

Содержание

Акт о прохождении практики	
Дневник учебной практики	
Отзыв руководителя практики	
Введение	
1. Характеристика деятельности ПАО «Росбанк»	
2. Основные мероприятия по совершенствованию ИТ-инфраструктуры ПАО «Росбанк»	
Заключение	
Список используемой литературы	

Введение

Производственная практика проводилась в Южном филиале ПАО «Росбанк» в экономическом отделе с--- по ----. Публичное акционерное общество — это общество, акции которого свободно выпускаются и размещаются на рынке ценных бумаг. Ограничение на количество акций, которые могут, принадлежат одному акционеру (что предусматривалось ранее) - отменено. Также отменена возможность размещения привилегированных акций с номинальной ценой ниже, чем у обычных.

Актуальность практики заключается в том, что она помогает закрепить полученные теоретические знания и применить их на практике деятельности банка.

Цель практики – изучить структуру и провести анализ совершенствования ИТ – инфраструктуры ПАО «Росбанк».

Для достижения поставленных целей были сформулированы следующие задачи практики:

- дать характеристику деятельности ПАО «Росбанк»;
- провести анализ совершенствования ИТ-инфраструктуры ПАО «Росбанк»;

Объект исследования – ПАО «Росбанк».

Предмет исследования – структура и совершенствование ИТ-инфраструктуры организации на примере ПАО «Росбанк»

Научная значимость заключается в обобщении полученных сведений для последующей оценки действий, направленных на модернизацию ИТ-инфраструктуры ПАО Росбанк.

Практическая значимость проведенного исследования заключается в том, что результаты могут успешно использоваться коммерческими банками в практической деятельности по улучшению организации обслуживания клиентов в банковских организациях.

Методы исследования

1. Характеристика деятельности ПАО «Росбанк»

Росбанк — российский универсальный банк, находившийся в составе международной финансовой группы Société Générale до апреля 2022 года. С 2022 года главным акционером банка является российская Группа Интеррос. Полное наименование — Публичное акционерное общество Росбанк. Штаб-квартира находится в Москве. В октябре 2019 года включён Банком России в перечень системно значимых кредитных организаций, основан в 1993 году. ПАО «Росбанк» занимает 14 место по объему собственного капитала среди крупнейших российских банков по версии «РИА Рейтинг» на 1 июля 2022 года. Банк имеет следующие долгосрочные рейтинги международных рейтинговых агентств: «BB-» Standard & Poor's (прогноз негативный), «Ba3» Moody's Investors Service (прогноз негативный).

ПАО «Росбанк» универсальный коммерческий банк, основными направлениями деятельности которого являются:

- банковские услуги корпоративным клиентам: в том числе кредитование, расчетные операции, факторинг, документарные операции, финансирование с участием эка, проектное финансирование, управление потоками денежных средств и платежами, брокерские услуги на валютных рынках и рынках ценных бумаг, прием депозитов;

- банковское обслуживание малого и среднего бизнеса: в том числе коммерческое кредитование, прием депозитов, расчетно-кассовое обслуживание, включая выдачу векселей, денежные переводы, предоставление гарантий, а также брокерские услуги на валютных рынках и рынках ценных бумаг;

- розничные банковские услуги частным лицам: в том числе розничное кредитование и прием депозитов у физических лиц (текущие счета и срочные вклады), денежные переводы, выпуск банковских карт, расчетно-кассовое обслуживание и валютные операции, управление денежными средствами через удаленные каналы обслуживания;

- инвестиционно-банковские и финансовые услуги: сделки на рынках заемного капитала, в том числе их организация, андеррайтинг муниципальных и корпоративных облигаций (таких как местные рублевые облигации, евробонды, кредитные ноты и векселя), торговля акциями и инструментами с фиксированной доходностью, услуги по корпоративному финансовому консультированию, брокерские услуги, сделки репо, операции с драгоценными металлами, управление активами и частное банковское обслуживание состоятельных клиентов (private banking);

Клиентами банка уже стали более 10 000 российских предприятий, а количество розничных клиентов достигает 820000 человек. Региональная сеть ПАО «Росбанк» насчитывает около 55 офисов, более 800 банкоматов (включая банкоматы банков-партнеров) и более 100 терминалов самообслуживания по всей России. Продукты и услуги представлены в подавляющем большинстве регионов, охватывающих порядка 28% населения России. ПАО «Росбанк» также имеет офис на Кипре и представительство в Китае, которые, в первую очередь, осуществляют поддержку российских клиентов. Система управления Южного филиала ПАО «Росбанк» представляет собой многоуровневую структуру, каждый уровень которой отвечает за отдельные направления деятельности банка. Схему организационной структуры управления банка рассмотрим на рис.1.

Организационная структура является линейно-функциональной, каждый специалист выполняет конкретные поставленные задачи. Секретарь осуществляет обработку входящих, исходящих и внутренних документов банка, контролирует правильность документов, представленных на подпись руководству банка, по инструкции по эксплуатации редактирует документы, контролирует правильность документов и обеспечивает методическую и организационную помощь сотрудникам банка при подготовке документов.



Рисунок 1 - Схема организационной структуры управления ПАО «Росбанк»

Юридический отдел выполняет следующие функции:

- Защищает права и интересы банка;
- использует правовые средства для укрепления финансового положения банка и улучшения экономических показателей его работы;
- оказывает помощь органам управления банка в обеспечении законности его деятельности;
- контролирует правильное применение законодательства Российской Федерации, нормативными документами Центрального банка Российской Федерации.

Главный бухгалтер выполняет следующие задачи:

- формирует полную и точную информацию о бизнес-процессах и результатах деятельности;
- обеспечивает контролирует наличие и движение имущества, использование материальных, трудовых и финансовых ресурсов в соответствии

с утвержденными стандартами, нормативами и сметами; компонентных отчеты о результатах банка;

- Проводит учет и контроль за движением средств учреждений банка. Особое внимание уделено урегулированию банковского и кассового обслуживания.

Для этих целей банк создает контроль расчетно-кассовое обслуживание, чьи функции включают в себя: открытие и ведение счетов, расчеты; ведения кассовых операций. Отдел кадров выполняет следующие функции: - планирует численность и использование персонала; - организует обучение и повышение квалификации; - проводит начисления заработной платы; Отдел автоматизации проводит работу со всей системой обеспечения банка, проводит организацию и контроль за техническим обеспечением банка, составляет программы и т.д.

2. Анализ мероприятий по совершенствованию ИТ-инфраструктуры ПАО «Росбанк»

Централизация и унификация ИТ-платформ во всех регионах — важнейшая технологическая задача Банка. Одним из шагов по централизации технологий стало создание ЦОД (Центр обработки данных), который начал занимать ключевое место в бизнес-процессах Банка, так как позволяет увеличить надежность и пропускную способность по всем операциям. Растущие объемы бизнеса, в особенности розничных операций, также требуют более мощных технологий, что станет еще одной важнейшей сферой инвестиций в информационные технологии Банка.

Для проведения анализа подробно остановимся на мероприятиях, направленных на совершенствование информационной инфраструктуры банка.

Первое это система мониторинга информационной безопасности. 21 ноября 2019 года компания Infotecs сообщила о завершении внедрения системы мониторинга информационной безопасности в Росбанке.

В рамках модернизации системы управления ИТ-инфраструктурой, перед специалистами стояла задача подбора решения, которое будет обеспечивать защиту данных, не замедляя работу информационных систем. Кроме того, решение должно способствовать повышению эффективности управления ИТ-инфраструктуры.

Сотрудниками ИТ-службы заказчика, в качестве программных инструментов контроля и управления ИТ-активами, выбрана система мониторинга информационной безопасности Symantec Security Information Manager.

Проект реализован в сжатые сроки и состоял из четырех основных этапов:

- анализ информационной и сетевой инфраструктуры;
- проектирование и разработка эксплуатационной документации с учётом специфики бизнеса заказчика;

- внедрение и конфигурирование систем,
- ввод ПО в эксплуатацию. Результаты внедрения системы мониторинга: повышение эффективности управления ИТ-инфраструктурой, снижение затрат на управление инцидентами и упрощение контроля за соблюдением регламентов информационной безопасности. Следующим нововведением явилось создание мобильного приложения для работы с ERP-системой на планшете iPad, которое вступило в силу в 2017 году.

Результатом реализации проекта является централизованная и введенная в промышленную эксплуатацию в центральном аппарате и Московском банке Росбанка система, соответствующая функциональным, эксплуатационным, архитектурным требованиям и требованиям по безопасности.

К основным бизнес-задачам относятся:

1. Обеспечить доступ через мобильные устройства к следующим процессам Росбанка:

- планирования и управления бюджетом;
- управления персоналом;
- управления имуществом.

2. Обеспечить формирование гибкой отчетности по процессам. Требования к системе.

Источником информации для аналитических панелей должны служить системы программы «внедрение ERP», а также геоинформационная система Банка на платформе ПО ArcGIS. Мобильное решение должно обеспечивать доступ к аналитическим панелям с мобильных устройств под управлением iOS не ниже версии 9 (iPad, iPad2, iPad3). Система должна поддерживать до 650 одновременных подключений в режиме обучения/тестирования, в том числе:

- планирование и управление бюджетом – 150 пользователей,
- управление персоналом – 400 пользователей,
- управление имуществом – 100 пользователей.

Максимальная цена договора: 78,3 млн. рублей без НДС, включая стоимость проекта разработки системы на 1 этапе 19,2 млн. рублей без НДС, на

2 этапе 22,1 млн. рублей без НДС и сопровождение решения в течение одного года 24 млн. рублей без НДС.

Далее рассматривается, так называемая, «Кредитная фабрика» - новая система выдачи быстрых кредитов, которая позволяет в минимальные сроки выдавать денежные займы как физическим, так и юридическим лицам. Основными принципами действия данного процесса кредитования является автоматизация, централизация и централизация всех внутренних процессов, происходящих при рассмотрении очередной заявки и выдаче кредита. За пять лет действия программы было выдано порядка 3 млн. кредитов, общая сумма которых превышает 1 трл. рублей.

По словам руководства Росбанка, по этой программе ежедневно выдается около 2 тыс. кредитов, т.е. на один кредит приходится не более 25 минут. Особой популярностью программа «Кредитной фабрики» пользуется у индивидуальных предпринимателей, так как позволяет получить достаточно крупную сумму денежных средств в течение 3-х дней, при этом пакет необходимых документов будет минимален. Для них доступны такие продукты, как «Доверие», «Экспресс-актив» и «Экспресс-Авто», где можно в короткие сроки получить займ размером до 5 млн. рублей на срок до 5 лет.

В 2023 году, Росбанк будет оформлять кредит «Доверие» в рамках действия «Кредитной фабрики» по сниженной ставке в размере от 0,9% годовых.

Теперь перейдем к самому, пожалуй, главному мероприятию, а именно, к рассмотрению ЦОДа. В 2021 году перед банковской группой Societe Generale в России встала задача по модернизации и созданию единой системы BMS Центра Обработки Данных, так как существующая система не контролировала более 70% установленного оборудования.

Инженерами компании ИНЕ лтд было проведено обследование объекта и подготовлено предложение по замене существующего ПО на современную систему мониторинга Simplascope, разработанную нашими специалистами, с расширением количества наблюдаемых параметров оборудования объекта.

В ходе выполнения работ по модернизации BMS к вновь вводимой системе мониторинга Simplascope было подключено инженерное оборудование различных производителей в 14-ти помещениях (РУ, ГРЩ, ЩГП, АВР, ИБП, кроссовые, серверные), расположенных в различных частях здания на первом, втором и третьем этажах.

«Парк» оборудования включает в себя:

- 140 электрических силовых щитов распределения электроэнергии;
- 1590 автоматических выключателей и рубильников;
- 102 реле контроля напряжения;
- 54 прибора качества электроэнергии Lovato серии DMK;
- 4 источника бесперебойного питания Chloride 90-NET;
- 21 кондиционер Liebert HPM и CRV;
- 37 датчиков температуры и влажность Lumel P18;

Новая система контролирует более 7 000 технологических параметров на объекте.

Рабочее место оператора оснащено двумя 32 мониторами, расположенными в помещении диспетчерской на первом этаже здания. На эти мониторы выводится информация о состоянии объекта в виде схем, графиков, светозвуковой индикации, визуализации, событий и сообщений. Предусмотрена возможность гибкой настройки аварийных и предупредительных границ контролируемых параметров, формирование отчетов о работе оборудования.

Оператор системы мониторинга в режиме реального времени может контролировать ход технологического процесса электроснабжения объекта, параметры качества электроэнергии ответственных потребителей, состояние и режимы работы инженерного оборудования, климатические характеристики помещений ЦОД. На основе полученных данных SIMPLASCOPE позволяет предотвращать аварийные ситуации при эксплуатации инженерного оборудования объекта. В установленную систему заложена возможность

масштабирования. В нее можно добавить как новое оборудование, так и новые функции, которые необходимы заказчику.

Исходя из вышеизложенного, становится очевидным то, что безопасность данных занимает ключевую роль. В связи с этим, особое внимание должно уделяться именно защите данных. За образец предлагается использовать решение, разработанное компанией Cisco Systems.

Решения Cisco для обеспечения безопасности реализуют системный подход к обеспечению безопасности ЦОД предприятия и предназначены для защиты производственных процессов и ресурсов предприятия. Cisco разделяет свои продукты для обеспечения безопасности на три категории: защита от угроз, управление доверительными отношениями и проведение идентификации, обеспечение безопасного взаимодействия. Большая часть этих функциональных возможностей реализуется с помощью программного обеспечения Cisco IOS, интегрированных сервисных модулей для обеспечения безопасности для платформы Cisco Catalyst 6500 Series, а также средств обеспечения безопасности, интегрированных в коммутаторы Cisco MDS 9000 Series.

Стратегия Cisco по обеспечению безопасности ЦОД предоставит предприятию следующие преимущества:

- Защита на всех уровнях;
- Безопасная консолидация;
- Снижение риска успешного проведения атак на "неизвестные уязвимости" (0-day);
- Повышение степени целостности сервисов;
- Более простые средства управления, меньшая стоимость владения;
- Гибкость;
- Снижение капиталовложений;

Управление безопасностью необходимо для выявления и блокирования нарушений политики прежде, чем возникнет реальный ущерб. Не представляется возможным измерить ни ценность доверия, которое испытывает

пользователь к ресурсам ЦОД, ни стоимость ущерба, нанесенного организации в том случае, когда из-за нарушения безопасности нарушается целостность данных или останавливается работа приложений и серверов.

Системы управления безопасностью ЦОД должны удовлетворять высочайшим стандартам простоты использования, степени автоматизации, качеству обработки данных, а также скорости и адекватности реакции.

Важным фактором обеспечения безопасности является конфигурирование, в ходе которого задаются правила обнаружения возможных вторжений, реакции на них, а также способы устранения уязвимостей. Система управления изменениями должна быть простой и должна предоставлять администраторам безопасности автоматизированные инструментальные средства обновления конфигурации устройств, выполняющих обнаружение угроз.

Основным инструментом системы управления безопасностью является мониторинг, и администраторам необходимы инструментальные средства для обработки больших объемов данных, полученных от компонентов системы обеспечения безопасности, а также средства выявления подозрительной активности и упреждающего реагирования на угрозы. Для обеспечения эффективной совместной работы компонентов системы безопасности на разных уровнях требуется эффективный процесс поиска и устранения неполадок, что и позволит сделать предложенная нами система.

Заключение

В данном исследовании мной была изучена структура и меры предпринимаемые по совершенствованию ИТ-инфраструктуры ПАО «Росбанк»

Научная значимость заключается в обобщении полученных сведений для последующей оценки действий, направленных на модернизацию ИТ-инфраструктуры ПАО Росбанк.

Практическая значимость проведенного исследования заключается в том, что результаты могут успешно использоваться коммерческими банками в практической деятельности по улучшению организации обслуживания клиентов в банковских организациях.

В ходе исследования мной были изучены организационные вопросы, структура