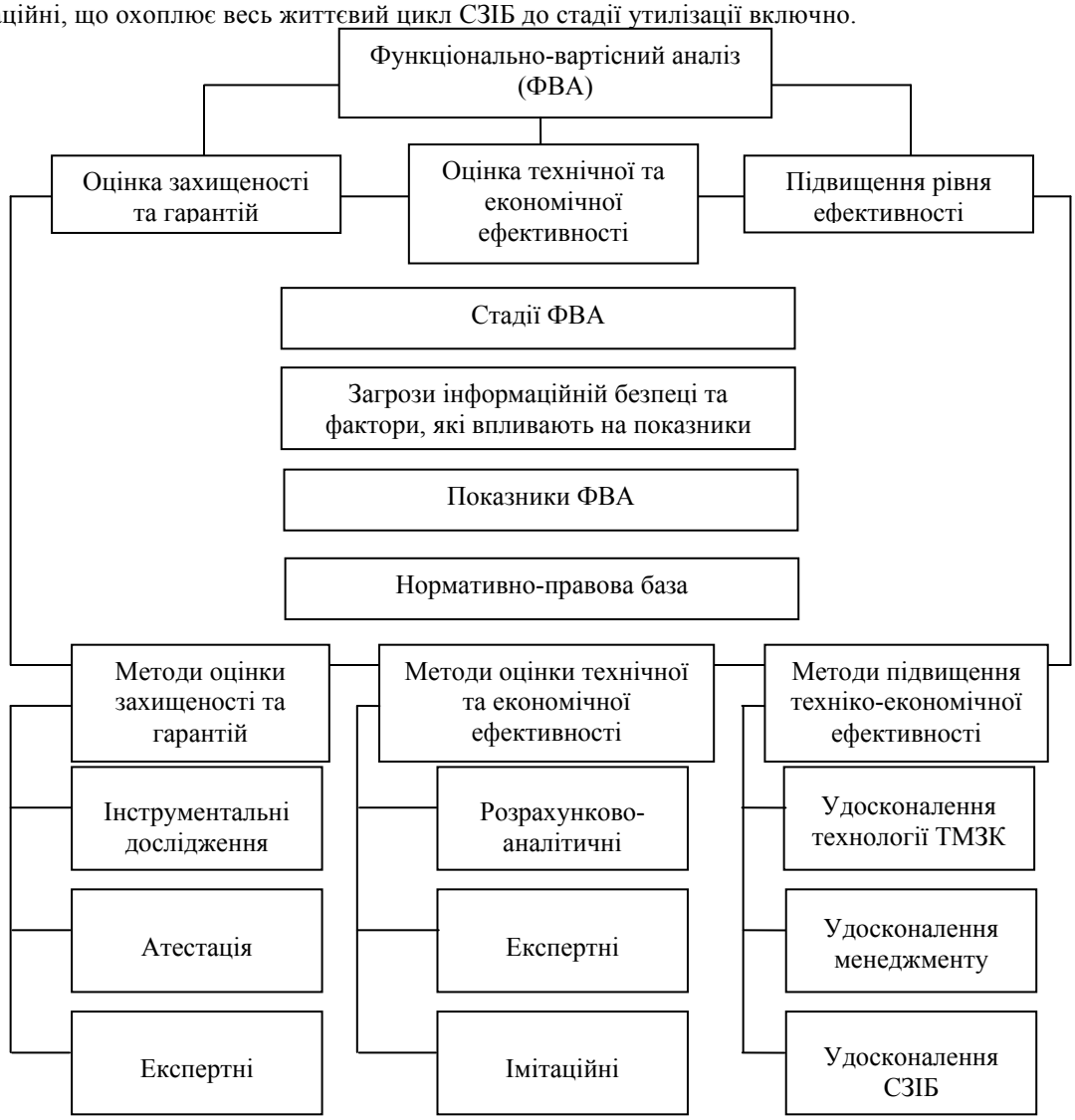

Рисунок 2 – Задачі функціонально-вартісного аналізу СЗІБ ТМЗК на різних стадіях

Стадіями функціонально-вартісного аналізу є:

- проектні;
  - наукові дослідження;
  - проектування;
- дослідні експлуатації;
- передавання до будівництва (технологічність);
- впроваджувальні (будівничі);
- передавання до експлуатації (випробування);
- експлуатаційні;
  - технічне обслуговування;
  - відновлення після атак, аварій та відмов;
  - зняття з експлуатації та утилізація.

Показники та обмеження функціонально-вартісного аналізу поділяють на якісні, структурні та кількісні. До показників відносяться: працездатність, захищеність, гарантії реалізації, функціональна повнота, комплексність, ергономічність, технологічність, сертифікованість та атестованість. Кількісні

показники можна поділити на матеріальні, часові, вартісні.

Фундаментом функціонально-вартісного аналізу є нормативно-правова база. З точки зору забезпечення безпеки інформації, комплекс засобів захисту можна розглядати як набір функціональних послуг, що в сукупності створюють необхідний функціональний профіль захисту. Кожна послуга являє собою набір функцій, які дозволяють протистояти певній множині загроз. Політику безпеки може бути здійснено з використанням різних механізмів, окремо чи в комбінації, залежно від об'єктів політики. Загалом механізми належатимуть до одного з трьох класів, які можуть перетинатись: запобігання, реєстрування, відновлення. Вибір раціональних варіантів, оптимальне планування захисту, оцінку ефективності проектування та експлуатації СЗІБ можна здійснити на базі науково та технічно обґрунтованих норм, які відповідають сучасному рівню техніки та технології.

Економічний ефект від впровадження системи забезпечення інформаційної безпеки (СЗІБ) пропонується розраховувати за такою формулою:

$$E_c = \sum_{t=0}^{T} (\Delta П_t - Bn_t + A_t) \times (1+E)^{-t} - \sum_{t=0}^{Tc} Kc_t \times (1+E)^{-t} \ , \qquad (1)$$

де: $\Delta П_t$ – величина збитку, якому запобігає СЗІБ, у році t після впровадження (грн); Bn_t – експлуатаційні витрати на підтримання системи забезпечення інформаційної безпеки (СЗІБ) у році t, (грн.); A_t – амортизація на реновацію у році t, яка обумовлена капіталовкладеннями (грн.); Kc – сумарні витрати на проектування, створення, впровадження СЗІБ та її експлуатації та підтримки у році t (грн.); T_C – період створення, впровадження системи менеджменту інформаційної безпеки; T – період дії атестованої СЗІБ; E – норма дисконтування; t – рік, результати і витрати якого приводяться до початкового моменту часу.

Величина Ec відображає ефективність застосування, забезпечену за період t. При оцінюванні ефективності впровадження СЗІБ необхідно враховувати усю систему інформаційної безпеки і проводити підсумовування за всіма її модулями.

Таким чином, методи функціонально-вартісного аналізу мають бути динамічними, з нарощуванням деталізації та зменшенням невизначеності за стадіями реалізації проектів: технічного завдання, техно-робочого проекту, дослідних випробувань, експлуатації. При створенні СЗІБ методами функціонально-вартісного аналізу вирішуються такі групи задач: пошук технічних та програмних рішень, оцінка захищеності та гарантій реалізації, вибір раціональних (оптимальних) рішень. Методи оцінки ефективності вибору варіантів побудови системи інформаційної безпеки мають забезпечити виконання політики інформаційної безпеки телекомунікаційних мереж та прийнятний рівень інформаційної безпеки при допустимій величині витрат. Складність цих задач залежить від типів і складності об'єктів ТМЗК. Для простих об'єктів оцінка захищеності і економічної ефективності може бути проведена методом експертних оцінок, заснованих на чинній нормативно-правовій базі. При функціонально-вартісному аналізі складних вузлів мережі та мережі в цілому оцінка захищеності є важкою задачею і її вирішення може бути досягнуто при застосуванні адекватних методів колективної роботи експертів. Оцінка захищеності інформаційних ресурсів пов'язується із задачами моніторингу інформаційної безпеки телекомунікаційних мереж з метою одержання статистики експлуатації СЗІБ.

Висновки

Функціонально-вартісний аналіз на всіх стадіях життєвого циклу СЗІБ ТМЗК дозволяє виділити область раціональних рішень та сформувати проектні процедури знаходження оптимальних рішень. Напрямком подальших досліджень може бути розробка практичних методик аналізу по кожному модулю СЗІБ, удосконалення методів та засобів постійного моніторингу інформаційної безпеки МЗК з метою накопичення та аналізу статистик, розробка методик оцінки ефективності СЗІБ МЗК та відповідних техніко-економічних обґрунтувань.

Література: ***1.*** *Кононович В. Г., Тардаскіна Т. М., Гладиш С. В. Розподіл ресурсів інформаційної безпеки телекомунікаційних мереж загального користування. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 10, 2005. С 62-68.* ***2.*** *Закон України "Про телекомунікації" (від 18. 11. 2003 р).* ***3.*** *Тардаскін М. Ф., Кононович В. Г. Правові засади інформаційної безпеки телекомунікаційних мереж // "Зв'язок", № 4, 2004. С.35-38.* ***4.*** *Кононович В. Г., Тардаскін М. Ф., Тардаскіна Т. М. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікаційних систем. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С 62-68.* ***5.*** *Хорошко В., Ковальова Ю., Плус Д. Розподіл ресурсів у багаторубіжній системі*

захисту."Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 39-43. ***6.*** *Кононович В. Г., Тардаскіна Т. М. Алгоритм розподілу ресурсів інформаційної безпеки документальних телекомунікацій. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, 2004. С 152-161.* ***7.*** *Носов В., Манжай А. Метод проектирования оптимальной системы защиты информации. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 94-103.* ***8.*** *ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. С. 28.* ***9.*** *Ліцензійні умови провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного міжміського, місцевого зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку" (наказ Держкомзв'язку № 132 від 17. 06. 2004 р.), С. 25.* ***10.*** *Ліцензійні умови провадження діяльності у сфері телекомунікацій з технічного обслуговування і експлуатації мереж ефірного теле- та радіомовлення та телемереж, надання в користування каналів електрозв'язку" (наказ Міністерства транспорту та зв'язку України № 984 від 10. 11. 2004 р.) С. 20.* ***11.*** *Тесля В. Я., Бабосюк А. Л., Сикорский В. В., Рудниченко А. Е. Концептуальные подходы к технологии сетей нового поколения NGN // "Зв'язок", № 2, 2004. С.70-73.* ***12.*** *ITU-T Recommendation X.200. Reference model of open systems interconnection for CCITT applications. Geneva. 1991. С. 75; (Стандарт ISO 7498-1:1984. Базова модель ВВС).* ***13.*** *ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. Geneva.1991. С. 48; (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС).*

УДК 621.395:338.47

ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ АСПЕКТИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тетяна Тардаскіна

Одеська національна академія зв'язку ім. А. С. Попова

Анотація: **Розроблено організаційні рекомендації управління персоналом системи інформаційної безпеки.**

Summary: **Development organizational recommendation personal management of information security system.**

Ключові слова: **Інформація, інформаційна безпека, управління персоналом, кадровий консалтінг.**

Вступ

Проблема захисту мереж телекомунікацій та інформації, що циркулює в них, вимагає великої уваги в зв'язку з тим, що в інформаційному суспільстві, до якого прагне Україна, захист інформаційного середовища стає таким же важливим для кожного громадянина, суспільства і держави, як і захист навколишнього середовища, власного майна.

В Україні до інформаційних ресурсів прийнято відносити технічну інфраструктуру й інформацію, що в ній обробляється, циркулює і зберігається. Недостатня увага приділяється колосальному пласту питань, який впливає на забезпечення безпеки інформаційних систем: діяльність персоналу, адміністративна і юридична підтримка. Проблема захисту ускладнюється тим, що загрози, від яких доводитися захищати мережі та інформацію, дуже різноманітні і мають навіть різне походження: природне, техногенне, антропогенне. Однак для загроз природного, техногенного та ненавмисного антропогенного походження прогноз частково можливий, а наслідки рідко корелюються із діями або інформацією користувачів, тому рідко бувають катастрофічними. Принципи захисту від таких загроз відомі, і, як правило, їх можна реалізувати під час розробки, впровадження та експлуатації мереж телекомунікацій [1]. Ця проблема вирішувалась у багатьох суміжних областях безпеки, управління та прийняття рішень [2 – 7], але відносно управління персоналом системи інформаційної безпеки така задача остаточно не вирішена.

Слід відзначити, що багато питань інформаційної безпеки вже вирішуються системою технічної експлуатації, системою управління електрозв'язком, системою управління якістю та менеджменту телекомунікацій. Але це стосується в основному протидії техногенним загрозам інформаційним ресурсам. Антропогенні загрози враховуються мало. Водночас, необхідність управління персоналом тісно пов'язана з захистом комерційної таємниці фірми, бо персонал є одним з основних носіїв інформації, і як вважають фахівці, імовірність витоку інформації через підкуп, переманювання співробітників складає 43%, а через вивідування – 24%. Найнепередбачуваніші загрози виникають внаслідок навмисної, особливо зловмисної антропогенної діяльності, саме захист від таких загроз найбільш складний і потребує особливої уваги при