сложных систем.– М.: Наука, 1982.– 286 с. ***7.*** *Зайченко Ю. П. Исследование операций: 6-е изд.– К.: Слово, 2003.– 688 с.* ***8.*** *Новиков А., Тимошенко А. Определение множества механизмов защиты, обеспечивающих оптимальный уровень защищенности информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– 2002.– вип. 4.– С.98 – 105.* ***9.*** *Сергиенко И. В. Математические модели и методы решения задач дискретной оптимизации.– К.: Наукова думка.– 1985. – 384 с.* ***10.*** *Сергиенко И. В., Лебедева Т. Т., Рощин В. А. Приближенные методы решения дискретных задач оптимизации.– К.: Наукова думка.– 1980. – 276 с.* ***11.*** *Geoffrion Arthur M. Integer Programming by Implicit Enumeration and Balas' Method // SIAM Review.– 1967.– Vol. 9, No. 2.– p. 178 – 190.* ***12.*** *Систематический каталог библиотеки численного анализа НИВЦ МГУ http://srcc.msu.su/num_anal/lib_na/cat/cat0.htm*

УД УДК 681.321;322:621.395

ФОРМУВАННЯ ВИМОГ ЩОДО БЕЗПЕКИ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Сергій Гладиш
Одеська національна академія зв'язку ім. О. С. Попова

Анотація: **Досліджується проблема проектування системи інформаційної безпеки в телекомунікаційній мережі загального користування, в якій обробляються і передаються державні інформаційні ресурси з різним режимом доступу та різними вимогами безпеки. Проведено аналіз вітчизняних та міжнародних нормативних документів. Визначена ієрархія понять щодо державних інформаційних ресурсів та їхньої безпеки. Розроблено вимоги до системи інформаційної безпеки.**
Summary: **The problem of information security system projecting in public telecommunication network, in which state information resources with different access mode and different security requirements are processed and transmitted, is researched. Ukrainian and international normative documents are analyzed. The hierarchy of terms concerning to state information resources and their security is defined. The requirements of information security system are developed.**
Ключові слова: **Державні інформаційні ресурси, інформаційна безпека, телекомунікаційні мережі.**

І Вступ

Загальна проблема забезпечення інформаційної безпеки (ІБ) в телекомунікаційних мережах загального користування (ТМЗК) в останній час стає все більш важливою. Така тенденція зумовлена рядом чинників, головними з яких можна назвати наступні:

– динаміка розвитку та широке розповсюдження інформаційно-комунікаційних технологій як у державному секторі (національна система конфіденційного зв'язку, електронний уряд, інфраструктура центрів сертифікації ключів та електронного цифрового підпису, електронне голосування, телемедицина, дистанційне навчання), так і в недержавному (стаціонарні та мобільні мережі зв'язку загального користування, Інтернет, електронна комерція, приватні та відомчі корпоративні мережі тощо);

– високі вимоги до показників якості, сталості та безпеки телекомунікаційних мереж (ТМ) як базової складової сучасних інформаційно-телекомунікаційних систем (ІТС);

– висока критичність ТМЗК як основного технічного ресурсу національного інформаційного простору держави та як складової глобальної інформаційної інфраструктури.

В умовах переходу до інформаційного суспільства, поширення міжнародного тероризму, розвитку концепції інформаційної війни та розробки інформаційної зброї підвищується значущість ІБ як важливого компонента безпеки суспільства. ІБ держави є невід'ємною складовою частиною національної безпеки України. На відміну від США, де з 1963 р. існує автономна і фізично відокремлена від ТМЗК Національна система зв'язку (NCS) спеціального призначення [1], в Україні вся національна інформаційна інфраструктура, включаючи національну систему конфіденційного зв'язку та інші мережі спеціального призначення, принаймні на нижчих рівнях (фізичному, канальному) використовують канали магістральної первинної мережі ТМЗК (ВАТ «Укртелеком»). Це зумовлює актуальність завдання забезпечення ІБ державних інформаційних ресурсів в ТМЗК України.

Питанням створення комплексних систем захисту інформації (КСЗІ) в автоматизованих (інформаційних) системах (АС, ІС) присвячено багато робіт. На сьогодні в світі існує досить розвинута нормативна база щодо різних аспектів та етапів створення КСЗІ. На пострадянському просторі першим фундаментальним дослідженням, в якому була чітко сформульована методологія проектування КСЗІ є

монографія [2]. В Україні існує нормативно-правова база з технічного захисту інформації (ТЗІ), де зокрема прописані загальні вимоги щодо проектування КСЗІ в АС [3, 4]. Вітчизняними фахівцями проводяться дослідження, в яких вирішуються ті чи інші окремі задачі або аспекти проектування КСЗІ, наприклад [5, 6]. Існує програмне забезпечення (ПЗ), яке дозволяє автоматизувати деякі етапи та процедури створення КСЗІ: оцінку ризиків ІБ; аналіз вразливостей системи; розробку та верифікацію політики інформаційної безпеки (ПІБ); вибір та оцінку функціонального профілю захисту (ФПЗ) тощо.

Однак, всі вище згадані дослідження стосуються створення КСЗІ в АС (ІС). Треба підкреслити, що проектування систем інформаційної безпеки (СІБ) в ТМЗК має принципово відрізнятися. По-перше, як об'єкт захисту, ТМ від ІС відрізнятимуться масштабами, глобально-розподіленим характером, великою довжиною ліній та каналів зв'язку, що знаходяться на неконтрольованій території, різними загрозами та відповідно різними вимогами безпеки). По-друге, згідно з дослідженням [7], на яке спирається автор, термін «*інформаційна безпека*» має дещо ширший зміст ніж «*захист інформації*», тому, на відміну від поняття «*комплексна система захисту інформації*», яке офіційно закріплено в українській нормативній базі, - термін «*система інформаційної безпеки*» відповідає мережецентричній парадигмі (network-centric paradigm) [8] та концепції інформаційної гарантії (information assurance) [9], які розвиваються в США.

Хоча питанням ІБ ТМ присвячено ряд міжнародних стандартів ISO/IEC, технічних звітів ETSI, низка рекомендацій ITU-T різних серій, і за останні роки почала активно розроблятися вітчизняна нормативна база в частині ІБ ТМ [10 – 12], але треба визнати що в Україні ця робота фактично знаходиться на самому початку. Невирішеним залишаються завдання створення методології проектування СІБ державних інформаційних ресурсів ТМЗК, яка б дозволяла комплексно вирішувати проектні процедури, була б адекватною специфіці забезпечення ІБ державних інформаційних ресурсів в ТМЗК, використовувала б як вітчизняні так і міжнародні нормативи щодо ІБ, і за необхідності могла б бути сумісна або інтегрована до вже існуючих систем проектування ТМ.

Метою даної статті є формування вимог щодо безпеки державних інформаційних ресурсів в ТМЗК. При цьому потрібно вирішити наступні завдання:

- проаналізувати порядок створення КСЗІ, який відповідає існуючим нормативним документам;
- ліквідувати прогалини в вітчизняній нормативно-правовій базі в частині ІБ ТМ;
- виробити комплексне ієрархічне визначення терміна «державний інформаційний ресурс»;
- розробити принципи проектування СІБ;
- визначити завдання захисту та вимоги до СІБ державних інформаційних ресурсів в ТМЗК.

В дослідженні використовуються методи порівняння міжнародних та вітчизняних нормативних документів, ретроспективний аналіз, системний підхід до проектування, структурний синтез.

II Порядок створення КСЗІ згідно з існуючими нормативами

Порядок створення КСЗІ розглядається в [2] як сукупність впорядкованих у часі, взаємопов'язаних, об'єднаних в окремі етапи робіт, виконання яких необхідно й достатньо для КСЗІ, що створюється.

Створення КСЗІ включає такі основні етапи [3…5], дослідження першого з яких пов'язане з метою статті.

1. Формування загальних вимог до КСЗІ.

1.1. Обґрунтування необхідності створення КСЗІ. Виконується аналіз нормативно-правових документів, на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями; визначаються переліки інформації, яка підлягає автоматизованій обробці, та здійснюється її класифікація за правовим режимом, за рівнем обмеження доступу до неї, за вимогами до забезпечення цілісності та доступності відповідно до нормативно-правових актів, визначених на попередньому кроці; оцінка можливих переваг експлуатації об'єкта захисту у разі створення КСЗІ.

1.2. Обстеження середовищ функціонування. Метою обстеження є надання уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту. Обстеженню підлягають інформаційне середовище, фізичне середовище, середовище користувачів. Результати обстеження оформляються у вигляді актів і включаються, до відповідних розділів плану захисту інформації. За результатами обстеження середовищ функціонування затверджується перелік об'єктів захисту, а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника.

1.3. Формування завдання на створення КСЗІ. Визначаються завдання захисту інформації, мета створення КСЗІ, варіант вирішення задач захисту, основні напрями забезпечення захисту; здійснюється

аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз; визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних ресурсів, заходів і засобів захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ. Здійснюється оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ (тактико-технічного завдання на створення КСЗІ).

2. Розробка політики безпеки інформації в ІТС.

2.1. Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт.

2.2. Вибір варіанту КСЗІ.

2.3. Оформлення політики безпеки.

3. Розробка технічного завдання на створення КСЗІ.

4. Розробка проекту КСЗІ.

4.1. Ескізний проект КСЗІ.

4.3. Технічний проект КСЗІ.

4.3.1. Розробка проектних рішень КСЗІ.

4.3.2. Розробка документації на КСЗІ.

4.3.3. Розробка документації на постачання засобів захисту інформації та/або технічних вимог (технічних завдань) на їх розробку.

4.3.4. Розробка завдань на проектування в суміжних частинах.

4.4. Робочий проект КСЗІ.

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

5.1. Підготовка КСЗІ до введення в дію.

5.2. Навчання користувачів.

5.3. Комплектування КСЗІ.

5.4. Будівельно-монтажні роботи.

5.5. Пусконалагоджувальні роботи.

5.6. Попередні випробування

5.7. Дослідна експлуатація.

5.8. Державна експертиза КСЗІ.

6. Супроводження КСЗІ.

Підсумком виконання всіх вимог на етапах створення КСЗІ повинна бути захищеність системи за принципом розумної достатності. Кінцевою метою мають бути чотири змістовних результати [5]: архітектура КСЗІ; кількісна оцінка якості її функціонування; оцінка практичної чутливості розроблених моделей до відхилень від апріорних даних; фізична реалізованість КСЗІ (відповідність технології обробки інформації рівню її захисту).

ІІІ Державний інформаційний ресурс як багаторівневий об'єкт захисту в ТМЗК

Перед тим, як проектувати СІБ, потрібно визначити сам об'єкт захисту та його структуру. Вимагає свого визначення найбільш загальне абстрактне поняття *ресурси* (англ. resources): 1) матеріальні засоби, цінності, запаси, кошти, що в разі потреби можна використати; 2) будь-які з компонентів (засобів) обчислювальної системи та можливості, які можуть бути надані нею для процесу оброблення даних на певний проміжок часу [13, с. 529].

Порівняємо, як змінилось визначення похідного поняття *інформаційні ресурси* з сімдесятих років XX століття. Згідно з [14, с. 221] *інформаційні ресурси* – відомості, що отримуються та накопичуються в процесі розвитку науки і практичної діяльності людей, використовуються в суспільному виробництві та керуванні. Інформаційні ресурси відображають природні та суспільні процеси і явища, що зафіксовані у результатах наукових досліджень та розробок, проектно-конструкторської документації, обліково-статистичних даних, нормативних, методичних і т. ін. в формі понять, суджень та більш складних моделей реальності.

У [13, с. 530]: *ресурси інформаційні* (англ. information resources) - 1) результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі); вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших *носіях* (мікрофішах, магнітних стрічках, відеодисках і т. ін.)., що зберігаються у довідково-інформаційних фондах інформаційних органів та бібліотек. 2) окремі документи

і окремі масиви документів, документи і масиви документів в системах інформаційних (бібліотеках, архівах, фондах, банках, банках даних і т. ін.), що містять інформацію з усіх напрямків життєдіяльності суспільства; 3) сукупність даних, що являє собою цінність для установи (підприємства) і виступає як матеріальні ресурси. До ресурсів інформаційних відносяться основні та допоміжні масиви, що зберігаються у зовнішній пам'яті комп'ютерних систем, та вхідні документи.

Ретроспективний аналіз цих визначень дозволяє побачити еволюцію поняття *інформаційні ресурси* в напрямку від його розуміння лише як деякої інформації, абстрагованої від носія, середовища обробки тощо - до сучасних спроб розробки комплексної концепції розуміння інформаційного ресурсу як багатовимірного ієрархічного об’єкта. Інформаційні ресурси можна класифікувати: за видом інформації; за режимом доступу; за видом носія; за способом формування і розповсюдження; за способом організації зберігання і використання; за формою власності. Доцільно відобразити структуру поняття інформаційні ресурси у вигляді наступної ієрархічної схеми (рис. 1):

Рисунок 1 – Схема структурна поняття «інформаційні ресурси»

Вперше у вітчизняній нормативно-правовій базі використаний був термін *національні інформаційні ресурси*: «Основою інформаційного суверенітету України є національні інформаційні ресурси. До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Інформаційний суверенітет України забезпечується: виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України;

використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами» [15, ст. 53, 54]. Визначення, як бачимо, дуже абстрактне. Далі, в [16, п. 5.1] зазначається, що інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

В [10, п. 1] наведено наступні визначення термінів: *державні інформаційні ресурси* – інформація, яка є власністю держави та (або) необхідність захисту якої визначено законодавством; *інформаційно-телекомунікаційна система* - організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних; *мережа передачі даних* - організаційно-технічна система, яка складається з комплексів телекомунікаційного обладнання (вузлів комутації) та реалізує технологію інформаційного обміну з використанням первинної мережі зв'язку.

Наступним кроком є закон [11], в якому можна побачити еволюцію базових понять: відтепер терміни *автоматизована система* та *інформаційна система* визнаються синонімами та визначаються як організаційно-технічна система, що реалізує інформаційну технологію і об’єднує операційне середовище, фізичне середовище, персонал і інформацію, що обробляється. Як об’єкт захист нарешті визначено телекомунікаційну систему; підкреслено єдність і тісний взаємозв’язок ІС та ТС в процесі обробки інформації в ІТС. В статті 5 визначено, що власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Ще одним значущим документом в цьому напрямку (останнім на момент написання статті) є [12], де визначено загальні вимоги та засади забезпечення ІБ державних інформаційних ресурсів, які підлягають захисту в ІТС.

Тепер можемо представити структуру державних інформаційних ресурсів у вигляді схеми (рис. 2).

Рисунок 2 – Схема структурна поняття «державні інформаційні ресурси»

Підводячи підсумок аналізу, проведеного в цьому підрозділі статті, зазначимо:

1. Термін *державні інформаційні ресурси* - це складна багатовимірна ієрархічна категорія. Тому, під час проектування СІБ державних інформаційних ресурсів в ТМЗК має бути враховано особливості різних рівнів ієрархії державних інформаційних ресурсів, оскільки для них має бути застосовано різні критерії та навіть різні нормативно-правові документи.

2. Оскільки інформаційний ресурс

а) для свого існування завжди вимагає наявності *носія*, яким може виступати поле, речовина або людина, а втрата інформаційним ресурсом своєї цінності (порушення безпеки інформаційного ресурсу) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія;

б) є взаємопов'язаний з *обчислювальними ресурсами*, *засобами передачі* та *обслуговуючим персоналом*;

в) обробляється в ТМЗК, яка є складною соціально-технічною системою,

то при проектуванні СІБ (яка теж є соціально-технічною системою) для визначення та уніфікації об'єктів захисту пропонується ввести більш розширені поняття *інформаційний ресурс* та, відповідно *державний інформаційний ресурс*, під якими слід розуміти взаємопов'язану і взаємозалежну сукупність інформації (відповідно – інформації, яка належить державі), носіїв, обчислювальних ресурсів, засобів передачі та обслуговуючого персоналу як одного абстрактного елементарного об'єкту, що захищається СІБ в ТМЗК.

IV Принципи проектування СІБ згідно з мережецентричною парадигмою

Узагальнення основних положень парадигми мережецентричної безпеки [8] та концепції інформаційної гарантії [9] дозволяє сформулювати ряд принципів проектування СІБ.

1. Проектування систем технічного захисту інформації перетворюється у проектування СІБ інформаційних ресурсів, де інформаційний ресурс розуміють як сукупність інформації та засобів, в яких вона обробляється і циркулює, а також персонал.

2. Змінились пріоритети проектування. В цілому забезпечення ІБ сьогодні включає в себе такі поняття, як цілісність (integrity) інформації, конфіденційність (confidentiality), захищеність від несанкціонованого доступу (authentication, non-repudiation), та забезпечення надійності (availability) функціонування системи. Проблема забезпечення цілісності й автентичності користувача найбільш ефективно реалізується за рахунок використання цифрового підпису на основі несиметричних криптографічних алгоритмів з двома ключами – особистим і публічним – у поєднанні з інфраструктурою засвідчуючих центрів. Така концепція проектування дає гарантію, що, навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні в контур керування, втрати частини ресурсів та перенавантаження трафіка комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих задач.

3. Під час проектування треба враховувати що, процес забезпечення ІБ все більше перетинається з 1) процесами керування якістю телекомунікаційних послуг (де захищеність інформаційних ресурсів є складовою частиною оцінки якості) і управління економічною ефективністю (де є взаємозв'язок між інформаційними та економічними ризиками) 2) задачами технічної експлуатації в частині забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості інформаційних систем, до запасу стійкості при дії дестабілізуючих факторів зовнішнього середовища. Тому під час проектування постає задача аналізу взаємозв'язків і взаємозалежності задач ІБ із задачами в зазначених сферах [7].

На різних етапах проектування СІБ формуються взаємопов'язані показники захищеності, гарантій, якості та техніко-економічні показники: живучість систем – працездатність та надійність систем, цілісність даних – достовірність даних, цілісність структури – відновлюваність систем та резервування, спостережність процесів – контрольованість процесів функціонування, стійкість алгоритмів – стійкість систем до зовнішніх дестабілізуючих впливів середовища.

Мережецентрична модель проектування СІБ витікає з підвищених вимог до живучості ІТС, які характеризуються високим ступенем розподілу ресурсів (обслуговуванням, логікою, алгоритмами, програмним та апаратним забезпеченням, телекомунікаціями) і практично повною відсутністю централізованого керування. «Гомеостаз» ТМ підтримується забезпеченням цілісності мережі, її живучості, пропускної здатності та активності елементів [7].

З практичної точки зору важливо, що в рамках системи проектування ТМ вироблено засоби проектування заданого рівня достовірності передавання даних і надійності функціонування ТМ та інших показників якості передавання інформації, які є спорідненими показникам ІБ.

У проектуванні в технічній сфері і в сфері безпеки склалися різні підходи до ряду розглянутих понять. Взаємозв'язок базових понять ІБ з поняттями інших взаємно проникаючих систем полягає в тому, що базові поняття і властивості інших систем ґрунтуються, в цілому, на техногенних чинниках і входять як важлива складова частина у базові поняття і властивості ІБ. Останні базуються як на техногенних чинниках, так і, в першу чергу, на антропогенних чинниках. Проте різниця у поняттях не може бути перешкодою для комплексного проектування.

V Вимоги до СІБ державних інформаційних ресурсів в ТМЗК

Захист державних інформаційних ресурсів може бути визначений як комплексна діяльність, що спрямована на забезпечення усіма можливими заходами та засобами (соціально-психологічними, морально-етичними, управлінськими, організаційно-правовими, інженерно-технічними, програмно-математичними, фізичними) властивостей конфіденційності, цілісності, доступності та спостережності державних інформаційних ресурсів в інформаційно-телекомунікаційних, інформаційних, телекомунікаційних системах і на об'єктах інформаційної діяльності.

Міжнародні рекомендації визначають перелік функціональних вимог, послуги, які ці вимоги забезпечують та особливості реалізації послуг безпеки за рівнями моделі взаємодії відкритих систем. Вимоги з ІБ ТМ включені до рекомендацій ITU-T серії Е: загальна експлуатація мережі, функціонування служб та людські фактори, управління мережею. В [17] визначені функціональні класи (Functional Classes, FC), за якими можна класифікувати заходи безпеки. *Функціональний клас* – це послідовний комплекс заходів безпеки для задоволення вимог до безпеки на різних функціональних рівнях. Запропоновані функціональні класи на трьох рівнях безпеки: мінімальний функціональний клас (FC 1), базовий функціональний клас (FC 2) та удосконалений функціональний клас (FC 3). Функціональний клас послуг безпеки базового рівня може бути впроваджений у ТМ шляхом деякої реорганізації служби технічної експлуатації. Якщо порівняти FC з класами АС та функціональними профілями захищеності (ФПЗ) в [18], можна помітити значні розбіжності у міжнародній та вітчизняній нормативній базі.

У вітчизняному законодавстві необхідність створення КСЗІ для захисту державних інформаційних ресурсів в ІТС закріплена в [10, п. 7]. В цьому ж наказі викладено основи організації та порядок захисту державних інформаційних ресурсів в ІТС. В мережі передачі даних захисту підлягають державні інформаційні ресурси, інформація користувачів, яка передається мережею незалежно від способу її фізичного та логічного представлення, технологічна інформація та інформація бази даних захисту самої КСЗІ. При цьому, здійснення заходів щодо забезпечення конфіденційності державних інформаційних ресурсів та захист від несанкціонованого доступу (НСД) до них в АС покладається не на оператора, а на користувачів мережі передачі даних, тобто на власників АС. У ТМ має забезпечуватись її власником цілісність, доступність інформації та інформаційних ресурсів мережі, а також живучість, сталість, надійність мереж.

Згідно з [12], обов’язковими вимогами до ІБ ІТС є: автоматизована ідентифікація та автентифікація всіх користувачів системи; забезпечення цілісності та доступності відкритої інформації; захист від НСД до конфіденційної інформації; забезпечення спостережності всіх подій в системі, шляхом їхньої автоматизованої реєстрації в захищеному журналі, який може бути використано для проведення аудиту адміністратором безпеки; забезпечення передачі конфіденційної і таємної інформації в зашифрованому виді або захищеними каналами зв’язку; забезпечення контролю цілісності ПЗ, яке використовується для обробки інформації; контроль за цілісністю програмних та технічних засобів захисту інформації, та припинення роботи системи у разі порушення їхньої цілісності; забезпечення захисту від НСД та антивірусний захист усіх систем; забезпечення захисту інформації від витоку технічними каналами у разі, якщо в системі обробляється інформація, що становить державну таємницю. Особливо слід підкреслити, що відповідальність за забезпечення захисту інформації в системі покладається на власника (керівника) системи.

Можемо узагальнити вимоги до СІБ державних інформаційних ресурсів у ТМЗК (табл. 1).

Таблиця 1 – Вимоги до СІБ державних інформаційних ресурсів в ТМЗК залежно від цілей проектування

Показник інформації	Режим доступу до інформації, що належить державі		
	відкрита	конфіденційна	таємна
конфіденційність	не важлива, факультативна	визначна	дуже визначна
цілісність	важлива (захист від НСД, антивірусний, контроль цілісності ПЗ та засобів захисту)		
доступність	важлива	другорядна	другорядна
спостережність	важлива (ідентифікація, автентифікація, автоматизована реєстрація подій)		
цінність	відносно невелика	велика	абсолютна
рівень захищеності	помірний	підсилений	максимально можливий
рівень витрат на ІБ	обмежений	оптимальний	максимально можливий
критичність	незначна	велика	дуже велика

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС.

Висновки

Аналіз вітчизняної нормативно-правової бази з ІБ свідчить, що найбільш розробленими є питання щодо ТЗІ в АС та в АТС з програмним керуванням. Що стосується ІБ ТМ, в особливості ТМЗК, то слід відзначити, що ці питання тільки почали висвітлюватись і поки ще досить слабо прописані.

Під терміном *державний інформаційний ресурс* слід розуміти взаємопов'язану і взаємозалежну сукупність інформації, яка належить державі, носіїв, обчислювальних ресурсів, засобів передачі та обслуговуючого персоналу. Мережецентрична модель проектування СІБ державних інформаційних ресурсів в ТМЗК витікає з підвищених вимог до живучості, які характеризуються високим ступенем розподілу ресурсів та децентралізованим керуванням. Під час проектування СІБ в ТМЗК повинно бути враховано особливості різних рівнів ієрархії державних інформаційних ресурсів, оскільки для них повинно бути застосовано різні критерії та навіть різні нормативно-правові документи. Підсумком виконання вимог безпеки на етапах створення СІБ повинна бути захищеність державних інформаційних ресурсів в ТМЗК за принципом розумної достатності.

Література: ***1.*** *Establishment of the National Communications System. Special memorandum of the USA President J. Kennedy. – Washington, USA. – 21.08.1963.* ***2.*** *Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, кн. 1 и 2. – 1994.* ***3.*** *ДБН А.2.2-2-96. Державні будівельні норми України. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. - Держкоммістобудування України. – Київ. – 1996.* ***4.*** *ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.* ***5.*** *Домарев В. В. Безопасность информационных технологий. Системный подход - К.: ООО ТИД «Диасофт», 2004.* ***6.*** *Потий А. В. Технология проектирования систем обеспечения ИТ-безопасности // Служба безопасности. – 2002. - № 2 (68). - с. 24-25.* ***7.*** *Кононович В. Г., Тардаскіна Т. М., Гладиш С. В. Реалізація концепції захисту інформаційних ресурсів у телекомунікаційних мережах загального користування // Зв'язок. - 2007. - вип. 3.* ***8.*** *Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations.-MILCOM, USA.-2001.* ***9.*** *Information Assurance in Networked Enterprises: Definition, Requirements, and Experimental Results. CERIAS TR 2001-34. - School of Industrial Engineering, No. 01-05. - Purdue University. - January 2001.* ***10.*** *Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. - Затверджено наказом ДСТСЗІ СБ України № 76 від 24. 12. 2001 р.* ***11.*** *Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №2594-IV від 31. 05. 2006.* ***12.*** *Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29. 03. 2006 р. № 373. – 9 с.* ***13.*** *Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека. Термінологічний електронний навчальний довідник. – К.: ДУІКТ. – 2004. -758 с.* ***14.*** *Словарь по кибернетике / Под ред. академика В. М. Глушкова. – К.: Главная редакция украинской советской энциклопедии, 1979. – 623 с.* ***15.*** *Закон України "Про інформацію" від 02.10.92 р.* ***16.*** *НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***17.*** *ITU-T Recommendation E.408 Требования к безопасности сетей электросвязи. – 30 с.* ***18.*** *НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.*

УДК 681.32 (075)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СКАНИРОВАНИЯ ИЗОБРАЖЕНИЙ

Михаил Глухимчук, Евгений Подгорный, Любовь Рябова
Национальный авиационный университет

Аннотация: **Статья посвящена решению вопроса построения автоматизированных систем управления доступом по биометрическим характеристикам радужной оболочки глаза человека. Рассмотренная проблематика касается процесса формирования информационного описания изображений с помощью традиционных и рекурсивных алгоритмов сканирования. По результатам компьютерного моделирования шумового поля Гаусса-Маркова и обработки реальных изображений радужной оболочки глаза человека проведен сравнительный анализ спектральных и**