

УДК 658:004.9(470.571)

*Рузманова А. П., Жаркова О. С., студентки 3 курса экономического факультета,  
Мордовский государственный университет имени Н. П. Огарёва, Саранск*

## **СОВЕРШЕНСТВОВАНИЕ ИТ-ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ ОАО «СБЕРБАНК РОССИИ»)**

**Аннотация.** В данной статье рассматриваются основные мероприятия по совершенствованию ИТ-инфраструктуры. Особое внимание было уделено созданию центра обработки данных в Москве. В ходе работы были выявлены возможные угрозы, связанные с большими объемами данных, и, как следствие, проблемы ее защищенности. Исходя из этого, было предложено решение компании Cisco Systems для обеспечения безопасности данных ЦОДа.

**Ключевые слова.** ИТ-инфраструктура, Сбербанк, МегаЦОД, безопасность данных, совершенствование, ИТ-проект, ERP-система, централизация, мобильное приложение, кредитование, автоматизация.

**Annotation.** In this article are considered the main actions for improvement of IT infrastructure. The special attention was paid to creation of a data-processing center in Moscow. In the course of work identified potential threats associated with large volumes of data, and as a result, the problem of its security. On this basis, it was suggested solution from Cisco Systems for data security data center.

**Keywords.** IT infrastructure, Sberbank, MEGATSOD, data security, improvement, IT project, ERP-systems, centralization, mobile application, crediting, automation.

В рамках общемирового тренда ИТ-инфраструктура российского банковского сектора становится все сложнее, а требования к ее качеству — выше. Приняв в качестве одной из ключевых стратегических целей быстрый скачок в обеспечении клиентов высокотехнологичными продуктами и услугами, Сбербанк продолжает инвестировать в развитие информационных технологий.

Централизация и унификация ИТ-платформ во всех регионах — важнейшая технологическая задача Банка. Одним из шагов по централизации технологий стало создание МегаЦОД (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. [2]

В рамках данной статьи более подробно остановимся на последних мероприятиях, направленных на совершенствование информационной инфраструктуры банка.

Первое это **система мониторинга информационной безопасности**. 21 ноября 2013 года компания Softline сообщила о завершении внедрения системы мониторинга информационной безопасности в Сбербанке.

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-инфраструктурой. 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 четырёх 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 2013 году.[4]

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

К основным бизнес-задачам относятся:

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

- 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 5 (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: 145,2 млн. рублей без НДС, включая стоимость проекта разработки системы на 1 этапе 39,6 млн. рублей без НДС, на 2 этапе 81,6 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 15 млн. кредитов, общая сумма которых превышает 3 трл. рублей. По словам руководства Сбербанка, по этой программе ежедневно выдается около 24 тыс. кредитов, т.е. на один кредит приходится не более 15 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 2014 году, Сбербанк будет оформлять кредит «Доверие» в рамках действия «Кредитной фабрики» по сниженной ставке в размере 14,5% годовых.

Теперь перейдем к самому, пожалуй, главному мероприятию, а именно, к рассмотрению **МегаЦОДа**.

В 2011г. в Москве состоялось открытие центра обработки данных (ЦОД) Сбербанка «Южный порт», который стал крупнейшим в Восточной Европе. Общая площадь здания центра – около 16500 кв.м, площадь ИТ-залов – 5000 кв.м., энергопотребление - около 25 МВт. Он приходит на смену тем 36 ЦОДам, которые сейчас работают у банка в регионах. На создание ЦОДа потребовалось 15 месяцев. Инвестиции в проект составили около \$1,2 млрд. [5]

ЦОД централизует информационные ресурсы всех территориальных банков Сбербанка, что позволит максимально эффективно осуществлять информационную поддержку подразделений, занимающихся обслуживанием клиентов, и в разы увеличить производительность вычислительных процессов.

ЦОД «Южный порт» позволит унифицировать сопровождение практически всех банковских процессов, значительно сократит сроки внедрения новых банковских продуктов, надеются в Сбербанке.

Расчетная экономия расходов банка на сопровождение ИТ-инфраструктуры начиная с 2015 г., как ожидается, составит около \$500 млн в год. Срок окупаемости проекта – порядка 2,5 лет.[6]

Целями построения МегаЦОДа являлись:

1. Виртуализация как рабочих мест, так и различных банковских программных систем, работающих в клиент-серверной архитектуре.
2. Построение совершенно нового класса SaaS-систем. Прежде всего - это системы клиентского обслуживания - клиент-банк, интернет-банк и т.д.
3. Централизация бэк-офисных систем территориальных банков.

Как и планировалось ранее, в текущем году, т.е. в 2014, начнется строительство второго ЦОДа, который будет расположен в Сколково. Проект будет реализован в течение 1,5 года и станет первым опытом реализации проектов Microsoft Consulting Services на территории России. Строительство ЦОДа позволит Сбербанку централизовать ИТ-системы финансового учреждения.

Так же следует отметить то, что Сбербанк планирует открыть новую дочернюю компанию, которая будет играть в дальнейшем немаловажную роль.

«Сбербанк-Сервис» будет заниматься обслуживанием ИТ-инфраструктуры, банкоматов и терминалов банка. Перед компанией поставлены три основных КРП – повышение доступности систем, повышения удовлетворенности клиентов и повышение качества сервиса. [1]

«Сбербанк-Сервис» станет второй по счету крупной ИТ-компанией «Сбербанка». В ноябре 2011 г. банк создал компанию «Сбербанк-Технологии» с целью развития внутренних ИТ-систем, а впоследствии и оказания услуг сторонним организациям. В отличие от «Сбербанк-Сервиса», ее основной задачей является разработка и модернизация ПО.[3]

Ранее «Сбербанк» объяснял создание собственных ИТ-компаний стремлением повысить эффективность внутренних ИТ-проектов. Практика

создания собственных технологических подразделений в крупных компаниях наблюдается и на мировом рынке. Так, недавно автопроизводитель General Motors сообщало переводе в свой штат порядка 3 тыс. сотрудников HR, которые были задействованы в ИТ-проектах компании.

Сбербанк России и IBM заключили меморандум о стратегическом сотрудничестве, который направлен на оптимизацию поставок оборудования и программного обеспечения, а также модернизацию ИТ-инфраструктуры Банка. В соответствии с этим компания IBM приняла решение изменить формат взаимодействия со «Сбербанком» уже в 2013 г., что позволит перейти к прямым поставкам оборудования и программного обеспечения (ПО).

В рамках заключенного соглашения IBM намеревается авторизовать компанию «Сбербанк-Сервис», являющуюся дочерней компанией «Сбербанка», на поставки широкого спектра аппаратного и программного обеспечения IBM. По окончании процесса авторизации «Сбербанк» сможет значительно повысить эффективность закупок продуктов IBM, осуществляя их через «Сбербанк-Сервис» напрямую у логистических партнеров IBM. Согласно меморандуму, «Сбербанк» также получает возможность использования новейших технологий IBM, а специалисты обеих компаний будут совместно участвовать в программе модернизации ИТ-инфраструктуры банка. [1]

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.[9]

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.[7] 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.[8] 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.

### Список литературы

1. Глухова Т. В., Жаркова О. С., Рuzманова О. П. Исследование информационно-аналитической системы предприятия (на примере Сбербанка) [Электронный ресурс]. – Режим доступа: [http://sisupr.mrsu.ru/2012-2/PDF/Glukhova\\_Zharkova\\_Ruzmanova.pdf](http://sisupr.mrsu.ru/2012-2/PDF/Glukhova_Zharkova_Ruzmanova.pdf)
2. Официальный сайт Сбербанка России. [Электронный ресурс]. – Режим доступа: <http://www.sberbank.ru>
3. Российское издание, Интернет-портал и одноименный ежемесячный журнал «CNEWS – издание о высоких технологиях». [Электронный ресурс]. – Режим доступа: [http://www.cnews.ru/top/2012/11/19/novaya\\_itkompaniya\\_sberbanka\\_nayden\\_direktor\\_oboznacheny\\_pervye\\_plany\\_510237](http://www.cnews.ru/top/2012/11/19/novaya_itkompaniya_sberbanka_nayden_direktor_oboznacheny_pervye_plany_510237)
4. Портал выбора технологий и поставщиков - TADVISER Государство. Бизнес. ИТ. [Электронный ресурс]. – Режим доступа: [http://www.tadviser.ru/index.php/Проект:Сбербанк\\_РФ\\_\(Мобильное\\_приложение\\_для\\_ERP\\_платформы\)](http://www.tadviser.ru/index.php/Проект:Сбербанк_РФ_(Мобильное_приложение_для_ERP_платформы))
5. Комплексное проектирование зданий и сооружений – Cronta Construction. [Электронный ресурс]. – Режим доступа: <http://www.cronta.ru/projects/with-participation-of-specialists-cronta-construction/the-computer-centre-megatsod-jsc-sberbank-of-russia/>
6. Ирландская строительная компания **Mercury Engineering**. [Электронный ресурс]. – Режим доступа: <http://mercuryeng.ru/>
7. Ефремова Л. И. Автоматизированный офис (Проектирование баз данных в среде СУБД MS ACCESS): Учебное пособие / Л. И. Ефремова, Т. В. Глухова. – Саранск, 2009. (2-е изд., перераб. и доп.) – 97 с.



8. Зинина Л. И. Введение в информационный менеджмент: Учебное пособие / Л. И. Зинина, Т. В. Глухова. – Саранск, 2009. – 75 с.

9. Ефремова Л. И. Разработка реляционных баз данных: Учебное пособие / Л. И. Ефремова, Т. В. Глухова. – Саранск, 2006. – 120 с.