УДК 621.391

Добуш Ю. Д., асп.**; Демидов І. В.**, к.т.н., **Климаш М. М.**, д.т.н., проф.
(Національний університет «Львівська політехніка»)

АНАЛІЗ ЗАГРОЗ ПЕРЕДАВАННЯ ДАНИХ У СИСТЕМІ «ЕЛЕКТРОННОГО УРЯДУВАННЯ»ТА ОЦІНКА ЇЇ ЕФЕКТИВНОСТІ

Добуш Ю. Д., Демидов І. В., Климаш М. М. Аналіз загроз передавання даних у системі «електронного урядування» та оцінка її ефективності. Статтю присвячено аналізу загроз поширенню даних у інфокомунікаційних системах, що реалізують концепцію державного управління в Інформаційному суспільстві – «електронне урядування». Виконано класифікацію таких загроз та визначено відповідні методи протидії. Запропоновано критерії оцінювання ефективності захищених мультисервісних систем передавання даних для інфраструктури «електронного урядування».

Ключові слова: ІНФОКОМУНІКАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО, ЕЛЕКТРОННЕ УРЯДУВАННЯ, МУЛЬТИСЕРВІСНА СИСТЕМА, ПЕРЕДАВАННЯ ДАНИХ, ЗАГРОЗИ

Добуш Ю. Д., Демидов И. В., Климаш М. М. Анализ угроз передачи данных в системе «электронного правительства» и оценка её эффективности. Статья посвящена анализу угроз распространению данных в инфокоммуникационных системах, реализующих концепцию государственного управления в информационном обществе – «электронное правительство». Выполнена классификация таких угроз и определены соответствующие методы противодействия. Предложены критерии оценки эффективности защищенных мультисервисных систем передачи данных для инфраструктуры «электронного правительства».

Ключевые слова: ИНФОКОММУНИКАЦИОННАЯ СИСТЕМА, ИНФОРМАЦИОННОЕ ОБЩЕСТВО, ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО, МУЛЬТИСЕРВИСНАЯ СИСТЕМА, ПЕРЕДАЧА ДАННЫХ, УГРОЗЫ

Dobush Yu. D., Demydov I. V., Klymash M. M. Analysis of the data transmission threats into e-Government system and its efficiency evaluation. This article examines the threats of data propagation into info-communication systems that implementing the concept of governance in the Information Society – "electronic Government". The classification of such threats was carried out and appropriate methods of counteraction are determined. The criteria of the evaluating of effectiveness of secure multi-service transmission systems for "e-Government" infrastructure are proposed.

Keywords: INFO-COMMUNICATION SYSTEM, INFORMATION SOCIETY, ELECTRONIC GOVERNMENT, E-GOVERNMENT, MULTI-SERVICE SYSTEM, DATA TRANSMISSION, THREAT

Вступ. Розвиток концепції «електронного урядування» в Україні. Розвиток сучасного інформаційного суспільства неможливий без формування та впровадження глобально доступної моделі «електронного уряду» (англ. e-Government) – моделі державного управління, яка заснована на використанні сучасних інформаційних та комунікаційних технологій з метою підвищення ефективності та прозорості влади, а також встановлення суспільного контролю над нею. У даній моделі вся сукупність як внутрішніх, так і зовнішніх зв'язків і процесів підтримується й забезпечується відповідними інформаційно-комунікаційними технологіями, базами даних та обчислювальними засобами [1, 2]. Іншими словами, необхідною умовою переходу до електронного уряду є широка інформатизація всіх процесів у звичайній діяльності міністерств, відомств, місцевих органів виконавчої влади, причому як внутрішніх, так і зовнішніх.

Виділяють 5 основних етапів розвитку системи Електронного уряду [3]:

1. Створення веб-ресурсів міністерств і відомств, що містять інформацію про їхню місію і напрямки діяльності. Сайти державних органів, як правило, не підтримуються централізовано і не об'єднуються в єдиний портал.

2. Введення елементів інтерактивності (наприклад, відправлення питань і одержання відповідей громадян за допомогою електронної пошти). Постійно публікуються новини про діяльність державних органів влади. В Україні перші два етапи де-факто реалізовані протягом останніх 5 років.

3. Поява повноцінної інтерактивності – можливості здійснювати операції (сервіси) в режимі он-лайн (наприклад, сплатити штрафи, замовити паспорт, продовжити дію деяких ліцензій і патентів тощо). Така конкретизація роботи електронного управління, що полягає вже не стільки в інформуванні, скільки в обслуговуванні, припускає створення спеціальних сайтів для підтримки цих сервісів не тільки для центральних, але і для міських і навіть

районних органів влади. Даний етап успішно реалізований у Великобританії, США та деяких інших країнах, а в Україні внаслідок впливу застарілої організаційної парадигми у сфері держаного управління знаходиться в зародковому стані.

4. Створення об'єднаних мультимедійних порталів різних відомств і служб, через які можна здійснювати будь-які види трансакцій, для яких раніше було потрібно звертатися безпосередньо в державний орган. Через регіональні портали стає можливою реєстрація підприємств, оформлення фінансових документів, легалізація іноземних документів тощо. З'являються регіональні портали, що поєднують у собі як увесь спектр державних послуг, так і послуги недержавного сектору – підключаються системи електронної комерції, інтернет-банкінгу. Впровадженню даного етапу сприятиме глибоке переродження інформаційних технологій в Україні, спрямоване на підвищення ефективності роботи державного апарату за рахунок здешевлення утримання відповідних організаційних структур, пришвидшення реакцій на всі актуальні події та запити соціально-економічного, виробничого, екологічного та фіскального характеру, спрощення процедур доступу та звернень громадян, скорочення використання паперових носіїв та форм для ведення справ.

5. Створення електронної системи державного управління на основі єдиних стандартів, а також урядового порталу як єдиної точки доступу до всіх послуг – і для громадян, і для бізнесу. Більшість фахівців вважає, що найвищим ступенем розвитку електронної демократії є запровадження електронної системи волевиявлення (електронного голосування). На жаль впровадження даного етапу в Україні потребує значних політичних трансформацій органів влади в бік відкритості та редукування їх організаційної структури, службових апаратів, а також нівелювання можливості корумпованого впливу держслужбовців на прийняття рішень із одночасним підвищенням рівня контролю та прямої відповідальності їх керівництва.

Останніми роками в Україні спостерігається перехід до стадії практичного формування урядових інституцій на основі визнання цінностей інформаційного суспільства шляхом концентрації управлінських документальних потоків у інфокомунікаційній площині. Розробленню Концепції електронного урядування в Україні присвячений ряд законодавчих ініціатив та доручень Кабінету Міністрів України, зокрема характерним є курс на реалізацію механізмів електронного урядування (доручення Прем'єр-міністра України № 3923/0/1-11 від 25 січня 2011 року) стосовно запровадження документообігу з використанням електронного цифрового підпису, щодо центру сертифікації ключів, щодо формування державного реєстру персоніфікованих баз даних, регламенту електронного документообігу в органах виконавчої влади.

Застосування інфокомунікаційних технологій при передаванні, обробленні та зберіганні персональних даних громадян, управлінської та іншої, як правило, мультимедійної інформації урядових міністерств та відомств в Україні стикається з низкою специфічних загроз – в основному щодо безпеки інформації та несанкціонованого доступу до неї. Надамо стислу класифікацію та аналіз таких загроз.

Класифікація загроз поширенню даних в інфокомунікаційній площині «електронного урядування». Загрози утворюються внаслідок існування типових сценаріїв можливих дій порушників (атак), що описують послідовність (алгоритм) дій груп та окремих порушників, способи їх дій на кожному етапі. Не будемо зупинятися на класифікації типів порушників, оскільки їх діяльність може мотивуватися ситуативно та не була метою даного дослідження. Натомість, мета даної роботи – дослідити можливі інфокомунікаційні загрози функціонуванню електронного урядування в Україні та запропонувати методи протидії таким загрозам.

Оскільки для реалізації інфокомунікаційної системи передавання інформації згідно концепції «електронного урядування», що функціонує в захищеному режимі і реалізує сценарій «комп'ютер-комп'ютер», пропонується використовувати можливості операційних систем (наприклад ОС Windows), апаратні можливості сучасних ПЕОМ та можливості розподілених обчислювальних мереж, розглянемо можливі види атак порушника з використанням наведених тут засобів. Аналіз проведемо шляхом визначення найбільш

важливих, з точки зору безпеки, ділянок у інфокомунікаційній системі. Крім того, проводячи аналіз можливих атак на інфокомунікаційну систему передавання даних ми не розглядатимемо атаки безпосередньо на операційні системи, оскільки дослідження вразливості ОС виходить за рамки дослідження. Врахуємо також, що атаки на різні типи даних в цілому аналогічні атакам на мультимедійні інформаційні потоки [4].

Спрощена модель передавання даних через IP-мультисервісну мережу в захищеному від несанкціонованого доступу (НСД) режимі представлена на рис. 1.

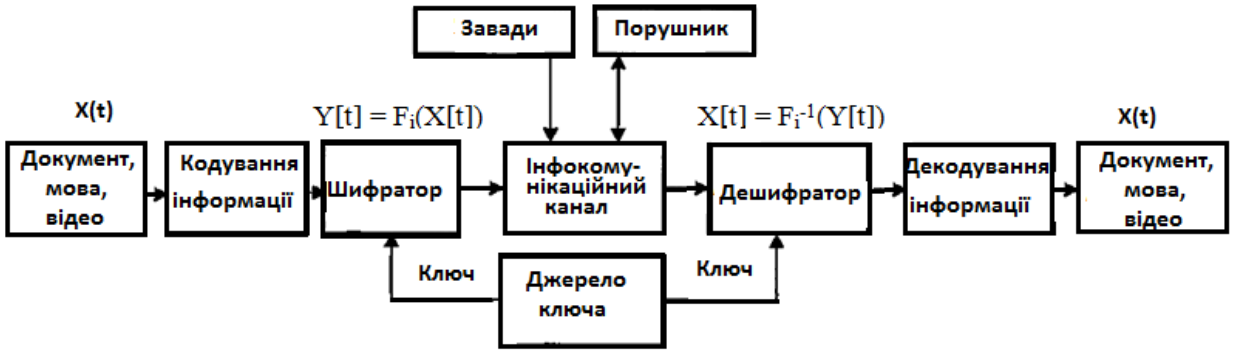

Рис. 1. Модель передавання даних в захищеному від НСД режимі

Під математичною моделлю атаки будемо розуміти її формалізований опис, побудований з точки зору прийнятої моделі захищеності. В даному дослідженні приймемо до уваги ймовірнісну та теоретико-ігрову моделі захищеності та атак. У рамках ймовірнісної моделі значущою буде ймовірність запобігання атаці системою захисту, ймовірність її виявлення та локалізації, або, з іншого боку, імовірність успішного завершення атаки. Ця ймовірність в загальному випадку буде залежати від часу, а отже від характеру часової залежності і становитиме суть моделі атаки. Перерахованим в даній роботі атакам відповідають дві математичні моделі: модель перебору і модель перевірки [7].

Атаки, пов'язані з перевіркою деякого числа варіантів критично важливих параметрів безпеки інфокомунікаційної системи, можна описати моделлю перебору. Типовим прикладом таких атак є характерна для більшості сучасних систем, у тому числі і для системи «електронного урядування», атака підбором паролю або ключа (атаки типу А7, див. табл. 1). В табл. 1 для зручності кожному типові атаки привласнено унікальний індекс, що складається з префікса «А» і номера (табл. 1).

Атаки, засновані на помилках (недоліках) в системі безпеки і їм подібні, можна описати за допомогою моделі перевірки. Такі атаки використовують уразливість системи захисту, перевіряючи єдиний варіант – наявність або відсутність даної уразливості:

$$p(t) = \begin{cases} 1, \text{якщо уразливість існує;} \\ 0, \text{якщо уразливості немає.} \end{cases} \quad (1)$$

Дана математична модель відображає більшість існуючих на даний час атак (А1-А6, А8-А10), оскільки під поняття вразливості підпадають як помилки (недоліки) в системі безпеки, так і помилки адміністрування [5].

З точки зору теоретико-ігрової моделі ключове значення має шкода, яка заподіюється застосуванням тієї або іншої атаки і ймовірність запобігання цій атаці різними методами захисту. Збиток є основною характеристикою при описі атак з позицій цієї моделі. Проблема полягає в тому, що оцінити можливий збиток буває досить складно, а самі оцінки, як правило, виявляються частковими і суб'єктивними, тому поширити їх на всю множину застосування інфокомунікацій, захищених від несанкціонованого доступу, виявляється проблематично [6]. Логічним виходом у даній ситуації є відмова від ранжування і прийняття всіх існуючих атак рівно небезпечними.

При аналізі вразливостей захищеної інфокомунікаційної системи «електронного урядування» виділимо атаки, засновані не на помилках в її програмному забезпеченні, які

розробник системи може де-факто виправити за лічені дні, а на концептуальних властивостях функціонування системи.

Атаки на інфокомунікаційну систему, що працює в захищеному режимі Табл. 1.

Індекс	Назва атаки та можливі причини
A1	Доступ до інформації в обхід інфокомунікаційної системи, в обхід ОС і в обхід ПЕОМ (недоліки в організаційних заходах із захисту від несанкціонованого доступу, недбальство/саботаж причетних осіб або шпигунська діяльність)
A2	Доступ до інформації в обхід власне мережної системи (причини аналогічні пункту A1)
A3	Отримання інформації впровадженням «закладок» в модулі введення / виведення документальної/мультимедійної інформації ОС (наприклад, у Windows DirectSound) (недоліки в організаційних заходах із захисту від несанкціонованого доступу, цілеспрямована діяльність групи осіб з метою несанкціонованого доступу до інформації, недоліки системи мережної безпеки)
A4	Отримання інформації впровадженням «закладок» у модулі компресії / декомпресії ОС та стороннього програмного забезпечення (як для мультимедійної так і для документальної інформації) (причини аналогічні пункту A3)
A5	Отримання ключа та / або інформації, що передається впровадженням «закладок» у програмні модулі захисту від несанкціонованого доступу ОС та стороннього програмного забезпечення для шифрування (цілеспрямована діяльність групи осіб з метою несанкціонованого доступу до інформації, недоліки системи мережної безпеки)
A6	Збір паролів програмою типу "Троянський кінь" (причини аналогічні пункту A5)
A7	Перехоплення пакетів з даними (виконується групою осіб через підключення до інфокомунікаційних каналів, атака неефективна в разі стійких алгоритмів шифрування, цифрового підпису та спеціальної розподіленої архітектури передавання /зберігання інформації)
A8	Нав'язування користувачеві неправдивого повідомлення (причини та коментар аналогічні пункту A7)
A9	Відмова в обслуговуванні (DoS, атака виконується на визначені заздалегідь інформаційні ресурси групою осіб через використання розподілених підконтрольних мереж типу «бот-нет», що виконують розсилання екстремально великої кількості запитів до серверів інфокомунікаційної системи, призводячи до їх перевантаження та/або недоступності)
A10	Підміна програмного забезпечення інфокомунікаційної системи «електронного урядування»(причини аналогічні пунктам A1, A3)

Розглянуті окремі типи атак не завжди можуть привести порушника до позитивного для нього кінцевого результату, тому активність порушника в загальному випадку може складатися з деяких послідовностей атак, які залежать як від цілей порушника, так і від його можливостей. Можливі варіанти послідовностей застосування атак складають стратегії дій порушника. У кожній конкретній атакуючій дії може бути реалізована тільки одна з можливих стратегій. Для аналізу загроз захищеності системи «електронного урядування» велике значення буде мати розуміння взаємозв'язків між елементами цієї множини – можливими стратегіями дій порушника і складовими його атак. Найбільш зручним способом відображення і дослідження цих взаємозв'язків є граф, що пояснюється такими особливостями стратегії дій порушника, як спрямованість та спільність складових елементів атаки.

Коротко розглянемо стратегії дій порушника, спрямовані на несанкціонований доступ (НСД) до інформації або на порушення роботи інфокомунікаційної системи «електронного урядування». Граф можливих стратегій дій порушника представлений на рис. 2.

На рис. 2 елементи Ai позначають атаки, Sj – проміжні результати (S0 відповідає вихідному стану, S1 відповідає стану, коли порушникові відомий ключ), НСД і DOS – позначають результати дій порушника.

При визначенні якості захисту інфокомунікаційної системи нас буде цікавити максимальна серед усіх можливих стратегій дій ймовірність успіху, тобто критичний шлях графу. Найбільш ймовірними та успішними, а також і популярними в Україні стратегіями дій порушника згідно рис. 2 є три наступні: A7-S1-НСД; A7-S1-A8-НСД; A9-DOS. Однак імовірність успіху цих стратегій дій (A7-S1-НСД або A7-S1-A8-НСД) за прийнятний час низька при виборі стійкого шифру.

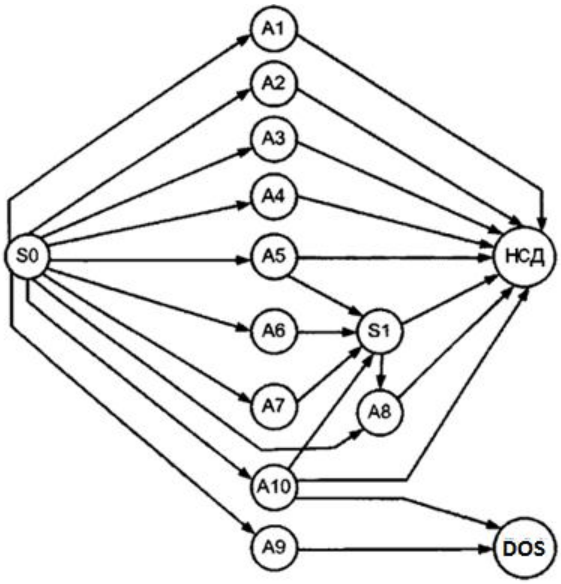

Рис. 2. Граф можливих стратегій дій порушника

Для загальнодоступних мереж критичний шлях A9-DOS завжди має ймовірність успіху, яка дорівнює 1, на підставі чого можна прийти до висновку, що забезпечити якісну та доступну комунікацію через інфокомунікаційну систему «електронного уряду», не використовуючи додаткові методи захисту, важко (особливо у випадку якщо порушник володіє значними технічними засобами, розосередженими по різних сегментах мережі – наприклад створив «бот-нет»).

Після проведеного розгляду можливих загроз поширенню даних в інфраструктурі інфокомунікаційної системи «електронного урядування» у вигляді аналізу можливостей атак з метою отримання НСД або блокування роботи такої системи, стає актуальною та зрозумілою необхідність запропонувати і проаналізувати відповідні контрзаходи та методи запобігання подібним загрозам. Таким чином, у табл. 2 виділимо 4 основні групи методів та заходів (М1-М4) запобігання атакам, наведеним в табл. 1.

Методи та заходи запобігання атакам на систему «електронного урядування» Табл. 2.

Індекс	Опис
М1	Організаційні та інженерно-технічні методи, спрямовані на забезпечення надійного захисту приміщення проти фізичного проникнення в приміщення випадкових осіб, здатних принести записуючі або радіопередавальні пристрої, а також заходи спрямовані на нейтралізацію радіопередавальних або записуючих пристроїв; пріоритетне використання захищених баз даних і мереж урядового зв’язку.
М2	Використання лише сертифікованого програмного забезпечення, якісний антивірусний захист, здатний запобігти зараженню програмного забезпечення шкідливими троянськими програмами, несанкціонованому мережному доступові до ПЕОМ, а також обмеження прав звичайних користувачів в частині встановлення програмного забезпечення, зміни мережних параметрів. Також організаційні та інженерно-технічні методи, у напрямку на забезпечення цілісності комп'ютерного обладнання та обмеження доступу в приміщення і фізичного доступу до комп'ютерів, у тому числі жорстка регламентація порядку роботи на комп'ютерах системи, порядку їх ремонту, заміни і т.д.
М3	Обмеження завантаження альтернативних операційних систем, щоб запобігти, для прикладу, заміні бібліотеки advapi32.dll, що здійснює перевірку цифрового підпису модулів захисту даних в ОС Windows.
М4	Використання методів та режимів шифрування в яких неможлива або не має сенсу маніпуляція блоками шифрованих; виконання дій з додавання до кожного пакету з відкритою інформацією деяких даних, які характеризують унікальність пакету, наприклад час і / або порядковий номер пакету, використання цифрових підписів усіх документів, використання захищеної розподіленої архітектури всіх баз даних.

При аналізі якості захисту реальної інфокомунікаційної системи «електронного урядування» до уваги необхідно приймати адміністративні, організаційні та інженерно-технічні методи, а також використання додаткових програмних або апаратних засобів захисту. Найбільше значення при цьому будуть мати засоби захисту від атак, що входять до стратегій дій порушника, яким не запобігають відповідні засоби власне інфокомунікаційної системи: *обмеження* фізичного доступу в приміщення, де розташовані комп'ютери; *обмеження* фізичного доступу до комп'ютерів; *використання* сертифікованого програмного забезпечення; *обмеження* використання засобів мережного і локального адміністрування; *наявність* розгорнутого плану дій з протидії атакам виду DoS «Відмова в обслуговуванні».

При цьому необхідне використання спеціальної серверної архітектури та інтелектуального серверно-шлюзового програмного забезпечення, що визначатиме характер і походження «шкідливих» запитів та відкидатиме їх.

При використанні для оцінки теоретико-ігрової моделі, якість захисту можна оцінити як відношення кількості передбачених політикою безпеки атак до загальної кількості можливих атак на систему, однак така оцінка в класичному формулюванні теоретико-ігрової моделі можлива тільки в статичному режимі і не є такою показовою, як ймовірнісна.

Оцінювання ефективності захищених мультисервісних інфокомунікаційних систем передавання даних для інфраструктури «електронного урядування». Дослідження будь-якої складної інфокомунікаційної системи включає в себе комплекс питань, пов'язаних з вибором методології дослідження; дослідженням програмної та телекомунікаційної архітектури, програмної платформи; застосуванням методів оцінки якості програмних застосувань, гнучкості реалізації і тестування функціонального змісту системи; формуванням вимог рекомендаційного характеру, орієнтованих на підвищення якості продукту. Важливим є дослідження структури систем подібного класу з метою виявлення загальних елементів структури, вироблення єдиних вимог до їх реалізації. Це дає можливість виконати дослідження з позицій універсального підходу, що дозволить використовувати єдині методи для побудови цілого класу стандартизованих на державному рівні систем.

Як вже стало зрозуміло, основним методом структуризації в нашому дослідженні є системний метод, який є основою теорії системного аналізу. У системно-структурному методі акцент переважно робиться на дослідженнях внутрішньої структури системи, внутрішніх зв'язків, тоді як системний підхід, крім цього, передбачає дослідження поведінки системи та її елементів залежно від зв'язків із зовнішнім середовищем, від походження ситуації, в яку потрапляє система. Важливою рисою системно-структурного методу є те, що він разом із розглядом структурних зв'язків розглядає і структуру функцій системи.

Дослідити структуру складних мультисервісних мережних систем можна з використанням двох підходів: інформаційного та функціонального [8]. Інформаційний підхід передбачає аналіз на основі розгляду транспортних потоків даних, що циркулюють між елементами інфокомунікаційної системи, у той час як функціональний ґрунтується на розгляді різноманітних зв'язків усередині системного комплексу, виділяючи в окремі одиниці функціонально завершені компоненти [9].

Функціональний підхід. Функціональна схема повинна відображати загальну структуру захищеної інфокомунікаційної системи передавання даних у інфраструктурі «електронного урядування» у вигляді множини закінчених елементів, що реалізують певні функції в рамках вимог, які пред'являються до систем зв'язку для оперативного обміну повідомленнями різного типу (наприклад, документальними або мультимедійними), а також надають різні додаткові діагностичні або сервісні можливості. Деталізація функціональної схеми передбачає врахування конкретної програмно-апаратної платформи, на базі якої будується реалізація, що накладає свій відбиток на структуру зв'язків і набір функціональних компонентів, присутніх у структурній схемі. Функціональна схема інфокомунікаційних систем зв'язку для реалізації концепції «електронного урядування» повинна передбачати високий рівень надійності роботи, регламентувати допустимі часові затримки інформації, ступінь захисту від НСД, визначати програмно-апаратні середовища оброблення і передавання даних.

Структурно інфокомунікаційні системи зазначеного типу складаються з наступних підсистем: *введення-виведення* звукового і відео сигналу, зображень, зокрема документів та іншої важливої інформації; *цифрової обробки* зображень, звукового і відео сигналу (компресія і шифрування документів та мультисервісних інформаційних потоків); *серверної* інфраструктури, баз даних та відповідних систем управління базами даних і взаємодії між ними; *управління,* візуалізації і реєстрації статистичної та діагностичної інформації, що відображають процес функціонування системи; *телекомунікаційних* мережних інтерфейсів.

Компоненти підсистем, які відповідають за оброблення інформації, що надходить до системи «електронного урядування», зберігається в ній та виводиться користувачам, створюються на основі програмного забезпечення сертифікованих розробників, яким комплектується більшість робочих станцій інфокомунікаційної системи в залежності від їх призначення та функціональності.

Забезпечення ефективного функціонування телекомунікаційних інтерфейсів у конвергентній інфокомунікаційній системі визначає як якість отриманого цифрового каналу передавання даних (у IP-мережі), так і економічний ефект від застосування технологій і рішень «електронного урядування».

Інформаційний підхід. З точки зору формалізації структури та інформаційних потоків захищеної інфокомунікаційної системи більш універсальним є інформаційний підхід, оскільки він надає можливість кількісно і якісно проаналізувати та представити внутрішню структуру зв'язків системи на основі графоаналітичних методів, а також визначити найбільш важливі, з точки зору безпеки, ділянки.

Особливістю систем, що досліджуються нами, як і багатьох інших сучасних інфокомунікаційних систем є модульність. Використання при розробці програмного забезпечення програмної архітектури заснованої на динамічному підключенні компонентів і модулів, у тому числі вбудованих в ядро ОС, дозволяє вже на рівні загального проектування архітектури інфокомунікаційної системи «електронного уряду» збільшити надійність, а також спростити розробку, тестування і налагодження створюваного програмного забезпечення. На рівні експлуатації спрощується оновлення складових частин системи.

Визначимо критерії оцінювання ефективності реалізації інфокомунікаційної системи передавання даних для інфраструктури «електронного урядування», що функціонує в захищеному режимі.

Для складних інформаційних розподілених апаратно-програмних систем практично неможливе вироблення якого-небудь єдиного сукупного критерію, тому оцінка ефективності може бути проведена на підставі дослідження декількох груп часткових показників [4], вага яких може бути різною у кожному конкретному випадку [7]. Оцінка за кожним частковим показником виводиться за деякою уніфікованою шкалою.

У якості таких груп автором були обрані наступні групи часткових показників:

1. Якісні показники (М), що характеризують суб'єктивні результати вимірювання та оцінювання якості поширення даних на основі оцінок окремих експертів. Вони характеризують ефективність та ступінь відповідності системи в цілому встановленим при проектуванні вимогам.

2. Технологічні показники (Т), що характеризують якість програмних рішень із загальних позицій сучасної технологічної бази. Для систем реального часу такими показниками можуть бути коефіцієнти використання ЦП (T_1) і мережних ресурсів системи (T_2), простота і функціональність налаштування параметрів системи (T_3), оперативність відображення необхідної статичної та динамічної інформації (T_4), надійність функціонування (T_5), можливість динамічного нарощування функціональних можливостей щодо алгоритмів компресії (T_6) і захисту інформації (T_7), наприклад, шляхом використання кодеків та / або алгоритмів для захисту від несанкціонованого доступу на основі апаратних інтерфейсів і модулів для захисту від несанкціонованого доступу операційної системи.

3. Показники, що характеризують якість захисту інформації (К): стійкість захисту пакетів даних - алгоритм шифрування (K_1), сукупна довжина ключа шифрування (K_2), алгоритм хешування (K_3), довжина криптовставки (K_4), простота і безпека розповсюдження ключів (паролів) для захисту від несанкціонованого доступу (K_5), можливість вести контроль і налаштування режимів захисту від несанкціонованого доступу трафіку IP-телефонії (K_6), можливість використання сертифікованих СБУ алгоритмів і модулів захисту від несанкціонованого доступу для того, щоб офіційно застосовувати системи електронного документообігу, цифрових репозиторіїв та IP-телефонії в органах державної влади і силових відомствах (K_7).

4. Показники, що характеризують сукупну складність реалізації програмного забезпечення (Q), що включає в себе: алгоритми компресії зображень, мови та відео (Q_1), захисту даних (Q_2), формування і обробки IP-пакетів (Q_3) та їх передачі / прийому через IP-мережі (Q_4), алгоритми керування обслуговуванням з'єднання, тобто прийняття рішень про те, яким чином має бути встановлена комунікація між користувачами (Q_5).

5. Економічні показники (E), що характеризують витрати, пов'язані із забезпеченням необхідних функціональних характеристик, які складаються з вартості проектування і розробки програмного забезпечення (E_1), мінімально необхідної конфігурації апаратних засобів (E_2) та вартості експлуатації функціональних підсистем (наприклад, підсистеми IP-телефонії) (E_3).

У підсумку загальний критерій оцінки ефективності КЕ захищеної мультисервісної інфокомунікаційної системи передавання даних для інфраструктури «електронного урядування», набуде вигляду функції п'яти змінних:

$$K_E=(M, T, K, O, E).$$

Висновки. У результаті виконаних досліджень можливо сформулювати наступні висновки:

1. Проаналізовано загрози поширенню даних у інфокомунікаційних системах, що реалізують концепцію державного управління в Інформаційному суспільстві – «електронне урядування». Зазначені загрози визначено та класифіковано у вигляді множини можливих атак гіпотетичного порушника. Охарактеризовано найбільш імовірні стратегії втручання в роботу захищених інфокомунікаційних систем інфраструктури «електронного урядування».

2. Запропоновано методичні рекомендації, що дозволяють знизити ризики несанкціонованого доступу до захищуваної інформації і порушення нормального функціонування мультисервісної інфокомунікаційної системи передавання даних, як частини інфраструктури «електронного урядування».

3. На основі наведеного аналізу загроз показано, що в загальному випадку для забезпечення захищеності зв'язку через інфраструктуру «електронного урядування» засобів власне захищеної інфокомунікаційної системи недостатньо, оскільки ці засоби не можуть запобігати обходу системи безпеки на фізичному рівні і на нижньому рівні основних модулів системи. Показано, що захищеність можна забезпечити тільки комбінацією технічних і організаційних методів та заходів із застосуванням додаткових технічних засобів захисту.

4. Розроблено загальний критерій оцінки ефективності захищеної від несанкціонованого доступу мультисервісної інфокомунікаційної системи передавання даних для інфраструктури «електронного урядування».

Література

1. World Bank: Definition of E-Government [Електронний ресурс] / – Режим доступу: http://www.worldbank.org/egov/World Bank: Definition of E-Government

2. Clift S. E-Government and Democracy Report, 2004.

3. «Електронний уряд» [Електронний ресурс] / – Режим доступу : http://uk.wikipedia.org/wiki/Електронний_уряд

4. Бакланов И. Г. NGN: принципы построения и организации. –М.: Эко-Трендз, 2008. – 399с.

5. Нопин С.В. Моделирование защиты речевой информации с помощью персонального компьютера. / С.В. Нопин, В.Г. Шахов // Омский научный вестник. – 2004. – №4(29). – С. 124-126.

6. Родионов Д. Е. Методика анализа защищенных систем IP-телефонии. Автореф. дис. .канд. техн. наук / Д. Е. Родионов. – М., 1999. – 24 с.

7. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.

8. Волкова В. Н. Теория систем / В. Н. Волкова, А. А. Денисов – М.: Высшая школа, 2006. – 512 с.

9. Саати Т. Принятие решений. Метод анализа иерархий / Т. Саати – М.: Радио и связь. – 1993. – 278 с.