УДК 004.725.5

ЗАХИСТ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ МЕРЕЖАХ БАНКУ

Копичинська І.А., Йона Л.Г., Йона О.О.

Одеська національна академія зв`язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Ковальська,1.
Одеський національний економічний університет,
65082, Україна, м. Одеса, вул. Преображенська,8.
irina.kopichinskaya@gmail.com, lyona@list.ru, eyona@mail.ru

ЗАЩИТА ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ БАНКА

Копычинская И.А., Йона Л.Г., Йона Е.О.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная,1.
Одесский национальный экономический университет,
65082, Украина, г. Одесса, ул. Преображенская, 8.
irina.kopichinskaya@gmail.com, lyona@list.ru, eyona@mail.ru

INFORMATION SECURITY IN BANK LOCAL NETWORKS

Kopichinska I.A., Yona L.G., Yona O.O.

O.S. Popov Odessa National Academy of Telecommunications,
1 Kovalska St., Odessa 65029, Ukraine.
Odessa National Economic University
8 Preobrajenskaya St., Odessa 65029, Ukraine.
irina.kopichinskaya@gmail.com, lyona@list.ru, eyona@mail.ru

Анотація. Розглядається захист інформації в локальних мережах банку, способи та методи захисту інформації в програмно-технічному середовищі, зокрема, рішення на базі технологій “тонкий клієнт” і “товстий клієнт”. Проводиться порівняльна характеристика двох технологій. Наведено принцип роботи мережі, побудованої на технології “тонкий клієнт”.

Ключові слова. захист банківської інформації, інформаційна безпека, захист локальної мережі, технологія “товстий клієнт”, технологія “тонкий клієнт”.

Аннотация. Рассматривается защита информации в локальных сетях банка, способы и методы защиты информации в программно-технической среде, в частности, решения на базе технологий “тонкий клиент” и “толстый клиент”. Проводится сравнительная характеристика двух технологий. Приведен принцип работы сети, построенной на технологии “тонкий клиент”.

Ключевые слова: защита банковской информации, информационная безопасность, защита локальной сети, технология “толстый клиент”, технология “тонкий клиент”.

Abstract. System of information security in bank local networks, means and methods of information security in software and hardware environment, in particular, solutions based on technology "thin client" and "fat client" are considered. The comparative characteristic of the two technologies is carried out. Principle of network operation built on the "thin client" technologies is shown.

Key words. protection of bank information, information security, protection network, technology "fat client", technology "thin client".

Проблема навмисних порушень функціонування автоматизованих систем обробки інформації банку різного призначення є актуальною. Це особливо стосується країн з сильно розвиненою інформаційною інфраструктурою [1].

Політика інформаційної безпеки банківських і платіжних систем дуже відрізняється від аналогічних політик інших компаній. Це пояснюється, в першу чергу, специфічним характером загроз, а також публічною діяльністю банків. Оскільки для клієнтів робота з банком повинна бути легкою та зручною, то банки змушені робити доступ до рахунків досить простим.

Для забезпечення фізичної та класичної інформаційної безпеки існують вироблені стандартні заходи. У напрямі безпеки автоматизованих систем обробки інформації банку ситуація складніша. Методи та засоби безпеки автоматизованих систем вимагають постійного оновлення та модернізації, оскільки комп'ютерні технології схильні до частих радикальних змін.

Захист банківської інформації – це комплексна задача, яка не може вирішуватися тільки у межах банківських програм. Для ефективної реалізації захисту необхідно спочатку вибрати та налаштувати операційні системи та мережні системні засоби, які підтримують функціонування банківських програм. Необхідно виділити два напрями серед дисциплінарних засобів забезпечення захисту. Перший – користувач системи повинен володіти мінімально достатньою кількістю інформації щодо особливостей побудови системи. Другий – система повинна містити багаторівневі засоби ідентифікації користувачів та контролю їх прав.

Задача захисту інформації у банківській є набагато складнішою, ніж в інших організаціях. Розв'язання такої задачі передбачає планування організаційних, системних заходів, які забезпечують захист. При плануванні захисту необхідно дотримуватися межі між необхідним рівнем захисту і тим рівнем, коли захист починає заважати нормальній роботі персоналу [2].

У банківській системі важливу роль відіграє локальна мережа, за допомогою якої передається та функціонує вся банківська інформація. Тому важливою проблемою залишається захист локальної мережі банку.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ. Проблемам дослідження методів захисту інформації в локальних мережах банку присвячені праці багатьох учених, таких як Гайкович Ю.В., Першин А.С., Преображенський Н.Б., Дьомін В.С. та інші [1…3]. В даному напрямку розглядались такі роботи: Йона Л.Г., Йона О.О., Терешко В.С. "Криптографічний захист електронного документообігу" [4]; Копичинська І.А. за кер. Йони Л.Г "Методи інформаційної безпеки в банківських і платіжних системах" .[5]; Запороженко О.О. за кер. Йони Л.Г "Методи захисту інформації в системах електронної комерції" .[6] Оскільки методи і засоби безпеки інформації стрімко розвиваються, виникає необхідність у подальших дослідженнях в даному напрямку.

Статті є вивчення проблеми забезпечення захисту інформації в локальних мережах банку. Проведено дослідження методів та способів захисту інформації в локальних мережах та в програмно-технічному середовищі. Особлива увага була приділена розгляду рішень на базі технологій "тонкий клієнт" і "товстий клієнт". Була проведена порівняльна характеристика двох технологій: "тонкий клієнт" та "товстий клієнт". Після чого наведено принцип роботи мережі побудованої на технології "тонкий клієнт".

ОСНОВНА ЧАСТИНА. Локальні мережі об'єднують комп'ютери, які виконують обробку текстових і графічних даних, розподілені обчислення, а також звертаються до баз даних. Комп'ютери в мережі мають рівні права, тому користувач одного комп'ютера може звертатися до обчислювальних ресурсів іншого комп'ютера. В невеликих за розміром мережах зазвичай використовується однорангова організація. У однорангових мережах відсутній виділений сервер. Окремим користувачам надаються права доступу, і вони регулюють доступ до різних обчислювальних ресурсів.

У разі, коли можливостей однорангових мереж явно недостатньо, може бути організована мережа з виділеним сервером, який називається файл-сервером. В якості сервера застосовується мережний комп'ютер, що має достатній об'єм оперативної і дискової пам'яті.

На рис.1 представлені елементи локальної мережі.

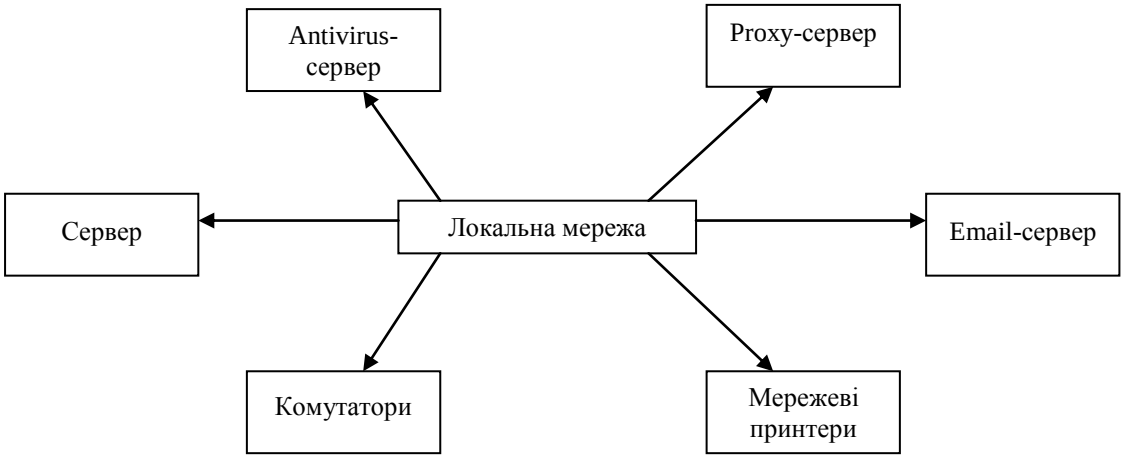

Рисунок 1 – Елементи локальної мережі

Обчислювальна мережа є потенційно ненадійним середовищем передачі даних. Системи обробки та захисту інформації відображають саме такий підхід до обчислювальної мережі. Існує декілька основних способів забезпечення безпеки програмно-технічного середовища, які реалізуються різними методами. На рис. 2 подані способи забезпечення безпеки програмно-технічного середовища [3].

Рисунок 2 – Способи забезпечення безпеки програмно-технічного середовища

При створенні інформаційних систем все більшої популярності набувають два рішення на базі технологій “тонкий клієнт” та “товстий клієнт”.

“Тонкий клієнт” – комп`ютер або програма-клієнт в мережах з клієнт-серверною або термінальною архітектурою, який переносить всю або велику частину задач по обробці інформації на сервер.

“Товстий клієнт” – це додаток, який забезпечує розширену функціональність незалежно від центрального сервера. Часто сервер в цьому випадку являється сховищем даних, а вся робота з обробки та надання цих даних переноситься на машину клієнта.

У табл.1 показані переваги і недоліки технологій “тонкий клієнт” і “товстий клієнт”.

Таблиця 1 – Переваги та недоліки технологій “тонкий клієнт” і “товстий клієнт”

Переваги і недоліки технологій “тонкий клієнт” та “товстий клієнт”			
Технологія “тонкий клієнт”		Технологія “товстий клієнт”	
Переваги	Недоліки	Переваги	Недоліки
Тривалий термін служби (5-10років). Надійність апаратного та програмного забезпечення. Захист даних та безпека. Відмовостійкість. Нечутливість до пропускної здатності мережі. Мінімальний ризик виникнення програмних конфліктів і зараження вірусами. Контроль за користувачами. Проста модернізація та обслуговування. Просте адміністрування. Проста масштабованість (збільшення числа робочих місць). Економія на ліцензіях програмного забезпечення. Максимальна віддача від вкладених коштів. Ергономічність	Безліч обмежень, які термінали накладають на систему. Неможливість роботи при виході сервера з ладу. Необхідні надійні правильно налаштовані конфігурації серверів і сховищ даних. Темпи зростання підприємства та зміни процесів здатні вплинути на архітектуру системи	Широкий функціонал. Режим багатокористувацької роботи. Можливість роботи при обривах зв'язку з сервером. Висока швидкодія (залежить від апаратних засобів клієнта)	Великий розмір дистрибутива. Багато чого в роботі клієнта залежить від того, для якої платформи він розроблявся. Виникають проблеми з віддаленим доступом до даних. Досить складний процес встановлення і налаштування. Складність поновлення і пов'язана з нею неактуальність даних. Наявність бізнес-логіки

Виходячи з цього, більш популярною та впроваджуваною являється технологія “тонкий клієнт”.

“Тонкий клієнт” працює під управлінням компактної версії вбудованої операційної системи (Windows CE, Windows XP Embedded або Linux), у складі якої присутні тільки необхідні для роботи програми. До “тонкого клієнту” можна підключити практично будь-який пристрій введення та виведення інформації [7].

У випадку використання “тонких клієнтів”, обчислювальні потужності на робочих місцях не використовуються. Співробітники банку, працюючи в термінальній системі, отримують видалені екрани програм і додатків, що обробляються високопродуктивними серверами. За допомогою тонких клієнтів знижується навантаження на канали зв`язку всередині банку та між філіями.

“Тонкий клієнт” може працювати тільки тоді, коли він підключений до локальної мережі, в якій присутній сервер з працюючою термінальною службою. “Тонкий клієнт” самостійно знайде термінальний сервер, підключиться до нього та запросить у користувача логін та пароль (або PIN у випадку використання USB-ключа або смарт-картки). Якщо логін та пароль будуть вірними, користувач отримає доступ до свого розділу на сервері, зможе запускати програми, встановлені та дозволені тільки для нього системним адміністратором. При цьому “тонкий клієнт” буде виводити зображення віддаленого робочого столу та обробляти дії клавіатури та мишки. Іншими словами, користувач може працювати з будь-яким “тонким клієнтом”, але володітиме лише інформацією, яка призначається йому. Такий підхід дозволяє легко керування ресурсом робочих місць та ефективно планувати розподіл даного ресурсу.

Крім того, необхідно зробити акцент на ще одній важливій перевазі технології “тонкий клієнт”. Технологія “тонкий клієнт” дозволяє захистити мережу та інформацію.

Технологія захищає мережу від шкідливих програм. Вся інформація зберігається тільки на сервері. Завдяки цьому поява в корпоративній мережі вірусів, троянів та інших шкідливих програм, яка викликана випадковими або навмисними діями користувачів, є малоймовірною.

Технологія захищає від витоків інформацію та контролює діяльність персоналу в робочий час. Відсутність локальних носіїв інформації не дозволяє персоналу робити копії документів на знімні носії інформації. Перелік програм, які доступні користувачам, є обмеженим, що підвищує продуктивність праці.

Зважаючи на вище зазначене можна зробити важливий висновок: захист інформації у фінансових організаціях будується трохи інакше, ніж у звичайних організаціях. Для захисту автоматизованих систем обробки інформації банку не слід застосовувати ті ж самі технічні й організаційні рішення, які були розроблені для стандартних ситуацій. Не потрібно використовувати системи інших організацій, які розроблялися для певних умов. Слід розробляти власні системні рішення, які задовольняють умовам даної ситуації.

Співпраця “тонких клієнтів” та персональних комп`ютерів, встановлене в безпечному місці серверне ядро банку, застосування засобів шифрування та авторизації – це головні аспекти, які забезпечують безпечну та ефективну роботу термінальної системи банку.

Отже, можна зробити висновок про необхідність подальшого розвитку та удосконалення методів і засобів захисту інформації в локальних мережах банку.

ЛІТЕРАТУРА

1. Гайкович Ю.В., Безопасность электронных банковских систем: учебник / Ю.В. Гайкович, А.С. Першин. – М.: Единая Европа, 1994. – 354 с.

2. Преображенский Н.Б., Автоматизация банковских операций: учеб. пособ. Ч.2 / Н.Б. Преображенский. – М.: АТиСО, 2008. – 286 с.

3. Демин В.С., Автоматизированные банковские системы / В.С. Демин. – М.: Менатеп-Информ, 2009. – 325 с.

4. Йона Л.Г. Криптографічний захист електронного документообігу./ Л.Г. Йона, О.О. Йона, В.С.Терешко // Цифрові технології. – Одеса. – 2013. – № 13. – С. 142–146.

5. Копичинська І.А. Методи інформаційної безпеки в банківських і платіжних системах / Копичинська І.А.; під керів. доц. Йони Л.Г. // Современные проблемы радиотехники и телекоммуникаций РТ-2014. – 2014. – С. 318

6. Запороженко О.О. Методи захисту інформації в системах електронної комерції. / Запороженко О.О.; під керів. доц. Йони Л.Г. // Современные проблемы радиотехники и телекоммуникаций РТ-2014. – 2014. – С. 319

7. TONK умные тонкие клиенты [Электронный ресурс] Что это – тонкий клиент и чем он лучше традиционного ПК? – 2013. – Режим доступа: http://www.tonk.ru/technology/thin_clients_in_banks/

REFERENCES

1. Gaykovich, Y., and A. Pershin. “Security of Electronic Banking Systems.” *Threats to the Security of Automated Banking Systems* (1994): 186-89. Print.

2. Priobrajenskiy, N. “Automation of Banking Operations.” (2008): 127. Print.

3. Demin, V. “Automated Banking System.” (2009): 89. Print.

4. Yona, L., E Yona, and V. Tereshko. “Cryptography Security Of Electronic Document Circulation.” *Digital Technology* 13 (2013): 142-46. Print.

5. I. Kopichinska. “Means of Information Security in Banking and Payment Systems.” *Modern Problems of Radio Engineering and Telecommunications* 10 (2014): 318. Print.

6. O. Zaporojenko. “Means of Information Security in Electronic Commerce.” *Modern Problems of Radio Engineering and Telecommunications* 10 (2014): 319. Print.

7. “TONK Intelligent Thin Clients.” *What Is It - a Thin Client and He Is Better than the Traditional PC?* (2013). *Http://www.tonk.ru/technology/thin_clients_in_banks/*. Web.