УДК 004

О РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

Николашин М.В.

магистрант 3 курса,

ФГБОУ ВО «Калужский государственный университет им. К.Э. Циолковского»

Калуга, Россия

Белаш В.Ю.

к.пед.н., доцент,

ФГБОУ ВО «Калужский государственный университет им. К.Э. Циолковского»

Калуга, Россия

Аннотация: Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий. В статье исследуется процесс обеспечения информационной безопасности банка в условиях импортозамещения. Рассмотрен процесс реализации требований информационной безопасности с использованием метода моделирования и диаграмм в нотации IDEF0. Дано подробное описание этапов в рамках подхода к реализации требований информационной безопасности банков в условиях импортозамещения. Кроме того, проведено моделирование процесса с помощью диаграммы в нотации UML.

Ключевые слова: безопасность, импортозамещение, информация, программное обеспечение, экономика.

ON THE IMPLEMENTATION OF INFORMATION SECURITY REQUIREMENTS IN THE CONTEXT OF IMPORT SUBSTITUTION

Nikolashin M.V.
3rd year master's student,
Kaluga State University named after K. E. Tsiolkovsky
Kaluga, Russia
Belash V.Yu.
Ph.D., Associate Professor,
Kaluga State University named after K. E. Tsiolkovsky
Kaluga, Russia

Annotation: The computerization of banking activities has significantly increased the productivity of the bank's employees and introduced new financial products and technologies. However, progress in crime technology is no less rapid than the development of banking technology. The article examines the process of ensuring the bank's information security in the context of import substitution. The process of implementing information security requirements using the modeling method and diagrams in the IDEF0 notation is considered. A detailed description of the stages in the approach to the implementation of information security requirements of banks in the context of import substitution is given. In addition, the process was modeled using a diagram in UML notation.

Keywords: security, import substitution, information, software, economics.

Современные реалии и вызовы динамично меняющихся социально-экономических условий предъявляют новые требования к деятельности во многих сферах. Сфера экономики активно развивается за счет разработки и внедрения новых программных решений. Однако, переход на российское программное обеспечение требует тщательной проработки, создания ряда

новых программных средств, а также, зачастую, и поиска новых методов их внедрения.

Организация защиты автоматизированных систем управления информационной безопасностью – это единый комплекс мер, которые должны учитывать все особенности процесса обработки информации. Несмотря на неудобства, причиняемые пользователю во время работы, во многих случаях средства защиты могут оказаться совершенно необходимыми для нормального функционирования системы. К основным из упомянутых неудобств следует отнести:

1. Дополнительные трудности работы с большинством защищенных систем.

2. Увеличение стоимости защищенной системы.

3. Дополнительная нагрузка на системные ресурсы, что потребует увеличения рабочего времени для выполнения одного и того же задания в связи с замедлением доступа к данным и выполнения операций в целом.

4. Необходимость привлечения дополнительного персонала, отвечающего за поддержание работоспособности системы защиты.

Современный банк трудно представить без автоматизированной информационной системы. Компьютер, находящийся на столе банковского служащего, уже давно стал привычным и необходимым инструментом, без которого невозможно осуществлять банковские операции. Связь между компьютерами внутри банка, а также с вычислительными машинами (ЭВМ) других банков, является важным условием для эффективного функционирования финансовых учреждений, так как объем операций, выполняемых в течение короткого временного промежутка, значительно возрос.

Для реализации требований информационной безопасности банков в условиях импортозамещения можно предложить поэтапный подход, который будет включать в себя следующие ключевые этапы, рассмотренные далее и

представленные на диаграмме в нотации IDEF0 (рис. 1), а также ее декомпозиции (рис. 2, рис. 3).

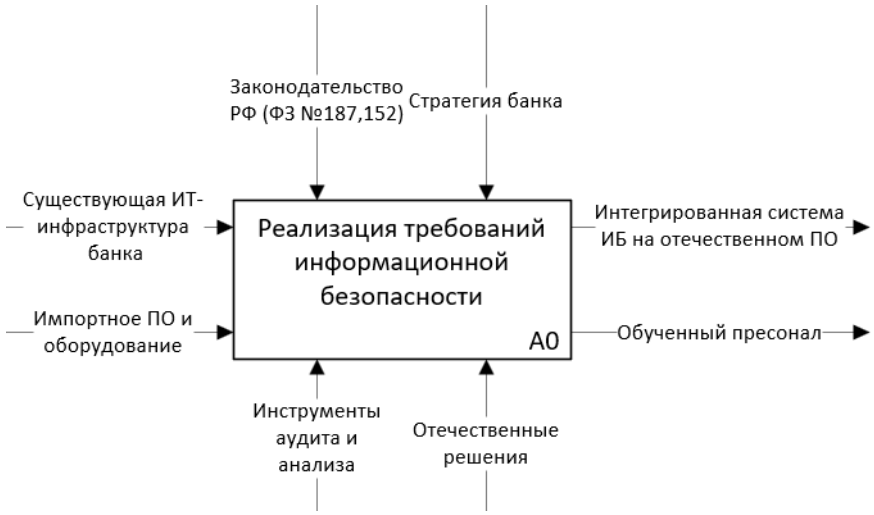

Рис. 1. Реализация требований информационной безопасности

1.Анализ текущего состояния

Первым шагом в процессе импортозамещения является проведение аудита используемых информационных технологий. На этой фазе следует:

- Провести всесторонний анализ существующих информационных систем для выявления критически важных компонентов, зависимых от импортного программного обеспечения и оборудования.
- Оценить риски и потенциальные последствия перехода на отечественные решения, включая финансовые, операционные и юридические аспекты.
- Сформировать реестр импортного программного обеспечения и оборудования, подлежащих замене, что позволит систематизировать данные и создать базу для последующих этапов.

2.Разработка стратегии импортозамещения

На данном этапе необходимо:

- Определить приоритетные направления импортозамещения, учитывающие требования информационной безопасности и стратегию организации.
- Разработать детализированную дорожную карту, описывающую поэтапную замену импортных решений на отечественные аналоги с учетом временных рамок и ресурсов.
- Согласовать данную стратегию с руководством компании и регулирующими органами, что обеспечит легитимность и поддержку инициативы на всех уровнях.

3. Выбор и внедрение отечественных решений в области информационной безопасности

На этом этапе рекомендуется:

- Провести анализ рынка отечественных средств защиты информации, оценивая их функциональные возможности и соответствие требованиям законодательства и стандартам безопасности.
- Организовать пилотные проекты для тестирования и оценки эффективности выбранных решений, что позволит выявить их сильные и слабые стороны в рамках конкретной инфраструктуры.
- Разработать планы внедрения новых систем информационной безопасности, включая инструкции по эксплуатации и поддержанию.

4. Обеспечение интеграции и совместимости

Данная фаза включает:

- Интеграцию новых отечественных решений в существующую IT-инфраструктуру, что потребует детального планирования процессов и ресурсов.
- Обеспечение взаимодействия между различными компонентами системы информационной безопасности, что критично для эффективного функционирования всей системы.

- Проведение тестирования и верификации корректности функционирования интегрированной системы, направленного на минимизацию уязвимостей и оптимизацию процессов.

5. Развитие компетенций персонала

Для успешной реализации процесса необходимо:

- Организовать обучение и повышение квалификации сотрудников в сфере эксплуатации и администрирования отечественных решений в области информационной безопасности.
- Внедрить программы обучения и информирования персонала о новых технологиях и практиках обеспечения информационной безопасности, что создаст базу для повышения общей осведомленности и профессионализма.

1. Контроль и совершенствование

На завершающем этапе следует:

- Регулярно проводить аудит и тестирование эффективности внедренных решений, что обеспечит актуальность и защищенность системы.
- Анализировать результаты мониторинга и оперативно вносить необходимые изменения и улучшения в системы обеспечения информационной безопасности.
- Взаимодействовать с регуляторами, поставщиками и экспертным сообществом для обмена опытом и лучшими практиками, что будет способствовать развитию и адаптации к новым вызовам в сфере информационной безопасности.

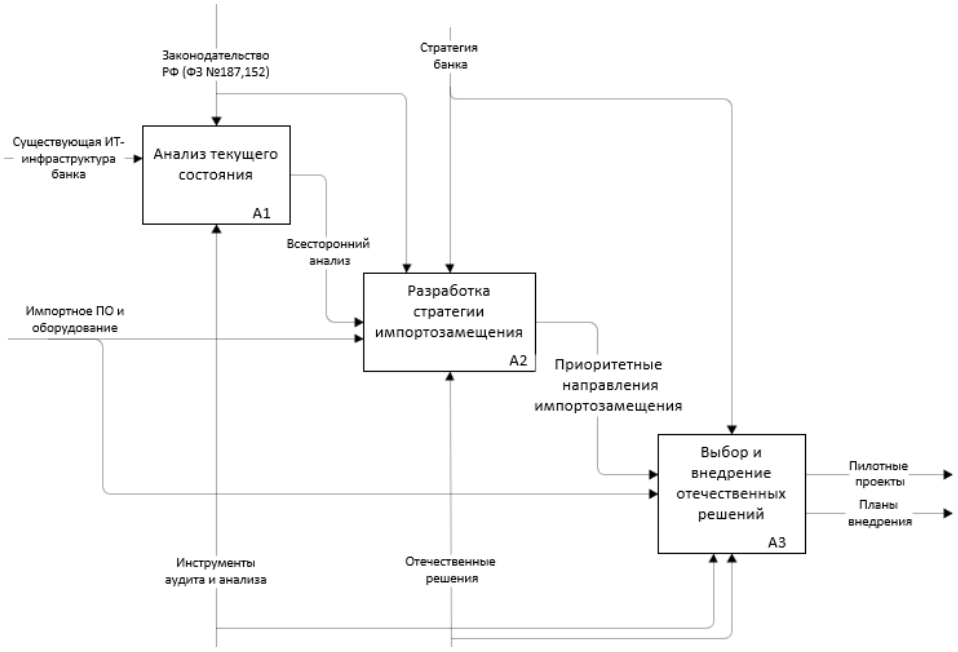

Рис. 2. Декомпозиция диаграммы (блоки A1-A3)

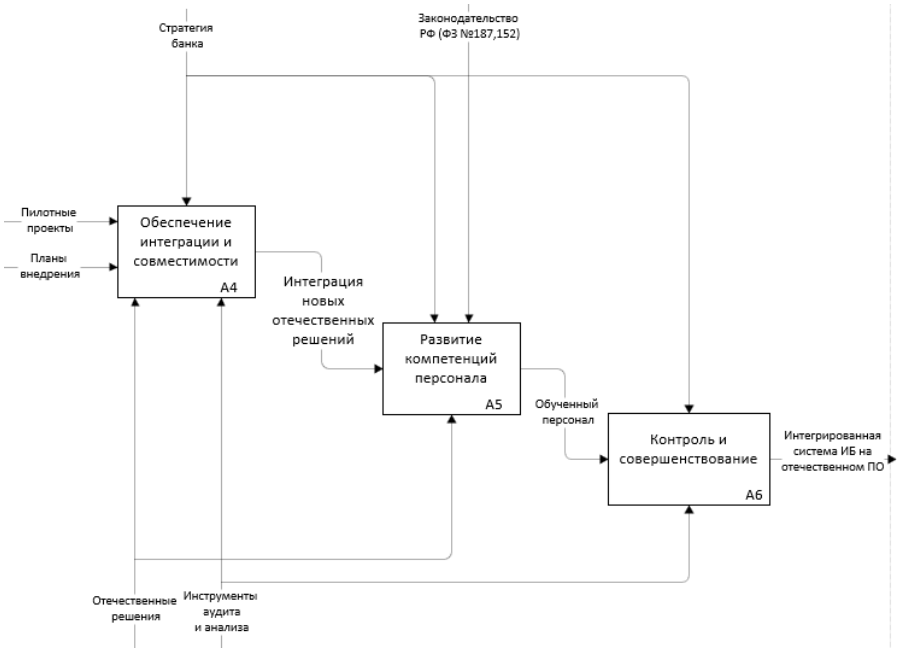

Рис. 3. Декомпозиция диаграммы (блоки A4-A6)

В заключение, предложенный поэтапный подход к реализации требований информационной безопасности банков в условиях импортозамещения демонстрирует комплексный и системный подход к решению данной проблемы. Каждый из этапов — от анализа текущего

состояния до контроля и совершенствования внедренных решений — играет ключевую роль в успешной замене импортных технологий на отечественные аналоги.

Проведение тщательного аудита и анализа существующих информационных систем позволяет выявить критически важные компоненты и оценить риски, связанные с переходом на новые решения. Разработка стратегии импортозамещения обеспечивает четкую дорожную карту, что, в свою очередь, способствует легитимности и поддержке на всех уровнях управления. Продемонстрируем процесс реализации требований информационной безопасности банка в условиях импортозамещения с помощью диаграммы в нотации UML (рис. 4).

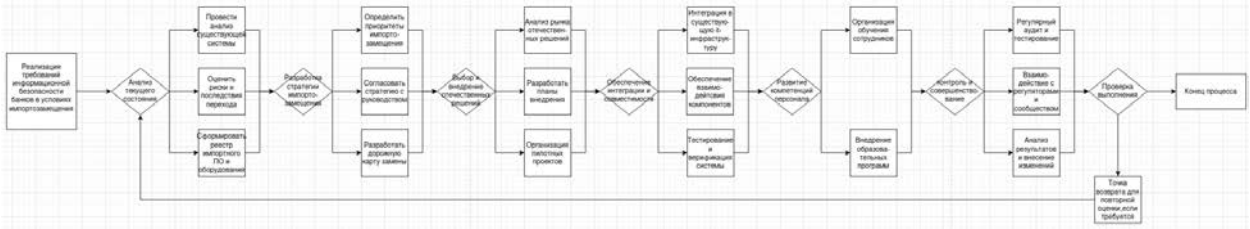

Рис. 4. Процесс реализации требований информационной безопасности банка

Выбор и внедрение отечественных средств защиты информации, их интеграция в существующую инфраструктуру, а также развитие компетенций персонала создают основы для эффективной работы системы информационной безопасности. Важно, что финальный этап, связанный с контролем и постоянным совершенствованием, настоятельно подчеркивает необходимость оперативного реагирования на изменения внешней среды и технологические новшества.

Таким образом, реализация данного подхода позволит не только соответствовать современным требованиям информационной безопасности, но и укрепить позиции банков за счет повышения надежности и защищенности их информационных систем.

Библиографический список

1. Агапов, Д.С. Информационная безопасность банковских систем: современные угрозы и методы защиты / Д.С. Агапов // Финансы и кредит. – 2021. – Т. 27, № 3. – С. 619-633.

2. Баранов, С. Н. Обеспечение информационной безопасности банковских операций в условиях цифровой экономики / С. Н. Баранов, А. А. Петров // Банковские технологии. – 2022. – № 4. – С. 35-41.

3. Васильев, В. П. Актуальные проблемы информационной безопасности в банковской сфере / В. П. Васильев // Вестник экономической безопасности. – 2023. – № 1. – С. 78-84.

4. Козлов, А. С. Комплексный подход к обеспечению информационной безопасности банка / А. С. Козлов // Управление финансовыми рисками. – 2021. – № 2. – С. 45-52.

5. Петров, А. К. Информационная безопасность как фактор устойчивого развития банковского сектора / А. К. Петров // Финансовая аналитика: проблемы и решения. – 2022. – № 12. – С. 112-120.

6. Смирнов, Д. А. Влияние цифровизации на угрозы информационной безопасности банковского сектора / Д. А. Смирнов // Экономика и управление. – 2020. – № 8. – С. 88-94.

Оригинальность 81%