Інші події [3]:

- атаки на верхні рівні стека протоколів, що викликають спрацьовування "традиційної" IDS;
- сторонній адміністративний трафік, адресований точці доступу;
- постійне дублювання або повтор пакетів з даними;
- пакети з даними, у яких зіпсовані контрольні суми або MIC, формовані на канальному рівні;
- багаторазові спробами одночасного приєднання до мережі.

Такі події можуть свідчити про успішну або невдалу атаку, про наявність хоста з некоректними настроюваннями безпеки, про спроби одержати контроль над точкою доступу та змінити її конфігурацію, про застосування інструментів для впровадження свого трафіка, про DoS-атаку проти хостів із включеним протоколом 802.11i тощо.

Висновки

В результаті проведеної роботи проаналізовано, досліджено та виділені типові загрози інформації – потенційно несприятливі дії на інформацію. Проведений аналіз загроз інформації є одним з найбільш важливих питань при побудові захищених безпровідних мереж. Такий аналіз має виявити можливі загрози інформації, аномалії та показати з якого боку мережі нам слід чекати атаки на безпровідні мережі. Виявлення таких аномалій - непросте завдання, по скільки практично не існує двох однакових бездротових мереж. Тому ефективне застосування IDS у бездротових мережах можливо тільки після тривалого періоду детального дослідження конкретної мережі. При розгортанні системи необхідно чітко розуміти, що, як і навіщо хочемо аналізувати і тільки тоді сконструювати потрібну систему безпеки. Зібравши значний обсяг статистичних даних про роботу конкретної мережі, можна вирішити, що є аномальним поводженням, а що – ні та ідентифікувати проблеми зі зв'язком, помилки користувачів і атаки.

Література

1. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО «ТИД ДС», 2004. – 992 с.

2. Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньган. - М.: ДМК Пресс, 2004. - 616 с.: ил.

3. Норткатт С. Обнаружение вторжений в сеть / С. Норткатт, Д. Новак, Д. Маклахлен. – Изд-во "ЛОРИ", 2001. - 384 с.

Надійшла до редакції
24.1.2013 р.

УДК 004

Є.С. ГРИЦАЮК, В.М. ЧЕШУН
Хмельницький національний університет

ПРОБЛЕМНІ АСПЕКТИ АВТОМАТИЗАЦІЇ В ПІДВИЩЕННІ НАДІЙНОСТІ РОБОТИ СИСТЕМИ КЛІЄНТ-БАНК

Досліджено проблеми забезпечення надійної роботи системи “Клієнт-банк” в умовах ризику спроб несанкціонованого доступу до приватної інформації та спроб крадіжок коштів. На сьогоднішній день в банківській сфері, з впровадженням автоматизованих технологій обробки інформації та розширенням спектру послуг, які надаються, і прискоренням оборотності коштів ці проблеми значно загострюються та потребують негайного вирішення. Визначено основні напрямки автоматизованого розв’язання виявлених проблем.

Ключові слова: інформація, система “Клієнт-банк”, захист інформації, засоби криптографії.

Investigated the problems to ensure reliable operation of the system "Client-Bank" at risk of unauthorized access to personal information and attempted theft of funds. To date, with the introduction of automated information processing technologies, expanding the range of services provided and to accelerating the turnover of funds greatly exacerbated these problems and require urgent attention in the banking industry. Defined the main directions of automatic decision of problems.

Keywords: information, system "Client-Bank", protection of Information, means of cryptography.

Вступ

Спосіб дистанційного надання послуг клієнтам у сфері банківського обслуговування перетворився на цілком самостійну форму ведення бізнесу. Технологія дистанційного банківського обслуговування “домашній банкінг” (home banking) або “віддалений банкінг” (remote banking), що дає змогу клієнту отримувати банківські послуги без відвідин офісу банку, існує вже більше двадцяти років.

Як видно із самої назви, “віддалений банкінг” є формою надання банківських послуг не в банківському офісі при безпосередньому контакті клієнта і банківського службовця, а в офісі клієнта, в його будинку і скрізь, де це допускається системою і є зручним.

Технологія “home banking” була розроблена на початку 80-х років XX ст., коли банки Західної

Європи розпочали активну конкуренцію за залучення нових клієнтів. Датою народження "домашнього банкінгу" вважається 1983 рік, коли будівельне товариство Nottingam Building Society разом з Банком Шотландії та телефонною компанією British Telekom впровадило систему Homelink.

Система "home banking" сьогодні – це зручна, оперативна, мобільна та технологічно надійна форма дистанційного банківського обслуговування, яка надає клієнту майже увесь спектр банківських послуг "на дому". Такі системи успішно функціонують як у зарубіжних банках, так і в банках України. У нашій країні найбільш розповсюдженою системою дистанційного банківського обслуговування є "клієнт-банк".

Питання щодо сутності системи "клієнт-банк", її особливостей та призначення, а також механізму роботи містяться у працях таких вітчизняних науковців, як І. Брітченко, О. Вовчак, В. Горобець, Н. Єрьоміна, І. Красовська, В. Міщенко, А. Нікітін, А. Олійник, І. Рогач, В. Степаненко та інших учених-економістів, але велика кількість проблем підвищення надійності роботи системи залишається невирішеною і з розвитком сфери банківських послуг набуває ще більшої актуальності.

Постановка задачі

Інформація – одне з найважливіших джерел процвітання будь-якої держави, банку чи фірми. Недарма кажуть: "Хто володіє інформацією, той володіє світом". Будь-яке управлінське рішення базується і коштує тієї інформації, на основі якої воно прийняте.

Витік інформації може завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді призводить і до банкрутства.

За законами бізнесу попит породжує пропозицію. Саме тому на сучасному ринку засобів захисту інформації з'являються все різноманітніші та потужніші засоби. Особливо цей процес активізувався в останні роки.

Помітно різке вторгнення на цей ринок іноземних фірм – виробників таких засобів і систем.

Розглянемо проблеми забезпечення інформаційної безпеки, в тому числі, звертаючи увагу на доцільність використання в Україні іноземних програмних засобів захисту інформації.

У 1990 р. тодішній директор Агентства Національної Безпеки (АНБ) США Уільям Студеман заявляв, що його агентству доведеться в найближчий час змінити напрям діяльності, зробивши своїм пріоритетом не військове, а економічне шпигунство. При цьому "під ковпаком" у АНБ виявиться багато країн – союзників США, не говорячи вже про країни колишнього СРСР, чиї банки, торговельні і промислові компанії виходять на світовий ринок та стають конкурентами американцям.

Мова йде про цілеспрямоване електронне стеження за конкретними банками і компаніями, що мають найбільші перспективи розвитку, з метою отримання відомостей про їхні нові товари, технології, фінансові та торгові операції, які плануються. Одним із способів отримання такої інформації є контроль каналів обміну інформацією. Незалежність держави багато в чому залежить від незалежності та надійності її інформаційних баз і каналів. Їх контроль ставить державу, її банки і компанії в залежність від того, хто контролює і взнає всі ходи наперед. Одним із способів контролю інформаційних каналів є електронні та програмні "закладки".

"Електронні закладки" ("жучки" тощо) вже давно використовуються спецслужбами для промислового шпигунства. За допомогою цих "жучків" можна перехопити не лише акустичну, але і спеціальну електронну інформацію. Припустимо, одна фірма продала іншій комп'ютер, ксерокс, телефон, факс, і "продавець" тепер знає все, що робиться у "покупця". "Жучок" справно поставляє своєму господарю інформацію радіоканалом чи, наприклад, через комп'ютерну мережу. І звичайно ж, продавець точно знає, кому дістанеться ця техніка. Отже, витрати на "жучка" швидко відшкодовуються.

Як дешевший, але не менш ефективний спосіб отримання інформації з комп'ютерів, використовують зняття з них електромагнітного випромінювання. Окремі види навіть побутової телевізійної техніки дають змогу отримати "картинку" з екрана дисплея комп'ютера на своїх екранах. Уявіть собі, що в машині, запаркованій недалеко від банку, сидять "електронні хакери" і спостерігають по телевізору, що відбувається на банківському комп'ютері. Однак, таке можливе лише з звичайним, незахищеним від випромінювання комп'ютером.

Фірми, які надають подібні послуги зі "зняття" інформації, уже з'явилися в Києві, Москві. Успіх їхньої діяльності зумовлений тим, що у нас поки або зовсім не захищають інформацію, або захищають її непрофесійно.

Іншим ефективним способом ведення промислового шпигунства є проникнення в комп'ютерні мережі, електронні бази даних банків, фірм тощо. У розвинених країнах збитки від подібних акцій становлять до кількох десятків міліардів доларів.

Якщо ж такі проникнення плануються заздалегідь, то для полегшення роботи "зломщику" до програми, яка поставляється клієнтові, розробник вносить "програмну закладку", яка дає можливість легко увійти в комп'ютерну систему того, у кого вона буде стояти. У зв'язку з цим у воєнній галузі з'явився новий термін – "інформаційна зброя".

Існує багато прикладів впровадження "програмних закладок" в інформаційні системи різних фінансових та комерційних структур. Ефективність дії лише однієї такої закладки може бути такою, що призведе до повного розорення власника інформаційної системи за рахунок витікання конфіденційної інформації або за рахунок несанкціонованого впливу розробника на саму систему. Особливо широко подібні

впливи застосовуються в країнах з дуже розвиненими комп'ютерними системами, коли розробник може продовжувати впливати на роботу своєї програми "дистанційно", зв'язуючись з нею через мережу. Однак, і в наших умовах уже з'являються повідомлення про подібні випадки.

Уряд США вважає за потрібне взяти розповсюдження криптосистем під свій контроль. У зв'язку з цим, в середині квітня 1993 р. президент США запропонував прийняти за стандартну для США шифр-систему Clipper замість стандарту DES. Уряд США закріплює за собою управління крипто-ключами шифр-системи Clipper. Ключ розділяється на дві частини і кожна частина зберігається в окремій організації, яку вибирає генеральний прокурор. Правоохоронні органи, при наданні дозволу суду на підслуховування, отримують обидві частини ключа і можуть розшифровувати інформацію, що передається.

Основою нової системи шифрування стане секретний криптоалгоритм Skipjack АНБ США. Секретність ключа шифрування системи Clipper заснована на принципі розділеного і депонованого ключа.

Крипточип Capstone є розширеним варіантом крипточипа Clipper і містить, крім інших елементів, додатково схему реалізації алгоритму цифрового підпису DSA (Digital Signature Algorithm), запропоновану національним інститутом стандартів і технологій NIST (США). Цей алгоритм використовуватиметься замість алгоритму цифрового підпису RSA.

За таких умов, зацікавленим фахівцям слід замислитись про доцільність використання в Україні іноземних програмних засобів захисту інформації та звернути увагу на створення і використання вітчизняних високоефективних та конкурентоспроможних систем.

Основна частина

На сьогоднішній день саме в банківській сфері спостерігається як позитивний ефект (пов'язаний з впровадженням сучасних автоматизованих технологій обробки інформації та пов'язаного з цим розширення спектру послуг, що надаються, і прискоренням оборотності коштів), так і неминучі негативні вияви, а саме:

- частішають спроби крадіжок грошових коштів, в тому числі за допомогою засобів комп'ютерної техніки;
- не завжди ефект від впровадження передових технологій адекватний витратам;
- не всі послуги надаються на досить якісному рівні.

Уже сьогодні потребують негайного вирішення такі проблеми:

- забезпечення безпеки обміну інформацією між відділами банків, що працюють в режимі єдиного кореспондентського рахунку в Національному банку України. Оскільки більше ніж 70 відсотків платежів у таких банках становлять внутрішньосистемні (міжфілійні) платежі, очевидно, що ця задача актуальна. За Промінвестбанком України, що працює в цьому режимі, на нього будуть переходити й інші банки (організація взаємодії за принципом "кожен з кожним");
- безпеки інформації, що циркулює у відомчих мережах передачі даних. Уже існує відомча мережа передачі даних банку "Україна";
- відсутності нормативно-правової бази, яка дає змогу вирішувати питання електронного грошового обігу – як між відділами банків, так і між банками і їхніми клієнтами (в системах "Клієнт–Банк");
- відсутності єдиних стандартів галузі – як найпоширеніших алгоритмів, так і термінології;
- на сьогоднішній день ніякими засобами, крім досить слабких інструментів найпопулярніших мережевих операційних систем, не забезпечується безпека інформації, що обробляється всередині відділу банку. Водночас, 70-90 відсотків усіх крадіжок грошових коштів в автоматизованих системах здійснюють співробітники банків;
- сертифікації програмних і апаратних засобів. З однієї сторони, НБУ справедливо вимагає використання для захисту банківської інформації лише сертифікованих програмних і апаратних засобів, з іншої – система державної сертифікації таких засобів ще реально не функціонує, а спроби НБУ виступати в ролі сертифікаційної організації не зовсім законні.

Без комплексного вирішення цих та інших питань створити надійну систему електронних розрахунків і зробити доступ до неї простим і зручним для всіх її учасників є завданням недосяжним.

У наш час спостерігається сповільнення темпів збільшення кількості банків, що працюють на території України. Цей процес замінюється процесом зростання якості та обсягу послуг, що надаються, у тому числі в області автоматизації електронного грошового обігу. Як приклад можна навести застосування у ряді банків кредитних карток, активний обмін фінансовою інформацією між відділами банків з використанням засобів телекомунікації, впровадження різноманітних автоматизованих систем обробки фінансової інформації всередині банків. Не останнє місце серед таких нововведень займають системи електронних платежів "Клієнт– Банк", що дають змогу клієнтам банку – юридичним особам виконувати операції зі своїм банківським рахунком безпосередньо з офісу.

Проаналізуємо проблеми забезпечення захисту інформації, яка обробляється в таких системах, а також визначимо рекомендації щодо їх рішення.

Для цього слід дослідити всі стадії процесу взаємодії клієнта з банком, виявити можливі загрози безпеці і вибрати методи, що дадуть змогу захисту від цих загроз.

Одну з можливих технологічних схем функціонування системи "Клієнт– Банк" наведено на рис. 1.

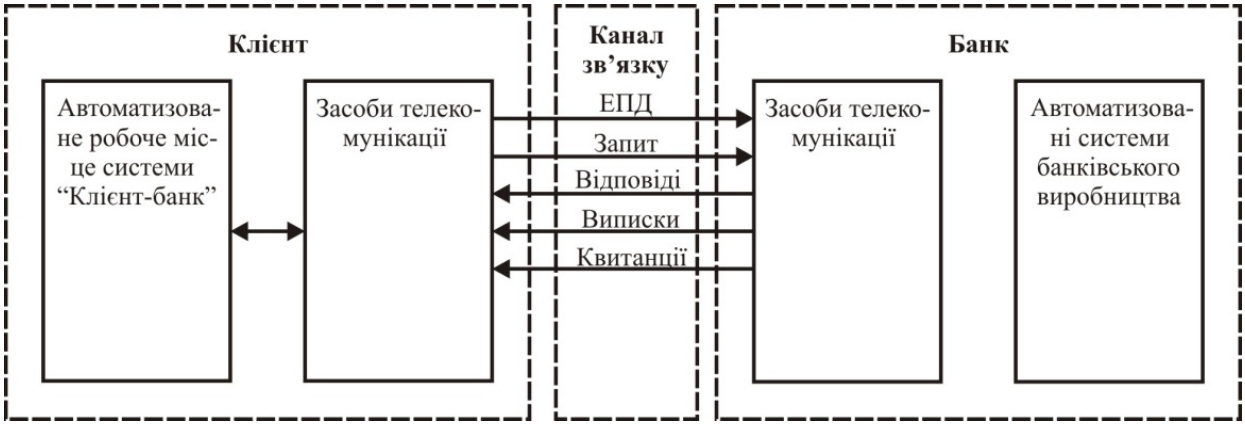

Рис. 1 Технологічна схема роботи системи "Клієнт– Банк"

Така схема використовується, наприклад, в АПБ "Україна", подібна – в кількох інших банках. Клієнт на своєму автоматизованому робочому місці (АРМ) виконує підготовку електронних платежів документів (ЕПД). ЕПД за допомогою програмно-технічних засобів телекомунікації (модему і відповідного програмного забезпечення) передаються до банку, де приймаються також через телекомунікаційні засоби, що функціонують на спеціально впровадженому комп'ютері (зв'язному сервері), включеному до локальної обчислювальної мережі банку. У цій локальній мережі функціонує програмний комплекс автоматизованої системи банківського виробництва (АСБВ), який називають комплексом операційного дня банку (ОДБ). Прийняті зв'язним сервером електронні платежі документів каналами локальної обчислювальної мережі передаються в АСБВ, де здійснюється їх подальша обробка. Після прийняття ЕПД і обробки АСБВ формує квитанцію і передає її на зв'язний сервер для наступної передачі клієнту. Протягом операційного дня і після його завершення АСБВ формує і передає на зв'язний сервер повідомлення про рух на рахунку клієнта (поточні та кінцеві виписки).

З точки зору забезпечення безпеки в цій технології можна виділити три групи проблем.

1. Такі, що виникають при обробці інформації всередині організації-відправника ЕПД.
2. Пов'язані з забезпеченням захисту ЕПД при пересиланні їх між клієнтом і банком.
3. Ті, що виникають у процесі обробки документа в банку і прийняття рішень про зміну стану рахунку клієнта (про переказ коштів).

Проблеми першої групи пов'язані в основному з такими причинами:

- необхідністю забезпечення юридичної значимості сформованого документа для установи банку (проблема автентифікації виконавця документа);
- блокуванням можливості внесення зловмисником змін в уже сформовані та підготовлені до відправки ЕПД (проблема автентифікації або захисту цілісності документа);
- захистом цілісності використовуваних при підготовці ЕПД програмних засобів для блокування можливостей несанкціонованого формування (відправки) ЕПД (проблема автентифікації або захисту цілісності програмних засобів).

Одне з вразливих місць – пересилання документів між клієнтом і банком. Це породжує три типи проблем, пов'язаних з необхідністю:

- взаємного розпізнавання абонентів (проблема автентифікації при встановленні зв'язку);
- захист документів, які передаються каналами зв'язку (забезпечення цілісності та конфіденційності документів);
- захист самого процесу обміну документами (проблема доведення факту відправлення/доставки документа).

У банку в процесі обробки прийнятого ЕПД можуть виникнути такі проблеми:

- підтвердження цілісності та юридичної значимості прийнятого документа (ідентифікація та автентифікація відправника, а також автентифікація повідомлення);
- забезпечення захисту від несанкціонованої модифікації вже прийнятого ЕПД або від нав'язування хибної інформації зловмисником всередині відділення банку;
- захист цілісності використовуваних при обробці ЕПД в банку програмних засобів для блокування можливостей несанкціонованого доступу і модифікації інформації про стан рахунків клієнта;
- оскільки клієнт і банк юридично незалежні, існує проблема недовіри – чи будуть вжиті щодо прийнятого документа відповідні дії.

Отже, для забезпечення надійності роботи системи "Клієнт– Банк" засоби захисту мають забезпечувати:

- ідентифікацію та автентифікацію клієнта-відправника ЕПД з однозначною авторизацією документа;
- автентифікацію ЕПД;
- автентифікацію програмного забезпечення, яке функціонує у клієнта в банку;
- автентифікацію абонентів у процесі встановлення зв'язку і передачі повідомлення;

- приховування смислового змісту повідомлення, що передається;
- захист сформованих ЕПД від несанкціонованого доступу як у клієнта, так і в банку;
- фіксацію фактів прийому (передачі) документів з веденням відповідних архівів і журнальних файлів;
- чітку регламентацію обов'язків клієнта і банку стосовно один одного.

Розглянемо методи і алгоритми, за допомогою яких можуть бути вирішені описані задачі.

Способом ідентифікації та автентифікації відправника ЕПД, а також авторизації самого документа є застосування цифрового підпису документа, що виконується за допомогою несиметричних криптоалгоритмів. Існує кілька алгоритмів для виконання цифрового підпису. Серед них алгоритм RSA і алгоритм Ель-Гамаля. У Росії діє набір стандартів (ГОСТ РФ 34.10, ГОСТ РФ 34.11), які визначають алгоритм формування цифрового підпису, а також алгоритм хешування (стиснення) повідомлень, що підписуються. В Україні стандарту на алгоритм цифрового підпису поки що немає.

Для автентифікації та приховування смислового змісту повідомлень, звичайно, застосовують симетричні криптоалгоритми, наприклад, DES, Clipper або діючий на території колишнього СРСР, в тому числі в Україні, ГОСТ 28147-89.

Розв'язок задачі автентифікації абонентів при встановленні зв'язку може виконуватися двома процедурами: простої та строгої автентифікації.

Процедура простої автентифікації полягає, загалом, в обміні паролями.

У процедурі строгої автентифікації застосовують несиметричні криптографічні алгоритми. При цьому зникає необхідність у попередньому обміні секретними паролями, що значно підвищує стійкість системи.

Захист ЕПД в процесі обробки їх у клієнтській і банківській автоматизованих системах не може бути реалізований без контролю повноважень операторів щодо запуску програмних засобів і доступу до даних.

Для фіксації процесів прийому (передачі) повідомлень засобами системи захисту слід підтримувати ведення архівів прийнятих і переданих документів, причому доступ до цих архівів має бути обмеженим, як програмно, так і організаційно. Всі повідомлення про спроби несанкціонованого доступу до інформації, виявлені засобами системи захисту, повинні фіксуватися в спеціальних журнальних файлах.

Починати використовувати систему "Клієнт– Банк" можна тільки після укладання між клієнтом і банком угоди, в якій чітко зафіксовані зобов'язання сторін стосовно одна одної, а також їхня згода підкорятися вимогам, викладеним у "Положенні про порядок використання засобів цифрового підпису", вирішувати всі спірні питання у відповідній експертній організації та підкорятися її рішенням.

Звідси випливає, що система захисту "Клієнт– Банк" має бути комплексом програмно-апаратних засобів, що функціонують у банку і у клієнта. Можливі схеми включення цих засобів до поданої на рис. 1 технології наведено на рис. 2 і рис. 3.

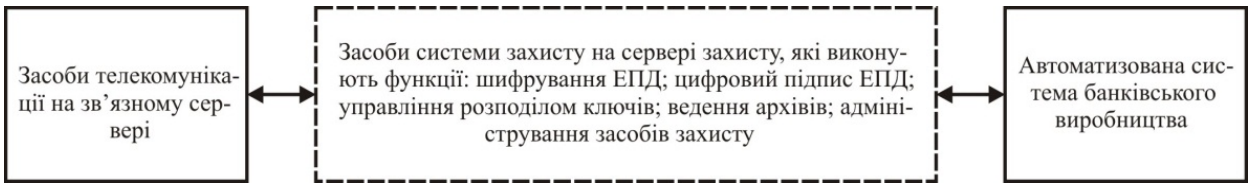

Рис. 2 Схема включення засобів захисту банку

Рис. 3 Схема включення засобів захисту у клієнта

Засоби захисту в клієнта містять програмні або апаратні засоби шифрування інформації, цифрового підпису, генерації ключів цифрового підпису.

Неодмінний компонент системи захисту – програмно-апаратні засоби захисту комп'ютерів від несанкціонованого доступу, які обов'язково мають встановлюватися в банку, але можуть бути встановлені також у клієнта.

Висновки

З вище сказаного випливає той факт, що, на жаль, сьогодні на ринку України практично немає

систем, які задовольняють наведені вимоги. Є лише окремі їх компоненти, що реалізують, як правило, функції шифрування і цифрового підпису. При цьому абсолютно не продумані питання інтеграції засобів захисту з елементами автоматизованої системи банківського виробництва і забезпечення надійного і безпечного їх взаємозв'язку.

Література

1. Тимошенко А.А. Защита информации в системах «Клиент-Банк» / А.А. Тимошенко // Безопасность информации. – 1995. – № 1. – С.39-44.

2. Хоффман Л.Д. Современные методы защиты информации, – М.: Сов.радио, 1980. – 264с.

3. Красовська І. Підключення до системи "Клієнт-банк" / І. Красовська // "ГоловБух". – 2007. – № 62 (541). – С. 24– 27.

4. Рогач І. Ф. Інформаційні системи у фінансово-кредитних установах: навч. посіб. – 2-ге вид., перероб. і доп. / І. Ф. Рогач, М. А. Сендзюк, В. А. Антонюк. – К. : КНЕУ, 2001. – 239 с.

5. Гайкович В. Безопасность електронных банковских систем. / В. Гайкович, А. Першин – М.: Единая Европа. – 1994. – 364с.

6. Боровиков А.М., Тимошенко А.А. Системы защиты информационного обмена «Клиент-Банк» / А.М. Боровиков, А.А. Тимошенко // Безопасность информации. – 1995. – № 1. – С.53-60.

7. Ивченко И.С. К вопросу об информационной безопасности платежных систем коммерческих банков Украины и снижению системных рисков. / И.С. Ивченко, И.Н. Новак // Безопасность информации. – 1996. – № 2 (5). – С.48-56.

Надійшла до редакції
16.3.2013 р.

УДК 621.397: 004.932

В.И. СОЛОДКАЯ
Одесская национальная академия связи им. А.С. попова

АНАЛИЗ СЕТОЧНЫХ МЕТОДОВ ПОСТРОЕНИЕ ОБЪЕКТОВ С ПОМОЩЬЮ ЗАДАЧ ТРИАНГУЛЯЦИИ

В данной работе рассматриваются методы визуализации трехмерных объектов с помощью сеток. Проводится описание и анализ методов построение объектов, показываются преимущества и недостатки используемых методов.

Ключевые слова: задача триангуляции, сеточные методы, трехмерные объекты.

In this work the methods of visualization of three-dimensional objects are examined by nets. Description and analysis of methods is conducted construction of objects, advantages and lacks of in-use methods are shown.

Key words: the problem of triangulation grid methods, three-dimensional objects.

Введение

Данная работа посвящается сравнительному анализу алгоритмов визуализирующих заданную поверхность с помощью аппроксимации её треугольниками. Это так называемая задача триангуляции. Проблема визуализации поверхности, заданной различными способами возникает во многих областях математики, физики, медицины и телевидении.

Под задачей триангуляцией понимается визуализация поверхности заданной с помощью функции от трех аргументов и фиксированного значения этой функции – уровня.

$$\{(x, y, z) \mid f(x, y, z) = c\}$$

где $f(x, y, z)$ – это заданная функция, а c – заданный уровень.

Множество точек, удовлетворяющее этой формуле, и есть искомая поверхность объекта. Однако удобнее восстанавливать не саму поверхность, а поверхность аппроксимирующую искомую с помощью треугольников. Такой способ визуализации называется триангуляцией[1].

При решении задачи визуализации важную роль играет способ задания функции, которая описывает искомую поверхность. В большинстве прикладных задач функция задается таблично на регулярной сетке или имеет явное отображение, описываемое заданной формулой.

Но могут возникать задачи, в которых нет явно заданного отображения, или таблица значений задана на сетке с неэквидистантным шагом. Такие задачи могут возникать во многих приложениях, например, в задаче реконструкции трехмерной структуры с помощью множества контуров- «срезов» (в медицинских исследованиях). В таких задачах предлагается использовать следующий алгоритм действий поверхность S, заданная выборкой X, аппроксимируется касательными плоскостями, проходящими через каждую точку выборки X. Затем искомая функция, задающая поверхность, считается следующим образом: для каждой точки P пространства R функция в этой точке равна расстоянию до ближайшей касательной плоскости, взятому со знаком «+», если точка находится внутри объема, ограниченного построенными