УДК 355.40

СЛУЖБА ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ ЦИФРОВОГО МОВЛЕННЯ

КОНОНОВИЧ В., ПРОКОФ'ЄВ М.

ОРЦ ТЗІ ВАТ "Укртелеком", НТУУ „КПИ" НДТ „ТЕЗІС"

SERVICE OF INFORMATION SEQURITY IN THE SYSTEM OF THE DIGITAL BROADCASTING

KONONOVICH V., PROKOFJEV M.

ORC TPI OC "Ukrtelecom", "KPI" SRS "TEZIS"

ВСТУП

Телекомунікації є важливою інфраструктурою суспільства, яка забезпечує оперативне та інтерактивне транспортування інформації в процесі соціальної й економічної діяльності суспільства. Проблема інформаційної безпеки телекомунікаційних мереж та систем займає одне з особливих місць в загальній системі інформаційної безпеки України. Вона не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації та інформаційної безпеки. Загальнонаціональний рівень важливості інформаційної безпеки країни, її комплексний характер потребують забезпечення безпечного функціонування телекомунікаційних мереж загального користування.

Існуюча система технічного захисту інформації (ТЗІ) побудована у відповідності до Законів України «Про інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах», «Концепції технічного захисту інформації в Україні». В галузі зв'язку розроблена відповідна галузева концепція ТЗІ [1]. В нормативно-правову та методично-правову базу ввійшли нормативні документи (НД) ТЗІ у програмно-керованих АТС, НД ТЗІ в комп'ютерних системах від несанкціонованого доступу, які гармонізовані з міжнародними стандартами, нормативно-методичні документи захисту інформації від витоку каналами ПЕМВН тощо. Розвитком законодавчої бази ТЗІ стали Закон України «Про основи національної безпеки України», внесені зміни до Закону України «Про захист інформації в автоматизованих системах» [2], задіяний новий Закон України «Про телекомунікації», прийняті закони, укази, постанови щодо електронних документів, електронного документообігу, електронного цифрового підпису, електронної інформаційної системи «Електронний Уряд».

Метою даної роботи є визначення функцій та структури служби захисту інформації в мережі цифрового мовлення як частини загальної служби безпеки мультисервісної мережі.

ОСНОВНІ ПОЛОЖЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Система ТЗІ мультисервісних мереж може базуватись на „Концепції системи інформаційної безпеки телекомунікаційних мереж загального користування (ТМЗК)", яка розроблена в ОНАЗ і викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформаційної сфери ТМЗК. Інформаційна інфраструктура ТМЗК – це сукупність центрів зберігання, обробки і передачі (транспортування) інформації, каналів інформаційного обміну, ліній телекомунікацій, систем і засобів забезпечення інформаційної безпеки. Інформаційні ресурси включають в себе сукупність даних, що обробляються і транспортуються, які використані для забезпечення процесів функціонування і містять інформацію

користувачів, а також систем сигналізації, систем управління та менеджменту мережі. Концепція інформаційної безпеки ТМЗК є частиною концепції єдиної системи інформаційної безпеки телекомунікацій і успадковує основні її принципи [3...8].

Забезпечення інформаційної безпеки – це діяльність, яка направлена на запобігання витоку інформації інформаційної сфери, несанкціонованих або ненавмисних впливів порушника інформаційної безпеки, на виявлення наслідків від не відвернутих впливів порушника інформаційної безпеки і на ліквідацію наслідків впливу порушника інформаційної безпеки на інформаційну сферу.

До основних проблем інформаційної безпеки систем цифрового мовлення (СЦМ) можна віднести: суттєве загострення проблем інформаційної безпеки в процесі глобалізації інформаційно-телекомунікаційних комплексів, впровадження у СЦМ телекомунікаційних технологій, в яких застосовуються здебільшого апаратно-програмні засоби закордонного виробництва; збільшення обсягів інформації, що зберігається і передається; нарощування потенційних можливостей порушника у несанкціонованому доступі до інформаційної сфери СЦМ та впливу на процеси її функціонування, особливо в умовах територіальної розподіленості мереж; апаратно-програмні засоби, які використовуються в СЦМ, об'єктивно можуть містити ряд помилок та недекларованих можливостей, які можуть бути використані порушниками; слабка захищеність деяких нових телекомунікаційних технологій внаслідок недостатньої уваги до їх інформаційної безпеки на етапах цифровізації мереж та інтеграції інформаційних та телекомунікаційних технологій.

Відсутність в СЦМ необхідних засобів захисту в умовах інформаційного протиборства робить СЦМ України в цілому вразливими від можливих ворожих акцій, недобросовісної конкуренції операторів зв'язку, кіберзлочинності та інших протиправних дій. Впровадження нових технологій в СЦМ повинне супроводжуватись адекватним вирішенням проблем інформаційної безпеки галузі в цілому: методологічних основ забезпечення інформаційної безпеки транспортних функцій СЦМ; нормативно-правової та нормативно-розпорядчої бази забезпечення інформаційної безпеки СЦМ; системи вимог до інформаційної безпеки СЦМ; організаційної структури забезпечення інформаційної безпеки СЦМ; виробництва вітчизняних засобів забезпечення інформаційної безпеки; системи підготовки кадрів.

Забезпечення інформаційної безпеки функціонування СЦМ повинне базуватись на аналізі вразливостей, які можуть бути використані порушником для подолання системи захисту СЦМ та призвести до нанесення збитків користувачу, підприємству або державі.

Розрізняють дві групи загроз за сферою їх дії: загрози, в даному випадку, державним інформаційним ресурсам та загрози інформації. *Загрози державним інформаційним ресурсам* в телекомунікаційних системах – це можливість здійснення несанкціонованих дій в телекомунікаційній системі. *Загрози інформації* – це можливість здійснення дій з порушення цілісності, конфіденційності та доступності інформації, що циркулює в телекомунікаційній системі.

Взагалі, загроза інформаційній безпеці СЦМ – це можливий вплив порушника інформаційної безпеки на інформаційну сферу СЦМ, не запобігання, не виявлення і не ліквідація наслідків якого засобами СЦМ, може привести до погіршення заданого рівня якості послуг або до погіршення заданих якісних характеристик функціонування СЦМ і, як наслідок, до нанесення збитків державі, користувачу, оператору. Загрози реалізуються через можливі вразливості інформаційної сфери СЦМ. Успішна атака порушника, направлена на реалізацію загроз інформаційній безпеці СЦМ, опирається на одержані порушником знання про особливості побудови та вразливості СЦМ.

Причинами появи вразливостей в СЦМ можуть бути: порушення технології процесу передачі інформації користувача; порушення технології системи керування СЦМ; впровадження в об'єкти СЦМ компонентів, які реалізують не декларовані функції; впровадження в об'єкти СЦМ програм, які порушують їх нормальне функціонування; незабезпеченість реалізованими механізмами захисту СЦМ або пред'явлення до механізмів захисту СЦМ непроду-

маного набору вимог, які роблять СЦМ незахищеною; внесення порушником навмисної вразливості при розробці алгоритмів і програм СЦМ, при розробці захищених процедур, протоколів і інтерфейсів взаємодії користувачів, операторів і адміністраторів з апаратно-програмним забезпеченням СЦМ при реалізації проектних рішень із створення СЗІБ СЦМ, які роблять неефективним реалізовані в СЗІБ СЦМ механізми захисту; неадекватне реагування підсистеми управління СЗІБ СЦМ на інформаційні впливи порушника в процесі експлуатації СЗІБ; використання несертифікованих, у відповідності з вимогами безпеки, вітчизняних і зарубіжних інформаційних технологій, засобів інформатизації і зв'язку, а також не атестованих засобів захисту інформації і контролю їх ефективності тощо.

Проведення аналізу вразливості СЦМ та можливих дій порушника дозволяє визначити перелік найбільш небезпечних наслідків дій порушників, загроз інформаційній безпеці СЦМ, захист від реалізації яких і повинен бути забезпечений. Конкретний перелік загроз залежить від типу телекомунікаційної технології, типу телекомунікаційних систем та умов їх застосування.

ЦІЛІ ТА ФУНКЦІЇ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЦМ

При формуванні цілей та задач служби інформаційної безпеки СЦМ необхідно враховувати її особливу роль в рамках національної безпеки держави. В інформаційно-телекомунікаційних системах повинен забезпечуватись захист не тільки інформації з обмеженим доступом, а й відкритої інформації, яка є власністю держави, також інформації про особу (персональних даних). Виключна роль телекомунікацій в сучасних інфраструктурах країни проявляється в тому, що національна безпека України залежить від цілісності, надійності й готовності критичних фізичних та інформаційних інфраструктур. *Поняття «критичної інфраструктури»* включає в себе сукупність фізичних або віртуальних систем і засобів, важливих для держави настільки, що їх вихід з ладу або знищення можуть привести до згубних наслідків у області економіки, оборони, охорони здоров'я та національної безпеки.

Телекомунікаційні мережі, інформаційна інфраструктура яких є сукупністю центрів зберігання, обробки і передачі інформації, каналів інформаційного обміну, ліній зв'язку, систем і засобів забезпечення інформаційної безпеки, можна вважати найкритичнішою інфраструктурою країни. Вирішальне значення має розробка заходів із захисту, дублювання, мобільності, сполучення, відновлення й безпеки телекомунікаційних систем країни для використання в інтересах управління державою критичних інформаційних послуг та телекомунікаційних ресурсів як у надзвичайних умовах, так і в режимі нормального функціонування. Тому, до інформаційної безпеки інформаційної інфраструктури СЦМ законом України «Про телекомунікації» ставляться вимоги забезпечення живучості, що передбачає підтримання таких властивостей як надійність функціонування мережі, її готовність, працездатність, сталість, доступність до інформаційних ресурсів та інформаційних систем, цілісність структури, відновлюваність.

Критичність телекомунікацій зв'язана також з проблемою забезпечення безпеки суспільно-політичних відносин, зокрема з виникненням загроз нового типу – впливів на системи зв'язку, збирання та обробки інформації. Такі засоби впливу базуються на автоматизованому аналізі структури повідомлень, слідкуванні за ключовими словами, синтезуванні мови у реальному масштабі часу. Результатом впливу є створення непомітних завад інтелектуального впливу шляхом блокування, підміни у повідомленнях ключових елементів і навіть введення у повідомлення хибних чи фальшивих ключових елементів. Небезпека таких загроз у тому, що фальсифікація може проводитись не лише власником чи розпорядником інформації, за що він несе відповідальність перед законом, а й противником, приховано, під час передачі інформації мережею.

Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації, мають широкомасштабні наслідки у політичному, релігійному або ідеоло-

гічному планах. Інформація викрадається, перекручується, обмежується, фільтрується з метою впливу (або виключення впливу) на психіку людини, психологію великих мас людей, суспільну свідомість з метою примусити їх думати і діяти в потрібному для того, хто організує та здійснює цей вплив, напрямі. Рівень небезпечності загроз цільового інформаційного впливу прямо пропорційний рівню технологічного розвитку мереж та масштабам застосування комп'ютерів у системах управління мережею, галуззю і державою в цілому.

В зв'язку з цим, для телекомунікаційних мереж зростає важливість вимог забезпечення цілісності та достовірності передачі інформації, захисту від порушень правил маршрутизації, точності й своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого доступу до інформаційних ресурсів мереж, та забезпечення фізичної безпеки інформаційної інфраструктури. Телекомунікації забезпечують транспортування інформації в інтересах її обробки автоматизованими системами на об'єктах інформаційної діяльності і, як наслідок, у телекомунікаціях маємо дещо інший підхід до оцінки цінності (вартості й ціни) інформації, ніж на звичайних об'єктах інформаційної діяльності.

При цьому, під транспортуванням інформації, у відповідності з рекомендаціями ITU-T, розуміються не тільки функції переносу (передачі) інформації в просторі, а й мережні функції, такі як моніторинг процесу переносу інформації, аудит і оперативне перемикання каналів і маршрутів, своєчасне відновлення порушеного процесу передачі інформації, керування мережами зв'язку, адміністрування. Вартість транспортування (доставки) інформації не залежить від цінності інформації, точніше цінність інформації визначається не оператором, а клієнтом, який обирає відповідні якість і вид телекомунікаційних послуг. Оператор надає телекомунікаційні послуги згідно певної шкали якості послуг або певного рівня захищеності інформації при її передачі мережею. А клієнт сам обирає на договірних засадах рівень якості телекомунікаційної послуги і захищеності своєї інформації.

В телекомунікаційній мережі відсутні засоби визначення категорії інформації, яка передається нею. Категорію інформації призначає, явно (як в телеграфному зв'язку) чи приховано, відправник (власник чи розпорядник) інформації.

Згідно нормативно-правових документів сфери ТЗІ, відповідальність за забезпечення конфіденційності інформації несе власник інформації. Оператор може надавати послуги забезпечення конфіденційності лише за договором з власником інформації. В результаті склався такий підхід до побудови системи інформаційної безпеки телекомунікаційних мереж.

Конфіденційність інформації, яка передається телекомунікаційною мережею, забезпечує власник інформації, а інші властивості інформації, яка передається мережею – цілісність, доступність та спостережність – захищає оператор мережі чи провайдер телекомунікаційних послуг. Що стосується технологічної інформації, інформації керування, сигналізації та технологічних інформаційних ресурсів, то в інтересах оператора чи провайдера в них мають захищатись всі властивості інформаційних ресурсів: конфіденційність, цілісність, доступність технологічної інформації та спостережність процесів надання послуг.

Забезпечення інформаційної безпеки СЦМ має включати в себе поняття, які за ступенем важливості розташовуються в такому порядку: цілісність (integrity) інформації; конфіденційність (confidentiality); захищеність від несанкціонованого доступу (authentication) до інформації, інформаційних ресурсів та обладнання мережі; неспростовність факту передачі та/чи прийому інформації (non-repudiation); забезпечення надійності (availability) функціонування та живучості СЦМ. Такий підхід дає гарантію, що, навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні в контур керування, втрати частини ресурсів та перенавантаження мережі внаслідок екстремального трафіка, комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих задач.

Основними цілями забезпечення інформаційної безпеки СЦМ є підтримка та збереження в умовах впливу порушника на інформаційну сферу СЦМ наступних основних характеристик інформаційної безпеки СЦМ: - цілісності інформаційної сфери СЦМ; конфіденційності

інформаційної сфери СЦМ, в тому числі і конфіденційності інформації системи керування; доступності інформаційної сфери СЦМ; - спостережності (підзвітності) інформаційної сфери СЦМ; неспростовності факту передачі чи прийому інформації; непорушності порядку маршрутизації трафіка; таємниці зв'язку та приватності (пункт 3.35 «Ліцензійних умов…» [4]); недопущення несанкціонованого доступу до інформаційної сфери СЦМ (пункт 3.34 «Ліцензійних умов…» [4]).

Забезпечення інформаційної безпеки СЦМ повинно досягатись комплексним використанням організаційних, технічних, апаратно-програмних і криптографічних засобів захисту інформаційної сфери СЦМ, а також здійсненням неперервного контролю за ефективністю реалізованих заходів із забезпечення інформаційної безпеки СЦМ. Забезпечення інформаційної безпеки СЦМ передбачає створення перешкод для можливого несанкціонованого втручання в процес її функціонування. В цьому смислі проблема забезпечення інформаційної безпеки СЦМ включає в себе як задачу захисту інформаційної сфери від несанкціонованого доступу, так і низку інших задач забезпечення процесів функціонування СЦМ, зокрема, забезпечення надійності функціонування телекомунікаційних систем, їх живучості та забезпечення узгодженої між оператором та користувачем СЦМ якості обслуговування в умовах впливу порушника.

У зв'язку з цим з'явились нові задачі, зв'язані з необхідністю: захисту мереж, вузлів і центру керування мережею від несанкціонованого доступу користувачів до послуг зв'язку (телекомунікаційних послуг), які надаються мережею:

- посилення захисту систем управління СЦМ, зокрема підсистеми керування інформаційною безпекою від можливості несанкціонованого доступу до процесів управління різними каналами доступу, із забезпеченням конфіденційності та цілісності інформації управління (команд, донесень та інформації маршрутизації), які циркулюють різними каналами зв'язку мережі, в умовах можливих навмисних дій (впливів) порушника; забезпечення заданої (гарантованої мережею) якості процесу передачі даних користувача (наприклад, вірність даних користувача, які передаються мережею) в умовах можливих навмисних впливів порушника на інформаційну сферу СЦМ; забезпечення своєчасного виявлення спроби блокування порушником процесу передавання даних користувача з локалізацією місця впливу порушника та ліквідацією в заданий проміжок часу наслідків впливу порушника; захисту інформаційної сфери СЦМ від можливості активізації порушником шкодоносних програм („закладок", „вірусів" тощо) за допомогою спеціальних команд, які посилаються порушником різними „легальними" та „нелегальними" каналам доступу (в тому числі каналами зв'язку при взаємоз'єднанні з іншими мережами телекомунікацій, зокрема, з мережею Інтернет); забезпечення можливості створення в СЦМ надійного шляху (тракту) транспортування інформації (даних) для визначеної (окремої) групи користувачів, в тому числі в умовах навмисних впливів порушника.

Забезпечення транспортних функцій СЦМ в умовах можливих впливів порушника на її інформаційну сферу зв'язано зі специфічними проблемами, які відносяться в основному до організації ефективного управління (на базі моніторингу стану мереж зв'язку) та взаємодією окремих апаратно-програмних засобів зв'язку СЦМ, розподілених на великих відстанях один від іншого. Транспортування повідомлень каналами зв'язку за допомогою засобів зв'язку СЦМ (маршрутизаторів, комутаторів, центрів комутації пакетів тощо) пов'язано з необхідністю забезпечення рівня основних характеристик якості обслуговування: надійного доведення отриманого від відправника повідомлення до одержувача; продуктивності; сталості; інформаційної безпеки.

В МЗК має бути створена *система забезпечення інформаційної без*пеки (СЗІБ), яка направлена на: формування єдиної політики в області забезпечення інформаційної безпеки при створенні, розвитку, модернізації і експлуатації СЦМ; вироблення підходів до забезпечення інформаційної безпеки в умовах навмисних і ненавмисних впливів порушника; виявлення вразливості СЦМ та здійснення комплексу адекватних і економічно обґрунтованих заходів

щодо їх зменшення, запобігання впливам порушника та ліквідації наслідків цих впливів на інформаційну сферу СЦМ; координації діяльності підприємств щодо забезпечення інформаційної безпеки СЦМ з контрольними органами державної влади, іншими операторами і організаціями; врахування вимог системи державного регулювання в області забезпечення інформаційної безпеки СЦМ (ліцензування, сертифікації і атестації); обґрунтування економічної доцільності забезпечення інформаційної безпеки; знаходження балансу між рівнем безпеки мережі і рівнем безпеки користувачів; впровадження управління ризиками та страхування відповідальності оператора СЦМ; використання механізмів страхування інформаційних ризиків; створення системи підготовки та перепідготовки кадрів в області забезпечення інформаційної безпеки СЦМ; розробку, вдосконалення і стандартизацію методів, способів, алгоритмів та засобів (механізмів) забезпечення інформаційної безпеки СЦМ.

СЗІБ СЦМ є складовою частиною єдиної системи національної безпеки України і забезпечується сукупністю служб інформаційної безпеки, які реалізують організаційні і технічні заходи, визначені комплексом нормативно-правових документів. Архітектура СЗІБ СЦМ розробляється у відповідності з принципами і положеннями, які містяться в нормативно-правових документах України, з врахуванням рекомендацій і стандартів Міжнародних організацій електрозв'язку.

Безпосередньо інформаційна безпека СЦМ реалізується службами інформаційної безпеки СЦМ і об'єктів зв'язку, які забезпечують виконання *основних функцій інформаційної безпеки*: аутентифікації (користувача, об'єкта та джерела даних); контролю доступу; забезпечення цілісності повідомлень; забезпечення конфіденційності; забезпечення доступності; неспростовності відправки/доставки та участі в обміні; локалізації місця впливу порушника; моніторингу і аудиту; сповіщення про порушення і відновлення порушеного процесу функціонування; адаптації до змінних умов функціонування СЦМ.

Вказані функції виконуються за допомогою відповідних *механізмів безпеки*: керування доступом; обміну інформацією аутентифікації; неспростовності; конфіденційності; безпечності з'єднання та керування маршрутизацією; цілісності (даних та інфраструктури) та захисту трафіка; доступності; приватності.

Безпосереднє керівництво заходами із забезпечення інформаційної безпеки СЦМ повинне здійснюватись службою безпеки СЦМ. Координацію роботи служб безпеки СЦМ має здійснювати координаційний центр з питань безпеки СЦМ та/або державні або недержавні компетентні центри реагування на інциденти з інформаційною безпекою в СЦМ.

Фінансові витрати на створення і технічну експлуатацію СЗІБ СЦМ повинні бути економічно обґрунтованими і виходити з потенційно-можливого нанесення збитку діями порушника інформаційної безпеки користувачу, оператору СЦМ і державі.

ОСНОВНІ НАПРЯМИ РОБІТ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЦМ

Роботи із забезпечення інформаційної безпеки СЦМ поділяються на три групи.

1. Вдосконалення нормативно-розпорядчої та нормативно-технічної бази забезпечення інформаційної безпеки, яка включає: принципи забезпечення інформаційної безпеки при взаємодії різних мереж електрозв'язку між собою та глобальними інфраструктурами зв'язку, зокрема, з Інтернет; порядок надання послуг зв'язку спецкористувачам; порядок керування СЦМ у «особливий період» та при надзвичайних ситуаціях; перелік найбільш критичних, з точки зору забезпечення інформаційної безпеки, сегментів СЦМ, які забезпечують передавання державних інформаційних ресурсів; вимоги інформаційної безпеки до об'єктів інформаційної безпеки СЦМ; методи оцінки і контролю стану інформаційної безпеки СЦМ; взаємодію, права і обов'язки суб'єктів СЗІБ на етапах її розробки створення; порядок підготовки до атестації та державної експертизи апаратних, програмно-апаратних і програмних засобів забезпечення інформаційної безпеки СЦМ та атестації СЗІБ в цілому щодо відповідності вимогам з інформаційної безпеки; організацію проведення робіт з виявлення закладок і недек-

ларованих можливостей у технічних засобах СЦМ; організацію роботи з впровадження державних і галузевих стандартів на технічні і програмні засоби і механізми забезпечення інформаційної безпеки СЦМ.

2. Забезпечення технічного захисту процесів передачі даних в СЦМ: виявлення та ліквідацію вразливості в інформаційній сфері СЦМ; забезпечення конфіденційності інформації про інформаційну сферу СЦМ; запобігання несанкціонованого доступу до СЦМ та інформації, що передається нею; виявлення і запобігання впливів порушника на інформаційну сферу СЦМ; аудит, контроль якості обслуговування і якісних характеристик процесу передачі даних в СЦМ в умовах навмисних дій порушника; своєчасне виявлення наслідків впливу порушника на інформаційну сферу СЦМ; локалізація місця дій порушника; ліквідація наслідків впливу порушника на інформаційну сферу СЦМ та відновлення порушеного процесу функціонування.

3. Забезпечення організаційно-технічного захисту об'єктів і процесів передачі даних: розробка і реалізація політик забезпечення інформаційної безпеки підприємств, філій, центів електрозв'язку, вузлів зв'язку тощо; організація контролю стану інформаційної безпеки СЦМ; технічне забезпечення інформаційної безпеки СЦМ; розробка заходів із забезпечення таємниці зв'язку; проведення заходів щодо ліквідації наслідків дії порушників і відновленню порушеного процесу функціонування; забезпечення додержання встановлених активноправовими актами норм порядку маршрутизації трафіка; удосконалення фізичного та інженерно-технічного захисту об'єктів СЦМ і недопущення несанкціонованого доступу до інформаційної сфери СЦМ; підбір, навчання і робота з кадрами в інтересах забезпечення інформаційної безпеки СЦМ.

Загальними задачами служби забезпечення інформаційної безпеки СЦМ є:

1. Розробка і проведення єдиної технічної політики в області забезпечення інформаційної безпеки СЦМ, які включають: розробку вимог політики інформаційної безпеки СЦМ та її складових частин; розробку критеріїв оцінки ефективності систем і засобів інформаційної безпеки СЦМ; розробку критеріїв і методів оцінки стану інформаційної безпеки СЦМ; встановлення відповідальності посадових осіб і операторів СЦМ за дотримання вимог інформаційної безпеки; навчання, підвищення кваліфікації і атестація фахівців в області забезпечення інформаційної безпеки; створення системи моніторингу стану інформаційної безпеки СЦМ; визначення політики по відношенню до закупок та використання імпортних та вітчизняних засобів захисту і програмної продукції.

2. Організація і проведення робіт із забезпечення інформаційної безпеки СЦМ, зв'язаних з обробкою, зберіганням і передачею інформації, віднесеної законодавством України до інформації для службового користування.

3. Створення умов для дотримання встановлених законодавством обмежень на доступ до конфіденційної інформації.

4. Організація взаємодії з органами державної влади та іншими операторами в області забезпечення інформаційної безпеки систем і мереж зв'язку.

5. Розробка механізмів протидії екстремістської діяльності на СЦМ.

6. Проведення галузевої політики розвитку засобів зв'язку і засобів забезпечення інформаційної безпеки СЦМ.

7. Контроль виконання вимог до інформаційної безпеки СЦМ. Проведення моніторингу функціонування СЦМ за вимогами інформаційної безпеки.

8. Створення і розвиток системи керування ризиками.

9. Забезпечення інформаційної безпеки інформаційних, ідентифікаційних і розрахункових систем з використанням ідентифікаційних карт.

10. Проведення робіт з підготовки атестації й державної експертизи СЦМ, систем і засобів зв'язку відповідно з вимогами до інформаційної безпеки СЦМ.

11. Залучати до робіт із забезпечення інформаційної безпеки СЦМ лише організації та підрозділи, які мають ліцензію на цей вид діяльності.

12. Забезпечення функціонування системи моніторингу і попередження інформаційних атак на критично важливі сегменти інформаційної інфраструктури СЦМ. Реєстрування, аналіз та інформування відповідальних органів щодо інцидентів з інформаційною безпекою.

13. Забезпечення розробки розпорядчих та нормативних документів з інформаційної безпеки СЦМ.

14. Створення служби інформаційної безпеки СЦМ у складі системи технічної експлуатації і системи управління СЦМ.

15. Забезпечення дотримування порядку маршрутизації трафіка, встановленого нормативно-правовими актами.

16. Вдосконалення політики інформаційної безпеки оператора СЦМ та її головних складових частин. Постійна модернізація системи забезпечення інформаційної безпеки СЦМ у відповідності з розвитком технологій.

17. Забезпечення вимог інформаційної безпеки СЦМ при взаємодії з мережами зв'язку інших операторів СЦМ.

Відповідальність за забезпечення інформаційної безпеки СЦМ несе ліцензіат-підприємство зв'язку. При здійсненні цієї діяльності підприємство взаємодіє з зацікавленими органами державної влади. Ліцензіат зобов'язаний встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення відповідно до діючого законодавства.

Згідно Закону України «Про телекомунікації» підприємство зобов'язано забезпечити захист зазначених засобів від несанкціонованого доступу. Контроль за застосуванням криптографічних заходів захисту при забезпеченні інформаційної безпеки СЦМ здійснюється у відповідності з діючим законодавством.

На об'єктах телекомунікацій, а також в окремих структурних підрозділах операторів, провайдерів телекомунікацій, де передається, оброблюється або зберігається інформація з обмеженим доступом, що є власністю держави, установлюється спеціальний режим доступу відповідно до законодавства.

Процес забезпечення інформаційної безпеки в значній мірі пересікається з процесами: управління якістю надання телекомунікаційних послуг, де захищеність інформаційних ресурсів є складовою частиною системи забезпечення та гарантій якості; менеджменту економічної ефективності, де ризики інформаційної безпеки взаємозв'язані з економічними ризиками; задачами технічної експлуатації в частині забезпечення вимог до збереження мінімального набору критично важливих функцій мережі в надзвичайних ситуаціях, до живучості інформаційних систем, до запасу стійкості при дії дестабілізуючих факторів зовнішнього середовища. Дійсно ряд властивостей інформації та систем захисту мають багато спільного, а саме спільними є:

- 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.

Постановка та вирішення проблем інформаційної безпеки витікає з підвищених вимог до живучості інформаційних систем, які характеризуються високим ступенем розподілу ре-

сурсів (обслуговуванням, логікою, алгоритмами, програмним та апаратним забезпеченням, телекомунікаціями).

ВИСНОВОК

Таким чином на підприємстві, що надає послуги цифрового мовлення необхідно створити систему інформаційної безпеки та служби інформаційної безпеки СЦМ, визначити їх функції згідно чинних законодавчих та нормативно-правових документів системи ТЗІ.

Література

1. Концепція технічного захисту інформації в галузі зв'язку України, від 24.09.1999 р.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» в редакції від 31 травня 2005 року, № 2599-IV.

3. Закон України "Про телекомунікації", № 1280-IV від 18.11.2003 р.

4. 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.

5. 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.

6. ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. Geneva. 1991. (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС). С. 48.

7. ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. С. 28.

8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – С 12.

9. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено наказом Держспецзв'язку № 112 від 04.07.2008 – С. 9.