Выводы

Информация и поддерживающие ее системы и сети являются ценными ресурсами. Из-за растущей зависимости организаций от информационных систем они становятся более уязвимыми. Использование систем защиты информации позволяет в большей или меньшей степени решить эту проблему, но требует определенных финансовых средств. Предложенная методика позволяет:

1) определить ценность информации, находящейся в данной организации;

2) оценить возможный ущерб от различных действий злоумышленника;

3) сравнить разные варианты КСЗИ и выбрать оптимальное соотношение по принципу «цена-качество».

*Литература **1**. Плоткин Я. Д., Львов Д. С. Зкономическая зффективность новой техники. - Львов, 1986, - 143 с. **2**. Методичні вказівки до розрахунку соціального-економічної ефективності заходів науково-технічного прогресу./Марченко О І. - ВІГІ, 1991. 3. Бланк И. А. Инвестиционный менеджмент - К.: Эльга-Н, Ника-Центр, 2001.- 448 с. **4**. Методика визначення економічної ефективності витрат на наукові дослідження і розробки та їх впровадження у виробництво, затверджена наказом Мінекономіки та європейської інтеграції N 218/446 від 25.09.2001 **5**. ГОСТ 12.1.004-91. Пожарная безопасность **6**. НД ТЗИ 1.1–003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. 7. Маркс К. Капитал / Маркс К., Энгельс Ф. Собрание сочинений в 30-ти томах, 2-е изд., Т.23.- М.: Госполитиздат, 1954. **8**. Fisher I. Mathematical Investigation in the Theory of Value and Prices. - N. Haven.: Gale Univers Press, 1977. - 126 p. **9**. Хикс Дж. Р., Аллен Р. Г. Пересмотр теории ценности // Теория потребительского поведения и спроса // Под ред. В. М. Гальперина. - СПб.: Экономическая школа, 1993. - 383с. **10**. Friedman M. Price Theory. A Provisional Text. - Addine: Publishing Company, 1967. - 285 p. **11**. Самуэльсон П. Экономика: Пер. с англ. - М.: Прогресс, 1964. - 844с.*

УДК 621.395:396.77

ОЦІНКА ВИТРАТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ЦИФРОВИХ СИСТЕМ КОМУТАЦІЇ

Тетяна Тардаскіна

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

Анотація: **Орієнтовна оцінка витрат на систему інформаційної безпеки типової цифрової системи комутації проводиться на етапі її технічного проектування.**

Summary: **Aproximate assessment costs of information security system of the standard digital switched systems is held on the stage of technical projection**

Ключові слова: **Інформація, інформаційна безпека, оцінка витрат, функціональні послуги зв'язку.**

Вступ

Законом України «Про телекомунікації» визначені ключові завдання забезпечення інформаційної безпеки телекомунікаційних мереж: охорона таємниці телефонних розмов, телеграфної, іншої кореспонденції, захист інформації з обмеженим доступом, що є власністю держави; захист державних інформаційних ресурсів, захист інформації про споживача; захист інформації, що передається телекомунікаційними мережами; забезпечення сталості, надійності, інформаційної безпеки телекомунікаційних мереж, підтримки рівня якості та безпеки телекомунікаційних послуг [1].

Система інформаційної безпеки телекомунікаційних мереж може бути ефективною, якщо витрати на її створення та управління будуть принаймі менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку маршрутизації інформації.

Метою роботи є отримання орієнтовної оцінки витрат на систему інформаційної безпеки типового цифрового вузла комутації при його проектуванні на етапі складання ескізного та технічного проекту. Передбачається, що комплексна система захисту інформації цифрової системи комутації створюється згідно з пакетом нормативних документів системи технічного захисту інформації (ТЗІ) на програмно-керованих АТС загального користування [2 - 16].

Цифрові системи комутації (ЦСК), як правило, оснащуються штатними і, при необхідності,

додатковими позаштатними засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів ЦКС, тобто спроможності системи ТЗІ протистояти впливам загроз.

Типова модель загроз, що впливають на інформаційні ресурси, які підлягають захисту, перелік загроз, типова модель порушника докладно розглянуті в чинних нормативних документах [8, 11] та роботах фахівців УНДІЗ та ОНАЗ [16, 17]. Порядок виконання робіт визначено в [11].

На стадії проектування замовником розробляється підрозділ технічного завдання на будівництво ЦСК за назвою "Вимоги до ТЗІ у ЦСК", технічний та робочий проекти. На стадії розробки робочого проекта системи ТЗІ у ЦСК виконавцем розробляється КЗМЗ у ЦСК, як взаємопов'язаний набір засобів і механізмів захисту, що реалізують обрану модель захисту. Модель захисту розробляється на стадії технічного проектування як взаємопов'язаний набір функціональних послуг захисту з необхідними рівнями ефективності і стійкості реалізації цих послуг, при яких забезпечується заданий у технічному завданні рівень захищеності інформаційних ресурсів в ЦСК.

І Функціональні послуги зв'язку

Для визначення структури витрат на інформаційну безпеку розглянемо структуру системи ТЗІ в ЦСК, яка, в свою чергу, залежить від структури вимог до необхідного рівня захищеності інформаційних ресурсів. Приклад структури ТЗІ в ЦСК подано на рис. 1, де види забезпечення систем ТЗІ подані з різною глибиною деталізації. Глибина деталізації залежить від методу обчислення витрат. На рисунку прийняті такі позначення:

ТС – технологічне середовище;

ФПЗ – функціональні послуги захисту. ФПЗ є набір елементарних функцій, виконання яких у середовищі експлуатації ЦСК дозволяє протистояти певній множині загроз для інформації.

Засоби ТЗІ в ЦСК складаються із сукупності фізичних, технічних і програмних підсистем захисту, що функціонують на стадії її промислової експлуатації, системи організаційно-технічних та організаційно-адміністративних заходів, системи ліквідації наслідків реалізованих загроз для інформації на АТС, системи керування засобами ТЗІ.

Підсистеми захисту в ЦСК класифікуються за способами здійснення загроз і в сукупності мають забезпечувати реалізацію на практиці обраної моделі захисту з необхідними гарантіями. Програмні підсистеми захисту забезпечують реалізацію визначеної номенклатури функціональних послуг захисту. ФПЗ в ЦСК здійснюються за допомогою конкретних засобів і механізмів, що поділяються на штатні та додаткові.

Штатні засоби і механізми захисту інформації здебільшого вже закладені в архітектуру сучасних ЦСК або в систему їхньої технічної експлуатації. Додаткові засоби і механізми захисту розробляються й застосовуються у випадках, коли штатні не забезпечують необхідного рівня захищеності.

Номенклатура штатних ФПЗ складається з функцій захисту від:

- несанкціонованих впливів через штатні засоби доступу;
- позаштатних впливів через штатні основні або додаткові програмні і/або технічні засоби ЦСК;
- позаштатних впливів на параметри середовища експлуатації ЦСК;
- впливів на програми, дані і процеси в ЦСК з використанням позаштатних програмних і/або програмно-технічних засобів, що встановлені в процесі її експлуатації;
- впливів закладних пристроїв і програмних закладок;
- впливів позаштатними технічних і/або програмно-технічних засобів на елементи устаткування в процесі експлуатації ЦСК;
- витоків інформації через канали побічних електромагнітних витоків та наводів (ПЕМВН);
- витоків інформації через канали побічних акусто-електричних перетворень;
- якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються ЦСК;
- збоїв і відмов у роботі ЦСК;
- загроз у системах збереження інформації на фізичних носіях.

Крім того, в штатні ФПЗ входять ФПЗ ліквідації наслідків реалізованих загроз для інформації в ЦСК та керування засобами ТЗІ.

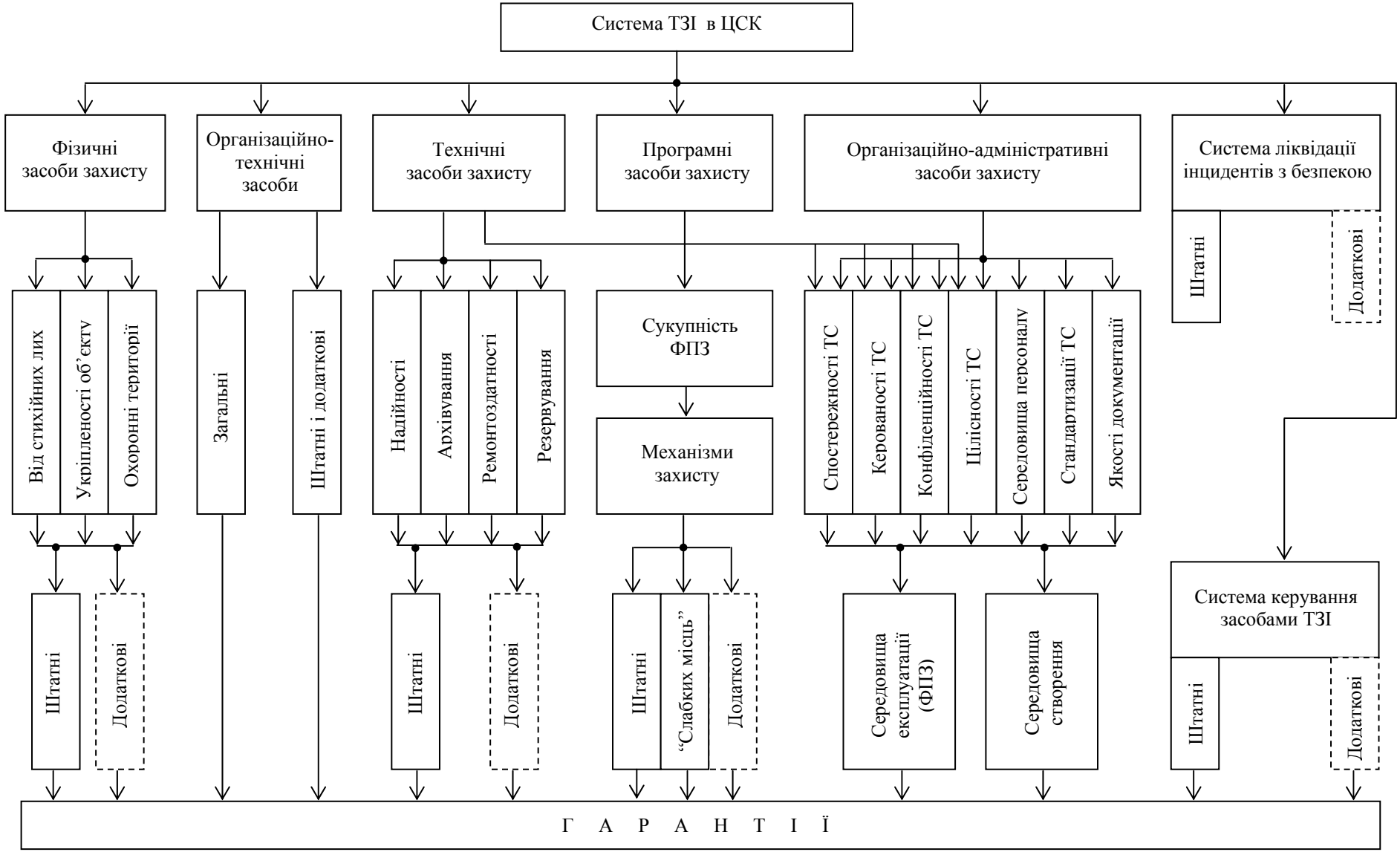

Рисунок 1 - Структура видів забезпечення системи ТЗІ в ЦСК

Технічні підсистеми захисту включають засоби підтримки надійності, архівування програм та даних, ремонтоздатності та резервування.

Система фізичних заходів захисту включає засоби укріпленості об'єкту, охорони території, засоби захисту від стихійних лих тощо.

Система організаційно-технічних заходів, що здійснюється на всіх стадіях життєвого циклу ЦСК, повинна знизити рівні кількісної і якісної недостатності компонентів і всієї ЦСК у цілому до можливих і/або припустимих значень.

Система ліквідації наслідків реалізованих загроз для інформації, що являє собою сукупність програмно-апаратних засобів і відповідних організаційних заходів, повинна знизити рівень втрат від реалізованих загроз для інформації до можливих і (або) припустимих меж.

Система керування засобами ТЗІ повинна забезпечувати безперервний контроль і підтримку певного рівня захищеності інформації в ЦСК на стадії її експлуатації.

Ресурси, що пов'язані з ТЗІ, включаються в об'єкти доступу і, отже, потребують захисту.

Система організаційно-адміністративних заходів разом з іншими системами захисту забезпечує гарантії захисту інформаційних ресурсів технологічних середовищ створення та експлуатації ЦСК. Ці гарантії необхідні для визначення рівнів довіри до коректності розробок, реалізацій та експлуатації систем ТЗІ в ЦСК. Оцінка рівнів довіри виконується відповідно до НД ТЗІ 3.7-002-99. Система гарантій включає п'ять аспектів забезпечення захищеності інформації в технологічному середовищі створення та експлуатації систем ТЗІ і ЦСК у цілому:

- гарантії безпеки середовища персоналу;
- гарантії стандартизації технологічного середовища;
- гарантії забезпечення спостережності і керованості технологічного середовища;
- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища;
- гарантії якості документації.

Кожен аспект деталізується на конкретні вимоги. Так, необхідно виконання низки вимог до безпеки середовища персоналу: вимоги до системи організації праці, до контролю системи організації праці, до поведінки персоналу та контролю поведінки персоналу в робочий та неробочий час. Для одержання гарантій забезпечення якості стандартизації технологічного середовища необхідно виконати вимоги: до повноти охоплення стандартами елементів середовища, до глибини охоплення стандартами технологій роботи в середовищі, до рівня значущості та взаємоузгодження. Для забезпечення гарантій якості документації необхідно виконати вимоги: до повноти документації, до рівня деталізації опису середовища і/або технологій, до вірогідності інформації, що міститься в документації та до якості оформлення документації.

Задоволення вимог до спостережності і керованості технологічного середовища та конфіденційності і цілісності інформаційних ресурсів технологічного середовища дозволяє реалізувати обраний функціональний профіль вимог до захищеності інформації в ЦСК.

Відповідно до принципу мінімальної достатності система захисту має бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для замовника системи ТЗІ, і тільки в тій мірі, у котрій необхідно нейтралізувати чи послабити, зменшити наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищили гранично припустимих рівнів.

На стадії технічного проектування розробляється модель захисту інформаційних ресурсів ЦСК. Вибір моделі захисту - це рішення задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів ЦСК. У результаті рішення визначається сукупність ФПЗ для реалізації КЗМЗ в системі ТЗІ.

Для вперше створюваних ЦСК спочатку виконується вибір системи з оглядом на реалізовані в ній ФПЗ таким чином, щоб мінімізувати вартість робіт із створення додаткових механізмів захисту, якщо в цьому виникає потреба. У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у ТЗ рівень захищеності інформації. Необхідно вибрати таку систему, штатні засоби захисту якої найбільш повним чином реалізовували б отриману за результатами технічного проектування модель захисту. Якщо тип ЦСК вже обрано, то виконується оцінка реалізованих у ній штатних ФПЗ на відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

Аналогічно, для штатних організаційно-технічних засобів і заходів (перепускний режим, охорона території, протипожежна сигналізація, кліматика тощо) проводиться оцінка достатньості рівня захищеності, які вони забезпечують. Додаткові засоби розробляються, якщо рівень захищеності та рівень

гарантій захищеності недостатній.

II Структура витрат на інформаційну безпеку

На цій стадії можна визначити структуру витрат на інформаційну безпеку. При цьому слід враховувати різницю в життєвих циклах штатних та додаткових засобів і механізмів захисту, а також їхню часткову реалізацію в існуючій системі технічної експлуатації ЦСК. Частина витрат на інформаційну безпеку на штатні заходи і засоби вже ввійшла у вартість системи, що постачається, а також у витрати в системі технічної експлуатації. Для штатних програмно-технічних засобів враховуються етапи життєвого циклу: проектування, тестування, атестація, експлуатація. Супроводження штатних програмно-технічних заходів - ФПЗ та механізмів захисту – входить у загальні витрати на технічну експлуатацію ЦСК. Деякі штатні ФПЗ та механізми захисту інформації залишились незадіяними в існуючій системі технічної експлуатації ЦСК і їх необхідно врахувати при обчисленні витрат на інформаційну безпеку.

Для додаткових засобів та механізмів захисту враховується повний життєвий цикл: пошук “слабких місць” та складання технічного завдання або технічних умов, проектування, створення, оцінка або тестування, атестація, супроводження, експлуатація.

Структура витрат на інформаційну безпеку в ЦСК показана в табл. 1

III Приклад розподілення витрат АТС за функціональними послугами зв’язку

Використаємо методику розрахунку собівартості послуг МТЗ, сформовану на основі чинної нормативно-правової бази з урахуванням системи управлінського обліку вітчизняних операторів телекомунікацій, яка наведена в [20]. Критерієм для розподілення усіх статей витрат пропонується взяти частку $ФЗП_{атс}$ (фонд заробітної плати працівників оператора телекомунікацій), які надають послуги АТС у загальному ФЗП оператора:

$$\text{dфзп атс} = \frac{ФЗП_{атс}}{ФЗП}. \qquad (1)$$

Таблиця 1 – Структура витрат на інформаційну безпеку в типовій ЦСК

№ п/п	Підсистема засобів та механізмів захисту інформації	Статті витрат						
		Пошук слабких місць	Проектування	Створення	Оцінка чи тестування	Атестація	Супроводження	Експлуатація
1	Штатні засоби фізичного захисту: укріпленості об’єкту, охорони території, захисту від стихійних лих тощо.	-	-	-	B_{14}	B_{15}	-	-
2	Додаткові засоби фізичного захисту	B_{21}	B_{22}	B_{23}	B_{24}	B_{25}	B_{26}	B_{27}
3	Штатні організаційно-технічні заходи підтримки надійності, архівування, резервування, ремонтоздатності.	-	-	-	B_{34}	B_{35}	-	-
4	Додаткові організаційно-технічні заходи	B_{41}	B_{42}	B_{43}	B_{44}	B_{45}	B_{46}	B_{47}
5	Штатні програмно-технічні заходи – ФПЗ та механізми захисту.	-	-	-	B_{54}	B_{55}	-	B_{57}
6	Додаткові програмно-технічні заходи – ФПЗ та механізми захисту.	B_{61}	B_{62}	B_{63}	B_{64}	B_{65}	B_{66}	B_{67}
7	Штатні організаційно-адміністративні заходи забезпечення гарантій безпеки середовища персоналу, стандартизації ТС, якості документації.	-	-	-	B_{74}	B_{75}	-	-
8	Додаткові організаційно-адміністративні заходи забезпечення гарантій безпеки.	B_{81}	B_{82}	B_{83}	B_{84}	B_{85}	B_{86}	B_{87}

9	Штатні організаційно-програмно-технічні заходи забезпечення гарантій спостережності і керованості ТС, конфіденційності і цілісності інформаційних ресурсів ТС.	-	-	-	$В_{94}$	$В_{95}$	-	$В_{97}$

Річний фонд заробітної плати за кожною j-ю ділянкою робіт визначається так:

$$ФЗП_{атсj} = З \cdot Ш_j(1 + Н_{фзп})12 \quad (2)$$

де *З* - середньомісячна заробітна плата по оператору телекомунікацій; $Ш_j$ - штат за j-ю ділянкою робіт; $Н_{фзп}$ - норматив відрахувань на соціальні заходи.

Частка фонду заробітної плати для кожної j-ї ділянки робіт розраховується за формулою:

$$\text{dфзп атсj} = \frac{ФЗП_{атсj}}{ФЗП_{атс}} \quad (3)$$

Амортизаційні відрахування за кожною j-ю ділянкою робіт обчислюються так:

$$А_{атсj} = d_{фзпатсj} \cdot А_{атс} \quad (4)$$

де $А_{атс}$ - амортизаційні відрахування по АТС.

Матеріальні витрати за кожною j-ю ділянкою робіт подаються у вигляді:

$$М_{атсj} = d_{фзпатсj} \cdot М_{атс} \quad (5)$$

де $М_{атс}$ - матеріальні витрати по АТС.

Інші операційні витрати за кожною j-ю ділянкою робіт визначаються так:

$$Е_{атсj} = d_{фзпатсj} \cdot Е_{атсін} \quad (6)$$

де $Е_{атсін}$ - інші витрати по АТС.

Під ділянкою робіт, у випадку розрахунку витрат на ЦСК, будемо розуміти створення та технічну експлуатацію ФПЗ. Далі розподіляються витрати ділянок (ФПЗ) відповідно до нормативного документа [8]. Середнє число робітників, зайнятих відновленням, методика розрахунку, наведена у [22] для ділянки (ФПЗ) 10 „Система захисту від збоїв та відмов у роботі АТС”

$$n_р = 1 - p_о. \quad (7)$$

Для 10 ділянки: $n_р = 0{,}001356$ 0,001356=1- $p_о$, $p_о = 0{,}998644$

Результати розрахунків витрат за ділянками робіт заносяться в табл. 2.

Оплата праці з відрахуваннями $ФЗП_{мтзj}$ визначається відповідно до нормативного штату АТС та середньої заробітної плати**.** Амортизаційні відрахування $А_{мтзj}$ визначаються відповідно до частки амортизаційних відрахувань у сумі витрат оператора або до частки амортизаційних відрахувань оператора у витратах на оплату праці оператора, за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт**.** Матеріальні витрати $М_{мтзj}$ визначаються відповідно до частки доходів від надання послуг АТС у сумі доходів оператора, або до частки матеріальних витрат оператора у витратах на оплату праці оператора, за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт [20].

Вихідні дані.

А. Розмір витрат за статтями по ділянкам робіт, грн. [20]:

- оплата праці з відрахуваннями ФЗП – 138087600;
- амортизаційні відрахування А – 630000,00;
- матеріальні витрати М – 460000,00;
- інші операційні витрати Е - 355000,00.

Б. Штат оператора телекомунікацій, залучений до надання ФПЗ, розрахований за нормативами чисельності штату, за ділянками робіт, осіб [8]:

- система захисту від впливів суб’єктів доступу через штатні термінали обслуговування і штатні прикінцеві пристрої - 0,45;
- система захисту від позаштатних впливів через штатні або основні або штатні додаткові програми і (або) технічні засоби - 0,3;
- системи захисту від позаштатних впливів на параметри середовища функціонування АТС - 0,3;

- система захисту від впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС - 0,7;
- система захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені в процесі її експлуатації -1,1;
- система захисту від впливів програмних закладок і (або) технічних закладних пристроїв, що встановлені на передексплуатаційних стадіях життєвого циклу АТС - 0,3;
- система захисту від витоків інформації через канали ПЕМВН - 0,3;
- система захисту від витоків інформації через канали побічних акусто-електричних перетворень - 0,3;
- система захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються АТС - 0,7;
- система захисту від збоїв та відмов у роботі АТС - 0,9986;
- система захисту від загроз у системах збереження інформації на фізичних носіях - 0,3;
- система ліквідації наслідків реалізованих загроз інформації на АТС - 1,1;
- система керування засобами ТЗІ - 1,0.

В. Середньомісячна заробітна плата - 839 грн.

Таблиця 2 – Розподілення витрат АТС за функціональними послугами зв'язку (ФПЗ)

Статті витрат	Номер j-ї ділянки роботи (ФПЗ)													
	Виробничий штат												Адміністр. штат	Усього
	1	2	3	4	5	6	7	8	9	10	11	12	13	
1.Оплата праці з відрахуван-нями ФЗПмтзj	6243	4162	4162	9711	15261	4162	4162	4162	9711	13854	4162	15261	13873	
2. Амортизаційні відрахування Амтзj	2835	1890	1890	4410	6961	1890	1890	1890	4410	6300	1890	6961	6325	
3. Матеріальні витрати Ммтзj	2070	1380	1380	3220	5083	1380	1380	1380	3220	4600	1380	5083	4618	
4. Інші операційні витрати Емтзj	1597	1065	1065	2485	3922	1065	1065	1065	2485	3550	1065	3922	3564	
5. Усього витрат	12745	8497	8497	19826	31228	8497	8497	8497	19826	28304	8497	31228	28381	222523
6. Структура витрат dфзп мтзj, %	5,73	3,82	3,82	8,91	14,03	3,82	3,82	3,82	8,91	12,72	3,82	14,03	12,75	100

Висновки

Витрати на штатні засоби і механізми інформаційної безпеки ЦСК на стадії її проектування і створення складають невелику частку загальних витрат. Вони включені у вартість систем, що постачаються, або у вартість будівництва об'єкту зв'язку. Витрати на інформаційну безпеку на стадії технічної експлуатації ЦСК можуть досягати 20 - 25% загальних витрат на цій стадії. Значна їхня частина вже врахована в

існуючій системі технічної експлуатації ЦСК.

Додаткові заходи і механізми забезпечення інформаційної безпеки, як правило, необхідні для досягнення високого рівня захищеності інформаційних ресурсів ЦСК. Для базового рівня захишеності доля витрат на додаткові засоби і механізми захисту може бути незначною. Найбільша доля витрат припадає на ділянки систему захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені в процесі її експлуатації (14%) та на систему ліквідації наслідків реалізованих загроз інформації на АТС (14%). Доцільність їх визначається на етапах оцінки захищеності інформаційних ресурсів та атестації КЗМЗ на відповідність вимогам системи технічного захисту інформації.

*Література: **1.** Тардаскін М. Ф. Особливості стратегії інформаційної безпеки цифрових автоматичних телефонних станцій // Зв'язок. – 2005. - № 1. – С. 31-33. **2.** ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. **3.** ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. **4.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. **5.** ДБН А.2.2-2-96. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва. Введено в дію 01.01.97 р. **6.** НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. **7.** НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. **8.** НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. 9. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. 10. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. **11.** НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. **12.** НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова). **13.** НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. **14.** НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. **15.** КНД 45-164-2001 Типова модель загроз для формування ресурсів цифрових АТС, що використовуються в мережах електрозв'язку загального користування України. **16.** Воробиенко П.П., Нечипорук О. Л., Щербина Ю. В. Модели угроз информационным ресурсам систем и сетей связи // Зв'язок. – 2003. - № 6. – С. 39-41. **17.** Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения моделей угроз информационным ресурсам систем и сетей связи // Правове нормативне та метрологічне забезпечення системи захисту інформації в Україні. К.: 2001, вип. 7. – С. 11-13. **18.** НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. **19.** НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супровадження і модернізації засобів технічного захисту інформації від несанкціонованого доступу. **20.** НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (Критерії базуються на аналізі Федеральних критеріїв США і критеріїв оцінки безпеки Канади). **21.** Князєва Н. О., Баландін І. О. Методика розрахунку собівартості послуг місцевого телефонного зв'язку // Зв'язок. – 2005. - № 1. – С. 9-15. **22.** КНД 45-076-98 Система автоматизованого телефонного зв'язку для мереж загального користування. Основні положення. Книга 1, книга 2. Київ. 2002. **23.** Демина Е. В., Иодко Е. К., Майофис Л. И., Резникова Н. П. Организация планирование и управление предприятиями связи.-М.: „Радио и связь", 1990.*

УДК 681.3

МЕТОДИКА ОЦІНКИ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ СИСТЕМ

Микола Будько
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонується методика оцінки загроз для інформації автоматизованих систем на основі аналізу моделей порушника, можливих каналів і видів загроз ресурсам автоматизованих систем, моделі загроз та методика аналізу можливих контрзаходів для забезпечення припустимої захищеності та залишкового ризику.**