МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

А.М. Кипкеева

ЭЛЕКТРОННЫЕ И ПЛАТЕЖНЫЕ УСЛУГИ БАНКОВ

Учебно-методическое пособие для обучающихся очной и заочной форм обучения по направлению подготовки 09.04.03 Прикладная информатика направленность профиль «Прикладная информатика в экономике и управлении»

Черкесск, 2025

УДК 336.7
ББК 6.262.5
К 42

Рассмотрено на заседании кафедры Прикладной информатики
Протокол № 3 от 16. 10. 2024 г.
Рекомендовано к изданию редакционно-издательским советом СКГА.
Протокол № 27 от 07.11.2024 г.

Рецензенты: Алиев О.И. – к.э.н., доцент кафедры Прикладной информатики

К 42 **Кипкеева, А.М.**: Электронные и платежные услуги банков: учебно-методические указания для обучающихся очной и заочной форм обучения по направлению подготовки 09.04.03 Прикладная информатика направленность (профиль) «Прикладная информатика в экономике и управлении» / А.А. Кипкеева. – Черкесск: БИЦ СКГА, 2025. – 32 с.

Учебно-методические пособие подготовлено в соответствии с ФГОС ВО и рабочей программой по изучению дисциплины «Электронные и платежные услуги банков». Учебно-методические пособие рекомендовано для обучающихся очной и заочной формы обучения по направлению подготовки 09.04.03 Прикладная информатика «Прикладная информатика в экономике и управлении»

УДК 336.7
ББК 65.262.5

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
Тема 1. Банковские и платежные системы	5
Тема 2. Нормативно-правовое обеспечение банковских и финансовых операций. Банковские платежные услуги	8
Тема 3. Финансовые инфраструктуры и инструменты	9
Тема 4. Межбанковские отношения	11
Тема 5. Взаимоотношения банка и его клиентов. Банковские и платежные агенты	12
Тема 6. Дистанционное банковское обслуживание	13
Тема 7. Безопасность электронных платежных систем	14
Вопросы к зачету	21
Тестовые задания	23
Темы рефератов	27
Лабораторная работа 1	29
Лабораторная работа 2	30

ВВЕДЕНИЕ

В современном мире цифровые технологии активно трансформируют банковскую сферу, делая электронные и платежные услуги неотъемлемой частью повседневной жизни. Рост популярности интернет-банкинга, мобильных приложений, электронных денег и криптовалют, а также развитие платежных систем свидетельствуют о значимости данной темы. Банки все чаще внедряют инновационные решения, такие как блокчейн, искусственный интеллект и биометрические технологии, чтобы повысить удобство и безопасность обслуживания клиентов.

Актуальность дисциплины «Электронные и платежные услуги банков» обусловлена следующими факторами:

1. Переход к цифровым технологиям требует от специалистов банковской сферы глубоких знаний в области электронных услуг;
2. Клиенты ожидают от банков удобства, скорости и безопасности при проведении операций;
3. Банки вынуждены внедрять новые технологии, чтобы оставаться конкурентоспособными;
4. Развитие международных платежных систем требует понимания их особенностей и механизмов работы.

Изучение данной дисциплины позволяет будущим специалистам адаптироваться к быстро меняющимся условиям банковской среды и эффективно использовать современные технологии в своей профессиональной деятельности.

Целью освоения дисциплины является изучение теоретических и практических аспектов предоставления и использования электронных банковских услуг.

Задачи курса:

1. Изучить основные понятия и виды электронных и платежных услуг банков.
2. Рассмотреть нормативно-правовую базу, регулирующую электронные платежи и банковские услуги.
3. Освоить технологии, обеспечивающие безопасность и эффективность электронных платежей.
4. Изучить современные тенденции и инновации в банковской сфере, такие как блокчейн, искусственный интеллект и биометрические технологии.
5. Развить навыки анализа рынка электронных платежных услуг и оценки их эффективности.
6. Рассмотреть риски и угрозы, связанные с электронными платежами, и методы их минимизации.

ТЕМА 1. БАНКОВСКИЕ И ПЛАТЕЖНЫЕ СИСТЕМЫ

Электронные банковские услуги (ЭБУ) – это комплекс услуг, предоставляемых банками с использованием информационных и телекоммуникационных технологий, которые позволяют клиентам осуществлять финансовые операции и получать доступ к банковским продуктам без необходимости посещения банковского отделения. Эти услуги стали неотъемлемой частью современного банкинга, обеспечивая клиентам удобство, скорость и безопасность.

Электронные банковские услуги включают в себя широкий спектр операций, которые выполняются через цифровые каналы, такие как:

1. Интернет-банкинг (online banking);
2. Мобильный банкинг (mobile banking);
3. Платежные терминалы и банкоматы;
4. Электронные кошельки и платежные системы;
5. Системы денежных переводов;
6. Услуги, предоставляемые через API и открытый банкинг.

Эти услуги позволяют клиентам управлять своими счетами, переводить деньги, оплачивать счета, получать кредиты, инвестировать и выполнять другие финансовые операции в режиме реального времени.

Электронные банковские услуги представляют собой важный элемент современной финансовой системы, который обеспечивает клиентам удобство, скорость и безопасность при выполнении финансовых операций. Их сущность заключается в использовании цифровых технологий для трансформации традиционных банковских процессов, что делает их более доступными и эффективными. В условиях цифровой экономики электронные банковские услуги становятся ключевым фактором конкурентоспособности банков и удовлетворения потребностей клиентов.

Электронная платежная система представляет собой систему расчетов между интернет-пользователями, финансовыми организациями и другими экономическими агентами при купле-продаже товаров и услуг посредством глобальной сети Интернет.

Электронные платежные системы (ЭПС) неразрывно связаны с таким понятием, как «электронные деньги». Электронные деньги собой представляют денежные обязательства организации-эмитента, находящиеся в управлении пользователей на электронных носителях.

Основными признаками и характеристиками электронных денег является следующее:

1. Их эмиссия *(выпуск денег в обращение, ведущей к увеличению денежной массы)* осуществляется в электронном виде;
2. Хранятся на электронных носителях;
3. Эмитент (*организация, выпускающая ценные бумаги с целью развития и финансирования своей деятельности*) гарантирует обеспечение электронных денежных средств «традиционными» деньгами;
4. Признание электронных денег в качестве платежного средства рядом пользователей и организаций.

Электронные деньги не следует путать с безналичной формой «традиционных» денег. Банковские карты также не имеют никакого отношения к электронным деньгам, поскольку представляют собой лишь средство управления счетом в банке. При использовании банковских карт операции осуществляются с «традиционными» деньгами (хоть и в безналичной форме).

Платежная система включает в себя процедуры осуществления платежей современный платежный инструментарий, операторов и участников расчетов. Основные параметры функционирования платежных систем, определяющие их качество и эффективность, – это надежность, безопасность и скорость осуществления платежей, а также их востребованность и экономичность использования.

Скорость расчетов также является фактором, определяющим безопасность и экономичность использования платежной системы. В настоящее время существуют как дорогие по стоимости одного платежа системы, позволяющие перевести средства за тысячи километров в течение нескольких минут, так и относительно недорогие системы, осуществляющие подобный

перевод в течение нескольких дней и в то же время не обладающие достаточно надежными и защищенными программными и техническими средствами.

Надежность и безопасность системы осуществления платежей является одним из самых важных ее параметров. Практически все платежные системы в мире, используют широкий спектр различных средств сохранения и защиты информации. Однако для обеспечения надежности и безопасность системы осуществления платежей весьма важным является обеспечение финансовой защиты и «окончательного расчета», что означает безусловное и безотзывное выполнение расчетов. Такой расчет может быть гарантированным только в системах, обладающих высоким уровнем доверия его участников и минимальным риском неплатежеспособности организаторов расчета.

Классификация их достаточно сложна: по месту регистрации, охвату стран и валют, типам контрагентов и так далее.

Электронные платежные системы (ЭПС) следует разделить на два типа: *кредитные и дебетовые.*

Кредитные платежные системы – это системы, построенные на использовании кредитных карт для электронных расчетов между участниками сделки. Все кредитные системы требуют подтверждения кредитоспособности клиента. *Дебетовые платежные системы* – это системы, основанные на использовании электронных эквивалентов чеков и наличных. Дебетовые системы, основанные на использовании цифровых наличных, не требуют подтверждения уполномоченной финансовой структурой. Стоимость применения дебетовой системы относительно невысока, поэтому она может использоваться для микроплатежей.

Преимущества и недостатки электронных платежных.

Преимущества: Быстродействие. Процедура регистрации занимает максимум минут 10-15. Некоторого времени требует проверка документов, но тут уже речь идет о безопасности пользователя. Зато после верификации аккаунта операции внутри системы совершаются практически мгновенно, невзирая на расстояния и границы. Средства переходят через тысячи километров моментально.

Простота. Практически все сервисы устроены максимально просто и продуманно. Разработчики кровно заинтересованы в увеличении числа пользователей, поэтому ориентируются на людей с минимальными пользовательскими навыками. Выгода. В большинстве случаев, совершать покупки в интернет-магазинах при помощи электронных денег гораздо выгоднее, нежели делать это в реальных торговых точках, расплачиваясь наличкой. В качестве дополнительного бонуса можно получить возможность контролировать собственные финансы вплоть до копейки - никаких дополнительных записей для этого вести не нужно. Обширный функционал. Чем популярнее платежная система, тем больше возможностей она предоставляет пользователю. Через многие сервисы можно проводить платежи по коммунальным и другим услугам, оплачивать штрафы и налоги, погашать кредиты и займы. Внутри ПС может быть встроен онлайн-обменник, предоставлена возможность онлайн-кредитования или автоматического отчисления фиксированных сумм на определенные аккаунты. Безопасность. Практически все авторитетные сервисы имеют многоступенчатые системы безопасности. Некоторые из них предусмотрены сервисами для всех пользователей по умолчанию, другие настраиваются вручную. Практически все трансакции *(операции с денежными средствами)* требуют дополнительного подтверждения в виде кодов, которые высылаются через СМС, по электронной почте либо при помощи инновационной платформы аутентификации E-num.

Недостатки. Обязательная авторизация. Чтобы получить доступ ко всем опциям ЭПС, нужно обязательно подтвердить собственную личность, то есть, представить на аттестацию соответствующие документы с личными данными. Анонимные ЭПС есть, но они иностранные (причем преимущественно маленьких государств *оффшорных зон*) и в России находятся вне закона.

Сложность восстановления. Если вы потеряете пароль доступа, восстановить его будет очень сложно. С одной стороны, это неприятно, но таковы требования безопасности, введенные ради спокойствия участников системы. Комиссии и другие расходы. Величина комиссии и других обязательных платежей зависит от политики конкретной ЭПС. Как правило, чем выше международный рейтинг системы, тем терпимее комиссия.

ТЕМА 2. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БАНКОВСКИХ И ФИНАНСОВЫХ ОПЕРАЦИЙ. БАНКОВСКИЕ ПЛАТЕЖНЫЕ УСЛУГИ

Нормативно-правовая база, регулирующая банковские и финансовые операции, является основой для обеспечения стабильности, безопасности и прозрачности финансовой системы. Она включает международные стандарты, национальное законодательство и внутренние регламенты финансовых институтов. Рассмотрим основные аспекты нормативно-правового обеспечения.

1. Международные стандарты и регуляции. Базельские соглашения (Базель I, II, III) – устанавливают требования к капиталу банков, управлению рисками и ликвидностью.

Директивы Европейского Союза:

– PSD (Payment Services Directive) - регулирует платежные услуги в ЕС.

– PSD2 (Revised Payment Services Directive) – расширяет права клиентов и стимулирует развитие открытого банкинга.

– FATF (Financial Action Task Force): разрабатывает рекомендации по противодействию отмыванию денег и финансированию терроризма (AML/CFT).

– ISO 20022: стандарт для унификации форматов данных в финансовых операциях.

2. Национальное законодательство

– В каждой стране существует своя нормативно-правовая база, регулирующая банковские и финансовые операции. Например, в России:

– Федеральный закон «О банках и банковской деятельности»;

– Федеральный закон «О национальной платежной системе»;

– Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

– Положения и инструкции Центрального банка РФ (например, Положение № 683-П о порядке осуществления переводов денежных средств).

Нормативно-правовое обеспечение банковских и финансовых операций играет ключевую роль в создании стабильной и безопасной финансовой системы. Банковские платежные услуги, регулируемые на международном и национальном уровнях, обеспечивают удобство, скорость и безопасность для клиентов, а также способствуют развитию цифровой экономики. Внедрение современных технологий и соблюдение регуляторных требований позволяют банкам оставаться конкурентоспособными и удовлетворять потребности клиентов в условиях быстро меняющегося финансового ландшафта.

ТЕМА 3. ФИНАНСОВЫЕ ИНФРАСТРУКТУРЫ И ИНСТРУМЕНТЫ

Финансовые инфраструктуры и инструменты являются основой функционирования современной экономики. Они обеспечивают проведение финансовых операций, управление рисками, а также способствуют эффективному распределению ресурсов. Рассмотрим их основные компоненты и роль в финансовой системе.

Финансовые инфраструктуры – это совокупность институтов, систем и механизмов, которые обеспечивают проведение финансовых операций, расчетов и управление рисками. Ключевые элементы финансовой инфраструктуры включают:

Национальные платежные системы обеспечивают проведение внутренних платежей (например, НПС в России, SEPA в ЕС). Международные платежные системы SWIFT, Visa, Mastercard (в настоящее время не действуют в России).

Финансовые инструменты – это контракты, которые дают право на получение денежных потоков или активов. Они используются для привлечения капитала, управления рисками и инвестирования.

Денежные инструменты – наличные деньги: банкноты и монеты.

Безналичные средства – средства на банковских счетах.

Кредитные инструменты – предоставление средств на условиях возвратности и платности.

Финансовые инфраструктуры и инструменты играют ключевую роль в функционировании современной экономики. Они обеспечивают проведение платежей, управление рисками и привлечение капитала, способствуя экономическому росту и развитию. В условиях цифровой трансформации и глобализации финансовые инфраструктуры и инструменты продолжают эволюционировать, предлагая новые возможности для бизнеса и частных лиц.

Разновидностью финансовых инструментов выступают фьючерсы. Эффективным инструментом снижения финансовых рисков и потерь является хеджирование, позволяющее исключить/минимизировать риски, связанные с колебаниями курсов валют на денежном рынке или процентных ставок. Не менее эффективны заключение форвардных и фьючерсных контрактов с целью снижения финансовых рисков.

В соответствии с Указанием Центрального Банка Российской Федерации от 16 февраля 2015 г. № 3565-У «О видах производственных инструментов», зарегистрированного в Минюсте России 27 марта 2015 г. № 35575 в пункте 3 отмечено «фьючерсным договором признается заключаемый на биржевых торгах договор, предусматривающий обязанность каждой из сторон договора периодически уплачивать денежные суммы в зависимости от изменения цен (значений) базисного актива и (или) наступления обстоятельства, являющегося базисным

активом»[1].

Фьючерсные контракты представляют собой соглашения между двумя сторонами о покупке или продаже актива (таких как товары, финансовые инструменты, валюты и другие) по определенной цене и в определенное время в будущем.

К другим видам финансовых инструментов следует отнести форвардные контракты и опционы. Слово «форвард» (forward) означает «вперед» и отражает основную особенность форвардных контрактов. Форвардные контракты – это соглашения между двумя сторонами, в которых условия сделки, включая цену и срок исполнения, фиксируются заранее, еще до заключения самой сделки. Смысл такого соглашения в том, что изначально обозначенные в нем условия не могут быть изменены ни одной стороной и гарантируются к выполнению на предусмотренную дату.

Управление валютным риском включает в себя различные стратегии и инструменты, такие как хеджирование (форвардные контракты, опционы), балансировка портфеля, диверсификация рисков и управление ликвидностью. Компании и инвесторы часто стремятся минимизировать валютные риски, чтобы защитить свои активы и обязательства от потенциальных неблагоприятных изменений валютных курсов.

Опционы также могут быть классифицированы по сроку исполнения. Европейский опцион может быть исполнен только в определенную дату, которая заранее оговорена, в то время как американский опцион может быть исполнен в любой день до истечения его срока действия.

Хеджирование опционами предоставляет инвесторам возможность защитить свои позиции от неблагоприятных изменений цены базового актива. Если инвестор хочет защитить свою длинную позицию от падения цены актива, он может приобрести опцион put или продать опцион call. В этом случае, если цена актива упадет, прибыль от опциона компенсирует потери по активу. С другой стороны, если инвестор хочет защитить свою короткую позицию от повышения цены актива, он может продать опцион put или приобрести опцион call. В этом случае, если цена актива возрастет, прибыль от опциона сгладит потери по короткой позиции. Одним из отличий варрантов от обычных опционов является их срок действия. Отличительной особенностью варрантов является то, что они могут быть бессрочными или наоборот иметь длительный срок чем обычные опционы. Это делает их более гибкими инструментами для инвесторов.

[1] Указание Центрального Банка Российской Федерации от 16 февраля 2015 г. № 3565-У «О видах производственных инструментов» – Режим доступа: URL: https://normativ.kontur.ru/document?moduleId=1&documentId=249991 (дата обращения 27.01.2025)

ТЕМА 4. МЕЖБАНКОВСКИЕ ОТНОШЕНИЯ

Межбанковские отношения представляют собой систему взаимодействия между банками, основанную на разнообразных соглашениях, операциях и расчетах. Они необходимы для обеспечения функционирования финансовой системы, ликвидности банковской системы и реализации денежно-кредитной политики. Основные формы межбанковских отношений:

Корреспондентские отношения – один банк (корреспондент) открывает счет в другом банке (банке-респонденте) для проведения расчетов и операций по поручению клиента. Позволяют проводить международные расчеты, операции в разных регионах страны, а также обслуживать клиентов, не имеющих счетов в данном банке.

Межбанковское кредитование – предоставление кредитов одними банками другим. Используется для управления ликвидностью (покрытие краткосрочных дефицитов), финансирования операций, а также для выполнения обязательных резервных требований. Рынок межбанковских кредитов (МБК) является важным индикатором финансового состояния банковской системы. Ставки МБК отражают уровень ликвидности и кредитного риска банков.

Совместное участие в синдицированном кредитовании – несколько банков объединяются для предоставления крупного кредита одному заемщику. Позволяет распределить риски и предоставить финансирование, превышающее возможности одного банка.

Операции на валютном рынке – взаимодействие банков при покупке и продаже валюты. Обеспечивает конвертацию валют для международных расчетов и операций.

Соглашения о сотрудничестве – взаимодействие в области обмена информацией, разработки новых продуктов и услуг, обучения персонала и т.д. Позволяет банкам расширять свою деятельность и повышать конкурентоспособность.

ТЕМА 5. ВЗАИМООТНОШЕНИЯ БАНКА И ЕГО КЛИЕНТОВ. БАНКОВСКИЕ И ПЛАТЕЖНЫЕ АГЕНТЫ

Взаимоотношения банка и его клиентов строятся на основе договорных обязательств, регулируемых законодательством и внутренними правилами банка. Эти отношения охватывают широкий спектр услуг, включая открытие и обслуживание счетов, кредитование, инвестиции, расчетно-кассовые операции и другие финансовые услуги. Рассмотрим основные аспекты этих взаимоотношений, а также роль банковских и платежных агентов. Договорная основа – отношения между банком и клиентом начинаются с заключения договора (например, договор банковского счета, кредитный договор, договор на обслуживание карты). В договоре прописываются права и обязанности сторон, тарифы, сроки, условия предоставления услуг и ответственность за нарушение обязательств. Конфиденциальность – банк обязан соблюдать конфиденциальность информации о клиенте (банковская тайна). Клиент, в свою очередь, предоставляет банку достоверные данные и документы. Обслуживание счетов - банк предоставляет услуги по открытию и ведению счетов, проведению платежей, переводов и других операций. Клиент имеет право распоряжаться средствами на счете в рамках действующего законодательства. Кредитование – банк предоставляет кредиты физическим и юридическим лицам на определенных условиях. Клиент обязан своевременно погашать кредит и выплачивать проценты. Инвестиционные услуги – банк может предлагать клиентам услуги по управлению капиталом, инвестированию в ценные бумаги, валютные операции и др. Клиент принимает на себя риски, связанные с инвестициями. Техническая поддержка и безопасность – банк обеспечивает безопасность операций клиента (например, защита от мошенничества, использование современных технологий шифрования). Клиент обязан соблюдать правила безопасности (например, не передавать третьим лицам данные карты или пароли). Претензионная работа – в случае возникновения споров или ошибок в проведении операций клиент имеет право обратиться в банк с претензией. Банк обязан рассмотреть претензию в установленные сроки и дать ответ.

Банковские агенты – это юридические или физические лица, которые действуют от имени банка и выполняют определенные функции, такие как: прием платежей (например, за коммунальные услуги, налоги, кредиты), выдача наличных средств, открытие счетов или оформление банковских продуктов, консультирование клиентов.

ТЕМА 6. ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

Дистанционное банковское обслуживание (ДБО) – это предоставление банковских услуг клиентам без необходимости их физического присутствия в отделении банка.

Основная цель ДБО – повышение удобства и доступности банковских услуг, сокращение времени на их получение.

ДБО включает в себя использование современных технологий, таких как интернет, мобильные приложения, SMS, телефонная связь и другие каналы коммуникации.

2. Основные формы ДБО

Интернет-банкинг – управление счетами через веб-сайт банка. Возможность совершать платежи, переводы, открывать вклады, получать выписки и т.д. Мобильный банкинг – управление финансами через мобильное приложение. Удобство для клиентов, которые часто используют смартфоны.

SMS-банкинг – получение уведомлений о состоянии счета, проведении операций через SMS. Простые команды для управления счетом (например, запрос баланса).

Телефонный банкинг – обслуживание через call-центр или автоматизированные системы. Возможность консультации с оператором или самостоятельного управления счетом.

Банкоматы и терминалы – проведение операций через устройства самообслуживания.

3. Преимущества ДБО

Для клиентов: удобство и экономия времени; круглосуточный доступ к услугам; возможность управления финансами из любой точки мира; снижение затрат на обслуживание (меньше комиссий).

Для банков: снижение нагрузки на отделения; уменьшение операционных издержек; расширение клиентской базы; повышение конкурентоспособности.

ТЕМА 7. БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Вопросы безопасности электронных платежных систем являются сложной задачей для финансового сектора и регуляторов. Существуют две серьезные проблемы – несанкционированные списания средств с банковских карт или счетов юридических лиц и общая гарантия сохранности платежей, совершаемых через небанковские системы переводы платежей. Принимаемые в последние годы меры смогли сделать электронные переводы более безопасными.

Под термином «электронная платежная система» (ЭПС) понимается система расчетов, при которой платежи проводятся по интернет-каналам, традиционной обработки платежных поручений не происходит.

Под это определение попадают:

– расчеты посредством банковских карт традиционных систем Visa, MasterCard, «Мир». Здесь при абсолютной гарантии защиты трансакций (*операции с денежными средствами*) возникает проблема несанкционированных списаний в результате перехвата трафика или получения номеров карт;

– программы межбанковских расчетов по электронным каналам связи, в том числе быстрых платежей, осуществляемых банками по номерам телефонов;

– расчеты через электронные кошельки (Яндекс деньги и другие);

– расчеты через инфраструктуру мобильных операторов и другие современные решения.

В Банке России организовано несколько моделей платежей по Интернету. Это программа внутрирегиональных расчетов по сети Интернет (ВЭР) и межрегиональных электронных расчетов (МЭР). Для крупных срочных платежей в России в 2007 году создана идеология банковских срочных платежей (БЭСП). Она является аналогом европейской программы RTGS. Подключенные к ней банки переводят друг другу крупные суммы с целью перечисления клиентам в течение одного операционного дня (*время в течении которого принимаются и проводятся операции по зачислению, списанию, переводу денежных средств клиентов и другие операции и сделки*).

Информационная безопасность электронных платежных систем обеспечивается требованиями, предъявляемыми к банкам-участникам:

– наличие корреспондентского счета в ЦБ РФ;

– действующая лицензия на осуществление банковской деятельности;

– отсутствие просроченных долгов перед ЦБ РФ;

– обмен сообщениями по установленному механизму коммуникации с Банком России на основе договора;

– соответствие ИС банка техническим требованиям и требованиям по ИБ кредитных организаций, предъявляемым ЦБ РФ.

Требования формулируются в Положениях Банка России и являются обязательными для исполнения. Отказ от выполнения требований может привести к полному или частичному отключению банка от технологии банковских срочных платежей.

Общие принципы информационной безопасности дистанционных переводов

Если говорить об защите от несанкционированных переводов ЭПС в общем, то вне зависимости от уровня каждой конкретной модели к ним действуют единообразные требования.

Среди наиболее уязвимых мест:

– интернет-трафик между участниками обмена электронными сообщениями о финансовых трансакциях (банками, операторами платежных кошельков, банкоматами, клиентами);

– обработка информации внутри банка или оператора (например, Яндекс денег), когда данные могут оказаться доступными сотрудникам;

– постоянная доступность систем платежей для клиентов, отсутствие сбоев в их работе и на линии связи.

Наличие этих уязвимостей вынуждает банки и операторов обеспечивать защиту трафика при пересылке доступными способами (передача по защищенным каналам, шифрование) и разрабатывать модели аутентификации[2] отправителя и получателя средств.

При этом в работе банка или оператора платежей возникают проблемы:

– определение взаимной подлинности участников трансакции при установлении соединения;

– обеспечение конфиденциальности и подлинности платежных поручений, отправляемых по интернету, и других документов;

– защита процесса отправки, формирование доказательств отправления и получения документов;

– обеспечение исполнения документа (например, постоянное нахождение остатка на корреспондентском счете банка, позволяющее организовать платеж).

Банк и оператор ЭПС обязаны реализовать механизмы защиты клиентов от несанкционированных списаний денежных средств, конкретные требования к которым определяются политиками операторов и регламентами ЦБ РФ:

– управление доступом клиента, сотрудников оператора и получателя, создание механизма аутентификации;

– контроль подлинности и целостности информации в сообщении;

– обеспечение конфиденциальности сведений в процессе передачи;

[2] средство защиты, устанавливающее подлинность лица, получающего доступ к автоматизированной системе, путем сопоставления сообщенного им идентификатора и предъявленного подтверждающего фактора.

– невозможность отказаться от авторства поручения на отправку средств или сообщения;

– гарантии доступа к ресурсам и неутраты сообщения в пути, его доставки;

– невозможность оператора или банка отказаться от исполнения поручения на перевод или платеж;

– сохранение данных по поручениям и сообщениям.

Для осуществления платежей посредством банковских карт международные системы переводов применяют собственные меры ИБ межкарточных переводов, корреспондирующие с требованиями Банка России. Для иных операторов безбумажных платежей, совершающих более 6 миллионов переводов в год, работает программа сертификации Qualified Security Assessor (QSA).

В России работают представительства нескольких организаций, имеющих право на выдачу сертификата, и он будет предоставлен, если оператор соответствует следующим требованиям:

– его деятельность соответствует международному стандарту Payment Card Industry Data Security Standard (PCI DSS);

– оператор сервиса платежей получил сертификат на соответствие международным требованиям к менеджменту ИБ кредитных организаций в сфере разработки, внедрения и сопровождения программных средств ISO/IEC 27001:2005;

– оператор работает с использованием электронно-цифровой подписи (ЭП);

– шифрование осуществляется разрешенными средствами криптографической защиты, разработанными организациями, имеющими лицензии на право осуществления деятельности по предоставлению, техническому обслуживанию криптографических средств.

Стандарт защиты информации в индустрии платежных карт PCI DSS (псай диэсэс) был разработан международными операторами платежных карт Visa и MasterCard. В него входит 12 детально описанных требований, согласно которым должна обеспечиваться защита платежных систем.

В последние годы ЦБ РФ от рекомендаций организациям финансового сектора по обеспечению защиты денежной системы перешел к требованиям, обязательным для выполнения и внесением изменений в законы и подзаконные нормативные акты. Теперь информацию о каждой зафиксированной хакерской атаке и о том, что она готовится, он должен получать в течение трех часов.

Сведения необходимо передавать в FinCERT (Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере, подразделение ЦБР). Передаются все данные, связанные с покушением на совершение несанкционированного перевода денежных средств со счетов компаний и физических лиц. Большинство банков и организаций финансового сектора уже подключены к системе горячего реагирования ФинЦЕРТ, если этого не

произошло, сведения направляются по e-mail, без гарантии его своевременного прочтения и регистрации. С этим связаны сложности: такое сообщение обязательно должно быть подписано ЭП, но, если киберпреступникам удалось разрушить важный сектор многоэшелонированной защиты банка, удостоверить сообщение ЭЦП окажется сложно.

В стандарте обеспечения информационной безопасности электронных платежных систем ЦБ РФ закрепил несколько обязательных требований:

– компьютер, подключенный к системе, не должен быть доступен из локальной сети банка (п. 5 Постановления ЦБ РФ №672-П);

– компьютер, отправляющий платежи на корреспондентский счет ЦБ РФ на обработку, должен постоянно мониториться с целью выявления несанкционированного вмешательства в ПО или подключения к сторонним серверам.

Интересно, что регулятор не требует от банка обязательного информирования о DDoS-атаках и других ситуациях, касающихся защиты системы обработки платежей самого финансового учреждения. Но все рекомендации, связанные с защитой от несанкционированных переводов и вмешательством в работу ЭПС любого уровня, как национального, так и международного, должны выполняться неукоснительно. Банки заявили после выхода рекомендаций о глобальном изменении правил игры, ранее они не сообщали о хакерских атаках по двум причинам:

– из страха репутационных рисков;

– из боязни быть оштрафованными за несоблюдение требований ИБ и правил корпоративного поведения.

Сейчас меры воздействия на банки за отказ от соблюдения требований регулятора более жесткие, чем просто штрафы. Одна из них отключение финансовой организации-нарушителя от системы банковских срочных платежей (БЭСП). Размер штрафа, согласно ст. 74 Закона «О Центральном Банке», может составить до 1 % от уставного капитала банка. Например, размер штрафа для такого финансового учреждения, как Сбербанк, может составить 670 миллионов рублей.

Положение 672-П

В рамках регулирования деятельности банков по обеспечению безопасности для клиентов электронных платежных систем Банком России в апреле 2019 года издано Положение № 672-П «О требованиях к защите информации в платежной системе Банка России». Основным посылом сообщения стала обязанность банков к середине 2021 года полностью выполнить требования ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций». Проверка выполнения действий этого и предыдущего Постановления № 552-П происходит во время проведения ежегодных аудиторских проверок и проверок ЦБР, а дополнительной гарантией соблюдения требований становится включение их в качестве обязательств кредитной организации в ее договор с Банком России.

Помимо требований к обеспечению информационной безопасности

электронных платежных систем, Стандарт содержит требования по обеспечению защиты данных, пересылаемых в рамках программы передачи финансовых сообщений (СПФС).

Требования ГОСТа касаются защиты двух механизмов отправления платежей:

– сервиса срочного перевода и сервиса несрочного перевода (ССНП);

– сервиса быстрых платежей (СБП).

Каждый участник системы переводов в целях обеспечения защиты электронных платежных систем обязан принять пакет внутренней ОРД, описывающий:

– процесс защиты данных при управлении доступом к ним;

– порядок обеспечения физической и программной защиты ИС любого уровня;

– контроль целостности и защищенности инфраструктуры, сети организации, осуществляющей переводы;

– использование антивирусных средств и способов защиты от внедрения вредоносного кода;

– защиту от утечек данных;

– управление инцидентами информационной безопасности;

– защиту среды виртуализации;

– защиту информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Нормы Постановления обязывают банки усилить внимание к собственным пробелам системы защиты, отказаться от самостоятельно разработанного программного обеспечения и перейти на единую системную концепцию безопасности платежей.

Яндекс деньги и другие платежные системы

Российские пользователи электронного кошелька Яндекс деньги часто интересуются, как именно устроены меры защиты платежей в ней. Платежный сервис использует следующие алгоритмы защиты:

– шифрование передаваемых данных с использованием криптоалгоритма RSA с хэшированием. Шифрование происходит на стороне отправителя средств, длина ключа составляет 1024 бит. Этот же метод шифрования применяют WebMoney и PayPal. Для сравнения, менее известная в России программа E-Port использует шифрование через SSL-протокол версии 3.0., что даже при применении 128-битного ключа оставляет место для уязвимостей;

– заверение трансакций подписью процессингового центра;

– применение сложного механизма аутентификации. Сначала пользователь вводит пароль, затем его подлинность проверяет программа-кошелек, для совершения платежей можно использовать смс-пароли;

– соединение происходит по протоколам HTTPS с использованием защищенного сертификата SSL;

– хранение всей информации организовано на защищенных серверах;

– от записи данные защищаются специальными программными решениями;

– используется программа «Яндекс кошелек», повышающая защиту трансакций.

В качестве одного из дополнительных решений введен код протекции, только при знании его получатель может забрать перевод, совершенный через оператора. Это позволяет избежать риска фишинга и отправки платежей неподтвержденным получателям.

Платежные приложения

Отдельным вопросом безопасности электронных платежных систем становится защита платежных приложений, таких как Apple Pay и Samsung Pay. ЦБ РФ, вводя регулирующие правила для иностранных операторов, часто входит в конфликт с уже разработанными и действующими нормами безопасности, чем может затруднить доступ российских граждан к этим ресурсам. Но своевременная реакция профессионального сообщества помогла внести изменения в новые регуляторные требования, и сервисы остались доступными для российских граждан.

Создаваемая система быстрых платежей (СБП), начало действия которой приходится на 28 января 2019 года, позволяющая отправлять деньги по номеру телефона, также имеет свои правила безопасности, утверждаемые регулятором. Для подключения к СБП от кредитных и финансовых организаций требуется:

– установить ПО с максимальной степенью защиты, рекомендуемое регулятором, или доработать собственное ПО в соответствии с требованиями и техническими спецификациями;

– провести тестовые испытания взаимодействия.

В настоящее время СБП уже зарегистрировалось более 30 участников, среди них 10 крупнейших банков страны. За промедление в подключении к СБП Сбербанк был оштрафован на 1 млн. руб., что стало важным индикатором для других участников рынка. ЦБ предупредил операторов платежей о существовании рисков атаки с целью сбора персональных данных клиентов. В письме, разосланном банкам, сообщается, что основным направлением атаки стал «автоматизированный или ручной процесс сбора информации о клиентах банков - участников СБП. Злоумышленник, используя имеющиеся данные идентификатора клиента (номер его мобильного телефона), теперь может получить дополнительную информацию об этом человеке, например, имя, отчество и первую букву фамилии, а также названия нескольких банков, где у него есть открытые счета». Полученные номера телефонов злоумышленники могут использовать для организации массовых звонков клиентам банков с целью получения паролей от личных кабинетов и других данных.

Центробанк предлагает следующий механизм борьбы с угрозой: Национальная система платежных карт, являющаяся операционно-клиринговым центром СБП, проводит круглосуточный мониторинг операций и блокирует в системе номера подозрительных телефонов, с

которых осуществляется массовый перебор. Помимо блокировки номеров ЦБ будет сообщать банкам об IP-адресах, с которых пытался осуществляться массовый перебор.

От принципа работы платежной системы и модели угроз зависят и способы защиты. Реализация рекомендуемых регулятором мер безопасности должна привести к повышению защищенности электронных платежей, снижению количества несанкционированных финансовых трансакций и списаний с банковских карт. Безопасность средств граждан целиком и полностью зависит от готовности банков и операторов выполнять требования регуляторов.

ВОПРОСЫ К ЗАЧЕТУ

1. Что такое электронные банковские услуги?
2. Назовите основные виды электронных банковских услуг.
3. В чем преимущества электронных банковских услуг для клиентов?
4. Какие технологии лежат в основе электронных банковских услуг?
5. Что такое дистанционное банковское обслуживание (ДБО)?
6. Какие каналы используются для предоставления электронных банковских услуг?
7. В чем разница между интернет-банкингом и мобильным банкингом?
8. Какие функции выполняет система клиент-банк?
9. Что такое API в контексте банковских услуг?
10. Какие нормативные документы регулируют электронные банковские услуги в вашей стране?
11. Что такое платежная система?
12. Назовите основные виды платежных систем.
13. В чем разница между национальными и международными платежными системами?
14. Какие функции выполняют платежные системы?
15. Что такое SWIFT и для чего он используется?
16. Какие виды платежных карт существуют?
17. В чем разница между дебетовой и кредитной картой?
18. Что такое виртуальная карта и как она используется?
19. Какие технологии используются в платежных картах (EMV, NFC)?
20. Что такое эквайринг и как он работает?
21. Что такое электронный платеж?
22. Какие виды электронных платежей существуют?
23. Как работает система переводов между счетами?
24. Что такое мгновенные платежи?
25. Какие преимущества у электронных платежей перед наличными?
26. Что такое платежные шлюзы и как они работают?
27. Как работает система оплаты через QR-коды?
28. Что такое P2P-платежи?
29. Какие риски связаны с электронными платежами?
30. Как обеспечивается безопасность электронных платежей?
31. Что такое интернет-банкинг?
32. Какие функции доступны в интернет-банкинге?
33. Что такое мобильный банкинг и чем он отличается от интернет-банкинга?
34. Какие технологии используются в мобильном банкинге?
35. Что такое push-уведомления в мобильном банкинге?
36. Как работает автоплатеж в интернет-банкинге?

37. Какие преимущества у мобильного банкинга для клиентов?
38. Какие риски связаны с использованием интернет-банкинга?
39. Как банки защищают данные клиентов в интернет-банкинге?
40. Что такое биометрия в мобильном банкинге?
41. Какие угрозы существуют для электронных банковских услуг?
42. Что такое двухфакторная аутентификация (2FA)?
43. Как работает электронная подпись (ЭЦП)?
44. Что такое токенизация и как она используется в платежных системах?
45. Какие методы шифрования используются в электронных банковских услугах?
46. Что такое фишинг и как от него защититься?
47. Как банки борются с мошенничеством в электронных платежах?
48. Что такое SSL/TLS и для чего он используется?
49. Какие меры безопасности должен соблюдать клиент при использовании электронных банковских услуг?
50. Что такое KYC (Know Your Customer) и как это связано с безопасностью?
51. Что такое Open Banking (открытый банкинг)?
52. Как работают криптовалюты в контексте банковских услуг?
53. Что такое блокчейн и как он используется в банковской сфере?
54. Какие преимущества у технологии NFC в платежных системах?
55. Что такое биометрическая аутентификация и как она применяется в банках?
56. Как искусственный интеллект используется в электронных банковских услугах?
57. Что такое чат-боты в банковской сфере?
58. Какие перспективы у развития цифровых валют (CBDC)?
59. Как работают смарт-контракты в банковской сфере?
60. Какие тренды в развитии электронных банковских услуг вы можете выделить?

ТЕСТОВЫЕ ЗАДАНИЯ

1. **Что из перечисленного является ключевым элементом Open Banking?**

a) Использование наличных денег;

b) Предоставление доступа к данным клиента третьим сторонам через API;

c) Отказ от цифровых технологий;

d) Увеличение числа физических отделений банка.

2. **Какая технология лежит в основе криптовалют, таких как Bitcoin?**

a) Централизованные серверы;

b) Блокчейн;

c) SQL-базы данных;

d) NFC.

3. **Что такое PSD2 (Revised Payment Services Directive)?**

a) Директива, регулирующая использование наличных денег;

b) Европейская директива, направленная на усиление конкуренции и безопасность платежных услуг;

c) Правила использования кредитных карт;

d) Стандарт для мобильных платежей.

4. **Какой из перечисленных методов аутентификации является наиболее безопасным?**

a) Пароль из 6 символов;

b) Двухфакторная аутентификация (2FA);

c) Использование одного и того же пароля для всех сервисов;

d) Отсутствие аутентификации.

5. **Что такое токенизация в платежных системах?**

a) Замена данных карты на уникальный токен;

b) Использование наличных денег;

c) Передача данных карты в открытом виде;

d) Увеличение лимитов на карте.

6. **Какая из перечисленных платежных систем является децентрализованной?**

a) Visa;

b) Mastercard;

c) Bitcoin.

Что такое эквайринг?

a) Процесс выпуска платежных карт;

b) Прием платежей по картам в торговых точках;

c) Перевод средств между счетами;

d) Блокировка карты.

7. **Какой из перечисленных стандартов используется для обеспечения безопасности платежных операций в интернете?**

a) HTTP;

b) SSL/TLS;

c) FTP;

d) SMTP;

8. **Что такое CBDC (Central Bank Digital Currency)?**

a) Криптовалюта, выпускаемая частными компаниями;

b) Цифровая валюта, выпускаемая центральным банком;

c) Наличные деньги;

d) Виртуальная карта.

9. **Какой из перечисленных элементов НЕ является частью системы клиент-банк?**

a) Электронная подпись;

b) API;

c) Бумажные чеки;

d) Шифрование данных.

10. **Что такое фишинг?**

a) Вид спорта;

b) Мошенническая схема, направленная на получение конфиденциальных данных;

c) Технология шифрования данных;

d) Вид электронного платежа.

11. **Какой из перечисленных сервисов НЕ относится к электронным банковским услугам?**

a) Интернет-банкинг;

b) Мобильный банкинг;

c) Оплата наличными в отделении банка;

d) Переводы через SWIFT.

12. **Что такое KYC (Know Your Customer)?**

a) Процесс проверки личности клиента;

b) Вид электронной подписи;

c) Технология для мгновенных платежей;

d) Метод шифрования данных.

13. **Какой из перечисленных элементов НЕ является частью экосистемы Open Banking?**

a) API;

b) Третьи стороны (TTP);

c) Централизованные базы данных;

d) Согласие клиента на доступ к данным.

14. **Что такое смарт-контракт?**

a) Договор, исполняемый автоматически при выполнении условий;

b) Вид кредитного договора;

c) Способ оплаты наличными;

d) Метод шифрования данных;

15. **Какой из перечисленных методов НЕ используется для обеспечения безопасности электронных платежей?**

a) Шифрование данных;

b) Использование открытых Wi-Fi сетей;

c) Двухфакторная аутентификация;

d) Токенизация.

16. **Что такое NFC (Near Field Communication)?**

a) Технология для бесконтактных платежей;

b) Вид криптовалюты;

c) Способ шифрования данных;

d) Метод аутентификации.

17. **Какой из перечисленных элементов НЕ является частью блокчейна?**

a) Централизованный сервер,

b) Блоки данных;

c) Децентрализованная сеть;

d) Хэширование.

18. **Что такое AML (Anti-Money Laundering)?**

a) Процедуры по борьбе с отмыванием денег;

b) Вид электронной подписи;

c) Метод шифрования данных;

d) Технология для мгновенных платежей.

19. **Что такое EMV-чип?**

a) Микропроцессор, повышающий безопасность платежных карт;

b) Виртуальная карта;

c) Метод шифрования данных;

d) Способ оплаты через NFC.

20. **Какой из перечисленных элементов НЕ является частью системы мгновенных платежей?**

a) Использование наличных денег;

b) Переводы в режиме реального времени;

c) Уникальные идентификаторы (например, номер телефона);

d) Участие банков в системе.

21. **Что такое биометрическая аутентификация?**

a) Использование отпечатков пальцев или сканирования лица для подтверждения личности;

b) Метод шифрования данных;

c) Вид электронной подписи;

d) Способ оплаты через NFC.

22. **Какой из перечисленных элементов НЕ является частью системы P2P-платежей?**

a) Использование наличных денег;

b) Переводы между физическими лицами;

c) Мобильные приложения;

d) Уникальные идентификаторы (например, номер телефона).

23. **Что такое API в контексте банковских услуг?**

a) Интерфейс для взаимодействия между программными системами;

b) Вид электронной подписи;

c) Метод шифрования данных;

d) Способ оплаты через NFC.

24. **Какой из перечисленных элементов НЕ является частью системы электронной подписи (ЭЦП)?**

a) Закрытый ключ;

b) Открытый ключ;

c) Централизованный сервер;

d) Сертификат.

25. **Что такое Ripple (XRP)?**

a) Криптовалюта для международных переводов;

b) Вид электронной подписи;

c) Метод шифрования данных;

d) Способ оплаты через NFC.

26. **Какой из перечисленных элементов НЕ является частью системы безопасности электронных платежей?**

a) SSL/TLS;

b) Фишинг;

c) Двухфакторная аутентификация;

d) Токенизация.

27. **Что такое QR-код в контексте платежей?**

a) Графический код для передачи платежных данных;

b) Вид электронной подписи;

c) Метод шифрования данных;

d) Способ оплаты через NFC.

28. **Какой из перечисленных элементов НЕ является частью системы блокчейн?**

a) Децентрализованная сеть;

b) Централизованный сервер;

c) Блоки данных;

d) Хэширование.

ТЕМЫ РЕФЕРАТОВ

1. Эволюция электронных банковских услуг: от первых систем до современных технологий.
2. Open Banking: концепция, преимущества и риски.
3. Роль блокчейна в трансформации банковских услуг.
4. Криптовалюты и их влияние на традиционные банковские системы.
5. Цифровые валюты центральных банков (CBDC): перспективы и вызовы.
6. PSD2 и его влияние на рынок финансовых услуг в Европе.
7. Безопасность электронных платежей: современные методы и технологии.
8. Токенизация платежных данных: принципы и применение.
9. Биометрическая аутентификация в банковской сфере: технологии и перспективы.
10. Искусственный интеллект в управлении рисками в электронных банковских услугах.
11. Мобильный банкинг: тенденции развития и влияние на потребительское поведение.
12. Электронная подпись (ЭЦП) и ее роль в цифровой экономике.
13. Системы мгновенных платежей: принципы работы и примеры внедрения.
14. Эквайринг: технологии, рынок и перспективы развития.
15. Фишинг и другие киберугрозы в электронных банковских услугах.
16. Технология NFC и ее применение в платежных системах.
17. Смарт-контракты в банковской сфере: возможности и ограничения.
18. Роль API в развитии Open Banking.
19. Электронные кошельки: виды, функции и перспективы развития.
20. Риски и преимущества использования криптовалют в банковской деятельности.
21. Регулирование электронных платежей: международный опыт и российская практика.
22. Технологии Big Data в анализе клиентского поведения в банковской сфере.
23. Роль чат-ботов в улучшении клиентского опыта в банках.
24. Электронные платежи в e-commerce: технологии и тенденции.
25. Системы P2P-платежей: принципы работы и примеры использования.
26. QR-коды как инструмент для упрощения платежей.
27. Электронные банковские услуги для малого и среднего бизнеса.
28. Роль KYC (Know Your Customer) в борьбе с отмыванием денег.
29. AML (Anti-Money Laundering) технологии в электронных платежах.

30. Технологии EMV: безопасность платежных карт.

31. Роль Ripple (XRP) в международных переводах.

32. Электронные банковские услуги в условиях пандемии: вызовы и возможности.

33. Цифровая трансформация банков: ключевые этапы и результаты.

34. Роль облачных технологий в развитии электронных банковских услуг.

35. Электронные платежи в социальных сетях: технологии и перспективы.

36. Технологии распознавания лиц в банковской аутентификации.

37. Электронные банковские услуги для людей с ограниченными возможностями.

38. Роль искусственного интеллекта в предотвращении мошенничества в платежных системах.

39. Электронные банковские услуги в развивающихся странах: проблемы и перспективы.

40. Технологии голосовой аутентификации в банковской сфере.

41. Электронные банковские услуги и их влияние на финансовую грамотность населения.

42. Роль RegTech в регулировании электронных платежей.

43. Электронные банковские услуги и их роль в сокращении использования наличных денег.

44. Технологии IoT (Интернет вещей) в банковской сфере.

45. Электронные банковские услуги и их влияние на конкуренцию в финансовом секторе.

46. Роль FinTech-компаний в развитии электронных платежей.

47. Электронные банковские услуги и их роль в устойчивом развитии.

48. Технологии виртуальной и дополненной реальности в банковской сфере.

49. Электронные банковские услуги и их роль в борьбе с бедностью.

Примерная структура реферата:

1. Введение (актуальность темы, цели и задачи).
2. Основная часть:

- теоретические аспекты
- современные технологии и практики
- примеры использования

3. Проблемы и перспективы.
4. Заключение (выводы и рекомендации).
5. Список использованных источников.

ЛАБОРАТОРНАЯ РАБОТА 1

Банковские риски

Для начала необходимо разобраться чем отличаются сложные проценты от простых.

Простые – те, что начисляются в конце срока вклада. Например, вы положили 100 000 Р на год под 5% годовых. Через год на вашем счете будет 105 000 Р. **Сложные**. Несмотря на название, принцип их **прост** – они начисляются в течение срока вклада через равные интервалы. Например, ежемесячно или ежеквартально. **Проценты** начисляются на первоначальную сумму и на **проценты от** предыдущих периодов – вы получаете **проценты** на **проценты**.

Под наращенной суммой ссуды (депозита, инвестированных средств, платежного обязательства и т.п.) понимается ее первоначальная сумма с начисленными на нее процентами к концу срока наращения. Величина наращенной суммы представляет собой произведение первоначальной суммы ссуды на множитель наращения, который показывает во сколько раз наращенная сумма больше первоначальной.

В зависимости от применяемой процентной ставки и условий наращения формула расчета множителя наращения записывается по-разному.

Простые проценты и расчет дисконта. Например, для наращения по простым процентам наращенная сумма (S) будет рассчитываться так:

S= P / (1+in)

где P – первоначальная сумма ссуды, ден. ед.; n – срок ссуды (а днях, месяцах, годах и т. п.); i – ставка наращения (простая постоянная), ед.

Выражение (1 + ni) называется множителем наращения.

Задача 1. Через 180 дней после подписания договора должник заплатит 310 тыс. руб. Кредит под 16% годовых. Какова первоначальная сумма долга? (Временная база – 365 дней). Чему равен дисконт? Расчеты произвести в MS Excel.

Задача 2. Найти первоначальную сумму, которая в итоге даст 30 000 руб. за 90 дней, банк предоставляет кредит под 10 % годовых. Расчеты произвести в MS Excel.

Задача 3. Какую сумму получит в банке кредитополучатель, если через 150 дней должен вернуть 7,5 млн. руб. ставка процента 27 %, период времени – 365 дней. Расчеты произвести в MS Excel.

Задача 4. Срок ссуды 5 лет. Договорная процентная ставка 12% годовых, маржа (доход дилера) 0,5% в первые два года и 0,75% в оставшиеся. Определить множитель наращивания. Расчеты произвести в MS Excel.

ЛАБОРАТОРНАЯ РАБОТА 2

Управление кредитным риском

Задача 1. Оценка кредитоспособности заемщика.

ЖСК «Жилье молодым семьям» занимается строительством жилых помещений для молодых семей. Для начала строительства нового объекта предприятие подала заявку в банк на получение кредита, предоставив все необходимые документы.

1. Денежные средства – 70 тыс. руб.;
2. Краткосрочные финансовые вложения – 28 тыс. руб.;
3. Дебиторская задолженность – 130 тыс. руб.;
4. Основные средства – 265 тыс. руб.;
5. Нематериальные активы – 34 тыс. руб.;
6. Производственные запасы – 155 тыс. руб.,
7. Кредиторская задолженность – 106 тыс. руб.,
8. Краткосрочные кредит банка – 95 тыс. руб.;
9. Долгосрочные кредиты – 180 тыс. руб.

Оценить возможность выдачи кредита предприятию и рассчитать коэффициент абсолютной, текущей, быстрой (срочной) ликвидности. Расчеты произвести в MS Excel.

Пример расчета коэффициента спреда. Для начала определимся что из себя представляет коэффициент спреда. *Итак, коэффициент спреда – это разница между ценой продажи и ценой покупки.*

Спред – это разрыв между минимальной ценой предложения и максимальной ценой спроса. Наиболее ликвидными являются ценные бумаги, у которых отношение спреда к максимальной цене спроса наименьшее (от 0-3 %).

Задача 1. Определить величину спреда по акциям и выявить наиболее ликвидную акцию. По первой акции минимальная цена предложения составила 2500 руб., максимальная цена спроса – 2450 руб. По второй акции: минимальная цена предложения равна 5030 руб., а максимальная цена спроса составляет 5 000 руб. Расчеты произвести в MS Excel.

Задача 2. Допустим, у вас есть акция компании, и цена продажи этой акции составляет 100 долларов, а цена покупки – 95 долларов. Необходимо определить разницу между этими двумя значениями и коэффициент спреда. Расчеты произвести в MS Excel.

Задача 3. Тинькофф банк получает процентные доходы на сумму 1 000 000 долларов и имеет процентные расходы на сумму 800 000 долларов. Рассчитать коэффициент фактической процентной маржи. Расчеты произвести в MS Excel.

КИПКЕЕВА Асият Магомедовна

ЭЛЕКТРОННЫЕ И ПЛАТЕЖНЫЕ УСЛУГИ БАНКОВ

Учебно-методическое пособие для обучающихся
очной и заочной форм обучения по направлению подготовки
09.04.03 Прикладная информатика направленность профиль
«Прикладная информатика в экономике и управлении»

Корректор Чагова О.Х.
Редактор Чагова О.Х.

Сдано в набор 24.03.2025 г.
Формат 60×84/16
Бумага офсетная
Печать офсетная
Усл. печ. л.1,86
Заказ № 5054
Тираж 100 экз.

Оригинал-макет подготовлен
в Библиотечно-издательском центре СКГА
369000, г. Черкесск, ул. Ставропольская, 36