УДК 004.7.052:004.414.2

Моденов С.Ю.

КОНЦЕПЦІЯ РОЗПОДІЛУ ВІДПОВІДАЛЬНОСТІ ЗА БЕЗПЕКУ ІНФОРМАЦІЇ ТА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Національний авіаційний університет

modenovs@mail.ru

Розглядається проблема співвідношення права на інформацію, права власників інформації з обмеженим доступом на її захист

Ключові слова: безпека інформації, телекомунікаційні мережі

Вступ

Згідно з результатами опиту, проведеного в травні 2014 року компанією *Gartner*, основними чинниками розвитку інформаційної безпеки є:

- удосконалення регулювання на рівні держави/галузі – 34% опитаних;
- зростання числа загроз – 27% опитаних;
- страх перед зловмисниками – 17% опитаних.

Перша строчка зайнята державним регулюванням невипадково – останнім часом і в світі, і в Україні прийнято і планується прийняти велику кількість різних державних і галузевих стандартів у області інформаційної безпеки. А паралельно з цим, актуалізуються і кодекси кримінальних і адміністративних правопорушень, що карають за недотримання нових законодавчих вимог. Тому дуже багато компаній починають упроваджувати у себе системи захисту у відповідність з вимогами *ISO* 17799, Базель II, *SOX* і т.п.

Основою побудови телекомунікаційних мереж як систем з відкритим доступом до послуг і стандартизацією устаткування, програмного забезпечення і основних характеристик є еталонна модель взаємодії відкритих систем (*Open System Interconnection – OSI).* Відповідно до цієї моделі однієї з основних характеристик мережі є якість послуг, що надаються, або якість сервісу (*Quality of Service – QoS).* У свою чергу, невід'ємною складовою *QoS* є гарантія безпеки передачі і обробки інформації

Надання гарантій безпеки інформації в мережах телекомунікацій взагалі і в системах і мережах з відкритими каналами зокрема є складною комплексною задачею. У міжнародних стандартах і українському законодавстві проблеми захисту інформації розв'язується одночасно із стратегічними і поточними задачами розвитку архітектури мережі.

Такий підхід відповідає комплексному підходу до задачі забезпечення безпеки мереж телекомунікацій на всіх етапах їх життєвого циклу – від концептуальних схем і проектування до технічної експлуатації і використання (надання телекомунікаційних послуг).

Архітектура забезпечення захисту інформації в рамках моделі взаємодії відкритих систем визначається необхідністю рішення наступних задач:

– застосування служб безпеки і відповідних механізмів, які включені до складу моделі OSI;

– розміщення цих служб і механізмів у вузлах телекомунікаційних мереж.

Таким чином, безпека даних – це захист ресурсів мережі від пошкодження і захист даних від випадкового або навмисного розголошування (витоку), а також від неправомірних змін, знімання, модифікації (порушення цілісності) інформації в процесі її передачі і обробки.

Принцип розподілу відповідальності за безпеку інформації у мережі

Згідно з законом України "Про захист інформації в інформаційно-

телекомунікаційних системах" суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

– власники інформації;
– власники системи;
– користувачі;
– уповноважений орган у сфері захисту інформації в системах.

Власник інформації – це створювач інформаційного контенту, який є суб'єктом авторського права. Згідно з законом України "Про авторське право і суміжні права" суб'єктами авторського права є автори творів, зазначених у частині першій статті 8 цього Закону, їх спадкоємці та особи, яким автори чи їх спадкоємці передали свої авторські майнові права. Об'єктами авторського права є твори у галузі науки, літератури і мистецтва.

Користувач телекомунікаційної системи – це безпосередньо власник інформації (автор, його спадкоємець чи особа, якій передано авторські права) або фізична чи юридична особа, яка по договору з власником інформації доручає передачу інформації через телекомунікаційну систему.

Найважливішим поняттям проблематики захисту є розмежування прав і відповідальності суб'єктів відносин у сфері надання і отримання телекомунікаційних послуг (ринку телекомунікацій). Відповідно до законодавства [1-2] до них відносяться оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та /або постачальники технічних засобів телекомунікацій. Крім того, законодавець [2] розмежовує власників системи і власників інформації.

Нагадаємо, що згідно з законом "Про телекомунікації" [1, стаття 1] Оператор телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій з правом на технічне обслуговування і експлуатацію телекомунікаційних мереж. Провайдер телекомунікацій - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій, без права на технічне обслуговування і експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку. Часто в якості оператора і провайдера телекомунікаційної мережі виступає одна і та ж юридична особа. В цьому випадку їх права і обов'язки розширяються.

Згідно з п. 4 статті 40 закону "Про телекомунікації" (Оператори, провайдери телекомунікацій не несуть відповідальності за зміст інформації, що передається їх мережами) власник інформації (автор, користувач) передає інформацію власнику системи (оператору) чи провайдеру у вигляді "як є", що відповідає міжнародному принципу "As is", тобто у такому вигляді, який він вважає необхідним і доцільним. Власник інформації самостійно оцінює ступінь конфіденційності інформації та вживає необхідних заходів по її захисту, криптографічному або іншому.

У свою чергу, власник системи вживає усіх заходів, необхідних для належного функціонування та захисту від будь-яких спроб несанкціонованого доступу. Звичайно, безпека даних не обмежується тільки захистом від несанкціонованого доступу, а передбачає також захист від збоїв і несправностей апаратури і програмного забезпечення, зовнішніх деструктивних дій (пожеж, підтоплень, крадіжок устаткування, вандалізму і т.д.).

Розподіл відповідальності за захист системи зв'язку в цілому та її складових (телекомунікаційної мережі, інформаційно-управляючої системи, комп'ютерної мережі тощо) і власне захист інформації з обмеженим доступом, що циркулює в системі, має такі принципові переваги:

– власник інформації сам визначає гарантований рівень захисту від порушення своїх майнових прав при спробах несанкціонованого зняття інформації з мережі власника системи;

– власник системи, який отримує інформацію у вигляді "As is" і передає її по своїм каналам зв'язку, не накопичує у своїх мережах зберігання даних масивів конфіденційної інформації, що йому не

належить, і не стає об'єктом посягань на цілісність та безпеку функціонування системи зв'язку.

Для забезпечення гарантій безпеки розробляють багаторівневі системи з технічною і програмною реалізацією (і відповідним розділенням відповідальності) на наступних рівнях:

– вбудованих засобів захисту (програмно-системні паролі, розмежування прав доступу і ін.);

– фізичні засоби захисту (замки, двері, охорона, сигналізація і ін.);

– рівень адміністративного контролю (організаційні заходи, накази і розпорядження адміністрації, відповідальність і обов'язки осіб, допущених до роботи на устаткуванні телекомунікаційної мережі);

– рівень законодавства і соціального середовища (законодавство про інформацію і телекомунікації, зокрема, [1-5], про безпеку [6], про соціальні гарантії трудящих [7]).

Відповідно до вище викладеного, розподіл відповідальності за надання гарантій безпеки, збереження цілісності і забезпечення якості телекомунікаційних послуг є багаторівневою моделлю, архітектура якої представлена на рис. 1.

У відповідністю з прийнятою концепцією розподілу відповідальності між учасниками ринку телекомунікацій у подальшому будемо приділяти увагу технічному захисту НССЗУ від загроз природного, техногенного характеру та від впливів людського фактору – внутрішніх загроз з боку персоналу та зовнішніх загроз з боку партнерів, клієнтів, конкурентів і звичайних зловмисників.

Концепція розподілу власності на об'єкти системи зв'язку

Крім розподілу прав та обов'язків взаємодіючих суб'єктів стосовно інформації, що передається, ключовим моментом для ефективного функціонування НССЗУ є розподіл прав власності, тобто володіння, розпорядження та користування об'єктами системи. Згідно з теорією цивільного права і законодавством України, побудованим на основі цієї теорії, оператор телекомунікацій є власником системи зв'язку, провайдер має право розпорядження системою, а власник інформації та створювач інформаційного контенту мають право користування системою за договором з власником системи.

Такий розподіл майнових прав є оптимальним для забезпечення балансу інтересів держави та приватних осіб як користувачів системи. Тільки будучи власником НССЗУ, уповноважений державою оператор зможе врівноважити інтереси державних користувачів системи зв'язку, користувачів інших форм власності, які бажають передавати інформацію з обмеженим доступом, творчих робітників чи колективів – створювачів інформаційного контенту для широкомовного розповсюдження та власників цього інформаційного контенту. Будь-яке інше співвідношення прав майнової власності призведе до неприпустимого зниження або взагалі до неможливості забезпечення належного рівня цілісності, достовірності та безпеки інформації при передаванні через НССЗУ.

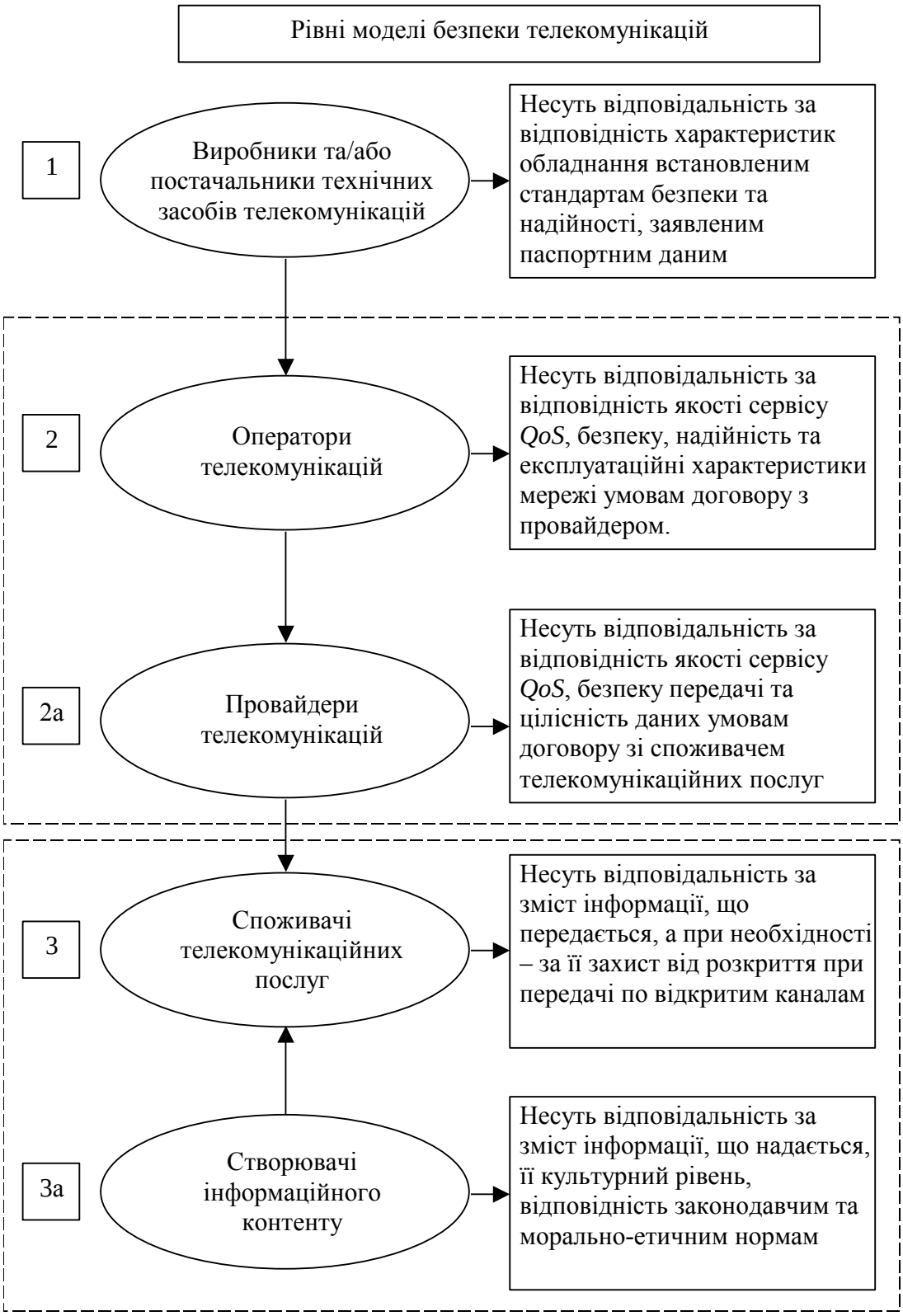

Рис. 1. Багаторівнева модель захисту інформації в мережі

Висновок

У даній статті розроблено багаторівневу модель захисту інформації в мережі. Дану модель гармонізовано з майновими правами та громадянськими обов'язками учасників телекомунікаційного ринку. При використанні багаторівневої моделі вдається оптимізувати систему захищеного обміну інформацією у відкритих мережах за критерієм "ефективність – вартість". У подальшому планується провести дослідження методів оптимізації за ключовими показниками ефективності як багатомірного (векторного) показника.

Список літератури

1. Про телекомунікації. Закон України від 18.11.2003 № 1280-IV.

2. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР.

3. Про інформацію. Закон України від 02.10.1992 № 2657-XII.

4. Про телебачення і радіомовлення. Закон України від 21.12.1993 № 3759-XII.

5. Про авторське право і суміжні має рацію. Закон України від 23.12.1993 № 3792-XII.

6. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII.

7. Про охорону праці. Закон України від 14.10.1992 № 2694-XII.

8. Конституція України // Відомості Верховної Ради України, 1996 р. – №30. – ст. 141

9. Закон України "Про Службу безпеки України" від 25 березня 1992 року // Відомості Верховної Ради, 1992. – № 27. – ст.382 (зі змінами).

10. Марущак А.І. Свобода слова та інформація з обмеженим доступом: співвідношення понять // Бюлетень Мін'юсту України. – К., 2005. – №.6 (44) – с. 44 – 49.

Статтю подано до редакції 26.02.2015