Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2019, №1, Том 11 / 2019, No 1, Vol 11 https://esj.today/issue-1-2019.html

URL статьи: https://esj.today/PDF/52ITVN119.pdf

Статья поступила в редакцию 30.01.2019; опубликована 21.03.2019

Ссылка для цитирования этой статьи:
Сиротский А.А. Некоторые особенности автоматизированных банковских процессов с позиций управления текущей операционной деятельностью // Вестник Евразийской науки, 2019 №1, https://esj.today/PDF/52ITVN119.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Sirotskiy A.A. (2019). Some features of the automated bank processes from positions of management of the current operating activities. *The Eurasian Scientific Journal*, [online] 1(11). Available at: https://esj.today/PDF/52ITVN119.pdf (in Russian)

УДК 65.011.56

ГРНТИ 06.81.12; 20.15.05; 20.15.13; 20.51.17; 20.51.23; 82.05.09; 82.05.21

Сиротский Алексей Александрович
ФГБОУ ВО «Российский государственный социальный университет», Москва, Россия
Доцент
Кандидат технических наук, доцент
E-mail: hotwater2009@yandex.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=525833

Некоторые особенности автоматизированных банковских процессов с позиций управления текущей операционной деятельностью

Аннотация. В статье рассматриваются неочевидные, но весьма существенные противоречия между задачами обеспечения целостности информации о финансовых операциях и функциональными возможностями информационных автоматизированных банковских систем, обусловленные совокупностью ролей корпоративных пользователей, их правами в системе и служебными полномочиями согласно организационной структуре банковских учреждений. Приводится конкретный пример и рекомендации по совершенствованию автоматизированных банковских бизнес-процессов.

Существующие модели управления и их информационное обеспечение в автоматизированных системах в целом соответствуют ключевым требованиям по защите информации, но не имеют достаточной гибкости и не учитывают все ветви возможных событий. Обратной стороной жёстко выстроенных политик в информационных системах является новый комплекс угроз, связанных с возникновением нетипичных ситуаций, требующих оперативного решения в действующих бизнес-процессах.

Прежде всего следует отметить необходимость совершенствования на основе научного подхода организационно-управленческих моделей в финансово-кредитных структурах и во взаимосвязи с ними – менеджмента информационной безопасности.

Наряду с необходимостью приведения в соответствие функциональных моделей автоматизированных банковских систем с инвариантным деревом бизнес-процессов в организационно-управленческой модели банковских организаций, возникает также задача технической реализации автоматизированных банковских систем на уровне разработки, тестирования и сопровождения безопасного программного обеспечения.

Устранение выявленных противоречий является необходимым условием дальнейшего развития финансово-кредитной сферы, как самостоятельной отрасли в условиях цифровой экономики. Для этого необходимо: совершенствование менеджмента в банковских организациях, разработка и внедрение моделей обработки нетипичных ситуаций в процессе выполнения бизнес-процессов, консолидированная разработка профессиональным сообществом требований к функциональности и безопасности автоматизированных банковских систем, инициирование нового направления подготовки специалистов по профилю безопасности программного обеспечения.

Ключевые слова: банк; информационная безопасность; угроза; информационная система; автоматизация; автоматизированная система; банковская система; функциональные возможности; требования; противоречия; роль; полномочия; алгоритм

Введение

В настоящее время средства информатизация и автоматизации применяются практически во всех бизнес-процессах. Ключевую роль занимают процессы банковского обслуживания, которые предоставляют на сегодняшний день широкий спектр сервисов как для физических, так и для юридических лиц.

В современных условиях есть определённое количество ключевых требований по выполнению банковских операций и обслуживанию клиентов, к которым относится:

- минимизация ручного заполнения документов;
- типизация форм;
- контроль ошибок оператора;
- управление тарифами;
- время обслуживания клиентов
- и др.

Совершенно очевидно, что операционная деятельность банка должна быть максимально автоматизирована, создание документов должно быть управляемым, а хранение информации о проведённых операциях должно отвечать требованиям по защите информации.

Современные банковские процессы и системы представляют собой сложные взаимосвязанные системы, характеризующиеся рядом особенностей по совокупности угроз информационной безопасности [1; 2; 3; 4].

Как известно, три аспекта информационной безопасности заключаются в обеспечении целостности, доступности и конфиденциальности информации.

Таким образом, автоматизированные банковские информационные системы с одной стороны должны обеспечивать полное соблюдение требований по защите информации, а с другой стороны, должны обеспечивать достаточный функционал, позволяющий банковскому работнику полноценно обслуживать и удовлетворять все запросы и потребности клиентов.

Анализ проблемы

Методы исследований основаны на прямом наблюдении, сопоставлении и анализе бизнес-процессов в банковских организациях в условиях использования им автоматизированных банковских систем.

Каждый банк волен самостоятельно определять и выбирать автоматизированную банковскую систему (АБС), на основе которой осуществлять построение своей операционной деятельности.

В зависимости от финансовых возможностей самой кредитной организации, в общем случае возможны три варианта выбора:

- внедрение готового продукта от стороннего производителя;
- разработка и внедрение своей АБС;
- самостоятельная доработка одной из коммерческих систем АБС под свои требования и задачи.

Первый путь выбирает ряд средних и мелких банков. Среди наиболее известных готовых решений АБС можно назвать: RS-Bank (производитель R-Style Softlab), Банкир/Про (производитель CSBI), линейка продуктов Diasoft (производитель Диасофт), Новая Афина (производитель Новая Афина), ЦФТ-Банк (производитель Центр Финансовых Технологий).

Второй путь зачастую непосилен даже очень крупным банкам.

Третий путь представляет собой некую комбинацию первых двух и его выбирают ряд крупных банков в расчёте на создание максимально адаптированного продукта под собственную инфраструктуру. Но создание системы таким путём далеко не всегда оказывается оптимальным. Так, к началу 2014 года Сбербанком было заключено соглашение об использовании платформы ЦФТ-Банк с правом самостоятельного модифицирования и сопровождения данной АБС силами дочерних компаний Сбербанка [5]. А уже в 2016 году руководство Сбербанка признало новую информационную систему неконкурентоспособной и решило полностью поменять платформу [6].

Главная проблема здесь заключается в том, что операционная деятельность банка не может быть остановлена, сотрудники не могут быть переобучены единомоментно, а применяемая АБС должна обеспечивать полную функциональность при одновременном соблюдении требований по информационной безопасности.

Ранжируя три аспекта информационной безопасности, не преуменьшая значения двух других, можно уверенно отметить, что главнейшим из них является аспект целостности информации, заносимой и обрабатываемой в применяющейся АБС.

Обеспечение целостности информации в АБС противопоставляется функциональной возможности внесения изменений и дополнений в хранимую информацию: операционный сотрудник, имеющий полномочия на внесение записи или проведение операции, не имеет права её отменить или изменить её условия. С одной стороны, это безусловно, правильно. Это предотвращает теоретическую возможность нарушения информационной безопасности внутренним сотрудником, т. е. предотвращает так называемую внутреннюю угрозу целостности информации. С другой стороны, в определённых случаях, отмена каких-либо действий, либо внесение изменений в записи просто необходима в силу объективных причин.

Для разрешения данного противоречия, в АБС должна быть выстроена чёткая система ролей и полномочий корпоративных пользователей (сотрудников банка), которая в свою

52ITVN119
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

очередь должна однозначным образом быть согласована с внутренней организационной структурой самого банка.

Права и обязанности корпоративных пользователей (сотрудников банка) должны не только совпадать с функциональными возможностями АБС, но и с их компетенциями в рамках выполняемых трудовых функций, а модель взаимодействия в АБС должна представлять некий конечный граф операций, который однозначно отрабатывает любую возможную входную ситуацию.

Чем полнее будет выполнено это условие, тем более эффективной будет бизнес-модель операционной деятельности банка с применением данной АБС.

Иными словами, любое отклонение от типового хода событий должно находить отработку в составе функциональных возможностей АБС с задействованием механизма оперативного подключения сотрудников с соответствующими ролями и полномочиями, которые, в свою очередь, должны быть предусмотрены в АБС.

Для пояснения вышеизложенного, следует привести конкретный пример, имевший место в действительности.

Два клиента обратились в банк для открытия аккредитива (аккредитив – условное денежное обязательство, принимаемое банком (банк-эмитент) по поручению плательщика, произвести платежи в пользу получателя средств по предъявлении последним документов, соответствующих условиям аккредитива, или предоставить полномочия другому банку (исполняющий банк) произвести такие платежи) при оформлении сделки купли-продажи).

Банковский работник стала оформлять аккредитив, для чего необходимо внести все сведения об открывателе аккредитива, договоре купли-продажи, и условиях исполнения аккредитива.

Согласно имеющимся правам в АБС, операционист банка не имеет права на выполнение данной операции без подтверждения операции старшим менеджером банка, что и было сделано.

Однако, и распечатать документ (черновик документа) на бумаге (для проверки и сверки заполненных сведений) операционист без подтверждения операции старшим менеджером также прав не имеет.

Таким образом, АБС позволила распечатать документ только после подтверждения выполнения операции старшим менеджером, имеющим соответствующие права в АБС.

После этого, в предъявленном документе клиентами банка были обнаружены опечатки (неточности), которые необходимо исправить. Казалось бы, клиент ещё не подписал никаких документов, и эти исправления логично внести, после чего распечатать на подпись исправленную форму.

Выяснилось, что распечатка документа возможна только после подтверждения операции менеджером, а после распечатки внести исправления в документ не может ни операционист, ни менеджер. Более того, поскольку клиент банка на распечатанном документе шариковой ручкой обвёл ошибки, перепечатать документ просто необходимо в любом случае. Но АБС позволяет распечатать документ только один раз (в нужном количестве экземпляров).

Ситуации, когда невозможно распечатать документ повторно (например, на случай застревания бумаги в принтере), либо когда невозможно распечатать черновик документа для сверки до подтверждения финансовой операции, сами по себе уже странны.

Однако, какие действия возможны далее в данном случае? Логично предположить два пути:

- вмешательство сотрудника, имеющего полномочия на корректировку сведений в АБС и соответствующую роль и права в АБС;
- отмену операции и удаление сведений из АБС с повторным оформлением процедуры заново.

Первоначально операционист и старший менеджер банка пытались пойти по первому из вышеназванных путей решения возникшей проблемы, обратившись в службу внутренней корпоративной поддержки банка. Однако многочисленные переговоры с различными сотрудниками и попытки внести изменения в записи в АБС успехом не увенчались. Сотрудниками поддержки банка был вынесен вердикт о невозможности внесения изменений и исправления ошибок в записях. Из этого можно сделать вывод о том, что, либо в АБС не предусмотрено корпоративного пользователя с соответствующей ролью и соответствующими правами, либо структура АБС не согласуется с организационной структурой банка, и данный функционал не задействован.

Во вторую очередь операционист и старший менеджер попытались отменить операцию, однако при этом выяснилось следующее:

- операция не может быть отменена немедленно, на это требуется длительное время;
- комиссия за операцию уже списана со счёта клиента и вернуть её невозможно.

Клиенты провели в банке несколько часов, при типовом времени на выполнение данной операции около 20 минут, что безусловно, неприемлемо, и затрагивает вопросы безопасности в контексте современного делового оборота [7]. В указанной ситуации сотрудники банка были вынуждены в итоге подать на утверждение сформированный с ошибкой комплект документов, приложив к нему отдельно правильно заполненные формы, сделанные вручную в обычном текстовом редакторе.

Здесь следует отметить, что налицо имеется противоречие между функциональными возможностями, правами и ролями корпоративных пользователей, алгоритмами функционирования АБС, и задачами обеспечения информационной безопасности при проведении финансовых операций в банковских учреждениях [8; 9].

Методы решения

В данной работе предлагается способ усовершенствования менеджмента в банковских организациях, интегрируемый с внутренними информационными автоматизированными системами банка, и направленный на гарантированное разрешение проблемных ситуаций, возникающих в ходе операционной деятельности банка.

С точки зрения организационно-управленческой модели бизнес-процессов, результатом любых операций должно быть нормальное их выполнение. При возникновении нетипичной ситуации (трудностей, ошибок, сбоев), такая нетипичная ситуация должны быть разрешена за приемлемое время. По каждой группе нетипичных ситуаций можно составить модель их обработки в виде ориентированного графа операций (рис. 1), в котором возникшая и требующая разрешения задача «i» инициирует запуск на выполнение соответствующей процедуры, описываемой графом операций. Результатом выполнения процедуры всегда должно являться состояние «o», которое позволит вернуться к нормальным условиям выполнения бизнес-процесса, что означает полное разрешение возникших сложностей.

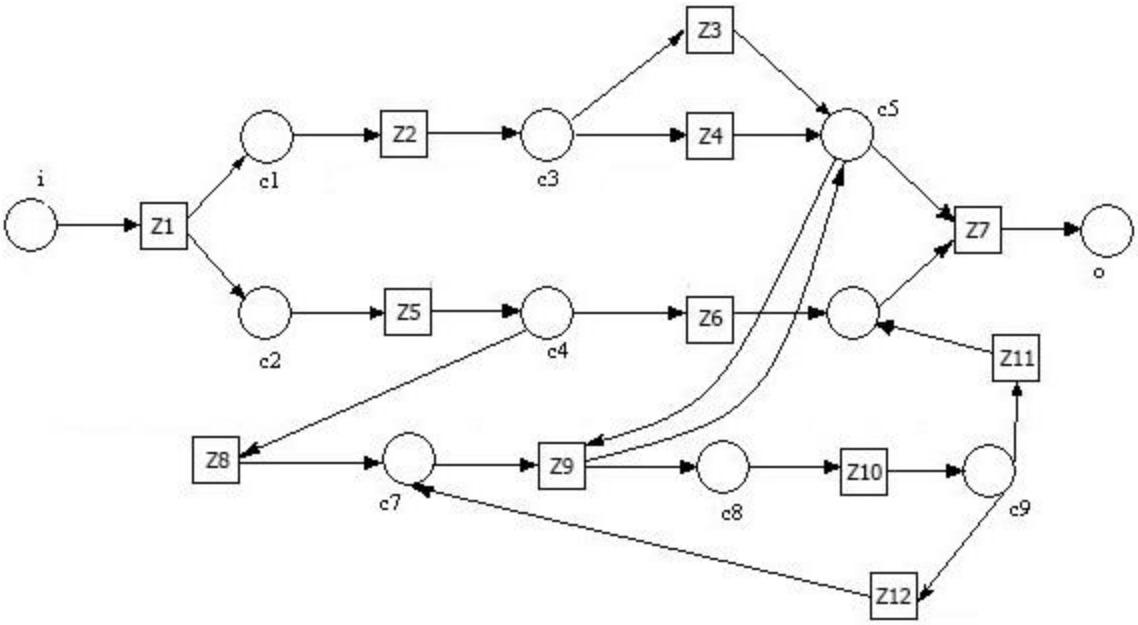

Рисунок 1. *Модель обработки проблемного события в виде ориентированного графа операций*

Ориентированный граф таким образом, имеет одну входную задачу «i» и одно конечное состояние «o», которое всегда должно являться достижимым.

Промежуточные задачи Z1…Zn представляют собой конкретные действия, выполняемые теми или иными сотрудниками банка, входят в состав их компетенций и должностных полномочий, а также могут быть реализованы в соответствии с имеющимися у них правами в АБС. К таким задачам, в частности, относятся: регистрация события, проверка данных (записей), уточнение (корректировка сведений) и т. п. Задачи связываются между собой переходами C1…Cn, каждый из которых содержит в себе условие выполнения.

Поскольку алгоритм функционирования ориентированного графа чётко определён, то бизнес-процедура разрешения проблемных событий может быть легко встроена во внутренние системы документооборота, учёта и контроля выполнения рабочих задач сотрудников банка, установив таким образом горизонтальные и вертикальные связи в управленческой модели внутреннего взаимодействия между сотрудниками различных служб и подразделений банка.

Автоматизация и цифровизация современных технологий хранения и обработки информации требует внедрения новых подходов к функциональному обеспечению банковских информационных систем и управления информационной безопасностью [10].

Существующие модели управления и их информационное обеспечение в автоматизированных системах в целом соответствуют ключевым требованиям по защите информации, но не имеют достаточной гибкости и не учитывают все ветви возможных событий. Обратной стороной жёстко выстроенных политик в информационных системах является новый комплекс угроз, связанных с возникновением нетипичных ситуаций, требующих оперативного решения в действующих бизнес-процессах.

Прежде всего следует отметить необходимость совершенствования на основе научного подхода организационно-управленческих моделей в финансово-кредитных структурах [11; 12] и во взаимосвязи с ними – менеджмента информационной безопасности [13].

Наряду с необходимостью приведения в соответствие функциональных моделей АБС с инвариантным деревом бизнес-процессов в организационно-управленческой модели

52ITVN119
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

банковских организаций, возникает также задача технической реализации АБС на уровне разработки, тестирования и сопровождения безопасного программного обеспечения (БПО).

Можно сформулировать следующие представления о БПО. Алгоритмы функционирования БПО должны строиться таким образом, что начало последующего действия может быть произведено только после завершения предыдущего действия, причём ни в коем случае не должно возникать ситуации, когда ошибка или некорректность обработки информации на предыдущем шаге приводят оператора в тупиковую ситуацию. С этих позиций, для исключения тупиковых ситуаций, необходимо предусмотреть профили пользователей, обладающих правами на коррекцию или отмену определённых действий. Оператор, под какими бы полномочиями он не находится, должен знать, видеть и понимать, какие последствия будут иметь завершение (подтверждение) выполнения текущей процедуры.

Следует отметить, что на текущий момент специалистов по профилю безопасности программного обеспечения просто не существует [14], а в ближайшем будущем, с учётом масштабной цифровизации экономики, потребность в специалистах, способных обеспечивать безопасность программного обеспечения, будет только возрастать.

Заключение

Современные финансово-кредитные организации, главными представителями которых являются банки, представляют собой сложные организационные структуры, в которых должны выполняться требования по информационной безопасности, устанавливаемые совокупностью нормативно-правовых документов, а также обеспечиваться операционная деятельность, эффективность которой определяется организационно-управленческой моделью, внутренними структурными взаимосвязями и функциональными возможностями автоматизированных информационных систем.

Проведенные исследования показали, что в ряде случаев в банковских организациях имеются существенные недостатки в организационно-управленческих моделях и определяется рассогласование между функциями сотрудников и алгоритмами обработки информации, заложенными в автоматизированные системы.

Наиболее ярко указанные недостатки и противоречия проявляются в случае возникновения неочевидных, нетипичных ситуаций, один из примеров которых рассмотрен в данной статье.

Устранение выявленных противоречий является необходимым условием дальнейшего развития финансово-кредитной сферы, как самостоятельной отрасли в условиях цифровой экономики. Для этого необходимо:

- совершенствование менеджмента в банковских организациях, введением вертикальных и горизонтальных связей между полномочными сотрудниками различных подразделений банка;
- разработка и внедрение моделей обработки нетипичных ситуаций в процессе выполнения бизнес-процессов;
- интеграция моделей обработки нетипичных ситуаций в процессе выполнения бизнес-процессов с действующими системами документооборота и контроля выполнения рабочих задач;
- разработка требований к безопасному программному обеспечению, реализующему функции АБС;

- консолидированная разработка профессиональным сообществом требований к функциональности и безопасности АБС;
- инициирование нового направления подготовки специалистов по профилю безопасности программного обеспечения.

ЛИТЕРАТУРА

1. Сиротский А.А. Обобщенная модель угроз и уязвимостей информационной безопасности в финансово-кредитных учреждениях / Информационная безопасность бизнеса и общества. Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016. – 111 с. – с. 33–39.
2. Сиротский А.А. Об угрозах целостности и достоверности финансовой информации при ликвидации банковских организаций // Информационные технологии. радиоэлектроника. Телекоммуникации, 2017. – с. 485–490.
3. Сиротский А.А. Метрический подход к оценке информационной безопасности в организациях банковской сферы // Системы безопасности, 2016. – №25, с. 126–129.
4. Сиротский А.А. Анализ типовых угроз информационной безопасности автоматизированных систем применительно к дистанционному банковскому обслуживанию / Информационная безопасность бизнеса и общества. Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016. – 111 с. – с. 40–45.
5. А. Левашов. Война за главную ИТ-систему Сбербанка завершилась / Режим доступа: http://www.cnews.ru/news/top/vojna_za_glavnuyu_itsistemu_sberbanka.
6. Греф признал устаревшей новую IT-систему Сбербанка за миллиарды рублей / Режим доступа: https://www.rbc.ru/finances/15/01/2016/5698ce9d9a794791cf2c1748.
7. Сиротский А.А. Экономико-правовая и информационная безопасность существования личности в современном деловом обороте // Педагогика безопасности: наука и образование. Сборник материалов Всероссийской научной конференции с международным участием 12 декабря 2011 г. Часть 2. Проблемы

и задачи педагогики безопасности в области образования. Екатеринбург, 2012. 216 с. с. 163–169.

8. Соляной В.Н., Сухотерин А.И., Сиротский А.А. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях / Информационная безопасность бизнеса и общества. Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016. – 111 с. – с. 46–56.
9. Соляной В.Н., Сухотерин А.И., Сиротский А.А., Морозов О.В. Особенности управления информационной безопасностью кредитно-финансовых структур региона // Информационно-технологический вестник, 2014. – №2. – с. 102–107.
10. Сиротский А.А. Предупреждение угроз безопасности финансовому сектору в цифровой экономике / «Интеллектуальные системы в информационном противоборстве». Сборник научных трудов Российской научной конференции 15–17 декабря 2017 г. В 2 томах. Том 1. Москва, ФГБОУ ВО «РЭУ им Г.В. Плеханова», 2017. – 446 с. – с. 379–385.
11. Сиротский А.А. Научный подход в управлении бизнесом / Преподавание информационных технологий в Российской Федерации: материалы Десятой открытой Всероссийской конференции (16–18 мая 2012 года). – М.: МГУ им. М.В. Ломоносова, 2012. – 476 с., с. 438–446. ISBN 978-5-9556-0135-9.
12. Сиротский А.А. Об инновационных подходах, средствах и методах эффективного управления предприятием // Человеческий капитал, №11 (35), 2011, с. 64–66.
13. Сиротский А.А. Исследование угроз и организация менеджмента информационной безопасности в финансово-кредитных организациях // Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2016): сб. статей VI международной заочной научно-технической конференции. Ч.2. / Поволжский гос. ун-т сервиса. – Тольятти: Изд-во: ПВГУС, 2016. – 346 с. – 213–221.
14. Сиротский А.А. Безопасность программного обеспечения – специальность будущего / Преподавание информационных технологий в Российской Федерации: материалы Шестнадцатой открытой Всероссийской конференции (Москва, 14–15 мая 2018 г.) / Московский государственный технический университет; Ассоциация предприятий компьютерных и информационных технологий. Москва, 2018. – 417 с. – с. 51–54.

Sirotskiy Alexey Alexandrovich
Russian state social university, Moscow, Russia
E-mail: hotwater2009@yandex.ru

Some features of the automated bank processes from positions of management of the current operating activities

Abstract. In article the unevident, but very essential contradictions between problems of ensuring integrity of information on financial transactions and functionality of the information automated banking systems caused by set of roles of corporate users, their rights in a system and office powers according to organizational structure of banking institutions are considered. The concrete example and recommendations about improvement of the automated bank business processes is given.

The existing models of management and their information support in the automated systems in general conform to key requirements for information security, but have no sufficient flexibility and do not consider all branches of possible events. A reverse side rigidly built the politician in information systems is the new complex of the threats connected with emergence of the atypical situations requiring the operational solution in the operating business processes.

First of all it should be noted need of improvement on the basis of scientific approach of organizational and administrative models in financial and credit structures and in interrelation with them – management of information security.

Along with need of reduction in compliance of functional models of the automated banking systems with an invariant tree of business processes in organizational and administrative model of the bank organizations, there is also a problem of technical implementation of the automated banking systems at the level of development, testing and support of the safe software.

Elimination of the revealed contradictions is a necessary condition of further development of the financial and credit sphere as independent industry in the conditions of digital economy. For this purpose it is necessary: improvement of management in the bank organizations, development and deployment of models of processing of atypical situations in the course of performance of business processes, the consolidated development by professional community of requirements to functionality and safety of the automated banking systems, initiation of the new direction of training of specialists on a profile of safety of the software.

Keywords: bank; information security; threat; information system; automation; the automated system; banking system; functionality; requirements; contradictions; role; powers; algorithm