Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК _____

Терентьев

Вадим Евгеньевич

Модель безопасности внутреннего контура ИТ-архитектуры банка

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Давыдов Геннадий Владимирович

кандидат технических наук, доцент

_____

Минск 2018

ВВЕДЕНИЕ

Двадцать лет назад появилось новое направление исследований, которое стали называть архитектурой предприятия. Это направление изначально предназначалось для решения двух следующих проблем.

Сложность систем – организации тратили все больше денег на построение ИТ-систем.

Неэффективная организация бизнеса – несмотря на всевозрастающую стоимость ИТ-систем, организациям с большим трудом удавалось поддерживать их соответствие требованиям бизнеса.

Итог: высокие затраты, низкая эффективность. Эти проблемы, впервые выявленные 20 лет назад, сегодня достигли критической точки. Стоимость и сложность ИТ-систем выросли экспоненциально, а реальная польза от них резко снизилась.

Текущее состояние банковских систем не стало исключением. Банки уже давно стали использовать ИТ-системы для реализации своей деятельности и для удовлетворения их потребностей, по мере развития ИТ-отрасли разрабатывались различные системы, которые внедрялись в банках, таким образом образую сложный ИТ-ландшафт, которым стало трудно управлять, так как стало необходимым интегрировать множество ИТ-систем, многие их которых являются унаследованными, устаревшими, но еще выполняющие свои функции, а также множество современных решений используемых для современных функций банков, таких как интернет-банкинг и мобильный банкинг. Учитывая быструю дигитализацию общества и изменения требований к современному банку, у предприятий этой отрасли возникают следующие задачи:

- соответствие изменяющимся трендам;
- выполнение изменений и адаптаций достаточно быстро и с умеренными расходами;
- обеспечение установленного уровня безопасности корпоративных систем.

Для соответствия современных трендам необходимо быть готовым к постоянным изменениям и перестроению ИТ-системы предприятия, но учитывая масштабы ИТ-ландшафта банка, необходимо эффективно управлять архитектурой предприятия, то есть содержать ее в состоянии готовом для быстрых и дешевых изменений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г, №190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Целью диссертационной работы является построение модели безопасности внутреннего контура ИТ-архитектуры банка.

Задачи:

Для достижения указанной цели в диссертации поставлены и решены следующие задачи:

Смоделировать и описать информационную банковскую архитектуру приложений, выделив ключевые интеграционные узлы, проанализировать существующие шаблоны интеграции корпоративных приложений.

Исследовать архитектуру корпоративных сервисных шин и их функциональные возможности.

Построить информационно-логическую модель процесса интеграции приложений через корпоративную сервисную шину, выделить ключевые информационные потоки.

Смоделировать правила обеспечения безопасности информации на инфраструктурном уровне, уровне приложений для обеспечения безопасности бизнес функций банковской системы.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на XXII Международной научно технической конференции «Современные средства связи» (Минск 2017), XIV Международной научно-практической конференции «Управление информационными ресурсами» (Минск 2017), VIII Всероссийской научно-технической конференция «Безопасные информационные технологии» (Москва 2017)

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 статьи в сборниках материалов конференций.

Личный вклад

Личное участие автора диссертации охватывает исследования по построению корпоративной архитектуры предприятий, существующих моделей безопасности и общемировых рекомендаций по управлению предприятиями. Автором проведен анализ существующих данных по описанным направлениями, разработка нового подхода к обеспечению безопасности на основе интеграции существующих данных, сформулированы общие положения диссертации, составляющие её новизну и практическую значимость.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТ

Используемая методология и инструменты для построения модели

Для построения модели безопасности ИТ-архитектуры банка необходимо моделирования основы ИТ-архитектуры. Для моделирования корпоративных архитектур существуют различные стандарты, нотации и фрэймворки. В основе моделирования используется на стандарт TOGAF, в частности его методе построения архитектуры – architecture development method, а также совместимая с ним нотация Archimate версии 3.0. Используемые инструменты позволили создать в данной работе блоки модели, которые могут быть переиспользованы в конкретных банках для построения и детализации своих архитектурых моделей и как следствие переиспользовать созданные взаимосвязи.

Моделирование ИТ-архитектуры банка

Для моделирования ИТ-архитектуры банка необходимо определить специфику работы банка, рассмотреть функции основных подразделений банка и программное обеспечение, которое при этом используется. Для выявление основных функций банка необходимо обратиться к литературе содержащей информацию о банковском секторе, финансах и функциях банка в настоящее время в обществе. Исходя из данных полученных из литературы и из опыта текущей работы в банке были выделены функциональные блоки основных подразделений банка, в данной работе выбраны подразделения отвечающее за взаимодействие с корпоративными клиентами и физическими лицами, это позволило смоделировать ИТ-архитектуру банка, представленной на рисунке 1 и рисунке 2.

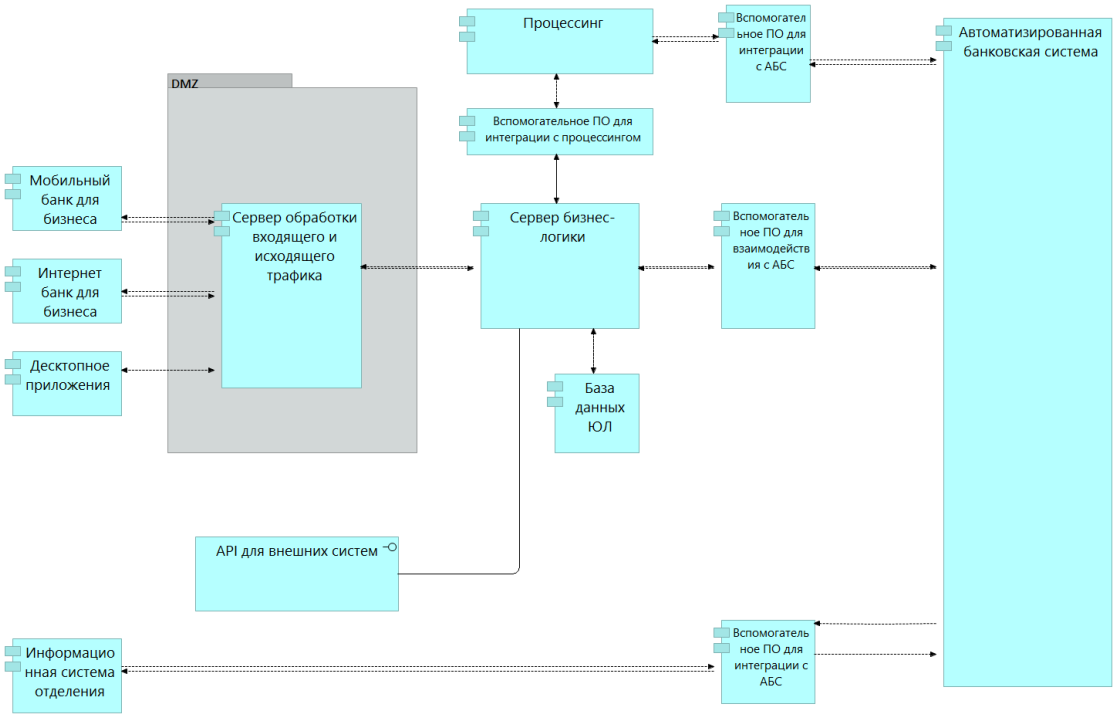

Рисунок 1 - Модель ИТ-архитектуры подразделения отвечающее за физических лиц.

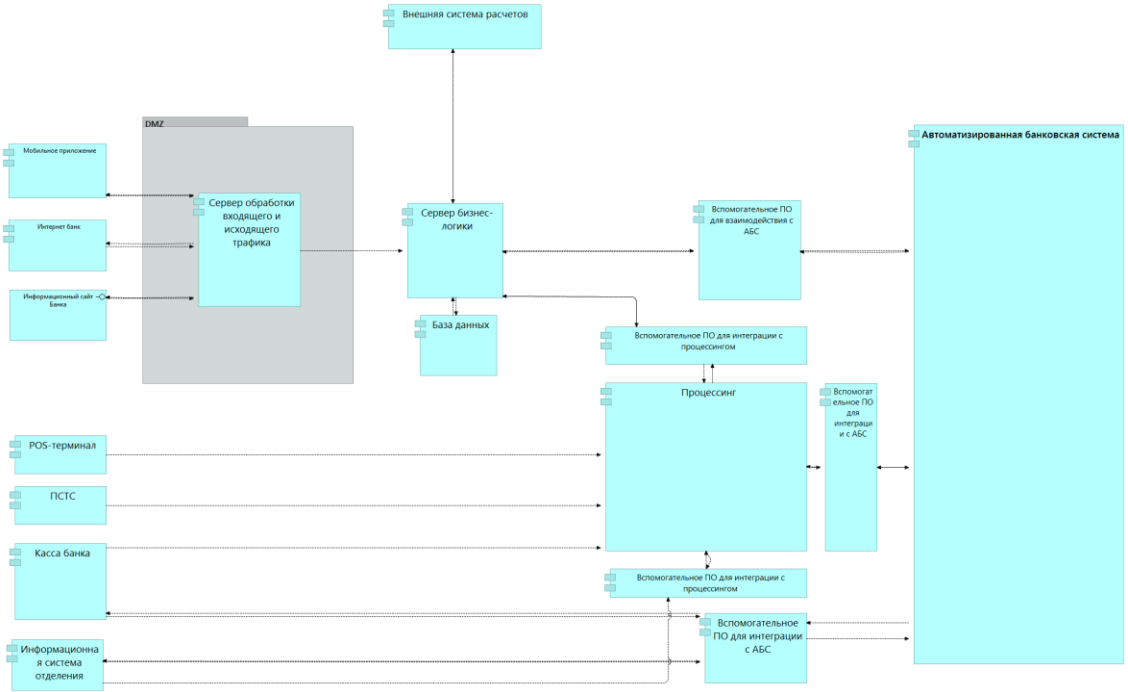

Рисунок 1 - Модель ИТ-архитектуры подразделения отвечающее за физических лиц.

Оптимальная ИТ-архитектура банка

Представленные выше схемы отображают только функционально необходимые блоки для реализации функций банка, но в данных схемах есть существенное дублирование интеграционных узлов. Для построения модели безопасности банка необходимо отталкиваться от максимально

оптимальной инфраструктуры. Для того, чтобы разобраться с вопросом интеграции корпоративных приложений была изучена современная литература и выбран оптимальный путь интеграции в виде корпоративной сервисной шины (ESB).Таким образом, ключевым узлом внутреннего контура ИТ-архитектуры является интеграционный узел выраженный корпоративной сервисной шиной. С текущим решением и добавлением к созданным моделям был добавлен уровень инфраструктуры (серверов), который необходим для функционирования описанного программного обеспечения. Таким образом получилась схема представленная на рисунке 3.

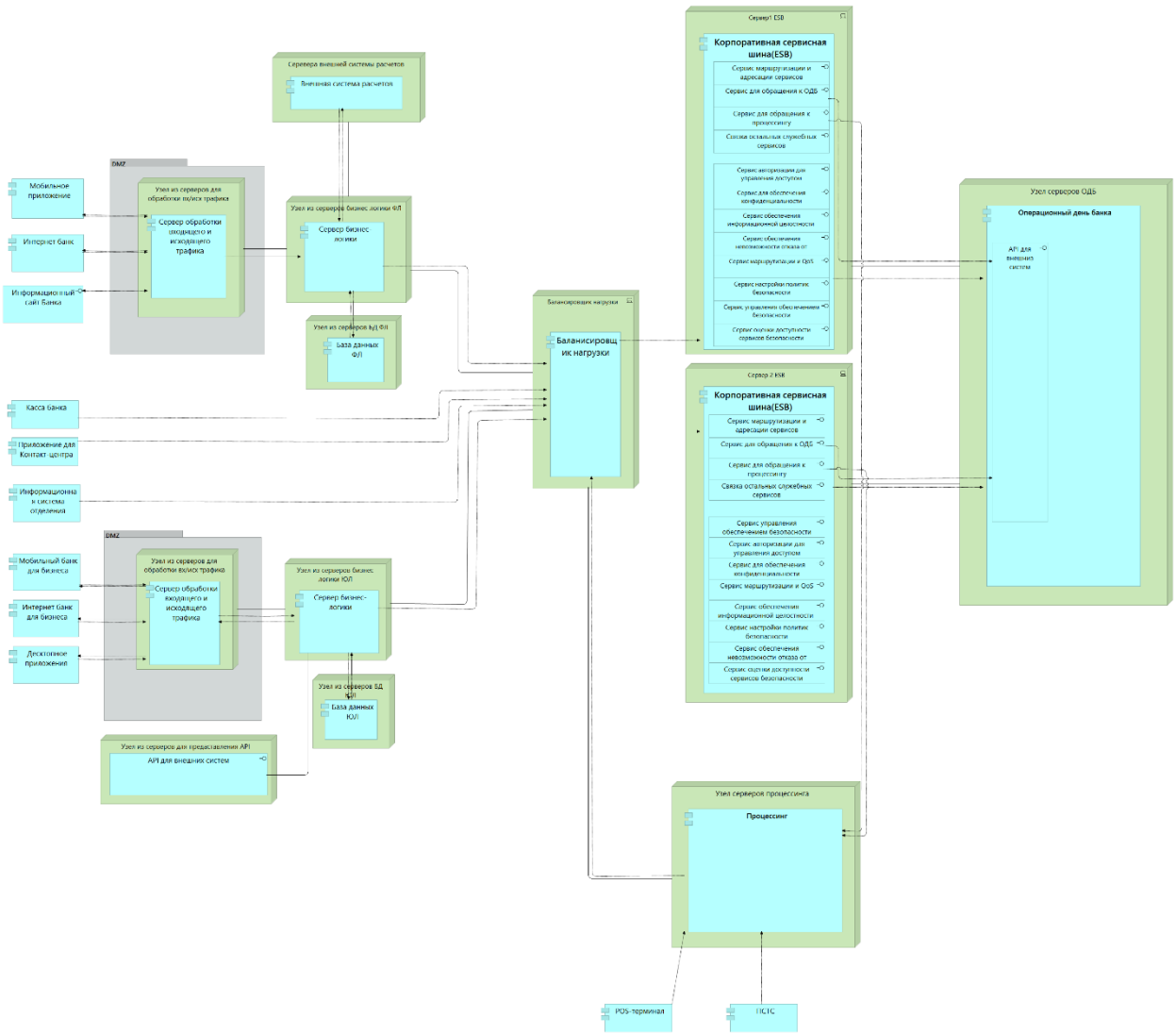

Рисунок 3 - Оптимальная ИТ-архитектура банка.

Построение модели безопасности

Для построения модели безопасности необходимо определить возможные угрозы предприятия. В классических моделях безопасности рассматриваются модели нарушителя, а также другие риски нанесения

угрозы предприятию. Разрабатываемая модель претендует зафиксировать взаимосвязи событий являющиеся угрозой функционирования банковской ИТ-архитектуры или каких-либо ее частей, с драйверами этих событий и провести взаимосвязи с элементами, которые должны среагировать на запуск таких событий с самой инициации события. Для этого в работе были выделены драйверы событий, которые могут являться угрозами, также были созданы документы регулирующие работу организации, взаимосвязи подразделений и необходимый уровень безопасности, кроме того были распределены зоны ответственности по ролям. Описанные взаимосвязи были отображены на рисунке 4.

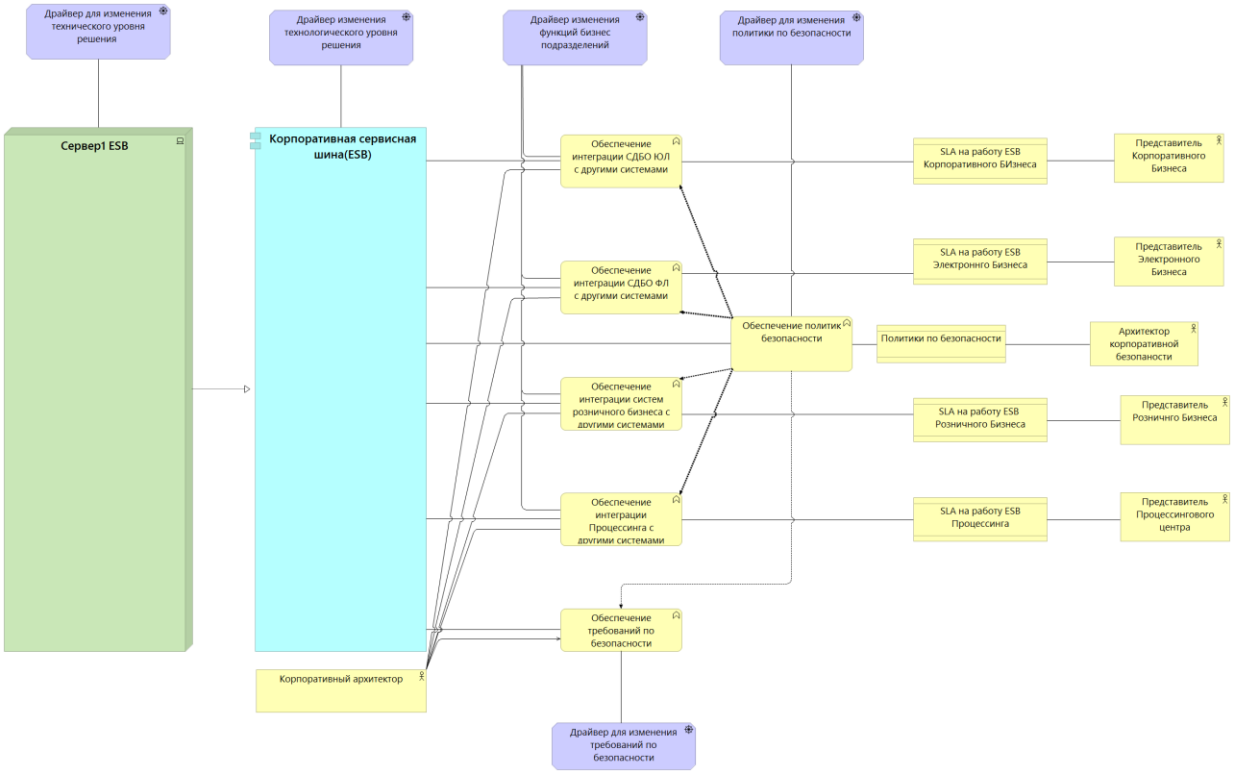

Рисунок 4 - Взаимосвязи драйверов изменений и регулирующих структур.

Имея в модели построенные взаимосвязи, можно построить обобщенное представление модели для упрощения работы с ней. В данном моменте следует учесть, что упрощенной представление лишь обобщает все проведенные представление, но сохраняет текущие взаимосвязи. Созданная модель представлена на рисунке 5.

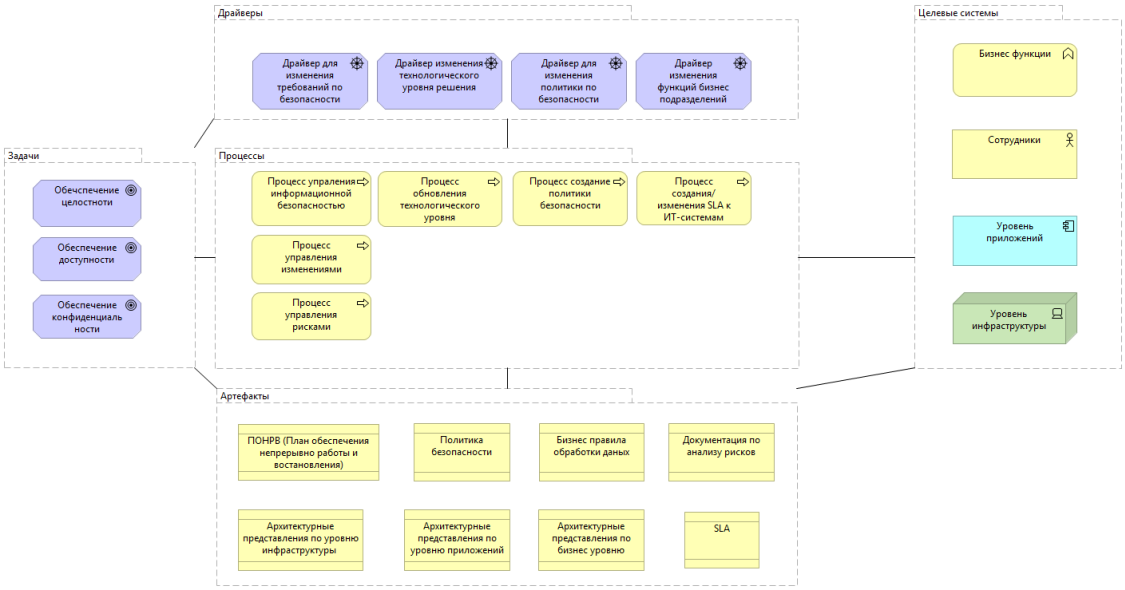

Рисунок 5- Модель построения системы защиты в корпоративной системе банка

Практическая значимость модели

Созданная модель позволяет предотвращать инциденты безопасности агрегируя поступающую информацию по обеспечению безопасности из различных источников тем самым не позволяя внутренним и внешним угрозам использовать уязвимости безопасности для нанесения ущерба организации. Каждый банк может адаптировать и расширить модель банковской среды проведя взаимосвязи к ключевым компонентам, что позволет на теоретическом уровне отслеживать и управлять работами, которые необходимо совершать при появлении факторов влияющих на информационную систему банка.

При каком-либо изменении корпоративный архитектор вносит запись изменения в компонент, на который непосредственно направлено изменение, далее он строит граф взаимосвязей с данным компонентом и получает все объекты, которые необходимо контролировать.

Пример визуализации такого взаимодействия можно рассмотреть на объекте политики безопасности, которое представлено на рисунке 7.4.

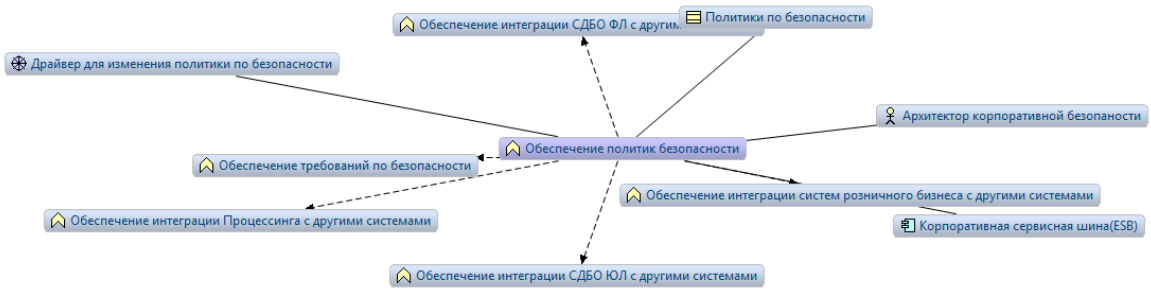

Рисунок 6 Граф взаимосвязей компонентов

Таким образом модель опираясь на метод построения корпоративной архитектуры стандарта TOGAF, рекомендация по управлению процессами на предприятии ITIL и на архитектурную модель банковской среды, позволяет эффективно управлять системой безопасности внутреннего контура банковской среды для предотвращения инцидентов безопасности.6

ЗАКЛЮЧЕНИЕ

В данной работе была смоделирована общая банковская архитектурная модель банка, был выделен внутренний контур данной архитектуры, а также решена проблема интеграции систем во внутреннем контуре с помощью корпоративной сервисной шины, таким образом интегрировав все основные банковские ИТ-системы через один интеграционный узел, что снимает необходимость соединения систем друг с другом по шаблону «точка-точка» заменяя все интеграции новых систем, их связью только с шиной, но тем самым увеличивая требования к обеспечению безопасности данного решения. Поэтому в работе уделяется особое внимание обоснованию оптимальности данного решения, а также уделено особое внимание к процессу построения требований безопасности и причины их возникновения и возможные драйверы их изменения. На основе проанализированной информации была построена модель описывающая все элементы архитектуры с точки зрения TOGAF и Archimate, являющимися объектами обеспечения безопасности. Проанализировав существующие обобщенные модели безопасности ИТ-систем, была построена частная модель безопасности внутреннего контура ИТ-системы банка. Данная модель может являть основой для перепроектирования автоматизированной банковской системы при изменении ИТ-ландшафта с целью перехода на SOA-архитектуру с использованием корпоративной сервисной шины

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Терентьев, В.Е. План реализации безопасности корпоративной сервисной шины в банке / В.Е. Терентьев // Современные средства связи: Тезисы докл. XXII Международной научно-технической конференции – Минск, 2017 – С.275 – 435.

2-А. Терентьев, В.Е. Модель безопасности внутреннего контура ИТ-архитектуры банка / В.Е. Терентьев // Управление информационным ресурсами: Тезисы докл. XIV Международной научно-практической конференции – Минск, 2017 – С.122 – 267.