данных и обработки информации в банкоматах, в процессе считывания информации с магнитных карточек, в системах разграничения доступа и т. д.

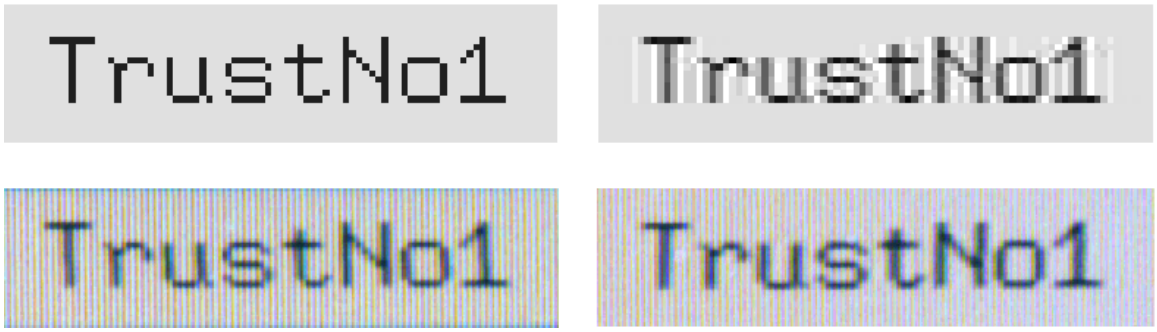

Рисунок 5

Основное достоинство – это относительная дешевизна и универсальность (применимо к любому уже установленному и работающему обычному компьютеру).

Оценить эффективность предложенного метода довольно сложно, хотя изначально очевидно уменьшение уровня информативного ПЭМИ при малых затратах.

Литература: 1. Збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформаціїї в Україні"- Київ, 2000. 2. Peter Smulders: The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security vol 9, pp 53-58, 1990. 3. W. Van Eck, Electromagnetic radiation from video display units. Computers&.Security vol. 4, pp. 269-286, 1985. 4. Markus G. Kuhn u Ross J. Anderson «Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations» - University of Cambridge, 1998.

УДК 681.3.067:336.71

ОСОБЕННОСТИ ЗАШИТЫ БАНКОВСКОЙ ИНФОРМАЦИИ

Светлана Шаповалова, Оксана Галепа, Владимир Кальганов
Национальный технический университет Украины "КПИ"

Аннотация: **Приводится обзор описанных в наиболее общей форме средств защиты информации в банках.**

Summary: **In this article was described the methods of information's protection in banks in the most general form.**

Ключевые слова: **Несанкционированный доступ к информации, защита информации в банках.**

I Задача определения необходимых мер для защиты банковской информации

Была поставлена задача определения в наиболее общей форме мер защиты информации в автоматизированных банковских системах (АБС). Задача рассматривается с точки зрения специалистов компьютерной безопасности банка, использующих готовые решения по аппаратному и программному обеспечению (ПО). Обзор охватывает основные аспекты планирования комплексной защиты, которые должны учитываться специалистами до покупки оборудования и ПО.

Под угрозой безопасности информации будем понимать несанкционированный доступ к данным на любом уровне без анализа действий нарушителя и возможных последствий.

Ограничим рассмотрение мер по защите информации следующими допущениями:

1. Будем считать, что безопасности не угрожают системные администраторы. Угроза исходит только извне или со стороны рядового пользователя.

2. Будем рассматривать работу АБС только в обычном рабочем режиме. Оставим без внимания такие аспекты проблемы, как обеспечение безопасности информации при проведении ремонтно-профилактических работ и при аварийных ситуациях.

3. Отнесем проблему заражения системы вирусами к последствиям несанкционированного доступа и вынесем за рамки нашего исследования.

4. И, наконец, поскольку банки относятся к организациям – потребителям, а не производителям ПО, отпадает необходимость изучения средств “защиты от копирования”.

II Особенности защиты информации в банковских системах и меры предотвращения несанкционированного доступа

Защита информации в банковских системах имеет следующие особенности:

1. АБС должны быть лицензионными и приобретаться исключительно у сертифицированных по квалификационным требованиям защищенности разработчиков.

2. Существует специальное для этой предметной области ПО, уже включающее в себя средства безопасности. Другими словами, для выбора АБС необходимо ориентироваться в критериях оценки безопасности, установленных для коммерческих программ.

3. ПО банковских систем многоуровневое, включающее в себя сетевое программное обеспечение, одну или несколько операционных систем (ОС) и систем управления базами данных (СУБД).

Рассмотрим влияние каждой особенности на меры, обеспечивающие безопасность информации:

1. Только организации, имеющие государственную лицензию [1], могут создать специализированное ПО банковских систем и гарантировать:

- грамотное решение задач делопроизводства банка;
- защиту информации в системах повышенной опасности несанкционированного доступа;
- защиту от несанкционированного доступа присущих для АБС атак.

К подобным атакам относятся:

- *“атака салями”*. Результаты округления результатов арифметических операций прибавляются к значению некоторого элемента базы данных (например, к сумме, хранящейся на личном счету хакера);
- *статистическая идентификация*. Эта атака позволяет получать конкретные значения тех полей базы данных, для которых доступна только статистическая информация;
- отсутствие недокументированных возможностей доступа к ресурсам системы (например, ”люков”).

Более того, установка ПО также должна быть проведена квалифицированными специалистами в области защиты информации для того, чтобы разработчик после запуска АБС не имел возможности ее вскрытия.

2. АБС должна быть сертифицирована по критериям государственной лицензии. Комбинацию требований выполнения мер безопасности может подобрать только специалист на основании анализа конкретной ситуации. С развитием аппаратных возможностей критерии защиты постоянно модифицируются. Со времен “Оранжевой книги” (отчета Trusted Computer Security Evaluation Criteria – TCSES подразделения Computer Security Center Министерства обороны США, опубликованного в 1983 году) нашли повсеместное применение локальные и глобальные компьютерные сети, для которых неприменим подобный подход. Но по концепции предлагаемые оценки безопасности и средства ее защиты остались прежними. Например, ограничение доступа, шифрование отдельных модулей, использование электронных подписей и т.п. можно считать развитием требований “Оранжевой книги”.

3. В общем случае АБС включает в себя три основных уровня:

- одну или несколько систем управления базами данных (СУБД);
- одну или несколько ОС, обслуживающих СУБД и систему документооборота;
- сетевое программное обеспечение, обеспечивающее информационное взаимодействие рабочих станций и серверов банковской сети.

В зависимости от уровня АБС можно предусмотреть различные методы защиты.

Защита базы данных является одной из наиболее простых задач защиты информации. Это обусловлено тем, что базы данных имеют четко определенную внутреннюю структуру, и операции над элементами баз данных также четко определены. В большинстве случаев хакеры даже не пытаются атаковать СУБД, поскольку преодолеть защиту АБС на следующих уровнях, а именно ОС и сети, гораздо проще.

Для реализации атаки на СУБД нарушитель должен как минимум являться пользователем СУБД.

Основным методом обеспечения безопасности на уровне СУБД является использование имени и пароля пользователя. Этот метод хорош тем, что дает возможность легко определить полномочия и права пользователя и выяснить, кем и когда произведена какая либо операция.

На уровне ОС возможны атаки в результате следующих упущений:

1. Использование ОС со слабой защитой, то есть можно загрузить ОС, минуя идентификацию пользователя и ввод пароля.

2. “Сборка мусора” на дисках и в оперативной памяти.

2. Хранение информации на жёстких дисках в открытом формате, и как следствие, возможность чтения этой информации нелегальным пользователем.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

3. Уход сотрудника с места работы без закрытия доступа к системе.

Самые простые способы решения этих проблем [2]:

- используется ОС с высокой степенью защиты;
- все важные программы и данные хранятся на серверах, к которым подключаются рабочие станции. Последние получают только те данные, которые запрошены уполномоченным пользователем;
- файлы БД, хранящиеся на сервере, не являются разделяемыми с точки зрения ОС (разделение данных между пользователями используется только на уровне СУБД);
- при сетевом взаимодействии рабочих станций и серверов БД не используются объектно-ориентированные сетевые протоколы;
- используются программы, которые автоматически закрывают систему при длительном отсутствии пользователей (хранители экрана с паролями и т. д.).

Банковские учреждения обязаны иметь каналы для обмена информацией с внешними абонентами. Этот обмен реализован **на сетевом уровне**.

На сетевом уровне возможны следующие атаки на АБС [2]:

1. Прослушивание канала (возможно только в сегменте локальной сети).

Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети. При этом рабочая станция может принимать пакеты, адресованные другим компьютерам того же сегмента сети. Таким образом, весь информационный обмен в сегменте сети становится доступным нарушителю.

2. Перехват пакетов на маршрутизаторе.

Поскольку через маршрутизатор обычно передается очень много пакетов, тотальный их перехват практически невозможен. Однако отдельные пакеты вполне могут быть перехвачены и сохранены для последующего анализа нарушителем. Наиболее эффективен перехват пакетов FTP, содержащих пароли пользователей, а также электронной почты.

3. Создание ложного маршрутизатора.

Осуществляется отправлением в сеть пакетов определенного вида, в результате чего компьютер нарушителя становится маршрутизатором и получает возможность осуществлять предыдущую угрозу. Ложный маршрутизатор необязательно заметен всем компьютерам сети. Поэтому можно создавать ложные маршрутизаторы для отдельных компьютеров сети и даже для отдельных соединений.

4. Навязывание пакетов. Отправление в сеть пакетов с ложным обратным адресом.

С помощью этой атаки нарушитель может переключать на свой компьютер соединения, установленные между другими компьютерами. При этом права доступа нарушителя становятся равными правам того пользователя, чье соединение с сервером было переключено на компьютер “взломщика”.

5. Атаки класса “отказ в обслуживании”.

Нарушитель отправляет в сеть пакеты определенного вида, в результате чего один или несколько компьютеров сети полностью или частично выходят из строя.

Сетевой уровень АБС обычно наиболее уязвим для атак хакеров. Это обусловлено тем, что канал связи, по которому передаются сетевые пакеты, является открытым – каждый, кто имеет физический доступ к этому каналу, может отправлять в канал пакеты произвольного содержания. Для обеспечения надежной защиты сетевого уровня АБС необходимо добиться максимальной “закрытости” сетевых каналов связи, другими словами, максимально затруднить несанкционированный информационный обмен в защищаемой сети.

Существуют следующие меры защиты, позволяющие минимизировать риск несанкционированного доступа на сетевом уровне:

1. Изоляция сети от внешнего мира.

Если сеть АБС имеет выход в Internet, то задача организации ее защиты существенно усложняется [3]. Это обусловлено тем, что в этом случае любой пользователь Internet имеет физический доступ к защищаемой сети. Если изолировать защищаемую сеть от Internet невозможно, администраторы защищаемой сети должны уделять особое внимание ограничению доступа к сети пользователей Internet.

2. Максимальное ограничение объема защищаемой сети.

Чем больше сеть (географически и по числу компьютеров), тем труднее ее защищать.

3. Шифрование сетевого трафика.

Эта мера защиты позволяет полностью устранить угрозу перехвата пакетов. С другой стороны, шифрование трафика несколько снижает производительность сетевого программного обеспечения.

4. Цифровая подпись сетевых пакетов.

Все пакеты, передаваемые по сети, должны быть подписаны криптографически стойкой цифровой подписью. Данная мера позволяет полностью устранить угрозу навязывания пакетов и большинство угроз, связанных с

отказом в обслуживании. Если защищаемая сеть имеет выход в Internet, цифровая подпись пакетов малоэффективна.

5. Межсетевые экраны (firewalls).

Межсетевые экраны фильтруют передаваемые через маршрутизатор пакеты, не пропуская через маршрутизатор потенциально опасные пакеты, которые, возможно, были отправлены в сеть в ходе атаки сети хакером.

III Заключение

1. Анализ, оценку, проектирование системы защиты информации, экспертизу защищенности необходимо проводить независимыми организациями, имеющими государственную лицензию на проведение указанных работ.

2. Архитектура системы должна быть построена таким образом, чтобы подключение к глобальной сети осуществлялось только в случае крайней необходимости.

3. Политика размещения данных должна проводиться из расчета их максимальной недоступности.

4. Осуществление аудита и проверок целостности ПО АБС должно быть систематическим. Желательно вести журнал аудита не только в электронном, но и бумажном виде.

5. Тестирование безопасности АБС специальными программами и анализ его результатов также должны быть регулярными мероприятиями.

Литература: 1. Максименко С., Осовецкий Л. Защита и беззащитность информации в банке. http://inf.susu.ac.ru/~tyrty/banky.html. 2. Проскурин В. Г. Проблемы безопасности: финансовая безопасность. Автоматизированная банковская система глазами хакера. http://infocity.kiev.ua/hack/title/bank.html. 3. SC-Банк: Руководство программиста. http://www.gis.minsk.by/softclub/doc/BANK_P/P1_1/ADMIN1.HTM.

УДК 681.06

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗПОДІЛЕНИХ БАЗ ДАНИХ

Ігор Нетесін

Міжнародний науковий центр технології програмування ТЕХНОСОФТ НАН України і Держкомітету зв'язку та інформатизації України

Анотація: **Аналізуються сучасні моделі та засоби захисту секретної інформації в комп'ютерних базах даних. Пропонується формалізований підхід до забезпечення безпеки розподілених баз даних, що спирається на принципи взаємодії та захисту об'єктів у комп'ютерних мережах**.

Summary: **Modern models and means of the secret information protection in computer data bases are analyzed. A formalized approach to the safety of distributed data bases that is based on principles of interaction and protection of network objects is suggested.**

Ключові слова: **Захист інформації, бази даних, моделі безпеки.**

I Вступ

Захист комп'ютерних мереж (КМ) значною мірою залежить від організації в ній доступу до інформації, що містить у собі оброблені дані і різні відомості про факти, події, явища і стани об'єктів КМ. Інформація накопичується в базах даних (БД), словниках, репозиторіях, сховищах і опрацьовується користувачами (застосуваннями, процесами); вона може бути відкритою для одних користувачів і закритою для інших або бути доступною тільки для визначеної категорії користувачів із відповідними правами і повноваженнями.

Забезпечення безпеки інформації у мережі - це спроможність КМ захищати інформацію від випадкових або навмисних впливів, різного роду поломок і відмов у системі, що завдають шкоди інфраструктурі КМ. Питанням безпеки інформації почали приділяти увагу наприкінці 80-х років. У наш час з'явилися перші моделі захисту інформації для вищих органів влади і потужних комерційних структур.

Оскільки основна шкода інформації, як правило, завдається злочинними діями (вірусами, зломами секретних ключів, викраденням даних тощо), для боротьби з ними створюються різні механізми безпеки, що включають організаційні, технічні і програмні заходи і засоби захисту інформації [1–5].

Наріжним каменем у вирішенні проблем безпеки є спеціальний документ «Критерії оцінки надійності комп'ютерних систем» в «Оранжевій книзі» [1], який визначає стандартизований підхід до оцінки

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.