МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

«СОГЛАСОВАНО»
Руководитель ОП

_____Л.К. Васюкова__
(подпись) (Ф.И.О. рук. ОП)
«_18_»____января__2021___г.

«УТВЕРЖДАЮ»
Директор
Департамента финансов

_____ ___Е.И.Бережнова
(подпись) (Ф.И.О. зав. каф.)
«_18__»_____января__2021___г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения
Направление подготовки 38.04.08 Финансы и кредит
магистерская программа «Финансовые стратегии и технологии банковского института»
(совместно с ПАО "Сбербанк")

Форма подготовки: заочная

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 38.04.08 Финансы и кредит, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 12.08.2020 № 991.

Рабочая программа обсуждена на заседании Департамента финансов,
протокол № 1 от «18» января 2021 г.
Директор Департамента финансов: канд. экон. наук, доцент Е.И.Бережнова

Составитель: канд. экон. наук Л.К. Васюкова

Владивосток
2021

Оборотная сторона титульного листа РПД

1. Рабочая программа пересмотрена на заседании Департамента/кафедры/отделения (реализующего дисциплину) и утверждена на заседании Департамента/кафедры/отделения (выпускающего структурного подразделения), протокол от «____» _____ 202 г. № _____

2.Рабочая программа пересмотрена на заседании Департамента/кафедры/отделения (реализующего дисциплину) и утверждена на заседании Департамента/кафедры/отделения (выпускающего структурного подразделения), протокол от «____» _____ 202 г. № _____

3.Рабочая программа пересмотрена на заседании Департамента/кафедры/отделения (реализующего дисциплину) и утверждена на заседании Департамента/кафедры/отделения (выпускающего структурного подразделения), протокол от «____» _____ 202 г. № _____

4.Рабочая программа пересмотрена на заседании Департамента/кафедры/отделения (реализующего дисциплину) и утверждена на заседании Департамента/кафедры/отделения (выпускающего структурного подразделения), протокол от «____» _____ 202 г. № _____

5.Рабочая программа пересмотрена на заседании Департамента/кафедры/отделения (реализующего дисциплину) и утверждена на заседании Департамента/кафедры/отделения (выпускающего структурного подразделения), протокол от «____» _____ 202 г. № _____

Аннотация дисциплины

Распределённые финансовые системы и
экономическая безопасность: проблемы и пути решения

Учебный курс дисциплины «Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения» предназначена для магистрантов направления подготовки 38.04.08 Финансы и кредит.

Дисциплина «Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения» включена в состав вариативной части блока «Факультативы».

Общая трудоёмкость освоения дисциплины составляет 1 зачётная единица, 36 часов. Учебным планом предусмотрены практические занятия (18 часов), самостоятельная работа студентов (18 часов). Дисциплина реализуется на 2 курсе, в третьем семестре, заканчивается сдачей зачёта.

Дисциплина «Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения» логически и содержательно связана с такими курсами, как «Эконометрика», «Введение в искусственный интеллект и анализ больших данных», «Финансовые технологии» и другими и позволяет подготовить студентов к освоению таких дисциплин, как «Технологии управления финансовыми рисками», «Корпоративные информационные технологии в управлении предприятием», «Управление стоимостью компании».

Содержание дисциплины охватывает следующий круг вопросов:

1. Модели распределённых информационных систем в финансовой сфере: понятия модели «клиент-сервер» и её логические уровни; уровень обработки данных, уровень данных, прикладные финансовые программы типа «клиент-сервер».

2. Организация связи между процессами: удалённый вызов процедур; обращение к удалённым объектам; связь посредством сообщений; связь на основе потоков данных.

3. Государственный финансовый контроль рисков потери информации: нормативно-правовые акты, регулирующие формирование и представление информации о финансовых показателях деятельности субъектов финансового рынка; регулирование сроков, форм и методов представление финансовой информации субъектами рынка; контроль доступа к ресурсам информационной системы.

4. Надёжность распределённой обработки информации: теория надёжности, методы обеспечения устойчивости формирования и передачи финансовой информации; физическая избыточность информации.

5. Защита информации в распределённых финансовых системах: понятие теории информационной безопасности в банковской (страховой) сфере; кибер-риски; управление рисками потери информации; современные системы защиты информации в финансово-кредитных организациях.

Цель: ознакомление студентов с различными методами защиты информации в распределенных финансовых системах.

Задачи курса:

1. Изучение практики использования современных компьютерных технологий для защиты информации распределённых финансовых систем.

2. Изучение основ государственного финансового контроля рисков потери информации и регулирования инфраструктуры рынка средств защиты информации в целях обеспечения экономической безопасности субъектов рынка, отрасли, региона и экономики в целом.

3. Формирование навыков управления рисками потери информации распределённых финансовых систем.

4. Ознакомление с практикой защиты информации в современных финансово-кредитных организациях.

Для успешного изучения дисциплины «Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения» у обучающегося по программе должны быть сформированы следующие предварительные компетенции:

− способность использовать основы экономических знаний в различных сферах деятельности;

− способность к самоорганизации и самообразованию;

− способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

− способность осуществлять сбор, анализ и обработку данных, необходимых для решения профессиональных задач;

− способность выбрать инструментальные средства для обработки экономических данных в соответствии с поставленной задачей, проанализировать результаты расчетов и обосновать полученные выводы.

В результате изучения дисциплины у обучающихся формируются следующие профессиональные компетенции.

Код и формулировка компетенции	**Этапы формирования компетенции**	
ПК-11 Способность анализировать и использовать различные источники информации для проведения экономических расчетов	Знает	Методы идентификации, оценки уровня рисков потери информации в распределённых финансовых системах
	Умеет	Идентифицировать риски и рассчитывать уровень рисков потерь информации в распределённых финансовых системах
	Владеет	Навыками идентификации и оценки уровня рисков потерь информации в распределенных финансовых системах
ПК-12 Способность составлять прогноз основных социально-экономических показателей деятельности предприятия, отрасли, региона и экономики в целом	Знает	Методы, модели и инструменты прогнозирования показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом
	Умеет	Составлять прогнозы показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом
	Владеет	Методикой прогнозирования показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе

		финансово-кредитного сектора, отрасли, региона и экономики в целом
ПК-14 Способность к применению теоретических знаний для решения практических проблем рационального и эффективного использования экономических ресурсов при осуществлении экономического выбора	Знает	Методы и практики информационной защиты распределённых финансовых систем, вопросы нормативно-правового регулирования рисков потери информации и создания инфраструктуры рынка средств защиты информации
	Умеет	Применять на практике методы информационной защиты распределённых финансовых систем, использовать возможности инфраструктуры рынка средств защиты информации для защиты информации предприятия, организаций, в том числе финансово-кредитных организаций, для обеспечения экономической безопасности
	Владеет	Навыками организации защиты информации предприятия, организации, в том числе финансово-кредитной, на основе эффективного использования возможностей инфраструктуры рынка

Для формирования указанных компетенций в рамках дисциплины «Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения» применяются следующие методы интерактивного обучения:

− технология кейс-стади;

− круглого стола с приглашением представителей финансовых, it-компаний, финтех-компаний; представителей регулятора рынка – Банка России;

− учебная групповая дискуссия.

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Тема 1. Информационная безопасность в предпринимательской деятельности (2 час.)

Необходимость защиты информации. Несанкционированный доступ. Защита банковской информации. Защита от физического доступа. Защита резервных копий. Защита от инсайдеров.

Тема 2. Концепции информационной безопасности коммерческого банка (2 час.)

Общие положения. Цели и задачи системы безопасности. Принципы организации и функционирования системы безопасности. Основные виды угроз потери информации коммерческого банка. Объекты защиты коммерческого банка. Нормативная база защиты информации в кредитно-финансовой сфере.

Тема 3. Безопасность электронных систем финансовых организаций (2 час.)

Аудит информационной безопасности. Определение степени соответствия безопасности основным нормам и стандартам. Автоматизация финансовых операций и их защита. Методы защиты автоматизированных систем обработки информации (АСОИ).

Тема 4. Влияние человеческого фактора на информационную безопасность в кредитно-финансовой сфере (3 час.)

Анализ риска. Основные этапы анализа риска. Планы защиты. Планы обеспечения

непрерывной работы восстановления функционирования АСОИ. Киберриски. Реализация технологии цифровой подписи. Страхование киберрисков.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Занятие 1. Государственное регулирование вопросов защиты информации в финансово-кредитной сфере (2 час.)

1.1 Доктрина информационной безопасности РФ

1.2 Обеспечение информационной безопасности коммерческих банков

1.3 Информационная безопасность небанковских организаций

Занятие 2. Программное обеспечение для контроля подлинности документов (2 час.)

1. Обзор программного обеспечения для контроля подлинности документов
2. Технологии компании ЛанКрипто
3. Деловая игра «Урок Криптографии» (сайт www.teachingame.ru/crypto)

Занятие 3. Круглый стол «Информационная безопасность в финансово-кредитных организациях и предпринимательской деятельности» (3 час.)

Занятие 4. Влияние человеческого фактора на информационную безопасность в кредитно-финансовой сфере (2 час.)

1.Работа в группах. Решение кейс-задачи.

2.Групповая дискуссия по результатам решения кейса.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» представлено в Приложении 1 и включает в себя:

−план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

−характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

−требования к представлению и оформлению результатов самостоятельной работы;

−критерии оценки выполнения самостоятельной работы.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые модули/разделы/ темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежу-точная аттестация
1	Тема 1. Информационная безопасность в	ПК-11 Способность анализировать и использовать	Методы идентификации, оценки уровня	УО-4	ПР-1

	предпринимательской деятельности Тема 2. Концепции информационной безопасности коммерческого банка	различные источники информации для проведения экономических расчетов	рисков потери информации в распределённых финансовых системах		
			Идентифицировать риски и рассчитывать уровень рисков потерь информации в распределённых финансовых системах	ПР-11	ПР-1
			Навыками идентификации и оценки уровня рисков потерь информации в распределенных финансовых системах	ПР-11	ПР-1
	Занятие 4. Влияние человеческого фактора на информационную безопасность в кредитно-финансовой сфере	ПК-12 Способность составлять прогноз основных социально-экономических показателей деятельности предприятия, отрасли, региона и экономики в целом	Методы, модели и инструменты прогнозирования показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	ПР-11	ПР-1
			Составлять прогнозы показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	ПР-11	ПР-1
			Методикой прогнозирования показателей, характеризующих последствия утраты информации для	ПР-11	ПР-1

			предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом		
	Тема 3. Безопасность электронных систем финансовых организаций	ПК-14 Способность к применению теоретических знаний для решения практических проблем рационального и эффективного использования экономических ресурсов при осуществлении экономического выбора	Методы и практики информационной защиты распределённых финансовых систем, вопросы нормативно-правового регулирования рисков потери информации и создания инфраструктуры рынка средств защиты информации	УО-4	ПР-1
			Применять на практике методы информационной защиты распределённых финансовых систем, использовать возможности инфраструктуры рынка средств защиты информации для защиты информации предприятия, организаций, в том числе финансово-кредитных организаций, для обеспечения экономической безопасности	ПР-10	ПР-1
			Навыками организации защиты информации предприятия, организации, в том числе финансово-	ПР-10	ПР-1

			кредитной, на основе эффективного использования возможностей инфраструктуры рынка		

Типовые вопросы тестов, докладов для участия в работе круглого стола, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2019. — 325 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-432966

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учеб. пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — М. : Издательство Юрайт, 2019. — 342 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-441287

3. Внуков, А. А. Защита информации : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 261 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/zaschita-informacii-444046

4. Внуков, А. А. Защита информации в банковских системах : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 246 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/zaschita-informacii-v-bankovskih-sistemah-414083

5. Хрусталев, Е.Ю., Елизарова, М.И. Концептуальные основы построения системы информационной безопасности производственного предприятия [Электронный ресурс] // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2017. - № 130 (06). - Режим доступа: https://cyberleninka.ru/article/n/kontseptualnye-osnovy-postroeniya-sistemy-informatsionnoy-bezopasnosti-proizvodstvennogo-predpriyatiya

6. Козьминых С.И. Моделирование обеспечения информационной безопасности объекта кредитно-финансовой сферы [Электронный ресурс]//Финансы: теория и практика. -2018. - № 22(5). – С. 105-121

https://cyberleninka.ru/article/n/modelirovanie-obespecheniya-informatsionnoy-bezopasnosti-obekta-kreditno-finansovoy-sfery

Дополнительная литература

(печатные и электронные издания)

1. Банковская система и новые финансовые технологии - вместе от кризиса к устойчивому развитию : сборник статей / Н.Э. Соколинская, В.Е. Косарев. — Москва : Русайнс, 2017. — 96 с. — ISBN 978-5-4365-1829-9.

2. Бакулина, А.А., Попова, В.В. Влияние финтеха на безопасность банковского сектора [Электронный ресурс] // Экономика. Налоги. Право. – 2018. - № 2. – С. 84-89.

3. Демьянова Е.А. Критерии оценки рисков развития компаний в условиях внедрения финансовых технологий // Финансы: теория и практика. 2017. Т. 21. Вып. 4. С. 182–190

4. Канашевский, В.А. Банковская тайна и использование банками услуг аутсорсинга информационной безопасности [Электронный ресурс]// Lex Russica/ - 2018. - № 7(140)/ - С. 92-97.

https://cyberleninka.ru/article/n/bankovskaya-tayna-i-ispolzovanie-bankami-uslug-autsorsinga-informatsionnoy-bezopasnosti

5.Мальцев, Г.Н. , Панкратов, А.Н. , Лесняк, Д.А. Исследование вероятностных характеристик изменения защищённости информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. – 2015. - № 1. – С. 50-58.

6.Ревенков, П.В., Бердюгин, А.А. Расширение профиля операционного риска в банках при возрастании DDOS-угроз // Вопросы кибербезопасности. – 2017. - № 3(21). – С. 16-23.

7.Сусляков, О.Н., Сергиенко, Н.С. Страхование как перспективный механизм защиты информации // Вестник Московского финансово-юридического университета. – 2015. - № 4. – С. 69-76.

8. Mumenthaler, C. (2018) Fair risk assessment in the era of big data, EY, available at https://www.swissre.com/risk-knowledge/driving-digital-insurance-solutions/fair-risk-assessment.html

9. New paper examines central bank digital currency models (2017) //Central banking.com URL: https:// www.centralbanking.com/central-banks/currency/digitalcurrencies/3225036/new-paper-examines-central-bankdigital-currency-models

10.Naydenov, R., Liveri, D., Dupre, L. and Chalvatzi, E. (2015) Secure Use of Cloud Computing in the Finance Sector, European Union Agency for Network and Information Security, available at https://www.enisa.europa.eu/publications/cloud-in-finance, accessed 03 October 2016.

11. The Dark Side of Fintech: Navigating the Hidden Risks of Digital Financial Services // Chipin. URL: https://www.chipin.com/fintech-cybersecurity-risks/

12. 12. The Pulse of Fintech Q22017. Global analysis of investment in Fintech // KPMG International Cooperative (“KPMG International”), август, 2017. URL: http://www.agefi.fr/sites/agefi.fr/files/fichiers/2017/08/pulse_of_ fintech-q2_2017_0.pdf

Нормативно-правовые материалы:

1. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 05.12.2016 N 646. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2. Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]:

утверждена Распоряжением Правительства от 28.07.29017 г. № 1632-р. – Режим доступа: http://static.government.ru/media /files/9gFM4FHj4Ps B79I5v7yLVuPgu4 bvR7M0.pdf

3. Основные направления развития финансовых технологий на период 2018-2020 гг. [Электронный ресурс]: Банк России.Финтех: развитие и проекты. – Электрон. дан. – Режим доступа: http://cbr.ru/fintech/

4. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" СТО БР ИББС-1.4-2018" [Электронный ресурс]: стандарт Банка России: принят и введен в действие Приказом Банка России от 06.03.2018 N ОД-568. – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_294526/

7. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения" (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 532-ст) из информационного банка "Отраслевые технические нормы"

8. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной налоговой службы и подведомственных ей организаций, а также формы паспорта безопасности этих объектов (территорий) [Электронный ресурс]: Постановление Правительства РФ от 07.04.2018 N 424. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_295341/

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Правительство Российской Федерации: http://government.ru/
2. Банк России: www.cbr.ru
3. Министерство финансов РФ: www.minfin.ru
4. Федеральная служба государственной статистики РФ : www.fsgs.ru

Перечень информационных технологий и программного обеспечения

1. Справочно-правовая система «КонсультантПлюс». Режим доступа: http://www.consultant.ru/
2. Справочно-правовая система «Гарант». Режим доступа: www.garant.ru
3. Справочная система «Кодекс». Режим доступа: http://www.kodeks.ru/
4. Сайт проекта «Уроки криптографии» teachingame.ru/crypto

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Реализация дисциплины «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» предусматривает следующие виды учебной работы: лекции, практические занятия, самостоятельную работу студентов, текущий контроль и промежуточную аттестацию.

Освоение курса дисциплины «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» предполагает рейтинговую систему оценки знаний студентов и предусматривает со стороны преподавателя текущий контроль за посещением студентами лекций, подготовкой и выполнением всех тестовых заданий, выполнением всех видов

самостоятельной работы.

Промежуточной аттестацией по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» является зачёт, который проводится в виде собеседования в режиме онлайн с проктором.

В течение учебного семестра обучающимся нужно:

− решить кейс-задачу (20 баллов);

− принять участие в работе круглого стола (30 баллов);

− принять участие в деловой игре «Урок криптографии» (10 баллов)

− успешно сдать зачёт в форме тестирования (40 баллов).

Студент считается аттестованным по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Критерии оценки по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» для аттестации на зачёте следущие: 61-100 баллов – «зачтено», 60 и менее баллов – «не зачтено».

Пересчет баллов по текущему контролю и самостоятельной работе производится по формуле:

$$P(n) = \sum_{i=1}^{m} \left[\frac{O_i}{O_i^{max}} \times \frac{k_i}{W} \right],$$

где: $W = \sum_{i=1}^{n} k_i^n$ для текущего рейтинга;

$W = \sum_{i=1}^{m} k_i^n$ для итогового рейтинга;

P(n) – рейтинг студента;

m – общее количество контрольных мероприятий;

n – количество проведенных контрольных мероприятий;

O_i – балл, полученный студентом на *i*-ом контрольном мероприятии;

O_i^{max} – максимально возможный балл студента по *i*-му контрольному мероприятию;

k_i – весовой коэффициент *i*-го контрольного мероприятия;

k_i^n – весовой коэффициент *i*-го контрольного мероприятия, если оно является основным, или 0, если оно является дополнительным.

В таблице приведена система бальной оценки результатов выполнения заданий по текущему контролю и самостоятельной работе студентов по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»:

Наименование контрольного мероприятия	Единица *j-ой* составной части контрольного мероприятия	Балл за выполнение *j-ой* составной части контрольного мероприятия	Максимально возможный балл по *i-ому* контрольному мероприятию O_i^{max}	весовой коэффициент *i*-го контрольного мероприятия k_i в общей рейтинговой оценке студента
Тесты (ПР-1) Тест В тесте 20 заданий	1 задание теста	2 балла/ 1 задание теста	40 баллов/тест	0,4
Выступление с докладом, содокладом, рецензией (круглый стол)	1 доклад	30 баллов	30 баллов	0,3
Решение кейс-задачи, представление	1 задача	20 баллов	20 баллов	0,2

результатов решения				
Деловая игра «Урок криптографии»		10 баллов	10 баллов	0,1
Итого:				1,0

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины «Финансовые технологии» включает:

1. Аудиторный фонд ШЭМ ДВФУ (корпус 22G).
2. Программное обеспечение: правовая информационная система «Консультант-плюс».
3. Техническое обеспечение – аудитория с мультимедийным оборудованием.
4. Презентации лекций ко всем темам дисциплины.
5. Учебная аудитория для проведения занятий лекционного типа; учебная аудитория для проведения занятий семинарского типа (практических занятий); учебная аудитория для текущего контроля и промежуточной аттестации на 25 посадочных мест, автоматизированное рабочее место преподавателя, переносная магнитно-маркерная доска, Wi-FI

Ноутбук Acer ExtensaE2511-30BO

Экран с электроприводом 236*147 см Trim Screen Line; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi; Подсистема специализированных креплений оборудования CORSA-2007 Tuarex; Подсистема видеокоммутации; Подсистема аудиокоммутации и звукоусиления; акустическая система для потолочного монтажа SI 3CT LP Extron; цифровой аудиопроцессор DMP 44 LC Extron.

Лицензионное программное обеспечение: Microsoft Office - лицензия Standard Enrollment № 62820593. Родительская программа Campus 3 49231495.

Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами видео-увеличителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками.

Учебный процесс обеспечен соответствующими противопожарным требованиям оборудованными аудиториями и лабораториями, предназначенными для проведения лекционных, лабораторных и практических занятий по дисциплинам учебного плана, а также помещениями для самостоятельной работы студентов. Посредством сети Wi-Fi, охватывающей все учебные корпуса, обучающиеся имеют доступ к сети «Интернет». Все аудитории, предназначенные для проведения занятий лекционного типа, оборудованы мультимедийными системами, проекторами, презентационными экранами.

Все здания ДВФУ спроектированы с учетом доступности для лиц с ограниченными возможностями. В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

План-график выполнения самостоятельной работы по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

№ п/п	Дата/Сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1.	1-9 неделя семестра	Изучение основной и дополнительной литературы	4	Кейс-задача (ПР-11), Доклад (УО-4) Деловая игра (ПР-10)
		Подготовка к текущей аттестации – подготовка к деловой игре	2	
		Подготовка доклада (содоклада) для участия в работе круглого стола	4	
		Подготовка материалов для решения кейс-задачи	3	
2.	10 нед	Подготовка к промежуточной аттестации зачёту в форме тестирования	5	Тест №1 (ПР-1)
	10 нед.	зачёт	-	
	Итого		18 час.	

Рекомендации по работе с литературой

При самостоятельной работе с рекомендуемой литературой студентам необходимо придерживаться определенной последовательности:

−при выборе литературного источника теоретического материала лучше всего исходить из основных понятий изучаемой темы курса, чтобы точно знать, что конкретно искать в том или ином издании;

−для более глубокого усвоения и понимания материала следует читать не только имеющиеся в тексте определения и понятия, но и конкретные примеры;

−чтобы получить более объемные и системные представления по рассматриваемой теме необходимо просмотреть несколько литературных источников (возможно альтернативных);

−не следует конспектировать весь текст по рассматриваемой теме, так как такой подход не дает возможности осознать материал; необходимо выделить и законспектировать только основные положения, определения и понятия, позволяющие выстроить логику ответа на изучаемые вопросы.

Рекомендации по выполнению самостоятельной работы

Тема 1. Информационная безопасность в предпринимательской деятельности

Вопросы для самопроверки:

1. Предпосылки и причины создания системы защиты корпоративной информации?
2. Какие самые распространённые способы несанкционированного доступа к корпоративной информации вам известны?

3. Назовите основные положения нормативного регулирования защиты банковской информации.

4. Какой способ защиты корпоративной информации от инсайдеров выделяют эксперты в области информационной безопасности?

5. Назовите основные принципы защиты корпоративной информации.

Подготовка доклада (сообщения) для выступления на заседании круглого стола

Доклад — вид самостоятельной научно — исследовательской работы, где автор раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды на нее.

Этапы работы над докладом.

1.Подбор и изучение основных источников по теме (рекомендуется использовать не менее 8 — 10 источников).

2.Составление библиографии.

3.Обработка и систематизация материала. Подготовка выводов и обобщений.

4.Разработка плана доклада.

5.Написание.

6.Публичное выступление с результатами исследования.

В докладе соединяются три качества исследователя: умение провести исследование, умение преподнести результаты слушателям и квалифицированно ответить на вопросы.

Отличительной чертой доклада является научный, академический стиль.

Академический стиль — это совершенно особый способ подачи текстового материала, наиболее подходящий для написания учебных и научных работ. Данный стиль определяет следующие нормы:

− предложения могут быть длинными и сложными;

− часто употребляются слова иностранного происхождения, различные термины;

− употребляются вводные конструкции типа «по всей видимости», «на наш взгляд»;

− авторская позиция должна быть как можно менее выражена, то есть должны отсутствовать местоимения «я», «моя (точка зрения)»;

− в тексте могут встречаться штампы и общие слова.

Общая структура такого доклада может быть следующей:

1.Формулировка темы исследования (причем она должна быть не только актуальной, но и оригинальной, интересной по содержанию).

2.Актуальность исследования (чем интересно направление исследований, в чем заключается его важность, какие ученые работали в этой области, каким вопросам в данной теме уделялось недостаточное внимание, почему учащимся выбрана именно эта тема).

3.Цель работы (в общих чертах соответствует формулировке темы исследования и может уточнять ее).

4.Задачи исследования (конкретизируют цель работы, «раскладывая» ее на составляющие).

5. Гипотеза (научно обоснованное предположение о возможных результатах исследовательской работы. Формулируются в том случае, если работа носит экспериментальный характер).

6. Методика проведения исследования (подробное описание всех действий, связанных с получением результатов).

7.Результаты исследования. Краткое изложение новой информации, которую получил исследователь в процессе наблюдения или эксперимента. При изложении результатов желательно давать четкое и немногословное истолкование новым фактам. Полезно привести основные количественные показатели и продемонстрировать их на используемых в процессе доклада графиках и диаграммах.

8. Выводы исследования. Умозаключения, сформулированные в обобщенной, конспективной форме. Они кратко характеризуют основные полученные результаты и выявленные тенденции. Выводы желательно пронумеровать: обычно их не более 4 или 5.

Рекомендуемые источники:

1. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 05.12.2016 N 646. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

2. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения" (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 532-ст)

из информационного банка "Отраслевые технические нормы"

3. Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной налоговой службы и подведомственных ей организаций, а также формы паспорта безопасности этих объектов (территорий) [Электронный ресурс]: Постановление Правительства РФ от 07.04.2018 N 424. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_295341/

4. Демьянова Е.А. Критерии оценки рисков развития компаний в условиях внедрения финансовых технологий // Финансы: теория и практика. 2017. Т. 21. Вып. 4. С. 182–190

5. Мальцев, Г.Н. , Панкратов, А.Н. , Лесняк, Д.А. Исследование вероятностных характеристик изменения защищённости информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. – 2015. - № 1. – С. 50-58.

Тема 2. Концепция информационной безопасности коммерческого банка

Вопросы для самопроверки.

1. К недостаткам новых моделей аутентификации на основе материального носителя относят:

а) сокращение времени обслуживания.

б) риск утраты всей информации при утере смартфона.

в) большее удобство пользователя.

г) большая простота использования злоумышленниками при похищении.

6. Недостатками биометрической аутентификации со стороны пользователя являются:

а) высокая чувствительность к изменению биометрических характеристик.

б) инвестиции во внедрение новой системы аутентификации.

в) неуникальность характеристик.

г) все варианты верные.

2. Среди преимуществ биометрической аутентификации со стороны коммерческого банка выделяют:

а) более высокий уровень безопасности.

б) инвестиции во внедрение новой системы аутентификации.

в) высокую чувствительность к изменению биометрических характеристик.

г) упрощение сбора и использования информации о клиентах.

8. К недостаткам биометрической аутентификации со стороны коммерческого банка:

а) более высокий уровень безопасности.

б) инвестиции во внедрение новой системы аутентификации.

в) высокая чувствительность к изменению биометрических характеристик.

г) все варианты верные.

3. В 2016-ом году заявление о переходе клиентов в перспективе 2-3 лет на биометрическую аутентификацию сделал:

а) глава Сбербанка.

б) глава Альфа-Банка.

в) глава ВТБ.

4. Верно ли утверждение: «Традиционная модель аутентификации является магистральным путем эволюции доступа к финансовым услугам»?

Рекомендуемые источники:

1. Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]: утверждена Распоряжением Правительства от 28.07.29017 г. № 1632-р. – Режим доступа: http://static.government.ru/media /files/9gFM4FHj4Ps B79I5v7yLVuPgu4 bvR7M0.pdf

3. Основные направления развития финансовых технологий на период 2018-2020 гг. [Электронный ресурс]: Банк России.Финтех: развитие и проекты. – Электрон. дан. – Режим доступа: http://cbr.ru/fintech/

4. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге" СТО БР ИББС-1.4-2018" [Электронный ресурс]: стандарт Банка России: принят и введен в действие Приказом Банка России от 06.03.2018 N ОД-568. – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_294526/

5. Канашевский, В.А. Банковская тайна и использование банками услуг аутсорсинга информационной безопасности [Электронный ресурс]// Lex Russica/ - 2018. - № 7(140)/ - С. 92-97.

6. Ревенков, П.В., Бердюгин, А.А. Расширение профиля операционного риска в банках при возрастании DDOS-угроз // Вопросы кибербезопасности. – 2017. - № 3(21). – С. 16-23.

Тема 3. Безопасность электронных систем финансовых организаций

Рекомендации для подготовки к решению кейс-задачи

Рекомендуемые источники:

1. Внуков, А. А. Защита информации : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2019. — 261 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/zaschita-informacii-444046

2. Внуков, А. А. Защита информации в банковских системах : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 246 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/zaschita-informacii-v-bankovskih-sistemah-414083

3. Хрусталев, Е.Ю., Елизарова, М.И. Концептуальные основы построения системы информационной безопасности производственного предприятия [Электронный ресурс] // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2017. - № 130 (06). - Режим доступа: https://cyberleninka.ru/article/n/kontseptualnye-osnovy-postroeniya-sistemy-informatsionnoy-bezopasnosti-proizvodstvennogo-predpriyatiya

4. Козьминых С.И. Моделирование обеспечения информационной безопасности объекта кредитно-финансовой сферы [Электронный ресурс]//Финансы: теория и практика. -2018. - № 22(5). – С. 105-121

https://cyberleninka.ru/article/n/modelirovanie-obespecheniya-informatsionnoy-bezopasnosti-obekta-kreditno-finansovoy-sfery

6. Внедрение и практическое применение современных финансовых технологий: законодательное регулирование : монография / Г.Ф. Ручкина, М.Ю. Березин, М.В. Демченко [и др.]. — М. : ИНФРА-М, 2019. — 161 с. — (Научная мысль). — www.dx.doi.org/10.12737/monography_5b59de9a8c7da8.15109074. - Режим доступа: http://znanium.com/catalog/product/978602

7. Сусляков, О.Н., Сергиенко, Н.С. Страхование как перспективный механизм защиты информации // Вестник Московского финансово-юридического университета. – 2015. - № 4. – С. 69-76.

Подготовка к участию в деловой игре «Уроки криптографии»

Ознакомиться материалами презентации «Ведение в криптографию» по ссылке: **https://www.dropbox.com/s/abap0gqd9dj21ec/%D0%98%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%D1%8F.pdf?dl=0**

Темы, затрагиваемые в презентации:

1. Описание науки, ввод определений.

2. Обзор истории криптографии от Древнего Египта до современного использования. Описание инструментов и алгоритмов шифрования с примерами взлома.

3. Последние научные разработки и направления исследований: шифрование звонков и сообщений, технологий Blockchain, квантовая криптографияи постквантовые алгоритмы.

Тема 4. Влияние человеческого фактора на информационную безопасность в кредитно-финансовой сфере

Рекомендуемые источники:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2019. — 325 с. Книга доступна в ЭБС biblio-online.ru

2. Внуков, А. А. Защита информации в банковских системах : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 246 с. Книга доступна в ЭБС biblio-online.ru

Режим доступа: https://biblio-online.ru/book/zaschita-informacii-v-bankovskih-sistemah-414083

3. Мальцев, Г.Н. , Панкратов, А.Н., Лесняк, Д.А. Исследование вероятностных характеристик изменения защищённости информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. – 2015. - № 1. – С. 50-58.

4. 6.Ревенков, П.В., Бердюгин, А.А. Расширение профиля операционного риска в банках при возрастании DDOS-угроз // Вопросы кибербезопасности. – 2017. - № 3(21). – С. 16-23.

5. 7.Сусляков, О.Н., Сергиенко, Н.С. Страхование как перспективный механизм защиты информации // Вестник Московского финансово-юридического университета. – 2015. - № 4. – С. 69-76.

6. Mumenthaler, C. (2018) Fair risk assessment in the era of big data, EY, available at https://www.swissre.com/risk-knowledge/driving-digital-insurance-solutions/fair-risk-assessment.html

7. New paper examines central bank digital currency models (2017) //Central banking.com URL: https:// www.centralbanking.com/central-banks/currency/digitalcurrencies/3225036/new-paper-examines-central-bankdigital-currency-models

8. Naydenov, R., Liveri, D., Dupre, L. and Chalvatzi, E. (2015) Secure Use of Cloud Computing in the Finance Sector, European Union Agency for Network and Information Security, available at https://www.enisa.europa.eu/publications/cloud-in-finance, accessed 03 October 2016.

9.Банковская система и новые финансовые технологии - вместе от кризиса к устойчивому развитию : сборник статей / Н.Э. Соколинская, В.Е. Косарев. — Москва : Русайнс, 2017. — 96 с. — ISBN 978-5-4365-1829-9.