час більшої актуальності, оскільки, з одною боку, дозволяє прискорити рішення кадрової проблеми за рахунок скорочення (у порівнянні з системою підготовки) термінів навчання, а з іншого - вносить внесок у рішення ще однієї проблеми - працевлаштування, у першу чергу, звільнених у запас офіцерів, забезпечуючи їх перепрофілювання. Перепідготовка кадрів може здійснюватися на базі ВУЗів. Вибір конкретного ВУЗу повинен проводиться з урахуванням характеру базової підготовки кожного фахівця.

Список літератури:

1. Закон України „Про державну таємницю".
2. Закон України „Про інформацію"
3. ДСТУ 3396.0-96 Технічний захист інформації. Основні положення.
4. Звіт відомостей, що становлять державну таємницю №52 від 01.03.2001р.
5. Постанова Кабінету Міністрів України від 8.10.1997 р. № 1126 „Концепція технічного захисту інформації в Україні".
6. Материалы VIII Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». К.: ДСТС ЗИ, 2005 г.
7. Богданов О.М., Додонов О.Г., Хорошко В.О. та інші. Проблеми становлення національної системи підготовки кадрів в області інформаційної безпеки. / Захист інформації, № 2, 2001 р. – с. 66-71.
8. Бабак В.П., Козловський В.В., Хорошко В.О., Чирков Д.В. Деякі аспекти підготовки фахівців із захисту інформації в Україні // Захист інформації, № 4. 2001. – с.57-69.
9. Гловань С.М. Організація навчального процесу на курсах підвищення кваліфікації з інформаційної безпеки // Захист інформації, № 4, 2002. – с.71-76.
10. Кривуца В.Г., Гніденко М.П. Закономірність природнго розвитку людини в ході сучасного навчального процесу. // Вісник ДУІКТ, 2004, т.2, № 3. – с.176-181.
11. Кривуца В.Г., Козловський В.В., Хорошко В.О., Чирков Д.В. Підготовка фахівців із інформаційної безпеки у ДУІКТ // Матеріали II МНМК „Болонський процес: Трансформація навчального процесу у технологію навчання, К.: ДУІКТ, 2005. – с.160-163

УДК 004.681

В.Г. Кононович
М. Ф. Тардаскін

ОСНОВНІ ПОЛОЖЕННЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Вступ

Сфера технічного захисту інформації (ТЗІ) набуває зростаючого значення з прискореним розвитком інформаційно-комунікаційних технологій (ІКТ). При цьому, задачі ТЗІ переростають у задачі захисту інформаційних ресурсів, що тепер називають інформаційною безпекою ІКТ [1]. Під інформаційним ресурсом розуміють сукупність інформації та засобів, в яких і за допомогою яких вона обробляється та циркулює, а також причетний персонал.

Система ТЗІ побудована у відповідності до Законів України «Про інформацію» (1994), «Про державну таємницю» (у редакції 1999), «Про захист інформації в автоматизованих системах» (1994), а також Концепції технічного захисту інформації в Україні (1997). В галузі зв'язку розроблена відповідна галузева концепція ТЗІ [2]. Нормативно-правовою та методично-правовою базою стали НД ТЗІ на програмно-керованих АТС, НД ТЗІ в комп'ютерних (автоматизованих) системах від несанкціонованого доступу, які гармонізовані з міжнародними стандартами [3], нормативно-методичні документи захисту інформації від

витоку каналами ПЕМВН, спеціальні документи ДСТЗІ та документи «Гостехкомісії СРСР».

Загострення проблем з інформаційною безпекою - в умовах широкого розповсюдження комп'ютерних технологій в усіх сферах діяльності людини, суспільства і держави, промисловості, виробництва, бізнесу, науки та культури – привели до необхідності вдосконалення системи ТЗІ. Замість концепції ТЗІ, не відміняючи, а доповнюючи та розвиваючи її, став чинним Закон України «Про основи національної безпеки України», внесені зміни у Закон «Про захист інформації в автоматизованих системах» [3], задіяний новий Закон України «Про телекомунікації». Але в галузі телекомунікацій створився деякий розрив між законодавчою і нормативно-методичною базою в області інформаційної безпеки телекомунікаційних мереж загального користування (ТМЗК).

Метою даної роботи є ліквідація цього розриву, розробка основних положень системи інформаційної безпеки ТМЗК як частини інформаційно-телекомунікаційних мереж, що дасть змогу створити та впровадити політики інформаційної безпеки як ТМЗК в цілому, так і всіх її ключових елементів.

1. Загальна характеристика концепції

З точки зору інформаційної безпеки, телекомунікаційні мережі, на відміну від інших типів об'єктів інформаційної діяльності, мають деякі суттєві особливості за їх роллю в інфраструктурах держави та суспільства і за характером обробки інформації.

Перша особливість полягає у виключній ролі телекомунікацій в сучасних інфраструктурах країни. Національна безпека України залежить від цілісності, надійності й готовності критичних фізичних та інформаційних інфраструктур, таких як сільське господарство, виробництво продовольства, національна оборона, органи державного управління, транспорт, трубопроводи, водопостачання, охорона здоров'я, виробництво, енергетика, атомні електростанції, банківська та фінансова система, інформаційні та телекомунікаційні системи і мережі, поштова служба, національні та історичні пам'ятники.

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. Серед критичних інфраструктур безпека комп'ютерних та телекомунікаційних мереж, інформаційних технологій, систем управління виробництвом, систем електропостачання та баз даних займає особливе місце. В Україні вразливість та безпека критичних інфраструктур - можливо у меншій мірі, ніж в інших розвинутих країнах - повністю залежить від інформаційних систем та мереж. 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. Ідеальною технічною політикою в області телекомунікацій в інтересах національної безпеки є створення спеціальної цифрової мережі зв'язку, послугами якої будуть користуватись практично всі громадяни в надзвичайних обставинах: пожежах, повенях, технологічних, екологічних та інших катастрофах, громадянських заворушеннях, епідеміях, терористичних актах, військових діях тощо.

Телекомунікаційні мережі можна вважати найкритичнішою інфраструктурою країни, інформаційна інфраструктура яких є сукупністю центрів зберігання, обробки і передачі інформації, каналів інформаційного обміну, ліній зв'язку, систем і засобів забезпечення інформаційної безпеки. Зокрема, до інформаційної безпеки інформаційної інфраструктури ТМЗК законом України «Про телекомунікації» ставляться вимоги забезпечення живучості, що передбачає підтримання таких властивостей як надійність функціонування мережі, сталість, доступність інформаційних ресурсів, цілісність структури, відновлюваність.

Друга особливість телекомунікацій зв'язана 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 несправжніх 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 і противником, приховано, під час передачі інформації телекомунікаційною мережею. Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації, мають широкомасштабні наслідки у політичному, релігійному або ідеологічному 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. В зв'язку з цим, для телекомунікаційних мереж зростає важливість вимог забезпечення цілісності та достовірності передачі інформації, захисту від порушень правил маршрутизації, своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого доступу до інформаційних ресурсів мереж, включаючи фізичну захищеність мереж.

Третя особливість полягає у характері обробки інформації – 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 розуміється не тільки функції переносу (передачі) інформації в просторі, а й також 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.

Побудова комплексної системи захисту інформації (КСЗІ) включає етапи: обстеження об'єкту інформаційної діяльності; прийняття рішення про створення КСЗІ та складання технічного завдання на створення КСЗІ; розробка проекту КСЗІ; побудова КСЗІ, тестування та здавання КСЗІ в експлуатацію; державна експертиза КСЗІ; експлуатація КСЗІ в реальних умовах функціонування об'єкту інформаційної діяльності, під час якої проводиться моніторинг захищеності інформаційних ресурсів та виявлення нових загроз; при необхідності проводиться удосконалення КСЗІ з проведенням повторної державної експертизи; і нарешті, утилізація при плановому виведенні з експлуатації.

Вирішальним є початковий етап, який визначає обсяг робіт та кінцеві витрати на створення КСЗІ. На цьому етапі проводиться аналіз і категоріювання інформації та інформаційних ресурсів, які підлягають захисту, визнають цінність інформації та можливі збитки при реалізації загроз.

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.

У ТМЗК захисту підлягає інформаційна сфера, яка є сукупністю інформаційної інфраструктури та інформаційних ресурсів. 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 надавання послуг.

Четверта особливість телекомунікацій проявляється в зв'язку з впровадженням електронного документообігу, електронного цифрового підпису, електронного уряду, електронної торгівлі тощо. Телекомунікаційна мережа, яка використовується для побудови цих систем, повинна забезпечувати новий рівень інформаційної безпеки і, зокрема забезпечувати приватність, взаємну автентифікацію і неспростовність. Останнє означає забезпечення неможливості відмови від факту передачі або прийому повідомлень (даних) в процесі взаємодії між мережею і користувачами та між взаємодіючими елементами мережі.

Таким чином, є необхідність у розширенні множини властивостей об'єкту захисту, які необхідно захищати, та в іншому порядку ранжувати ці властивості за критерієм їх важливості для інформаційної безпеки. Чинною нормативно-правовою базою сфери ТЗІ визначаються вимоги до захисту властивостей інформації: конфіденційності, цілісності та доступності інформації при безумовному забезпеченні вимог спостережності. Витрати на реалізацію механізмів забезпечення захисту цих властивостей інформації розподіляє власник інформації у залежності від важливості її властивостей для безпеки.

Забезпечення інформаційної безпеки телекомунікаційних мереж має включати в себе названі та додаткові 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 телекомунікаційної системи та її живучості [4]. 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 дає гарантію, що, навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні в контур керування, втрати частини ресурсів та перенавантаження мережі внаслідок екстремального трафіку, комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих задач.

2. Основні положення концепції та проблеми забезпечення інформаційної безпеки ТМЗК

Концепція інформаційної безпеки в ТМЗК викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації та інформаційних ресурсів. Розроблення концепції інформаційної безпеки включається в методологію розробки політики інформаційної безпеки у інформаційно-телекомунікаційних мережах. Розроблення концепції виконано на підставі аналізу правових засад, вимог до забезпечення інформаційної безпеки згідно з завданнями і функціями інформаційно-телекомунікаційних мереж, загроз, від яких зазнають впливу інформаційні ресурси ТМЗК, що підлягають захисту. Концепція захисту інформаційних ресурсів у ТМЗК є частиною Концепції єдиної системи інформаційної безпеки телекомунікацій і успадковує основні її принципи.

Концепція розвиває положення Закону України "Про основи національної безпеки України", Закону "Про телекомунікації", "Ліцензійних умов …" [5, 6], інших правових і нормативних актів України та рекомендацій міжнародних організацій електрозв'язку [7].

Концепція служить основою для розробки комплексу організаційних і технічних заходів із забезпечення інформаційної безпеки ТМЗК, а також нормативних і методичних документів, які забезпечують їх реалізацію підприємствами і не передбачає підміну

державних органів влади та підрозділів підприємств, що відповідають за забезпечення безпеки інформаційних ресурсів та захист інформації, які належать державі.

Забезпечення інформаційної безпеки ТМЗК – це діяльність, яка направлена на запобігання витоку інформації інформаційної сфери ТМЗК, 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 ТМЗК.

Процес глобалізації інформаційно-телекомунікаційних комплексів, впровадження у ТМЗК телекомунікаційних технологій, в яких застосовуються здебільшого апаратно-програмні засоби закордонного виробництва, суттєво загострили проблему інформаційної безпеки. Збільшення обсягів інформації, що зберігається і передається, територіальне розподілення мереж приводить до нарощування потенційних можливостей порушника по несанкціонованому доступу до інформаційної сфери ТМЗК та впливу на процеси її функціонування. Апаратно-програмні засоби, які використовуються в ТМЗК, об'єктивно можуть містити ряд помилок та не декларованих можливостей, які можуть бути використані порушниками. Відсутність в ТМЗК необхідних засобів захисту в умовах інформаційного протиборства робить ТМЗК України в цілому уразливими від можливих ворожих акцій, недобросовісної конкуренції операторів зв'язку, а також кримінальних та інших протиправних дій.

Впровадження нових технологій на МЗК повинне супроводжуватись адекватним вирішенням проблем інформаційної безпеки, які стосуються галузі в цілому:

- методологічних основ забезпечення інформаційної безпеки транспортних функцій ТМЗК;
- нормативно-правової та нормативно-розпорядчої бази забезпечення інформаційної безпеки ТМЗК;
- системи вимог до інформаційної безпеки ТМЗК;
- організаційної структури забезпечення інформаційної безпеки ТМЗК;
- вітчизняних засобів забезпечення інформаційної безпеки ТМЗК;
- системи підготовки кадрів.

Законом України «Про телекомунікації» інформаційна безпека телекомунікаційної мережі визначається як її здатність забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації в умовах можливих впливів порушника.

Основними цілями забезпечення інформаційної безпеки ТМЗК є підтримка та збереження в умовах впливу порушника на інформаційну сферу ТМЗК наступних основних характеристик інформаційної безпеки ТМЗК:

- цілісності інформаційної сфери ТМЗК;
- конфіденційності інформаційної сфери ТМЗК, в тому числі і конфіденційності інформації системи керування;
- доступності інформаційної сфери ТМЗК;
- спостережності (підзвітності) інформаційної сфери ТМЗК;
- неспростовності факту передачі чи прийому інформації;
- непорушності порядку маршрутизації трафіку;
- таємниці зв'язку та приватності (пункт 3.35 «Ліцензійних умов…» [5]);
- недопущення несанкціонованого доступу до інформаційної сфери ТМЗК (пункт 3.34 «Ліцензійних умов…» [5]);
- надійності функціонування телекомунікаційних систем та живучості ТМЗК.

Забезпечення інформаційної безпеки ТМЗК повинно досягатись комплексним використанням організаційних, технічних, апаратно-програмних і криптографічних засобів захисту інформаційної сфери ТМЗК, а також здійсненням неперервного контролю за ефективністю реалізованих заходів із забезпечення інформаційної безпеки ТМЗК.

Забезпечення інформаційної безпеки ТМЗК передбачає створення перешкод для можливого несанкціонованого втручання в процес функціонування. В цьому смислі проблема забезпечення інформаційної безпеки ТМЗК включає в себе як задачу захисту інформації від несанкціонованого доступу, так і низку інших задач забезпечення процесів функціонування ТМЗК, зокрема, забезпечення узгодженого між оператором та користувачем ТМЗК якості обслуговування в умовах впливу порушника на інформаційну сферу ТМЗК.

3. Загрози та порушники інформаційної безпеки ТМЗК

Загроза інформаційній безпеці ТМЗК – це можливий вплив порушника інформаційної безпеки на інформаційну сферу ТМЗК, не запобігання, не виявлення і не ліквідація наслідків якого засобами ТМЗК може привести до погіршення заданого рівня якості послуг або до погіршення заданих якісних характеристик функціонування ТМЗК і, як наслідок, до нанесення збитків державі, користувачу або оператору ТМЗК чи провайдеру послуг. Загрози реалізуються через уразливості ТМЗК, які можливо містяться в інформаційній сфері мережі. Успішна атака порушника, направлена на реалізацію загрози інформаційній безпеці ТМЗК, опирається на одержані порушником знання про особливості побудови та уразливості ТМЗК.

Забезпечення інформаційної безпеки функціонування ТМЗК повинно базуватись на аналізі уразливості, яка може бути використана порушником для подолання системи захисту ТМЗК та призвести до нанесення збитків користувачу, підприємству або державі.

Причинами появи уразливості в ТМЗК можуть бути:

- порушення технології процесу передачі інформації користувача;
- порушення технології системи керування ТМЗК;
- впровадження в об'єкти ТМЗК компонентів, які реалізують не декларовані функції;
- впровадження в об'єкти ТМЗК програм, які порушують їх нормальне функціонування;
- незабезпеченість реалізованими механізмами захисту ТМЗК або пред'явлення до механізмів захисту ТМЗК непродуманого набору вимог, які роблять ТМЗК незахищеною;
- внесення порушником навмисної уразливості при розробці алгоритмів і програм ТМЗК, при розробці захищених процедур, протоколів і інтерфейсів взаємодії користувачів, операторів і адміністраторів з апаратно-програмним забезпеченням ТМЗК при реалізації проектних рішень по створенню системи забезпечення інформаційної безпеки (СЗІБ) ТМЗК, які роблять не ефективним реалізовані в СЗІБ ТМЗК механізми захисту;
- неадекватного реагування підсистеми управління СЗІБ ТМЗК на інформаційні впливи порушника в процесі експлуатації СЗІБ;
- використання не сертифікованих 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 уразливості ТМЗК та можливих дій порушника дозволяє визначити перелік найбільш небезпечних наслідків дій порушників, загроз інформаційній безпеці ТМЗК, захист від реалізації яких повинно бути забезпечене.

Як порушники інформаційної безпеки можуть виступати фізичні особи і/або структури, дії яких можуть привести до погіршення якості процесів функціонування ТМЗК. Впливи на інформаційну сферу ТМЗК можуть здійснюватись на кожному з етапів життєвого циклу ТМЗК і особливо на етапах проектування, будівництва та експлуатації.

Дії порушників можуть носити як навмисний, так і ненавмисний характер. Впливи порушників на об'єкт інформаційної безпеки можуть здійснюватись: через зовнішні лінії зв'язку; через внутрішні лінії зв'язку; з робочих місць системи керування; через не декларовані канали доступу. При цьому можуть використовуватись як штатні засоби мереж зв'язку, так і спеціальні засоби.

Впливи порушника на інформаційну сферу ТМЗК можна представити у вигляді дій, направлених на виявлення вразливостей ТМЗК, на активізацію або використання наявної уразливості ТМЗК та дій, пов'язаних з внесенням уразливості в ТМЗК.

Внесення уразливості в інформаційну сферу ТМЗК можливе на таких етапах:

- проектування при виборі алгоритмів і технології зберігання, обробки і передачі інформації, які утруднюють або виключають реалізацію вимог інформаційної безпеки;
- вибору засобів захисту, які не забезпечують вимоги інформаційної безпеки ТМЗК.

На етапі експлуатації ТМЗК порушник може внести уразливості, які зв'язані з:
- помилками налаштування та використання програмно-апаратного забезпечення;
- помилками розробки і реалізації політики безпеки;
- помилками в реалізації організаційних методів захисту;
- навмисним впровадженням у компоненти апаратно-програмного забезпечення «люків», «закладок», «вірусів» тощо.

Виявлення уразливості здійснюється порушником шляхом збирання відомостей, які дозволяють йому здійснювати дії, направлені на погіршення характеристик інформаційної безпеки. Безпосередня активізація чи використання виявленої уразливості здійснюється порушником на етапі експлуатації шляхом:

1. Використання спеціального обладнання на зовнішніх і внутрішніх каналах зв'язку ТМЗК і здійснення з його допомогою: порушення цілісності повідомлень, які містять інформацію керування або інформацію користувачів; порушення конфіденційності інформації керування і параметрів передачі інформації користувачів; формування команд активізації і використання функцій «закладок» і «вірусів», впроваджених в інформаційну сферу; формування інформаційного впливу з метою отримання аутентифікаційних параметрів, які забезпечують доступ до інформаційної сфери об'єктів та мереж зв'язку; несанкціонованої модифікації програмного забезпечення об'єктів та мереж зв'язку і порушення їх працездатності.
2. Встановлення спеціального обладнання в канали мереж зв'язку для використання інформаційних «люків» або не декларованих можливостей.
3. Використання прикінцевого обладнання користувачів ТМЗК для отримання несанкціонованого доступу до інформаційної сфери об'єктів та мереж зв'язку.
4. Використання радіоканалів для активізації «закладок» і «вірусів».
5. Використання робочих місць обслуговуючого персоналу.

4. Основні напрями робіт та задачі по забезпеченню інформаційної безпеки

Роботи по забезпеченню інформаційної безпеки ТМЗК 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 надавання послуг зв'язку спец користувачам;
- порядок керування ТМЗК у «особливий період» та при надзвичайних ситуаціях;
- перелік найбільш критичних з точки зору забезпечення інформаційної безпеки сегментів ТМЗК, які забезпечують передавання державних інформаційних ресурсів;
- вимоги інформаційної безпеки до об'єктів інформаційної безпеки ТМЗК;
- методи оцінки і контролю стану інформаційної безпеки ТМЗК;
- 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 ТМЗК та атестації СЗІБ в цілому по відповідності вимогам з інформаційної безпеки;
- організацію проведення робіт з виявлення закладок і не декларованих можливостей у технічних засобах ТМЗК;
- організацію роботи з впровадження державних і галузевих стандартів на технічні і програмні засоби і механізми забезпечення інформаційної безпеки ТМЗК.

2. Забезпечення технічного захисту процесів передачі даних в ТМЗК:
- виявлення та ліквідацію уразливості в інформаційній сфері ТМЗК;
- забезпечення конфіденційності інформації про інформаційну сферу ТМЗК;

- запобігання несанкціонованого доступу до ТМЗК та інформації, що передається нею;
- виявлення і запобігання впливів порушника на інформаційну сферу ТМЗК;
- аудит, контроль якості обслуговування і якісних характеристик процесу передачі даних в ТМЗК в умовах навмисних дій порушника;
- своєчасне виявлення наслідків впливу порушника на інформаційну сферу ТМЗК;
- локалізація місця дій порушника;
- ліквідація наслідків впливу порушника на інформаційну сферу ТМЗК та відновлення порушеного процесу функціонування.

Реалізацію заходів технічного захисту повинні забезпечити: засоби криптографічного перетворення даних на канальному та мережному рівнях; засоби моніторингу і централізованого керування захистом процесів функціонування ТМЗК; система прихованого керування резервними каналами та засобами зв'язку, яка забезпечує оперативне відновлення порушеного процесу передачі даних в інтересах, передусім спец користувачів.

3. Забезпечення організаційно-технічного захисту об'єктів і процесів передачі даних: розробку і реалізацію політик забезпечення інформаційної безпеки підприємств, філій, центрів електрозв'язку, вузлів зв'язку тощо; організацію контролю стану інформаційної безпеки ТМЗК; технічне забезпечення інформаційної безпеки ТМЗК; розробку заходів по забезпеченню таємниці зв'язку; проведення заходів по ліквідації наслідків діяння порушників і відновленню порушеного процесу функціонування; забезпечення додержання встановленого нормативно-правовими актами порядку маршрутизації трафіку; удосконалення фізичного та інженерно-технічного захисту об'єктів ТМЗК і недопущення несанкціонованого доступу до інформаційної сфери ТМЗК; підбір, навчання і робота з кадрами в інтересах забезпечення інформаційної безпеки.

Загальними задачами підприємства по забезпеченню інформаційної безпеки ТМЗК є:

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

2. Організація і проведення робіт із забезпечення інформаційної безпеки ТМЗК, зв'язаних з обробкою, зберіганням і передачею інформації, віднесеної законодавством України до державної таємниці та 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 ТМЗК.

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

7. Контроль виконання вимог до інформаційної безпеки ТМЗК. Проведення моніторингу стану процесів функціонування ТМЗК за вимогами інформаційної безпеки.

8. Створення і розвиток системи керування ризиками і страхування відповідальності.

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

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

11. Залучати до робіт із забезпечення інформаційної безпеки ТМЗК 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 ТМЗК. Реєстрування, аналіз та інформування відповідальних органів щодо інцидентів з інформаційною безпекою.

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

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

15. Забезпечення дотримування встановленого нормативно-правовими актами порядку маршрутизації трафіку.

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

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

5. Забезпечення інформаційної безпеки ТМЗК при взаємо з'єднанні мереж

Забезпечення інформаційної безпеки ТМЗК при взаємо з'єднанні мереж зв'язку полягає у забезпеченні якості процесів функціонування ТМЗК, захисті її від несанкціонованого доступу і впливів порушника на систему управління ТМЗК.

Реалізація галузевої політики інформаційної безпеки повинна забезпечити взаємодію взаємо підключених мереж з заданою якістю обслуговування в умовах можливих дій порушників. При цьому рівень інформаційної безпеки взаємо підключених мереж зв'язку не повинен бути нижче базового рівня інформаційної безпеки ТМЗК.

Забезпечення інформаційної безпеки ТМЗК при приєднанні і взаємо з'єднанні мереж зв'язку України здійснюється в рамках розробки і реалізації розпорядчих і організаційно-технічних заходів по створенню СЗІБ ТМЗК. Забезпечення інформаційної безпеки ТМЗК при взаємо з'єднанні з глобальними інформаційно-телекомунікаційними мережами, зокрема з Інтернет, повинно основуватись на дотриманні сторонами міжнародних правових актів, які регламентують безпечний пропуск міжнародного трафіку, а також на застосуванні засобів захисту інформаційної сфери ТМЗК від несанкціонованого доступу із боку інших мереж, забезпеченні гарантованої якості функціонування ТМЗК в умовах можливих дій порушників.

Згідно «Ліцензійних умов...» правовою базою повинен бути договір про взаємо з'єднання телекомунікаційних мереж між операторами мереж, що взаємо підключаються. Предметом договору повинні бути: технічні, організаційні та економічні умови взаємо з'єднання мереж операторів; розрахункова такса за доступ до цих мереж; угода про порядок взаємодії операторів; угода про взаємний захист інформаційної сфери взаємо з'єднаних мереж; узгодження правил взаємодії та інтерфейси СЗІБ ТМЗК, що взаємо-підключаються; відповідальність за реалізацію заходів, які забезпечують задані вимоги інформаційної безпеки при взаємо з'єднанні мереж зв'язку.

6. Взаємодія з органами влади при забезпеченні інформаційної безпеки

Відповідальність за забезпечення інформаційної безпеки ТМЗК 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 ТМЗК

здійснюється ДСТЗІ СБ України у відповідності з діючим законодавством.

На об'єктах телекомунікацій, а також в окремих структурних підрозділах операторів, провайдерів телекомунікацій, де передається, обробляється або зберігається інформація з обмеженим доступом, що є власністю держави, установлюється спеціальний режим доступу відповідно до законодавства. Контроль за застосуванням засобів захисту від несанкціонованого доступу до інформації, віднесеної до інформації з обмеженим доступом, і захисту цієї інформації від ПЕМВН на ТМЗК, здійснюється ДСТЗІ у відповідності до діючого законодавства. Підприємства мають складати план взаємодії з правоохоронними органами та органами влади у процесі ліквідації наслідків інцидентів з інформаційною безпекою.

7. Політика інформаційної безпеки в умовах надзвичайних ситуацій, надзвичайного та воєнного стану

Заходи забезпечення інформаційної безпеки ТМЗК в умовах надзвичайних ситуацій, надзвичайного та воєнного стану регулюються Законом України «Про телекомунікації».

В умовах надзвичайних ситуацій, надзвичайного та воєнного стану підприємства зв'язку зобов'язане забезпечувати якісний зв'язок та оповіщення населення в порядку, визначеному Кабінетом Міністрів України.

Підприємство зв'язку повинне забезпечити готовність до виконання своїх функцій в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Під час надзвичайного стану всі засоби та телекомунікаційні мережі зв'язку, незалежно від форми власності, використовуються для забезпечення проведення мобілізації та задоволення потреб національної безпеки, оборони, охорони правопорядку. Оператори телекомунікацій взаємодіють при цьому з Національним центром оперативно-технічного управління мережами зв'язку в питаннях, віднесених до його компетенції.

В умовах надзвичайних ситуацій, надзвичайного стану оператори телекомунікацій з метою оповіщення та забезпечення телекомунікаційними послугами учасників ліквідації наслідків надзвичайних ситуацій, відбудовних робіт та здійснення відповідних заходів Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими державними адміністраціями та органами місцевого самоврядування можуть установлювати тимчасові обмеження в наданні телекомунікаційних послуг споживачам до ліквідації наслідків надзвичайних ситуацій та скасування режиму надзвичайного стану.

Забезпечення інформаційної безпеки систем управління ТМЗК умовах надзвичайних ситуацій, надзвичайного та воєнного стану необхідно передбачати завчасне створення запасних пунктів керування і та резервування обхідних каналів зв'язку.

8. Політика захисту інтересів користувачів ТМЗК

Захист інтересів користувачів ТМЗК регулюється Законом України «Про телекомунікації», «Ліцензійними умовами …» та іншими нормативно-правовими актами, де встановлюються права, обов'язки користувачів та відповідальність за відповідні порушення.

Необхідно задовольняти вимоги споживачів щодо збереження конфіденційності інформації, яка стосується цього споживача, а також забезпечувати та нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, їх оплати, маршрутів передавання тощо.

Оператор ТМЗК приймає заходи, які забезпечують:

- право на доступ користувачів ТМЗК до відкритої інформації, і обмеження доступу до інформації, яка підлягає захисту;
- виключення (недопущення) несанкціонованого доступу користувачів ТМЗК до ресурсів мережі і послугам зв'язку;
- захист персональних даних користувача ТМЗК, які стали йому відомі у процесі здійснення операторської діяльності, і інформації про надані послуги зв'язку;
- захист білінгових систем;

- надавання додаткових послуг захисту інформації користувача ТМЗК і забезпечення інформаційної безпеки процесу передачі по договору з конкретним користувачем ТМЗК.

Користувачі ТМЗК повинні бути проінформовані оператором ТМЗК про послуги зв'язку по забезпеченню інформаційної безпеки ТМЗК у частині, які їх стосуються.

9. Система забезпечення інформаційної безпеки ТМЗК

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

Безпосереднє забезпечення інформаційної безпеки ТМЗК реалізується службами інформаційної безпеки ТМЗК і об'єктів зв'язку, які забезпечують виконання основних функцій інформаційної безпеки: автентифікації (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 ТМЗК.

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

Безпосереднє керівництво заходами по забезпеченню інформаційної безпеки ТМЗК повинне здійснюватись службою безпеки ТМЗК.

Координацію роботи служб безпеки ТМЗК має здійснювати координаційний центр з питань безпеки ТМЗК та/або державні або недержавні компетентні центри реагування на інциденти з інформаційною безпекою в ТМЗК.

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

10. Умови впровадження концепції

В галузі телекомунікацій виконана значна робота в напрямі забезпечення інформаційної безпеки і створені умови для успішного впровадження запропонованої концепції. Дійсно, процес забезпечення інформаційної безпеки в значній мірі пересікається з процесами управління якістю надавання телекомунікаційних послуг, де захищеність інформаційних ресурсів є складовою частиною системи забезпеченні та гарантій якості; з процесами менеджменту економічної ефективності, де ризики інформаційної безпеки взаємозв'язані з економічними ризиками; з процесами й 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.

Аналіз взаємозв'язків і взаємозалежності задач інформаційної безпеки із задачами у зазначених сферах показує, що на різних стадіях життєвого циклу систем інформаційної безпеки в різних стадіях та етапах проектування, створення та експлуатації формуються показники захищеності, гарантій, якості та взаємопов'язані з ними техніко-економічні показники. Порівняємо між собою такі пари властивостей інформації або систем захисту: 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 ресурсів (обслуговуванням, логікою, алгоритмами, програмним та апаратним забезпеченням, телекомунікаціями). Для повноцінної роботи та збереження мінімального набору критично важливих функцій телекомунікаційна система повинна мати певний запас стійкості до дестабілізуючих факторів зовнішнього середовища.

Порушення цілісності системи на фоні зниження активності її елементів тягне за собою дезорганізацію управління, одночасне зниження активності елементів та їх живучості – втрату гнучкості, а зниження живучості і порушення цілісності системи – втрату найважливіших функцій. Поняття живучості системи передбачає її спроможність своєчасно виконувати свої функції в умовах дії дестабілізуючих факторів (фізичне руйнування, часткова втрата ресурсів, відмови та збої елементів, несанкціоноване втручання в контур управління). При цьому технічна надійність, яка проявляється як здатність системи працювати на протязі заданого проміжку часу в штатній системі без відмов, визначає мінімальний поріг стійкості системи, за яким без наявності відновлення втрачених елементів та функції може настати повна зупинка функціонування. Живучість інформаційних систем має визначальну роль для інформаційної безпеки в цілому.

З практичної точки важливо, що в рамках системи технічної експлуатації телекомунікаційних мереж вироблено розвинуті засоби підтримки заданого рівня достовірності передавання даних і надійності функціонування телекомунікаційних систем та інших показників якості передавання інформації і такі показники споріднені показникам інформаційної безпеки.

Конфіденційність залежить від цілісності і, у свою чергу, від надійності. Якщо цілісність і надійність системи буде порушена, то, скоріш, знизиться ефективність механізмів конфіденційності. Навпаки, порушення конфіденційності, приміром технологічної інформації, приведе до можливості обходу механізмів цілісності, доступності і спостережності. Також, якщо буде порушена цілісність системи, то це приведе до компрометації механізмів доступності і спостережності.

Показники доставки інформації – ймовірність втрат і перекручувань повідомлень (достовірність), час затримки, помилки адресації споживача і джерела повідомлень – впливають на ефективність механізмів конфіденційності і цілісності.

Показники якості в узагальненому вигляді входять у характеристики цілісності й доступності. Характеристики доставки інформації споживачеві та інших інформаційно-телекомунікаційних послуг в узагальненому вигляді входять у показники доступності і, частково, у показники конфіденційності й цілісності. Достовірність і надійність опосередковано взаємопов'язані з властивостями конфіденційності, цілісності, доступності. Кількісна або якісна недостатність компонентів системи впливає на показники ефективності захисту інформаційних ресурсів.

Звичайно, що в технічній сфері і в сфері інформаційної безпеки склалися різні підходи до ряду розглянутих понять і в різних сферах в них укладається різний смисл. Так поняття цілісності включає в себе не лише збереження кількісних характеристик інформації – бітів і байтів, а й семантичних характеристик інформації – змісту повідомлень. В сфері безпеки властивості інформації розглядаються з точки зору як техногенного так і антропогенного впливу. Проте різниця у поняттях не може бути перешкодою для комплексного аналізу. Показник цілісності є складною функцією надійності, завадостійкості, спостережності й доступності. Розділити такі поняття, скоріше, неможливо.

Таким чином, суть взаємозв'язку базових понять системи інформаційної безпеки з поняттями інших взаємно проникаючих систем забезпечення якості, керування мережами, менеджменту та технічної експлуатації 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 системи інформаційної безпеки. Останні базуються як на техногенних чинниках, так і, в першу чергу, на антропогенних чинниках.

Висновки. Галузь телекомунікацій готова до впровадження запропонованої концепції інформаційної безпеки при умові вирішення таких проблем: врахування загроз антропогенного характеру, а не лише загроз телекомунікаціям техногенного й природного характеру, тобто врахувати загрози «людського фактору» та від потенційних противників; створення системи інформаційної безпеки та служби інформаційної безпеки ТМЗК (наприклад, в системі технічної експлуатації) та визначення її функцій згідно чинних нормативно-правових документів системи ТЗІ.

Напрямом подальшої роботи може бути дослідження оцінки економічної ефективності впровадження концепції інформаційної безпеки, розробка політики інформаційної безпеки та розробка методів оцінки досягнутого рівня захищеності інформаційних ресурсів ТМЗК.

Список літератури:

1. Тардаскін М.Ф., Кононович В.Г., Вараксін О.О., Тардаскіна Т.М. Механізми забезпечення інформаційної безпеки телекомунікаційних мереж загального користування // Зв'язок. – 2005.- № 7 - 8. – С. 30-35.

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

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

4 Леваков А. Анатомия информационной безопасности США. Jet Info online #6(109), 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – С. 74.

5. 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 та інформатизації України від 17.06.2004 № 132. – С.25.

6. 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 від 10.11.200, № 984. – С.20.

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

УДК 681.003.4

В.В.Овсянников

ЗАЩИТА ИНФОРМАЦИИ ОТ АТАК ИЗ ИНТЕРНЕТ

Чтобы справиться со стремительно нарастающим потоком информации, вызванным научно-техническим прогрессом, субъекты предпринимательской деятельности, организации вынуждены постоянно пополнять свой арсенал различными техническими средствами и системами, предназначенными для приема, передачи, обработки и хранения информации. При этом следует учитывать, что главными носителями информации являются:

- знающие люди;
- документы;
- средства беспроводной и проводной связи;
- электронные системы обработки информации;
- разные отслеживаемые факторы (поведение, разговоры, результаты действий).

Центральной проблемой защиты информации является проблема защиты от несанкционированного доступа. Всем известен тезис, что главную угрозу для информации представляют собственные сотрудники. На основании этого тезиса некоторые пессимисты делают вывод о том, что не стоит предпринимать какие-либо шаги, в силу их бесполезности. На самом деле бесполезным в защите информации является только формальное выполнение