Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Сухотерин А.И. Рабочая программа дисциплины: «Информационная безопасность кредитно-финансовых операций». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н. доцент			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно-финансовых операций;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно- финансовых операций;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Профессиональные компетенции:

- ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

Профессионально - специализированные компетенции:

- ПСК-3: способность участвовать в разработке информационно-аналитических систем финансового мониторинга.

Основными **задачами** дисциплины являются:

- Теоретические основы подготовки студентов для самостоятельного решения поставленных задачи в области применения банковских информационных систем и технологий на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
- Практические аспекты формирования подходов обучаемых к выполнению самостоятельных исследований в области защиты информации в кредитно-финансовых организациях по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- Формирование, у обучающихся системы знаний для применения основных методов и средств защиты информации кредитно-финансовых операций инструментов и технологий функциональных и контролирующих подразделений кредитно-финансовой организации.

После завершения освоения данной дисциплины студент должен:

Знать:

- методику выявления и анализа потенциально существующих угроз информационной безопасности при проведении операций в кредитно-финансовых организациях;
- методы анализа и оценки рисков в результате утечки сведений конфиденциального характера при проведении операций в кредитно-финансовых организациях;
- порядок организации работы по обеспечению сохранности сведений, составляющих конфиденциальный характер в кредитно-финансовых организациях;
- основные положения законодательства РФ по защите государственной и коммерческой тайны в кредитно-финансовых организациях;
- меры и условия по обеспечению охраны конфиденциальности информации в кредитно-финансовых организациях;
- основы применения специальных аналитических технологий для выявления и предупреждения противоправных посягательств в кредитно-финансовых организациях;
- алгоритм подготовки типовых рекомендации по сохранности сведений конфиденциального характера для руководства в кредитно-финансовых организаций.

Уметь:

- использовать в практической деятельности знания по информационной безопасности в кредитно-финансовых организациях;
- анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной

деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;

- пользоваться нормативными документами по защите информации в кредитно-финансовых организациях.

Владеть:

- правилами хранения и обращения с документами, содержащими сведения конфиденциального характера, описанием потенциально уязвимых мест со стороны криминальных угроз и иных рисков, системному представлению угроз в кредитно-финансовых организациях;
- основными понятиями, раскрывающими содержание предметной области;
- организацией информационной безопасности в кредитно-финансовой сфере деятельности при проведении операций;
- базовыми положениями по организации защиты информации в кредитно-финансовой сфере деятельности.
- мерами гражданско-правовой, уголовной, административной и дисциплинарной ответственности за разглашение защищаемой информации и нарушение правил ее защиты и условия применения этих мер.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность кредитно-финансовых структур» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6, ОПК-2,4,6 и ПК-4,14.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Мониторинг рынка страхования», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетные единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр 6	Семестр …	Семестр …
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	76	76			
Контроль самостоятельной работы	-	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час Очное	Код компетенций
Тема 1: Информационная безопасность технологий электронных расчетов	2	2	2	ОПК-2,4 ПК-7,11 ПСК-3
Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях	2	2	2	ОПК-2,4 ПК-7,11 ПСК-3
Тема 3:Информационная безопасность при выполнении	2	2	2	ОПК-2,4 ПК-7,11 ПСК-3

электронных транзакций				
Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг	2	2	2	ОПК-2,4 ПК-7,11 ПСК-3
Тема 5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы	4	4	2	ОПК-2,4 ПК-7,11 ПСК-3
Тема 6: Информационная безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть	4	4	2	ОПК-2,4 ПК-7,11 ПСК-3
Итого:	16	16	12	

4.2. Содержание тем дисциплины

Тема 1: Информационная безопасность технологий электронных расчетов

Традиционные технологии расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Информационные технологии внешних взаимодействий КБ.

Назначение и архитектура системы «Клиент – банк». Способы передачи информации до компьютерной сети банка. Системы телефонного банкинга. Система «Клиент – банк» на основе технологии «толстого

клиента» Понятие и модели Интернет - банкинга. Организация Интернет – банкинга через портал посредника –аутсорсера. Направления удаленного банковского обслуживания.

Классификация пластиковых карт. Чековые расчеты – основа банковской информационной технологии электронных расчетов. Участники карточной платежной системы и схема их работы. Расчеты банковскими картами в Интернете.

Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях

Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Основные подходы, применяющиеся к решению задачи использования средств ЭЦП в сети межбанковских расчетов.

Тема 3. Информационная безопасность электронных транзакций

Основные понятия. Схема защищенного информационного обмена при использовании симметричных методов. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами. Симметричные алгоритмы шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг

Общее правило создания ЭЦП. Общее правило верификации ЭЦП. Защита электронных транзакций протокол (SSL). Схема работы протокола SET. Управление ключами. Распространение ключей в случае использования только симметричных методов преобразования информации. Распространение ключей в случае использования сертификатов открытых ключей. Электронные платежи с помощью цифровых денег.

Тема 5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы

Расчетная функция банков и ее автоматизация. Схема обработки платежного документа клиентами. Ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.

Тема 6: Информационная безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть

Правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД). Составление и направление ЭД участником – отправителем. Порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. Порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность кредитно-финансовых операций» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).
2. В.В. Дик. Банковские информационные системы: учебник. – М.: Маркет ДС, 2013. (Универсететская серия)
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.: - (профессиональное образование).
4. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

Дополнительная литература:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
2. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.

3. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
4. Кобелев О.А. Электронная коммерция: учебное пособие. – М.: Дашков и К, 2010 – 684 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
6. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.
7. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

Рекомендуемая литература:

1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006
3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».
8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
10. Дединев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. Учебно – справочное пособие – М.: КУДИЦ – ОБРАЗ, 2004. --512 с. (СКБ – специалиту по компьютерной безопасности).

Электронные книги:

1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с.
http://www.biblioclub.ru/book/54713/

2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с.
http://www.biblioclub.ru/book/140927/
3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с.
http://www.biblioclub.ru/book/54663/
4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А. Шапкин. — 5-е изд. — М.: Дашков и К, 2012. — 400 с.
http://www.biblioclub.ru/book/112204/
5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.
http://www.biblioclub.ru/book/116705/
6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.
http://www.biblioclub.ru/book/100020/
7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.
http://www.biblioclub.ru/book/118462/
8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.
http://www.biblioclub.ru/book/88353/
9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.
http://www.biblioclub.ru/book/79604/
10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с.
http://www.biblioclub.ru/book/78803/
11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р .] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с.
http://www.biblioclub.ru/book/118178/

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал
2. **http://informika.ru/** – образовательный портал
3. **www.wikIsec.ru -** Энциклопедия информационной безопасности. –

Публикации, статьи**.**

4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.window.edu.ru** - Единое окно доступа.
6. **http://grebennikov.ru/** - Издательский дом «Гребенников»
7. **www.rucont.ru** - ЭБС «Руконт»
8. **http://www.minfin.ru -** Официальный сайт Министерства финансов Российской Федерации
9. **http://www.gov.ru** -Официальный сервер органов государственной власти Российской Федерации.
10. **http://www.fsb.ru** - Официальный сайт Федеральной Службы Безопасности
11. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методичские указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Информационная безопасность кредитно-финансовых операций»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов по темам.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;

- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	Темы 1,2,3, 4, 5,6	основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права; правовые основы обеспечения национальной безопасности Российской Федерации	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач	навыками обоснования, выбора, реализации и контроля результатов управленческого решения
2.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Темы 1, 2,3, 4, 5,6	основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав	навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений; навыками критического восприятия информации; навыками письменного аргументированного изложения собственной точки зрения

				структурных подразделений		
3.	ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Темы 1, 2,3, 4, 5,6	типовые структуры и принципы организации компьютерных сетей; последовательность и содержание этапов построения компьютерных сетей;	пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет	навыками работы с технической документацией на ЭВМ и вычислительные системы
4.	ПК-11	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Темы 1, 2,3, 4, 5,6	Основные нормативные документы в области информационной безопасности	Выбирать методические и нормативные документы в соответствии с решаемой задачей	Навыками по работе с технической документацией, требуемой или рекомендуемой по соответствующему тематическому вопросу
5.	ПСК-3	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Темы 1, 2,3, 4, 5,6	Программу для исследования электрических цепей и электронных схем Multisim	Проектировать и анализировать отдельные узлы электрических цепей	Навыками практической работы по исследованию характеристик и режимов работы отдельных узлов электрической цепи

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-2	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ОПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5

			баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-7	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-11	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).

			Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПСК-3	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее информационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.

4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности

5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.

6. Информационная безопасность подсистемы работы с банковскими картами.

7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.

8. Информационная безопасность подсистемы операций с ценными бумагами.

9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.

10. Информационная безопасность подсистемы управления ресурсами (дилинга).

11. Информационная безопасность в подсистеме обеспечения безопасности.

12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.

13. Информационная безопасность подсистема удаленного банковского обслуживания.

14. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.

15. Информационная безопасность системы электронного документооборота банка.

16. Информационная безопасность традиционных технологий расчетов.

17. Информационная безопасность и архитектура системы «Клиент – банк».

18. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.

19. Информационная безопасность системы телефонного банкинга.

20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

21. Информационная безопасность модели Интернет - банкинга.

22. Информационная безопасность расчетов банковскими картами в Интернете.

23. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.

24. ИБ защищенного информационного обмена при использовании симметричных методов защиты информации.

25. ИБ защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

26. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
27. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
28. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
29. Информационная безопасность электронных платежей с помощью цифровых денег.
30. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
31. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
32. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД) в кредитно-финансовой организации.
33. Информационная безопасность при составлении и направлении ЭД участником – отправителем.
34. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
35. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Примерная тематика заданий на контрольную работу:

1. Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.
2. Система угроз информационной безопасности банка.
3. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
4. Система правового обеспечения информационной безопасности банка.
5. Правовые акты общего действия, обеспечивающие информационную безопасность банков методами охранительного содержания.
6. Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.
7. Организация системы информационной безопасности банка. Субъекты обеспечения информационной безопасности банка.
8. Средства и методы обеспечения информационной безопасности банка.
9. Организация внутреннего контроля банка ее информационная безопасность.
10. Организация службы безопасности банка.
11. Система технических средств безопасности банка.
12. Технические средства охраны.

13. Технические средства охраны банковских операций и продуктов.
14. Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.
15. Информационная безопасность при противодействии хищению денежных средств с незаконным использованием пластиковых карт.
16. Информационная безопасность при противодействии хищении денежных средств с использованием аккредитивов.
17. Информационная безопасность при противодействии хищению денежных средств с использованием чеков.
18. Информационная безопасность при противодействии хищению денежных средств с использованием платежных поручений
19. Правовая характеристика векселя. Риски в сфере вексельного обращения. Роль информационной безопасности при этом.
20. Преступления против собственности, в которых вексель является предметом посягательств. Роль информационной безопасности при этом.
21. Преступления против собственности, в которых вексель является средством совершения преступления. Роль информационной безопасности при этом.
22. Меры предупреждения преступлений в сфере вексельного обращения. Роль информационной безопасности при этом.
23. Злоупотребления полномочиями. Коммерческий подкуп. Роль информационной безопасности при этом.
24. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Роль информационной безопасности при этом.
25. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Роль информационной безопасности при этом.
26. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка. Роль информационной безопасности при этом.
27. Информационная безопасность при легализации (отмывания) доходов, полученных преступным путем.
28. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма
29. Информация, использующая в целях обеспечения безопасности (информационной безопасности) банка, и ее источники.
30. Бюро кредитных историй.
31. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность (информационную безопасность) банка.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Информационная безопасность кредитно-финансовых операций» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-2 ОПК-4 ПК-7 ПК-11 ПСК-3	20-40 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-2 ОПК-4 ПК-7 ПК-11 ПСК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-2 ОПК-4 ПК-7 ПК-11 ПСК-3	2 теоретических вопроса + практическое задание	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 35 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета.

						«**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не

						отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

Вариант (Технологии межбанковских электронных расчетов)

1. Что такое система межбанковских расчетов?
2. Какой нормативный срок установлен для проведения расчетов в замках субъекта РФ? А в пределах всей территории РФ?
3. С помощью каких видов счетов могут осуществляться расчеты через КО (филиалы)?
4. В какой очередности осуществляется списание денежных средств при недостаточности средств на счете?
5. Что такое операционный день банка?
6. Как осуществляется обработка платежного документа клиента банка?
7. Какие Вы знаете способы обработки электронных документов банком?
8. Какие Вы знаете способы защиты предупреждения ошибок ввода информации.
9. Перечислите основные параметры функционирования платежных систем?
10. Перечислите ключевые принципы для системно значимых платежных систем.
11. Расскажите о рисках, возникающих в процессе функционирования платежной системы.
12. Каковы основные направления решения проблемы распределению ресурсов, выделенных по корреспондентским счетам, участвующим в системе межбанковских расчетов?
13. Какими двумя способами может происходить исполнение платежей в любой платежной системе?
14. Каково главное достоинство брутто-расчетов?
15. Как решается проблема недостаточности средств при брутто - расчетах?
16. По какой причине в Швейцарии большинство банков не является участниками расчетов в национальной платежной системе?
17. Каким положением Банка России регулируется механизм содержания ликвидности кредитной организации в период временного отсутствия денежных средств в РФ?
18. По какой причине не оправдано развитие филиальной сети в России после кризиса 1998 года?

19. Перечислите известные Вам варианты технологий организации расчетов между филиалами внутри одного банка.
20. Каким образом определяется дата перечисления платежа?
21. Какие договоренности должны быть достигнуты между банком - респондентом и банком-корреспондентом?
22. Каким образом производится учет незавершенных расчетов собственным и транзитным платежам банка?
23. Перечислите наиболее часто используемые подходы при выборе окончательного решения кредитной организации по структуре и характеристикам ее корреспондентской сети.
24. Каковы недостатки действующей в настоящее время платежной системы РФ?
25. Каким образом формируется уникальный идентификатор составителя документа электронного документа?
26. В чем различие и особенности электронного платежного документа сокращенного формата и полноформатного?
27. Какова функция РКЦ (ГРКЦ) при организации расчетов через расчетную сеть Банка России?
28. Какой механизм межрегиональных расчетов в расчетной Банка России?
29. Какие Вы знаете преимущества и недостатки технологии клиринга?
30. Перечислите технологии расчетов между филиалами внутри одного банка.
31. Дайте определение и приведите классификацию клиринга?
32. Перечислите основные цели деятельности клиринговых организаций?
33. Какие операции клиринговых учреждений, обеспечивающие выполнение клиринга или способствующие осуществлению клиринговых взаиморасчетов, Вы знаете?
34. Опишите особенности построения коммуникационной сети которые обеспечивает транспорт сообщений между коммерческими банками и расчетными центрами.
35. Каковы основные функции коммуникационного центра?
36. Опишите схему модулей информационной системы автоматизированного расчетного центра и взаимодействия с коммерческим банком на основе электронной почты.
37. Какими тремя способами может быть организована технология взаимодействия расчетных центров по переводу средств?
38. Какова история появления и развития S.W.I.F.T.?
39. В чем состоят преимущества и недостатки системы S.W.I.F.T.?
40. Когда S.W.I.F.T. появилась в России (СССР)?
41. Какие функции у Российской Национальной Ассоциации ROS-S.W.I.F.T.?
42. Какова схема прохождения платежного поручения клиента в системе S.W.I.F.T.?

43. Что включает в себя стандарт SWIFT-RUR? .
44. По какой причине потребовалось введение стандарта SWIFT-RUR? Укажите текущую версию стандарта.
45. Назовите основные категории сообщений S.W.I.F.T.?
46. Опишите структуру сети S.W.I.F.T.?
47. Какие новые сервисы появились с переходом к SWIFTNet?
48. Перечислите 4 схемы доступа к сети S.W.I.F.T.
49. Какие интерфейсы системы S.W.I.F.T. Вы знаете?

Форма тестов

1. **Основные способы незаконного получения банковской тайны.**

Тайным;
Открытым;
В виде обмана;
С применением насилия;
Во всех перечисленных случаях.

2. **Основные направления, по которым осуществляется защита кадрового состава банка.**

Ограждение банка от проникновения в его личный состав нежелательных лиц;
Соответствие кадров системе требований;
Во всех перечисленных случаях.

4.2. Типовые вопросы, выносимые на экзамен

1. Технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее информационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
8. Информационная безопасность подсистемы операций с ценными бумагами.

9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
10. Информационная безопасность подсистемы управления ресурсами (дилинга).
11. Информационная безопасность в подсистеме обеспечения безопасности.
12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
13. Информационная безопасность подсистема удаленного банковского обслуживания.
14. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.
15. Информационная безопасность системы электронного документооборота банка.
16. Информационная безопасность традиционных технологий расчетов.
17. Информационная безопасность и архитектура системы «Клиент – банк».
18. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.
19. Информационная безопасность системы телефонного банкинга.
20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
21. Информационная безопасность модели Интернет - банкинга.
22. Информационная безопасность расчетов банковскими картами в Интернете.
23. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
24. ИБ защищенного информационного обмена при использовании симметричных методов защиты информации.
25. ИБ защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
26. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
27. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
28. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
29. Информационная безопасность электронных платежей с помощью цифровых денег.
30. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.

31. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
32. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД) в кредитно-финансовой организации.
33. Информационная безопасность при составлении и направлении ЭД участником – отправителем.
34. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
35. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРЕДИТНО-ФИНАНСОВЫХ ОПЕРАЦИЙ»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Целью изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно- финансовых операций;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно- финансовых операций;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

Задачи дисциплины:

- Теоретические основы подготовки студентов для самостоятельного решения поставленных задачи в области применения банковских информационных систем и технологий на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
- Практические аспекты формирования подходов обучаемых к выполнению самостоятельных исследований в области защиты информации в кредитно-финансовых организациях по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- Формирование у обучающихся системы знаний для применения основных методов и средств защиты информации кредитно-финансовых операций инструментов и технологий функциональных и контролирующих подразделений кредитно-финансовой организации.

2. Указания по проведению практических занятий

Тема 1: Информационная безопасность технологий электронных расчетов. Технологии защиты безналичных электронных расчетов на основе систем «Клиент – банк». Технологии защиты безналичных расчетов на основе банковских карт

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий электронных расчетов.

Основные положения темы занятия:

1. технологии защиты безналичных электронных расчетов на основе систем «Клиент – банк».

2. технологии защиты безналичных электронных расчетов на основе банковских карт.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Информационная безопасность технологий расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Защита информационных технологий внешних взаимодействий КБ.
2. Назначение и архитектура системы «Клиент – банк». Информационная безопасность передачи информации до компьютерной сети банка. Системы телефонного банкинга. Система «Клиент – банк» на основе технологии «толстого клиента» Понятие и модели Интернет - банкинга. Организация Интернет – банкинга через портал посредника –аутсорсера. Направления удаленного банковского обслуживания и их защита.
3. Информационная безопасность пластиковых карт. Карточные фокусы. Чековые расчеты – основа банковской информационной технологии электронных расчетов. Информационная безопасность карточной платежной системы и схема их работы. Расчеты банковскими картами в Интернете и их информационная безопасность.

Продолжительность занятия – 2 ч.

Тема 2: Информационная безопасность при применении средств электронной цифровой подписи в кредитно-финансовых организациях

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты с применением ЭП согласно существующего законодательства.
2. технологии защиты с применением ЭП для организации защищенного электронного документооборота в банках.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Место ЭЦП в ряду криптографических механизмов.
2. История возникновения ЭЦП в России.
3. Информационная безопасность при использовании средств ЭЦП в сети межбанковских расчетов.

Продолжительность занятия – 2 ч.

Тема 3. Информационная безопасность электронных транзакций

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа электронных транзакций.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Информационная безопасность защищенного информационного обмена при использовании симметричных методов.

2.Информационная безопасность защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

3.Симметричные алгоритмы шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги.

4.Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Продолжительность занятия – 2 ч.

Тема 4: Правовые и организационные основы применения ЭЦП в кредитно-финансовых организациях и оказании региональных электронных услуг

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
2. Защита электронных транзакций протокол (SSL).
3. Схема работы протокола SET. Управление ключами.
4. Распространение ключей в случае использования только симметричных методов преобразования информации.
5. Распространение ключей в случае использования сертификатов открытых ключей.
6. Информационная безопасность электронных платежей с помощью цифровых денег.

Продолжительность занятия – 2 ч.

Тема5: Информационная безопасность автоматизации расчетной функции в кредитно-финансовой организации и принципы построения защищенной электронной платежной системы

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной электронной платежной системы.

Основные положения темы занятия:

1. технологии защиты электронных платежных систем.
2. принципы построения защищенной электронной платежной системыие методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Расчетная функция банков и ее автоматизация.

2.Схема обработки платежного документа клиентами.

3.Ключевые принципы для системно – значимых платежных систем.

4.Определение количества ресурсов, которые банк будет держать на своих корсчетах.

Продолжительность занятия – 4 ч.

Тема 6: Информационная безопасность и правила обмена электронными документами кредитно-финансовой организации и ее клиентами при осуществлении расчетов через расчетную сеть

Практическое занятие 6.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной системы электронного документооборота в кредитно-финансовой организации.

Основные положения темы занятия:

1. ознакомиться с основными правилами работы с электронными документами.
2. принципы построения защищенной СОД.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
2. Составление и направление ЭД участником – отправителем. Порядок контроля ЭД, полученных от участников – отправителей.
3. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. Порядок приема к исполнению ЭД участником – получателем.
4. Порядок хранения и уничтожения ЭД.

Продолжительность занятия – 4 ч.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности кредитно-финансовых операций;

2) привить навыки самостоятельного решения задач в области организации защиты кредитно-финансовых операций.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**76**
Вопросы, выносимые на самостоятельное изучение	34
Подготовка к практическим занятиям	16
Подготовка к лабораторным занятиям	-
Подготовка докладов	10
Выполнение практических заданий	16

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.
2. Система угроз информационной безопасности банка.
3. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
4. Система правового обеспечения информационной безопасности банка.
5. Правовые акты общего действия, обеспечивающие информационную безопасность банков методами охранительного содержания.
6. Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.
7. Организация системы информационной безопасности банка. Субъекты обеспечения информационной безопасности банка.
8. Средства и методы обеспечения информационной безопасности банка.
9. Организация внутреннего контроля банка ее информационная безопасность.
10. Организация службы безопасности банка.
11. Система технических средств безопасности банка.
12. Технические средства охраны.
13. Технические средства охраны банковских операций и продуктов.
14. Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	34	Изучение открытых источников
2.	Подготовка к практическим занятиям	16	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	
4.	Тематика докладов	10	Методы анализа линейных и нелинейных электрических цепей
5.	Выполнение практических заданий	16	Расчет электрических характеристик заданных электрических цепей

Примерные темы докладов

1. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
2. Информационная безопасность подсистемы работы с банковскими картами.
3. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
4. Информационная безопасность подсистемы операций с ценными бумагами.
5. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
6. Информационная безопасность подсистемы управления ресурсами (дилинга).
7. Информационная безопасность в подсистеме обеспечения безопасности.
8. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
9. Информационная безопасность подсистема удаленного банковского обслуживания.
10. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.
11. Информационная безопасность системы электронного документооборота банка.
12. Информационная безопасность традиционных технологий расчетов.
13. Информационная безопасность и архитектура системы «Клиент – банк».
14. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.
15. Информационная безопасность системы телефонного банкинга.
16. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс анализа заданной

электрической цепи и должна содержать промежуточные и окончательные результаты расчетов, а также соответствующие временные или частотные диаграммы, поясняющие работу электрической цепи.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

основная:

1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).
2. В.В. Дик. Банковские информационные системы: учебник. – М.: Маркет ДС, 2013. (Универсететская серия)
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.: - (профессиональное образование).
4. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

дополнительная:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
2. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
3. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
4. Кобелев О.А. Электронная коммерция: учебное пособие. – М.: Дашков и К, 2010 – 684 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
6. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.

рекомендуемая:

1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006
3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».
8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Электронные книги:

1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с.
   http://www.biblioclub.ru/book/54713/
2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с.
   http://www.biblioclub.ru/book/140927/
3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с.
   http://www.biblioclub.ru/book/54663/
4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А. Шапкин. — 5-е изд. — М.: Дашков и К, 2012. — 400 с.
   http://www.biblioclub.ru/book/112204/
5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.
   http://www.biblioclub.ru/book/116705/

6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.
http://www.biblioclub.ru/book/100020/
7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.
http://www.biblioclub.ru/book/118462/
8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.
http://www.biblioclub.ru/book/88353/
9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.
http://www.biblioclub.ru/book/79604/
10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с.
http://www.biblioclub.ru/book/78803/
11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р .] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с.
http://www.biblioclub.ru/book/118178/

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал
2. **http://informika.ru/** – образовательный портал
3. **www.wikIsec.ru -** Энциклопедия информационной безопасности.

Публикации, статьи.

1. **www.biblioclub.ru** - Универсальная библиотека онлайн.
2. **www.window.edu.ru** - Единое окно доступа.
3. **http://grebennikov.ru/** - Издательский дом «Гребенников»
4. **www.rucont.ru** - ЭБС «Руконт»
5. **http://www.minfin.ru -** Официальный сайт Министерства финансов Российской Федерации
6. **http://www.gov.ru** - Официальный сервер органов государственной власти Российской Федерации.
7. **http://www.fsb.ru** - Официальный сайт Федеральной Службы Безопасности
8. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice*, *Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Информационная безопасность кредитно-финансовых операций».