УДК 004.052:336.71

Р.Н. ЛАХИЖА

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ТАКСОНОМИЧЕСКАЯ СХЕМА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ГАРАНТОСПОСОБНОСТИ БАНКОВСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Проведен анализ понятия гарантоспособности банковских информационных систем (БИС). Определены основные задачи функционирования гарантоспособных банковских систем (ГБС). Разработана таксономическая схема гарантоспоспособности БИС, учитывающая факторы эволюционирования. Выделены и проанализированы методы обеспечения гарантоспособности банковских систем. Конкретизированы подходы противодействия нарушениям безопасности. Определены важные требования специфические для гарантоспособности систем автоматизации банка, в отличие от других компьютерных систем.

Ключевые слова: *гарантоспособность, банковская информационная система, система автоматизации банка, таксономия, безопасность, угроза, дефект.*

Введение

Современные информационные технологии (ИТ) развиваются стремительными темпами, охватывают новые сферы человеческой деятельности, которые все больше становятся зависимыми от качественного и надежного функционирования ИТ. В работе [1] приводятся примеры как положительных, так и отрицательных аспектов существование таких зависимостей. Не вызывает сомнения, что классическое понятие надежности компьютерной системы уже не полностью описывает все требования, предъявляемые к ее функционированию. Учеными была сформулирована категория гарантоспособности информационных систем (англ. dependability) [2,3], которая не достаточным образом еще разработана по отношению ко многим типам ИТ, в том числе и банковским информационным системам.

Начало процесса компьютеризации банков в развитых странах относят к 1960-м годам, когда появились первые автоматизированные системы бухгалтерского учета, обработки клиентских счетов и платежей в виде чеков. В дальнейшем банки активно внедряли системы удаленного доступа к банковским счетам, системы автоматизированных межбанковских расчетов, внутренние платежные системы, автоматизированные системы принятия управленческих решений и контроля над рисками.

Банковские информационные системы отличаются от других в первую очередь тем, что информация, которая ими обрабатывается, должна быть надежно защищена от сторонних вмешательств, а сама система должна иметь свойства повышенной живучести и безотказности в работе. Поэтому проблема обеспечения всесторонней защищенности и надежности этих систем не только не перестает быть актуальной, а становится жизненно важной для любого банка, который хочет занимать достойное место на финансовом рынке и иметь безукоризненную репутацию.

Основы безопасности информационных систем были заложены в 60-х годах XX века исследованиями ученых различных американских государственных организаций, таких как Министерство обороны, Агентство по национальной безопасности и т.п. В дальнейшем эта область науки активно развивалась.

Банковская деятельность также не осталась вне внимания ученых, и с ростом разнообразия и сложности информационных систем и в зарубежной, и в украинской литературе появляется все больше работ, посвященных данной тематике. Проблемами безопасности, в том числе и банковских информационных систем, занимаются такие известные исследователи, как Андерсон Р., Столлингс В., Соммервиль, Лукацкий А.В., Конеев И.Р., Домарев В.В., Гуцалюк М.В., Голубев В.А., Поливанюк В.Д. и другие.

Этими учеными анализируется комплекс мероприятий, которые обеспечивают защищенность систем автоматизации банка (САБ), программно-технические средства ее достижения, меры борьбы с несанкционированными вмешательствами в работу информационных систем. Вместе с тем, в данных работах не рассматривается функционирование банковских информационных систем с точки зрения их гарантоспособности.

Таким образом, **целью** данной статьи является адаптация понятия гарантоспособности к функционированию банковских информационных систем и анализ основных методов ее обеспечения.

1. Анализ банковских информационных систем как объекта оценки и обеспечения гарантоспособности

Согласно Положению про обеспечение непрерывного функционирования информационных систем Национального банка Украины и банков Украины, утвержденного постановлением Правления НБУ 17.06.2004 № 265, банковские информационные системы – это комплексы программно-аппаратных средств, предназначенных для решения банками и их филиалами собственных задач в сфере автоматизации и взаимодействия с информационными системами НБУ. К этим системам относятся система автоматизации банка (САБ) и внутрибанковская платежная система.

В свою очередь, систему автоматизации банка можно определить как систему, функционирующую на основе компьютерных и других технических средств, которые обеспечивают процессы сбора, регистрации, передачи, обработки, сохранения и актуализации данных для решения задач управления банковской деятельностью. Типовая структурная схема САБ представлена на рис. 1 [4].

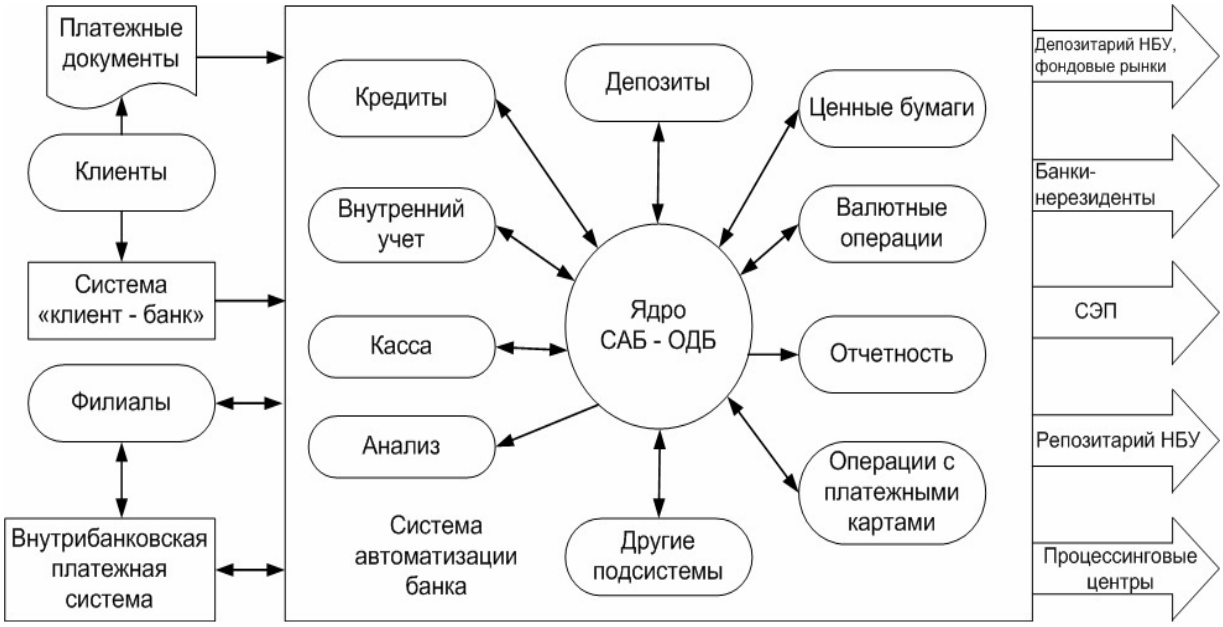

Рис. 1. Структурная схема системы автоматизации банка

Специалисты отмечают, что за пятнадцать лет существования банковской системы Украины сменилось уже шесть поколений систем автоматизации деятельности банка, и основными целями их внедрения можно назвать:

– увеличение возможностей банков в проведении операций на финансовом рынке и обслуживании населения – сокращение времени на проведение операций, увеличение пропускной способности;

– оптимизация численности персонала;

– улучшение качества обслуживания клиентов – гарантия непрерывного обслуживания, повышение квалификации персонала;

– снижение себестоимости банковских операций;

– обеспечение интегрирования в единые банковские сети.

Таким образом, банковские информационные системы позволяют реализовывать новые возможности в организации всей банковской деятельности, повышении оперативности и качества обслуживания. Но в то же время они являются одним из самых уязвимых аспектов безопасности современного банка.

Рассматривая особенности использования компьютерных систем и технологий в банках, следует отметить, что в основе их применения лежит обеспечение электронного денежного оборота. Сохраненная и обработанная в банковских системах информация является реальными деньгами. На ее основании осуществляются выплаты наличных средств, предоставляются кредиты, переводятся значительные суммы денег. Незаконное манипулирование данной информацией и не сохранение ее целостности может привести к серьезным потерям,

поскольку банковская информация затрагивает интересы большого количества юридических и физических лиц – клиентов банка, а, следовательно, и государства.

Поэтому особенностью подходов к обеспечению надежности и безопасности банковских информационных систем является, в том числе, их законодательное регулирование, что нашло отражение в принятии в 2004 году соответствующего постановления Правления НБУ.

2. Таксономическая схема гарантоспоспособности БИС

По определению, которое уже имеется в научной литературе, гарантоспособность — это комплексное свойство, определяющее способность системы предоставлять требуемые услуги, которым можно оправдано доверять [2,3]. Это означает, что гарантоспособная система должна продолжать функционирование при обнаружении ошибок в программном обеспечении или при наличии аппаратных дефектов. Кроме того, такая система должна продолжать корректную работу в случае попытки неправильного использования. Важно, чтобы ошибки, присутствующие в системе, в заданных условиях эксплуатации проявлялись достаточно редко.

Гарантоспособность является комплексным свойством и содержит в себе ряд других характеристик. По мнению автора, можно выделить следующие атрибуты гарантоспособности систем автоматизации банка, которые наиболее соответствуют требованиям, предъявляемым к САБ (рис. 2):

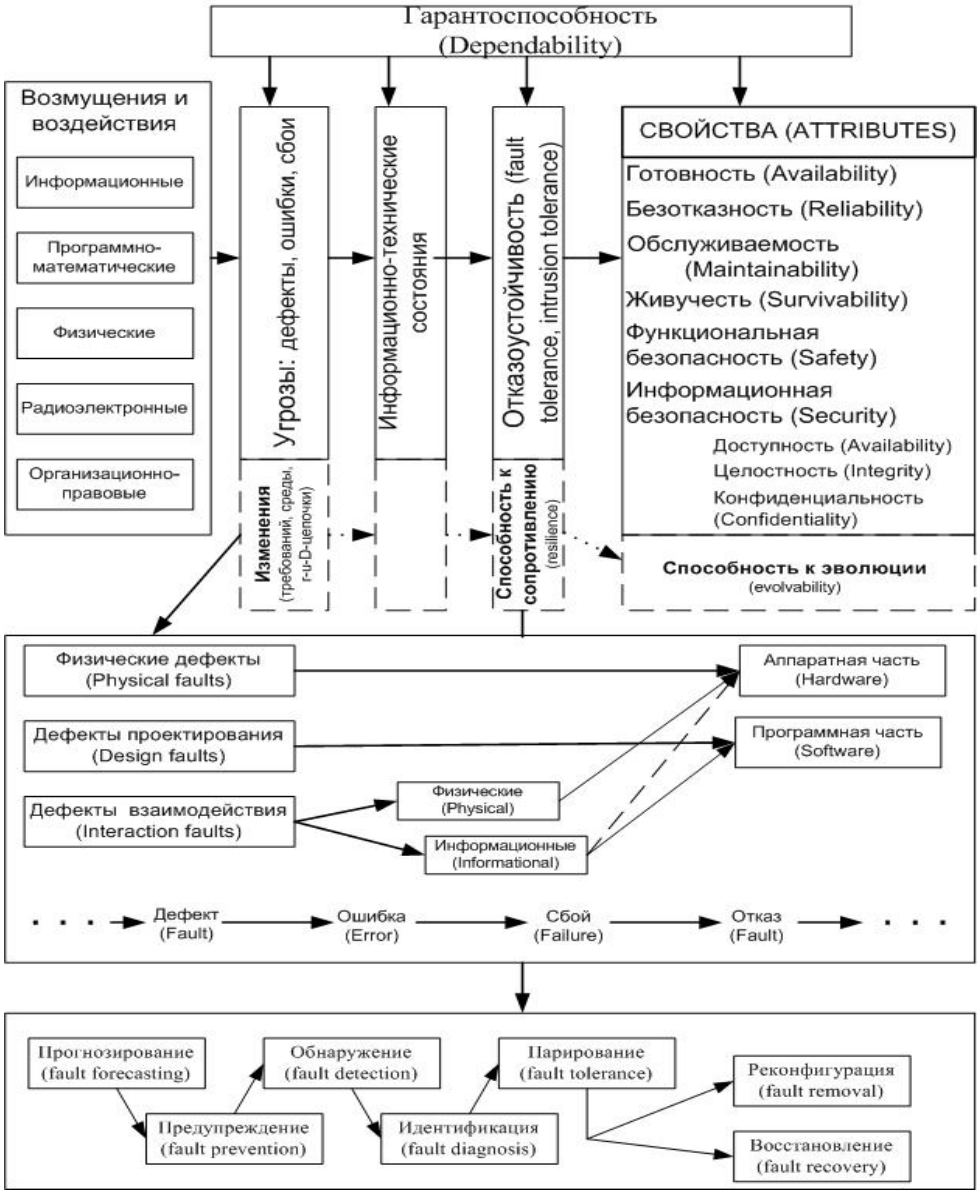

Рис. 2. Структура и взаимосвязь атрибутов гарантоспособности САБ

– безотказность (англ. reliability) – свойство непрерывно предоставлять корректные (требуемые) услуги;

– готовность (англ. availability) – свойство доступности ресурсов САБ для предоставления требуемых услуг;

– обслуживаемость (англ. maintainability) – свойство приспособленности к обновлениям, модификации и ремонту;

– живучесть (англ. survivability) – свойство минимизировать снижение и сохранять в приемлемых пределах объём и качество предоставляемых услуг при отказах;

– функциональная безопасность (англ. safety) – свойство исключать или минимизировать при отказах вредные (катастрофические) последствия для пользователей, других систем или окружающей среды.

Отдельно следует рассмотреть такой атрибут гарантоспособности, как информационная безопасность (англ. security). Этот атрибут также является комплексным свойством, которое обеспечивает для отрабатываемой информации следующие условия:

– конфиденциальность (англ. confidentiality) - свойство препятствовать неавторизованному доступу к информации об услугах;

– целостность (англ. integrity) – свойство исключать непредусмотренные изменения системы и предоставляемых услуг;

– доступность (англ. availability) – свойство возможности получения авторизированного доступа к информации со стороны уполномоченных лиц в соответствующий, санкционированный для работы период времени.

Также следует учитывать изменяемость как самих банковских информационных систем, так и условий их использования, что отобразилось в концепции «эволюционирующей системы» [5].

3. Методы обеспечения гарантоспособности БИС

На всех этапах жизненного цикла БИС – от этапа постановки задачи по ее созданию и до вывода системы из эксплуатации, с целью обеспечения ее гарантоспособности применяются определенные методы и технологии.

Данный механизм иногда также называют обеспечением отказоустойчивости БИС. Согласно [2], он включает в себя следующую последовательность действий (операций):

– прогнозирование (англ. fault forecasting) возможности появления дефекта и возникновения отказа вследствие этого дефекта;

– предупреждение (англ. fault prevention) появления дефекта и возникновения отказа;

– обнаружение (англ. fault detection) появления дефекта, ошибки вычислений, отказа;

– идентификация (англ. fault diagnosis) причины, вида и места дефекта (отказа);

– парирование (англ. fault tolerance) последствия дефекта и возникновения отказа.

Последнее действие может включать: реконфигурацию (англ. fault removal) структуры БИС путем исключения отказавшего компонента из конфигурации, замены работоспособным и восстановление вычислительного процесса (англ. fault recovery).

Рассмотрение методов и средств обеспечения безопасности применительно к банковским информационным технологиям (рис. 3), дает основание конкретизировать методы противодействия нарушениям безопасности, а именно:

– физическое препятствие доступа;

– управление доступом программно-аппаратными средствами;

– шифрование информации;

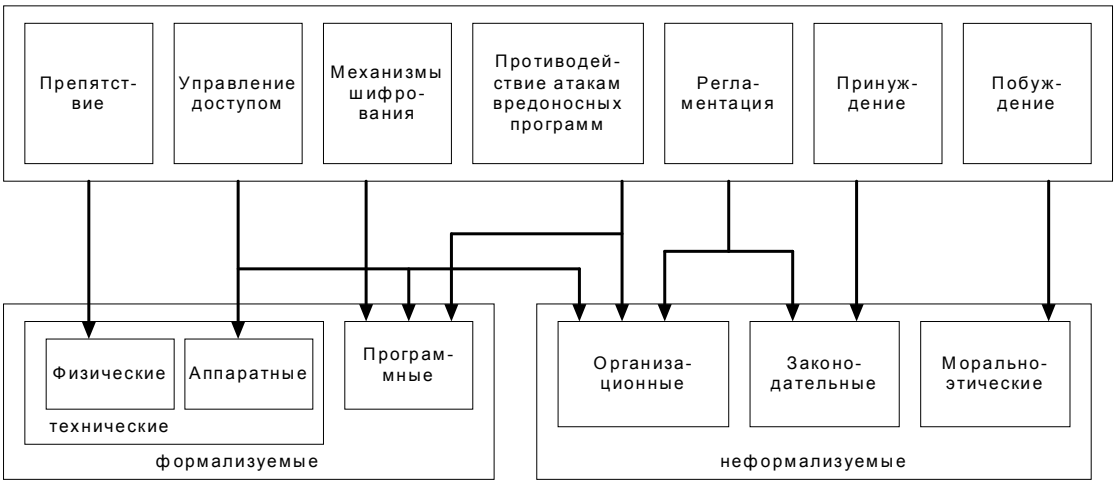

Рис. 3. Методы и средства обеспечения безопасности БИС

– использование различных программных средств борьбы с вредоносными программами;

– методы принуждения с применением материальной, административной или уголовной ответственности;

– методы побуждения не нарушать безопасность путем соблюдения морально-этических норм.

На первоначальном этапе создания САБ очень важным моментом является правильная постановка задачи и определение требований к системе. Уже тут должны быть четко сформулированы требования к ее гарантоспособности.

На сегодняшний день на рынке САБ существует довольно много фирм-разработчиков, которые предлагают свои программные продукты. Поэтому у банков появляется альтернатива разработке САБ собственными силами – возможность ее покупки. Решение о покупке принимается после тщательного анализа работы банка, изучения его информационных потоков и составления подробного технического задания. Эта работа проводится профессионалами-аналитиками (как правило, из внешней консалтинговой фирмы) при участии всех подразделений банка. Как пример реализации проекта по выбору и внедрению новой САБ на современном банковском рынке Украины, можно рассмотреть опытно-промышленную эксплуатацию новой САБ «GLOBUS T24» швейцарской компании TEMENOS в АКБ «Укрсоцбанк».

Согласно сообщениям пресс-службы банка, для реализации своих планов перед началом проекта банк предъявлял следующие требования к новой системе:

– отказоустойчивость – возможность быстрого восстановления работоспособности системы после любых сбоев и минимизация ущерба, связанного с возникновением аварийных ситуаций;

– катастрофоустойчивость – способность системы обеспечить непрерывность бизнеса в условиях чрезвычайных ситуаций;

– масштабируемость – способность системы в течение 5 лет соответствовать возрастающим требованиям относительно ресурсов информационной системы со стороны бизнеса;

– совместимость – возможность интеграции новой системы с существующими приложениями.

Специфическими для гарантоспособности систем автоматизации банка, в отличии от других компьютерных систем, являются следующие важные требования:

1. функциональная полнота – набор функций системы должен предоставлять возможность выполнять все необходимые операции банка;

2. гибкость – возможность САБ расширяться и развиваться в двух направлениях: количественном – при увеличении количества филиалов или клиентов, и качественном – при расширении спектра банковских операций и услуг;

3. надежность – состоит в том, что САБ должна обеспечивать работу большого количества пользователей, которые одновременно могут вводить, корректировать документы (счета и договора), формировать отчетность без любых конфликтов, связанных с одновременным доступом к данным;

4. обеспечение реального масштаба времени, когда после введения документа и совершения бухгалтерской проводки новое состояние счетов сразу же становится доступным для всех пользователей и может быть использовано при их дальнейшей работе;

5. интегрированность системы означает, что она должна состоять из информационно и функционально связанных между собой модулей. Информационная связь заключается в том, что все составляющие системы работают с общей базой данных, которая дает возможность избежать дублирования и обеспечивает целостность и согласованность данных. Вместе с тем функциональная связь позволяет функциональным задачам, которые характеризуются одинаковой прикладной логикой, но решаются различными пользователями, использовать общие процедуры, которые хранятся в соответствующих библиотеках (например, расчет сумм процентов и др.);

6. необходимость обеспечения многофилиальной работы банка. Выполнение этого требования в идеальном варианте реализуется распределенной обработкой данных в режиме on-line, однако пока это стоит довольно дорого и по силам не всем банкам. Поэтому более реальным является обеспечение единства технологий: как минимум, системы всех уровней должны иметь одинаковую структуру данных, одинаковые интерфейсы и инструментальные средства разработки программного обеспечения.

Выводы

Таким образом, понятие гарантоспособности систем автоматизации банка является значительно более широкой категорией, чем гарантоспособность иных, обычных компьютерных систем, что вызвано спецификой деятельности коммерческого банка. Потому направления ее обеспечения гораздо более разнообразны и сложны при реализации. В дальнейшем, на взгляд автора, необходимо более детально исследовать реальные угрозы безопасности САБ и методы их предупреждения и ликвидации. Важным направлением исследований можно считать разработку методов оценки гарантоспособности САБ.

Литература

1. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. - № 5 (17). – С. 7-19.

2. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie., B. Randel., C. Landweh. // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson - New York: John Wiley & Sons. – 2001. - 640 p.

4. Єрьоміна Н.В. Банківські інформаційні системи: Навч. Посібник / Н.В. Єрьоміна. – К.: КНЕУ, 2000. – 220 с.

5. Харченко В.С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – № 7 (41). – С. 46 – 59.

Поступила в редакцию 28.01.2010

Рецензент: д-р техн. наук, проф., проф. кафедры безопасности информационных технологий В.И. Долгов, Харьковский национальный университет радиоэлектроники, Украина.

ТАКСОНОМІЧНА СХЕМА ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНИХ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Р.М. Лахижа

Проведений аналіз поняття гарантоздатність банківських інформаційних систем (БІС). Визначені основні задачі функціонування гарантоздатних банківських систем (ГБС). Розроблена таксономічна схема гарантоздатності БІС, що враховує фактори еволюціонування. Виділені та проаналізовані методи забезпечення гарантоздатності банківських систем. Конкретизовані підходи протидії порушенням безпеки. Визначені важливі вимоги специфічні для гарантоздатності систем автоматизації банку, на відміну від інших комп'ютерних систем.

Ключові слова: гарантоздатність, банківська інформаційна система, система автоматизації банка, таксономія, безпека, загроза, дефект.

TAXONOMY SCHEME AND METHODS OF BANKING INFORMATION SYSTEMS DEPENDABILITY PROVIDING

R.M. Lakhyzha

The analysis of concept dependability of the banking information systems (BIS) is carried out. The primary goals of dependable banking systems functioning are defined. The BIS dependability taxonomy scheme is developed with the respect to evolvability factors. The methods of banking information systems dependability providing are allocated and analysed. The approaches to security violation counteraction are specified. The particular important requirements for banking systems are defined.

Keywords: dependability, banking information system, banking automation system, taxonomy, security, threat, defect, fault.

Лахижа Роман Николаевич – аспирант кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского, Харьков, Украина, e-mail: lahizha@gmail.com.