**1. Банки и их функции**

Банком является учреждение, созданное для привлечения депозитов и других денежных средств, в целях использования для кредитования на

принципах возвратности и точности, а также для осуществления расчётов по поручению клиентов

Банковская система РТ состоит из эмиссионного (NBT) и иных (государственные и негосударственные, банк с участием иностранного капитала и межгосударственные) банков. Деятельность банков воплощается в виде следующих банковских операций:

1. Кредитных
2. Расчётных
3. Кассовых
4. Комиссионных
5. Курсовых

Законодательство позволяет банкам самостоятельно устанавливать процентные ставки и размер комиссионных вознаграждений. Банки гарантируют конфиденциальность по операциям, счетам и вкладам своих клиентов.

**2. Классификация банков**

На практике функционирует многообразие банков. В зависимости от того или иного критерия их можно классифицировать следующим образом:

1. По форме собственности выделяют:

* Государственные
* Акционерные
* Смешанные

2. По правовой форме организации:

* Общества открытого типа (ОАО)
* Общество закрытого типа (ЗАО)

3. По функциональному назначению:

* ***Эмиссионные*** – являются все центральные/национальные банки. Их классической операцией выступает выпуск наличных денег в обращение, они не заняты обслуживанием индивидуальных клиентов.
* ***Депозитные*** – специализируются на аккумуляции сбережения населения, депозитная операция служит для данных банков основной операцией.
* ***Коммерческие*** – являются универсальными кредитными учреждениями, концентрирующими значительную часть финансируемых ресурсов в осуществлении широкого круга банковских операций и услуг. Коммерческие банки заняты всеми операциями, дозволенными банковским законодательством.

4. По числу филиалов:

* Без филиальные
* Многофилиальные

5. По сфере обслуживания:

* Региональные
* Национальные
* Международные

**3. Понятие процесса. Классификация процессов банка.**

Слово процесс означает ввод в какое-либо явление, последовательную смену состояния. Совокупность последовательных действий для достижения результата. В первом случае речь идет о изменении состояния одного или нескольких объектов. В качестве объектов может выступать документы, информация и т.п. Во втором случае речь идет о действиях одного или нескольких субъектов, направленных на достижение результатов.

Субъектами обычно являются люди, подразделения и иногда вычислительные машины.

В качестве примера рассмотрим процесс обработки платежного поручения, модель которого включает двух субъектов (операционист и менеджер операциониста) и один объект платежное поручение. Субъекты последовательно совершают действие над объектом – получение, проверка, авторизация и исполнение. А объект последовательно проходит следующие состояния – следующие состояния получено, проверено, авторизовано, исполнено.

**4. Цель внедрения АБС.**

Цель применения современных AБC это обеспечение роста прибыли банка, а также беспрепятственное развитие расширения бизнеса в будущем. Основой данного подхода является анализ и оптимизация бизнес-процессов банка, которые должны быть выявлены, отлажены, приведены в соответствие с эффективной стратегией развития банка и взаимоотношений с клиентами. Следующий шаг — это автоматизация, требующая:

1. Выбора информационных технологий адекватных к стратегиям банка;
2. Экономически эффективной последовательности внедрений, ориентированной на быстрый и поэтапный возврат инвестиций;
3. Привлечение высококвалифицированных специалистов по внедрению и сопровождению;
4. Обучение персонала банка.

Потенциальные возможности увеличения прибыли средствами повышения экономической эффективности с помощью АБС являются:

1. Активное их использование в бизнес-процессах, способствующих быстрому увеличению прибыли банка.
2. Снижение себестоимости услуг засечёт оптимизации бизнес-процессов банка и внедрение стратегии управления отношениями с клиентами.
3. Увеличение объёмов бизнеса засечёт значительного ускорения обслуживания каждого клиента.
4. Сокращение расходов засечёт значительно снижения общего числа рутинных операций, выполняемых сотрудниками банка.
5. Оптимизация управления финансовыми и информационными потоками банка.

**5. Функции АБС.**

Функции АБС:

1. Операционный день.

2. Операции на фондовом рынке, работа банка с ценными бумагами.

3. Внутрихозяйственная деятельность.

4. Дистанционные банковские услуги.

5. Платежная система.

6. Карточные продукты.

7. Модуль отчетности.

8. Управления счетами клиентов

9. Программы дооснасти клиентов, маркетинговая и QR услуга.

Прикладные программы АБС представляют собой набор программах модулей, функционально и информационно связанных между собой, обмен информацией между модулями идёт через БД

**6. Операционный день банка.**

Операционным днём называется период, в течении которого происходит переход банка из одного фиксированного финансового состояния в другое. Фиксированным состоянием банка является финансовое состояние, соответствующее балансу. Начала операционного дня характеризуется балансом на начало дня и датой операционного дня, при стандартном начале работы, дата операционного дня совпадает с текущей датой. Пока операционный день не определён заблокированы все операции с документами на эту дату

**7. Завершение операционного дня.**

Заверение операционного дня необходимо выполнить следующую операцию:

1. Провести соответствующие документы(оплатить), если по технологии они должны проводится
2. Выдать все необходимые отчёты (ежедневные, ежемесячные, годовые, декадные)
3. По окончанию операционного дня, фиксируется состояние БД и создаётся копия (backup)

**8. Внедрение АБС.**

Внедрение АБС предполагает:

1. Обследование, его цель понять, что банк хочет получить в итоге и каким образом это будет достигнуто, в результате обследования получаем техническое задание на внедрение
2. Настройку АБС с учётом специфика банка и параллельно адаптировать ряд технологий банка под АБС
3. Конвертацию данных из старой системы
4. Обучение IT персонала банка
5. Адаптацию имеющиеся в новой АБС очётности под требования банка и регулятора
6. Создание и настройка шлюзов с другими информационными системами

Целями этапа обследования являются:

1. Изучение документооборота банка используемых технологий бизнес-процессов в банке
2. Оценка необходимости доработки функциональности и отчётности по сравнению с тиражными(коробочными) возможностями АБС
3. Оценка необходимости конвертирования данных из используемого в банке ПО и возможность проведения этой конвертации
4. Анализ технологий взаимодействия АБС с другими информационными системам (с процессинговым центром, аналитическими приложениями) проверка соответствия установленного в банке опарного программного обеспечения к требованиям новой АБС

***Конвертация данных***

Конвертация данных завершает этап предварительной подготовки и является началом этапа реальной работы пользователей в АБС. Задача этапа конвертации является правильный перенос необходимых данных из ранее использовавшихся системы в новый АБС. Как правило конвертация включает перенос финансовых данных по проводкам и остаткам на счетах.

***Обучение сотрудников банка***

Для начала этапа обучения должен быть проделан ряд работе:

1. Определён состав служителей из соответствующих подразделений
2. Согласован график проведения занятий
3. Обеспечения условия для проведения обучения персонала, то есть подготовлен учебный класс с необходимым оборудованием или определён порядок обучения на рабочих местах
4. Обеспечена посеещяемость специалистов соответсвующих подразделений

***Опытная эксплуатация системы***

Задача этапа конвертации из ранней использовавшийся системы в новый

1. Окончательная откладка всех модулей и выходных форм
2. Оперативное решение возникающих вопросов
3. Окончательное обучение сотрудников банка методам и особенностям работы в новой АБС

Технология проведения опытной эксплуатации построено таким образом, что всегда сохраняется возможность отката на старую систему, для этого основная работа осуществляется в двух системах параллельно. При невозможности организации такой работы в связи с большой нагрузки на персонал используется технология тестового дня, когда сотрудники в выходной день дублируют свои действия в новый АБС с выводкой полученных результатов. При успешном завершении тестового дня принимается решение о работе банка в режиме опытной эксплуатации, а старая система останавливается, актуальность данных в ней не поддерживается. Результатом последнего дня является промышленная эксплуатация в банке новой АБС

***Сопровождение***

Не менее существенным чем внедрении является обеспечение бесперебойной работы АБС, для этого необходимо громадно администрировать АБС со стороны департамента IT банка, а также предоставление услуг технической поддержки со стороны разработчика АБС

**9. Стоимость АБС.**

Структура расходов для сложной информационной системы, включающей серверы рабочие станции программные обеспечения и линии связи весьма сложная, при этом из всей совокупности расходов можно выделить затраты явные (прямые) и неявные (косвенные).

Затраты явные:

* Лицензия
* Опаратное обеспечение
* Внедрение
* Сопровождение
* Обновление опаратного и прогрпммного обеспечения
* Обучение персонала
* Абонентская плата за интернет и содержание серверов

Затраты неявные:

* Зарплата сотрудников (участников внедрение АБС, дополнительные выплаты сотрудникам за сверхурочную работу), Финансовые потери за счёт временного снижения качества обслуживания клиентов

Суммы явных затрат можно легко определить, в то время посчитать неявные затраты бывает не просто.

**10. Основные требования к АБС.**

Несмотря на различные подходы к разработке, АБС должны удовлетворят ряду требований, наиболее важным следует отнести следующее:

* Достаточная функционнальная полнота
* Открытость системы (при необходимости внести изменения доработки)
* Информационная интеграция (может взаимодействовать с другими серверами)
* Достоверность информации (нужно заранее знать, что понадобиться чтобы нее покупать лишнее)
* Надёжность системы (способность долго работать)
* Безопасность системы

**11. Безопасность банка.**

 **Информационная безопасность:**

* **Защита данных клиентов:** Банки обязаны обеспечивать конфиденциальность и целостность персональной информации клиентов, такой как данные о счетах, платежные реквизиты, идентификационные данные и т.д.
* **Защита от киберугроз:** С увеличением цифровизации банковских услуг возрастает угроза кибератак. Банки должны иметь эффективные меры защиты от вирусов, вредоносного ПО, фишинга и других киберугроз.
* **Мониторинг и аудит безопасности:** Регулярное сканирование на уязвимости, мониторинг активности сети, анализ аудита безопасности помогают выявлять и предотвращать потенциальные угрозы.

 **Физическая безопасность:**

* **Охрана и защита помещений:** Защита от несанкционированного доступа в физические объекты банка, такие как офисы, серверные помещения и склады ценностей.
* **Контроль доступа:** Использование систем контроля доступа, включая электронные карты доступа, биометрическую идентификацию и другие технологии для ограничения доступа к чувствительным зонам.

**12. Межбанковские электронные расчеты.**

В РТ используются следующие системы электронных расчётов:

* Система внутри банковских межфилиальных расчётов
* Система НБТ (национальный банк)
* Система международных расчётов
* Система расчётов по пластиковым картам

**13. SWIFT.**

Инициатива создания международного проекта, который вставил бы своей целью обеспечение его участников возможностью высокоскоростного обмена банковской информацией при высокой степени контроля и защиты от несанкционированного доступа относится к 1968 году. В 1972 году эта инициатива была оформлена в проект, получивший название MSP (Message Swifting Protocol). В том же году фирма Logis были подготовлены отчёты и рекомендации по созданию рентабельной системы обмена банковской информацией, удовлетворяющей следующим требованиям

1. Система должна основываться:

* На создании международной сети и сетевой службы сервиса
* На стандартизации процессов, а также стандартизации сообщений
* На стандартизации способов и оборудований подключение банков к сети

1. Система должна содержать распределённые центры обработки данных и концентраторы к связи в каждой из стран участниц системы

Основываясь на этих рекомендациях 239 банков из 15 стран Европы и Северной Америки в 1973 году в соответствии с бельгийским законодательством создании компанию SWIFT (Society for Worldwide Interbank Financial Tecommunication). Целью компании стала создание, использование, поддержка и эксплуатация единой системы и средств необходимой для быстрой и безопасной передачи банковских и сообщений любого вида по сетям телекоммуникации.

**14. Системы ДБО.**

Системы ДБО (дистанционного банковского обслуживания) представляют собой комплекс программно-аппаратных средств, предназначенных для организации удаленного доступа клиентов к банковским услугам. Они играют ключевую роль в современной банковской деятельности, обеспечивая удобство, доступность и безопасность для пользователей. Вот основные аспекты и функции систем ДБО:

**Основные функции систем ДБО:**

* + **Интернет-банкинг:** позволяет клиентам управлять своими счетами и средствами через интернет. Включает функции просмотра баланса, истории транзакций, переводов между счетами, платежей и т.д.
  + **Мобильный банкинг:** приложения для смартфонов и планшетов, предоставляющие аналогичные функции интернет-банкинга, но с возможностью управления счетами и проведения операций в любое время и в любом месте.
  + **SMS-информирование:** системы, отправляющие клиентам SMS-уведомления о движении средств по их счетам, подтверждениях операций и других важных событиях.
  + **Платежные шлюзы:** интеграция с платежными системами для проведения онлайн-платежей, включая оплату услуг, покупку товаров и т.д.
  + **Дистанционное обслуживание клиентов:** возможность получения консультаций и поддержки клиентами банка через системы обратной связи (чаты, электронная почта, колл-центры).

**Преимущества систем ДБО:**

* + **Удобство и доступность:** клиенты могут управлять своими финансами в удобное для них время, не посещая банковское отделение.
  + **Экономия времени:** возможность быстро проводить операции без необходимости стоять в очередях в банке.
  + **Безопасность:** системы ДБО защищены многоуровневыми мерами безопасности, такими как двухфакторная аутентификация, шифрование данных, мониторинг подозрительной активности и т.д.
  + **Расширенный функционал:** помимо базовых функций, многие системы ДБО предоставляют возможности для инвестирования, взаимодействия с финансовыми рынками, управления портфелем и т.д.

**Требования к системам ДБО:**

* + **Надежность и доступность:** системы ДБО должны быть надежными и доступными 24/7, чтобы клиенты могли использовать их в любое время.
  + **Скорость и производительность:** быстрая обработка транзакций и операций с минимальными задержками.
  + **Соответствие законодательству и стандартам безопасности:** соблюдение требований законодательства в области финансов и защиты данных (например, GDPR в Европейском Союзе, PCI DSS для защиты данных платежных карт).

**15. Банковские платежные карты и виды банковских карт.**

**Дебетовые карты:**

* **Особенности:** средства для проведения операций с дебетовой карты снимаются непосредственно с текущего счета клиента. Карты обычно связаны с текущим или расчетным счетом.
* **Функции:** позволяют совершать покупки в магазинах, онлайн-магазинах, а также снимать наличные деньги через банкоматы.
* **Преимущества:** нет необходимости возвращать ссуды, отсутствие процентов и долговых платежей.

**Кредитные карты:**

* **Особенности:** кредитные карты предоставляют временное финансирование, которое позволяет пользователям пользоваться кредитными лимитами, предоставленными банком.
* **Функции:** предоставляют возможность совершать покупки, а также снимать наличные средства, если таковая функция предусмотрена.
* **Преимущества:** удобство и безопасность, нагрузка на бюджет.

**16. Платежные системы на основе банковских карт.**

VISA / MasterCard

**17. Виды мошенничества для кредитной организации (эмитента).**

 **Кража и утеря карты:**

* **Описание:** когда карта физически украдена или потеряна, мошенники могут использовать её для совершения незаконных транзакций.
* **Действия:** это может включать снятие наличных денег с банкоматов, покупки в магазинах или онлайн-транзакции.
* **Защитные меры:** быстрая блокировка карты после сообщения о потере или краже, мониторинг транзакций для выявления подозрительной активности.

 **Клонирование карт:**

* **Описание:** мошенники могут скопировать данные с магнитной полосы или чипа карты и использовать эти данные для изготовления клона.
* **Действия:** клоны карт могут быть использованы для совершения транзакций без ведома владельца карты.
* **Защитные меры:** внедрение технологий защиты, таких как чиповые карты с шифрованием данных, мониторинг сетевых активностей для выявления несанкционированного доступа.

 **Фишинг и мошенничество через интернет:**

* **Описание:** мошенники отправляют фальшивые электронные письма или создают веб-сайты, представляющиеся банковскими или платёжными системами, чтобы получить личную информацию клиентов.
* **Действия:** после получения личной информации, мошенники могут использовать её для несанкционированных транзакций.
* **Защитные меры:** обучение клиентов о методах фишинга, использование двухфакторной аутентификации для повышения безопасности онлайн-транзакций.

 **Неуполномоченные транзакции:**

* **Описание:** мошенники могут получить доступ к банковской информации или данным карты и совершать транзакции без ведома владельца.
* **Действия:** это может включать как физические транзакции (например, использование украденной карты в магазине), так и онлайн-транзакции.
* **Защитные меры:** мониторинг транзакций для выявления необычной активности, использование систем обнаружения мошенничества (Fraud Detection Systems, FDS).

 **Мошенничество с возвратами (chargeback fraud):**

* **Описание:** мошенники могут использовать карточку для совершения покупок и затем оспаривать эти транзакции, утверждая, что товары не были получены или были возвращены.
* **Действия:** это может привести к потере дохода для торговцев и убыткам для эмитента карты.
* **Защитные меры:** внедрение процедур проверки возвратов, анализ паттернов транзакций для выявления потенциальных мошеннических действий.

 **Мошенничество с переводами и международными платежами:**

* **Описание:** мошенники могут использовать данные карты для осуществления международных платежей или переводов средств, обманывая как клиентов, так и банки.
* **Действия:** это может привести к финансовым потерям и ухудшению репутации банка.
* **Защитные меры:** мониторинг международных транзакций, использование систем подозрительной активности и двухфакторной аутентификации для подтверждения легитимности транзакций.

**18. Виды мошенничества для кредитной организации (эквайера).**

 **Мошенничество с кредитными картами:**

* **Описание:** мошенники могут использовать украденные или скопированные данные кредитных карт для совершения незаконных транзакций.
* **Действия:** это может включать как физические транзакции в магазинах и ресторанах, так и онлайн-транзакции.
* **Защитные меры:** мониторинг транзакций для выявления подозрительной активности, использование систем обнаружения мошенничества (Fraud Detection Systems, FDS).

 **Фишинг и мошенничество через интернет:**

* **Описание:** мошенники могут использовать фальшивые электронные письма, веб-сайты или социальные сети, чтобы обмануть пользователей и получить их личные данные.
* **Действия:** полученные данные могут быть использованы для совершения незаконных платежей или взлома учетных записей.
* **Защитные меры:** обучение клиентов и торговцев о методах фишинга, мониторинг веб-трафика и использование технологий защиты.

 **Компрометация торговых точек (POS-терминалов):**

* **Описание:** мошенники могут взламывать или изменять POS-терминалы для сбора данных о кредитных картах клиентов.
* **Действия:** это может привести к потере конфиденциальной информации и использованию её для мошеннических транзакций.
* **Защитные меры:** регулярная проверка и обновление программного обеспечения POS-терминалов, использование защищенных сетевых соединений.

 **Мошенничество с возвратами (chargeback fraud):**

* **Описание:** мошенники могут использовать карты для совершения покупок, а затем оспаривать эти транзакции, утверждая, что товары не были получены или были возвращены.
* **Действия:** это может привести к финансовым потерям для эквайера и его клиентов.
* **Защитные меры:** внедрение процедур проверки возвратов, анализ паттернов транзакций для выявления потенциальных мошеннических действий.

 **Мошенничество с мобильными платежами и NFC:**

* **Описание:** мошенники могут использовать компрометированные мобильные устройства или NFC-технологии для совершения несанкционированных платежей.
* **Действия:** это может включать кражу данных или взлом технологических средств для проведения платежей.
* **Защитные меры:** внедрение современных методов аутентификации, использование защищенных элементов транзакций.

 **Мошенничество с международными платежами и переводами:**

* **Описание:** мошенники могут использовать данные карты для осуществления международных платежей или переводов средств, обманывая как клиентов, так и эквайера.
* **Действия:** это может привести к финансовым потерям и ухудшению репутации компании.
* **Защитные меры:** мониторинг международных транзакций, использование систем обнаружения мошенничества и двухфакторной аутентификации для подтверждения легитимности транзакций.

**19. Аудит ИС банка.**

Аудит информационных систем (ИС) банка — это процесс оценки и проверки информационных технологий и систем, используемых в банковском учреждении. Целью аудита ИС является обеспечение надежности, безопасности, доступности и эффективности информационных ресурсов банка. Вот основные аспекты и этапы аудита ИС банка:

**Этапы аудита ИС банка:**

1. **Подготовка и планирование:**
   * Определение целей аудита и ожидаемых результатов.
   * Сбор информации о текущих информационных системах, процессах и угрозах безопасности.
   * Разработка плана аудита, включая методики и инструменты оценки.
2. **Оценка рисков:**
   * Анализ угроз безопасности и уязвимостей информационных систем.
   * Оценка потенциальных последствий инцидентов безопасности для бизнес-процессов банка.
   * Определение приоритетов и объема проверок в рамках аудита.
3. **Проверка соответствия нормативным требованиям:**
   * Проверка соответствия информационных систем банка законодательным и регуляторным требованиям, таким как нормативные акты Центробанка, GDPR, PCI DSS и другим стандартам.
4. **Оценка систем управления ИБ:**
   * Проверка наличия и эффективности систем управления информационной безопасностью (ИБ) в банке.
   * Анализ политик, процедур, стандартов и мероприятий по обеспечению ИБ.
5. **Тестирование технических мер безопасности:**
   * Проверка уровня защиты информационных систем, включая сетевые устройства, серверы, базы данных и приложения.
   * Проведение сканирования уязвимостей, тестирования на проникновение (penetration testing) и анализа конфигураций.
6. **Оценка управления доступом и аутентификации:**
   * Проверка систем управления доступом (Access Control) и методов аутентификации пользователей.
   * Анализ уровня привилегий, мониторинга доступа и аудита событий.
7. **Проверка бизнес-процессов:**
   * Оценка безопасности ключевых банковских процессов, таких как обработка платежей, выдача кредитов, управление клиентскими данными и других операций.
8. **Составление отчета и рекомендации:**
   * Формирование отчета об аудите ИС с описанием выявленных уязвимостей, недостатков и рекомендаций по их устранению.
   * Предоставление руководству банка рекомендаций по повышению безопасности и эффективности информационных систем.

**Основные аспекты проверки в рамках аудита ИС банка:**

* **Физическая безопасность:** Оценка защищенности дата-центров, серверных помещений и доступа к ним.
* **Логическая безопасность:** Проверка наличия и правильности настроенных брандмауэров, систем детекции вторжений, защиты от вредоносного программного обеспечения и других средств защиты.
* **Управление и мониторинг:** Анализ системы мониторинга и управления безопасностью, включая реагирование на инциденты и анализ журналов событий.
* **Тестирование бизнес-процессов:** Проверка соответствия процессов банка внутренним стандартам и нормативам.

**20. CRM-системы.**

CRM-системы (Customer Relationship Management) представляют собой программные решения, направленные на управление взаимоотношениями с клиентами. Они помогают организациям эффективно взаимодействовать с клиентами, улучшать обслуживание, увеличивать лояльность клиентов и оптимизировать бизнес-процессы. Вот основные аспекты и функции CRM-систем:

**Основные функции CRM-систем:**

1. **Управление контактами и клиентской базой данных:**
   * Хранение и управление информацией о клиентах, включая контактные данные, историю взаимодействий, предпочтения и другие важные сведения.
2. **Управление продажами:**
   * Отслеживание воронки продаж, управление продажами, прогнозирование и анализ результатов продаж, автоматизация процессов продаж.
3. **Маркетинг и автоматизация маркетинговых кампаний:**
   * Сегментация клиентской базы, создание и запуск маркетинговых кампаний, отслеживание результатов кампаний, автоматизация рассылок и коммуникаций.
4. **Обслуживание клиентов и поддержка:**
   * Управление заявками клиентов (трекинг), система тикетов (tickets), автоматизация процессов поддержки, отслеживание уровня обслуживания клиентов (SLA).
5. **Аналитика и отчетность:**
   * Анализ данных о клиентах и продажах, создание отчетов и дашбордов, визуализация ключевых метрик и показателей эффективности.
6. **Интеграция с другими системами:**
   * Взаимодействие с другими информационными системами компании (ERP, бухгалтерские системы, системы электронной почты и т.д.) для обмена данными и автоматизации процессов.

**Виды CRM-систем:**

* **Он-премисные CRM:** Устанавливаются и настраиваются на серверах компании. Требуют значительных затрат на внедрение и поддержку, но обеспечивают полный контроль над данными и настройками.
* **Облачные (Cloud) CRM:** Развертываются в облаке и предоставляются как сервис (SaaS). Обычно имеют меньшие входные затраты, более легкие внедрение и масштабирование, требуют только доступа к интернету для использования.
* **Гибридные CRM:** Сочетают в себе черты обеих моделей, позволяя хранить часть данных в облаке, а часть — на внутренних серверах компании.

**Преимущества использования CRM-систем:**

* **Улучшение обслуживания клиентов:** Повышение качества обслуживания, персонализация подхода к клиентам.
* **Увеличение продаж и доходов:** Оптимизация воронки продаж, повышение конверсии и среднего чека.
* **Улучшение оперативности и эффективности:** Автоматизация повседневных процессов, улучшение координации работы отделов.
* **Аналитика и принятие решений:** Получение ценной аналитической информации для принятия стратегических решений.
* **Масштабируемость и гибкость:** Возможность адаптации системы под изменяющиеся потребности и условия рынка.

**21. Организация ИТ проектов в банке.**

Организация ИТ проектов в банке представляет собой сложный процесс, требующий четкой структуры управления, строгого контроля и специфических подходов к управлению рисками и безопасностью. Вот основные аспекты организации ИТ проектов в банковской среде:

**Этапы организации ИТ проектов в банке:**

1. **Инициация проекта:**
   * **Определение бизнес-целей и требований:** Четкое определение того, какие бизнес-цели должен достигнуть проект, и какие требования предъявляются к информационным технологиям.
   * **Формирование команды:** Назначение ответственных за проект ролей, включая спонсора проекта, менеджера проекта, членов команды и других ключевых участников.
2. **Планирование проекта:**
   * **Разработка плана проекта:** Включает определение целей, распределение ресурсов, определение задач и сроков выполнения, создание бюджета проекта.
   * **Оценка рисков:** Анализ возможных рисков и разработка стратегий их управления, особенно важно для банковских проектов, связанных с обработкой данных и безопасностью.
3. **Исполнение проекта:**
   * **Управление выполнением задач:** Распределение задач между участниками команды, мониторинг прогресса выполнения.
   * **Контроль изменений:** Управление изменениями в проекте, адаптация к изменяющимся условиям и требованиям.
4. **Мониторинг и контроль:**
   * **Отчетность и анализ:** Систематическое отслеживание и отчетность о прогрессе проекта, анализ сроков, бюджета и качества выполнения задач.
   * **Управление качеством:** Обеспечение соответствия результатов проекта заданным критериям качества и стандартам.
5. **Завершение проекта:**
   * **Оценка результатов:** Оценка достигнутых результатов по сравнению с начальными целями и требованиями.
   * **Документация и передача:** Составление документации о проекте, передача результатов и знаний заказчику или эксплуатационной команде.

**Особенности организации ИТ проектов в банке:**

* **Безопасность и конфиденциальность данных:** Особое внимание уделяется защите данных и информационной безопасности в процессе реализации ИТ проектов.
* **Соблюдение регуляторных требований:** Банки обязаны соблюдать строгие регуляторные стандарты и требования, что влияет на каждый этап проекта.
* **Интеграция с существующими системами:** Часто проекты в банках требуют интеграции с множеством существующих информационных систем и платформ.
* **Управление рисками:** Оценка и управление рисками, связанными с технологическими изменениями, является неотъемлемой частью процесса.
* **Согласование с бизнес-процессами:** Успешная реализация проектов требует глубокого понимания бизнес-процессов и потребностей банка.