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

«СОГЛАСОВАНО»
Руководитель ОП
_____ Кузнецова Н.В.
(подпись) (Ф.И.О. рук.ОП)
«_20» _сентября_____2018___ г.

«УТВЕРЖДАЮ»
Заведующая кафедрой «Финансы и кредит»
_____ Лялина Ж.И...
(подпись) (Ф.И.О. зав. каф.)
«__20__» ___сентября___2018____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Распределённые финансовые системы и экономическая безопасность: проблемы и пути решения»
Направление подготовки 38.04.01Экономика
программа «Международная экономика: инновационно-технологическое развитие»
Форма подготовки очная

курс 1 семестр 2
лекции 9 час.
практические занятия -9час.
лабораторные работы _____ час.
в том числе с использованием МАО лек. _____/пр.__/лаб.____ час.
всего часов аудиторной нагрузки 18 час.
в том числе с использованием МАО _ час.
самостоятельная работа 18 час.
в том числе на подготовку к зачёту__ час.
контрольные работы (количество)
курсовая работа / курсовой проект__семестр
зачёт 2 семестр

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ утвержденного приказом ректора от_07.07.2015_ №_12-13-1282_

Рабочая программа обсуждена на заседании кафедры «Финансы и кредит»
протокол № _1____ от «20__» ____сентября_____2018 г.

Заведующая кафедрой «Финансы и кредит» Ж.И.Лялина
Составитель:Л.К.Васюкова

Владивосток
2018

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «____» _____201_ г. №

Заведующий кафедрой _____ _____
(подпись) (И.О.Фамилия)

II. **Рабочая программа пересмотрена на заседании кафедры:**

Протокол от «____» _____20__ г. №

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in 38.04.01Economics, International Economics: Innovation and Technological Development

Course title: Distributed financial systems and economic security: problems and solutions.

Variable part of Block FTD Electives, 1 credits.

Instructor: Vasyukova Ludmila Konstantinovna, Associate Professor.

At the beginning of the course a student should be able to:

- the ability to use the basics of economic knowledge in various fields of activity;
- ability to self-organization and self-education;
- the ability to solve standard tasks of professional activity on the basis of information and bibliographic culture using information and communication technologies and taking into account the basic requirements of information security;
- the ability to collect, analyze and process the data necessary to solve professional problems;
- the ability to choose tools for processing economic data in accordance with the task, analyze the results of calculations and substantiate the findings.

Learning outcomes:

- the ability to analyze and use various sources of information for economic calculations (PC-11);
- the ability to make a forecast of the main socio-economic indicators of the enterprise, industry, region and the economy as a whole (PC-12);
- the ability to apply theoretical knowledge to solve practical problems of rational and efficient use of economic resources in the implementation of economic choice (PC-14).

Course description:

Objective: to familiarize students with various methods of protecting information in distributed financial systems.

Course objectives:

1. The study of the practice of using modern computer technology to protect the information of distributed financial systems.

2. Studying the fundamentals of state financial control of information loss risks and regulation of the infrastructure market of information protection media in order to ensure the economic security of market entities, the industry, the region and the economy as a whole.

3. Formation of risk management skills in information loss of distributed financial systems.

4. Acquaintance with the practice of information security in modern financial and credit organizations.

Main course literature:

1. Organizatsionnoyeipravovoyeobespecheniyeinformatsionnoybezopasnosti : uchebnik i praktikum dlya bakalavriata i magistratury / T. A. Polyakova, A. A. Strel'tsov, S. G. Chubukova, V. A. Niyesov ; pod red. T. A. Polyakovoy, A. A. Strel'tsova [Organizational and legal support of information security: a textbook and a workshop for undergraduate and graduate students / T. A. Polyakova, A. A. Streltsov, S. G. Chubukova, V. A. Niesov; by ed. T. A. Polyakova, A. A. Streltsova. - M.: Publishing house Yurayt, 2019. - 325 p. The book is available in the electronic library system biblio-online.ru]. Access Mode: https://biblio-online.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-432966

2. Kazarin, O. V. Nadezhnost' i bezopasnost' programmngo obespecheniya :ucheb. posobiye dlya bakalavriata i magistratury / O. V. Kazarin, I. B. Shubinskiy [Kazarin, O. Century. Reliability and security of software: studies. manual for bachelor and master / O. V. Kazarin, I. B. Shubinsky. - M.: Publishing house Yurayt, 2019. - 342 p. The book is available in the electronic library system biblio-online.ru]Access Mode:https://biblio-online.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-441287

3. Vnukov, A. A. Zashchitainformatsii :ucheb. posobiye dlya bakalavriata i magistratury / A. A. Vnukov. — 2-ye izd.,ispr. idop. — M. :Izdatel'stvoYurayt, 2019. — 261 s. [Vnukov, A. A. Information protection: studies. manual for undergraduate and

graduate / A. A. Vnukov. - 2nd ed., Corr. and add. - M.: Publishing house Yurayt, 2019. - 261 p. The book is available in the electronic library system biblio-online.ru]Access Mode:https://biblio-online.ru/book/zaschita-informacii-444046

4. Vnukov, A. A. Zashchitain formatsii v bankovski khsistemakh :ucheb. posobiye dlya bakalavriata i magistratury / A. A. Vnukov [Vnukov, A. A. Information security in banking systems: studies. manual for undergraduate and graduate / A. A. Vnukov. - 2nd ed., Corr. and add. - M.: Publishing house Yurayt, 2018. - 246 p. The book is available in the electronic library system biblio-online.ru]Access Mode:https://biblio-online.ru/book/zaschita-informacii-v-bankovskih-sistemah-414083

5. Khrustalev, Ye.YU., Yelizarova, M.I. Kontseptual'nyye osnovy postroyeniya sistemy informatsion noybezopasnosti proizvodstvennogo predpriyatiya [Khrustalev, E.Yu., Elizarova, M.I. Conceptual foundations of building an information security system for a manufacturing enterprise [Electronic resource] // Polythematic network electronic scientific journal of the Kuban State Agrarian University. - 2017. - № 130 (06).] Access Mode:https://cyberleninka.ru/article/n/kontseptualnye-osnovy-postroeniya-sistemy-informatsionnoy-bezopasnosti-proizvodstvennogo-predpriyatiya

6. Koz'minykh S.I. Modelirovaniye obespecheniya informatsionnoy bezopasnosti ob"yekta kreditno-finansovoy sfery [Kozminykh S.I. Modeling of ensuring information security of a credit and financial facility [Electronic resource] // Finance: theory and practice. -2018. - No. 22 (5). - p. 105-121] Access Mode: https://cyberleninka.ru/article/n/modelirovanie-obespecheniya-informatsionnoy-bezopasnosti-obekta-kreditno-finansovoy-sfery

Form of final control: credit

Аннотация к рабочей программе 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 38.04.01 Экономика, образовательная программа «Международная экономика: инновационно-технологическое развитие».

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 лекционные занятия (9 часов), практические занятия (9 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 «Математика», «Финансы», «Информационные системы в экономике» и другими и позволяет подготовить студентов к освоению таких дисциплин, как «Инновационное предпринимательство», «Концепции создания национальных инновационных систем», «Деятельность международных компаний в глобальной среде».

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 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-11Способность 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 международных компаний – субъектов инновационного предпринимательства
	Умеет	Составлять прогнозы показателей, характеризующихпоследствия утраты информации для предприятий, организаций, в том числе международных компаний – субъектов инновационного предпринимательства
	Владеет	Методикой прогнозирования показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе международных компаний – субъектов

		инновационного предпринимательства
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 международных компаний – субъектов инновационного предпринимательства
	Владеет	Навыками организации защиты информации предприятий, организаций, в том числемеждународных компаний – субъектов инновационного предпринимательства , 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:

− 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 предпринимательской деятельности Тема 2. Концепции информационной безопасности коммерческого банка	ПК-11Способность анализировать и использовать различные источники информации для проведения экономических расчетов	Методы идентификации, оценки уровня рисков потери информации в распределённых финансовых системах	УО-4	ПР-1
			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	ПР-11	ПР-1

			экономики в целом		
			Составлять прогнозы показателей, характеризующихп оследствия 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 предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	ПР-11	ПР-1
	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	ПР-10	ПР-1

			возможности инфраструктуры рынка средств защиты информации для защиты информации предприятия, организаций, в том числе финансово-кредитных организаций, для обеспечения экономической безопасности		
			Навыками организации защиты информации предприятия, организации, в том числе финансово-кредитной, на основе эффективного использования возможностей инфраструктуры рынка	ПР-10	ПР-1

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. Казарин, О. В. Надежность и безопасность программного обеспечения : учеб.пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — М. : Издательство Юрайт, 2018. — 342 с. Режим доступа:https://biblio-online.ru/book/nadezhnost-i-bezopasnost-programmnogo-obespecheniya-441287

2. Внуков, А. А. Защита информации : учеб.пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. https://biblio-online.ru/book/zaschita-informacii-444046

3. 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.

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

4. 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

5. 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)

Канашевский, В.А. Банковская тайна и использование банками услуг аутсорсинга информационной безопасности [Электронный ресурс]// LexRussica/ - 2018. - № 7(140)/ - С. 92-97. https://cyberleninka.ru/article/n/bankovskaya-tayna-i-ispolzovanie-bankami-uslug-autsorsinga-informatsionnoy-bezopasnosti

2. 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

3. 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

4.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.

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

6. 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/9gFM4FHj4PsB79I5v7yLVuPgu4 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/

6. 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"

7. 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 результатов решения	1 задача	20 баллов	20 баллов	0,2
Деловая игра «Урок		10 баллов	10 баллов	0,1

криптографии»				
Итого:				1,0

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для осуществления образовательного процесса по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» необходимы:

1) учебная аудитория с мультимедийным проектором и экраном;

2) компьютерный класс с компьютерами, отвечающими следующими обязательными техническими требованиями для выполнения тестовых заданий, контрольной работы:

− каждый компьютер должен быть оборудован внешней или встроенной работающей веб-камерой;

− на компьютере должна быть установлена операционная система Windows7, Windows8, Windows8.1, Windows10 или MacOSверсии 10.9 или более новая;

− интернет-браузер GoogleChromeпоследней, на момент сдачи зачёта, версии;

− соединение с интернетом на скорости не ниже 1 Мбит в секунду;

− успешное прохождение проверки «Настройки компьютера» в приложении «Экзамус».

Продолжительность выполнения одного задания текущей или промежуточной аттестации – 40 мин.

В читальных залах Научной библиотеки ДВФУ предусмотрены рабочие места для людей с ограниченными возможностями здоровья, оснащены дисплеями и принтерами Брайля; оборудованные портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами, видеоувелечителем с возможностью регуляции цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья ДВФУ все здания оборудованы

пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной системы.

Материально-техническом обеспечение дисциплины

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
690922, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус G, каб. G313, учебная аудитория для проведения занятий лекционного типа; учебная аудитория для проведения занятий семинарского типа (практических занятий); учебная аудитория для курсового проектирования (выполнения курсовых работ); учебная аудитория для текущего контроля и промежуточной аттестации	34 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.	ЭУ0198072_ЭА-667-17_08.02.2018_Арт-Лайн Технолоджи_ПО ADOBE, ЭУ0201024_ЭА-091-18_24.04.2018_Софтлайн Проекты_ПО ESET NOD32, ЭУ0205486_ЭА-261-18_02.08.2018_СофтЛайн Трейд_ПО Microsoft

Приложение 1

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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

«СОГЛАСОВАНО»
Руководитель ОП

_____ Кузнецова Н.В.,
(подпись) (Ф.И.О. рук.ОП)
«____» _____20___ г.

«УТВЕРЖДАЮ»
Заведующая кафедрой «Мировая экономика»

_____ Кравченко А.А.,
(подпись) (Ф.И.О. зав. каф.)
«____» _____20____ г.

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

Направление подготовки 38.04.01Экономика

программа «Международная экономика: инновационно-технологическое развитие»

Форма подготовки очная

Владивосток

2018

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.	1-9неделя 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.	10нед	Подготовка к промежуточной аттестации зачёту в форметестирования	5	Тест №1 (ПР-1)
	10нед.	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]// LexRussica/ - 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, квантоваякриптографияипостквантовые 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.

Приложение 2

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

ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

«СОГЛАСОВАНО»
Руководитель ОП

_____ Кузнецова Н.В..
(подпись) (Ф.И.О. рук.ОП)
«____» _____20___ г.

«УТВЕРЖДАЮ»
Заведующая кафедрой «Мировая экономика»

_____ Кравченко А.А.,
(подпись) (Ф.И.О. зав. каф.)
«____» _____20____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»
Направление подготовки 38.04.01Экономика
программа «Международная экономика: инновационно-технологическое развитие»
Форма подготовки очная

Владивосток
2018

Паспорт
фонда оценочных средств
по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

Код и формулировка компетенции	Этапы формирования компетенции	
ПК-11Способность 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, характеризующихпоследствия 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

№ п/п	Контролируемые модули/разделы/ темы дисциплины	Коды и этапы формирования компетенций	Оценочные средства - наименование	
			текущий	промежу-

				контроль	точная аттестация
1	Тема 1. Информационная безопасность в предпринимательской деятельности Тема 2. Концепции информационной безопасности коммерческого банка	ПК-11Способность анализировать и использовать различные источники информации для проведения экономических расчетов	Методы идентификации, оценки уровня рисков потери информации в распределённых финансовых системах	УО-4	ПР-1
			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, характеризующихп оследствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли,	ПР-11	ПР-1

			региона и экономики в целом		
			Методикой 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
	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	ПР-10	ПР-1

			обеспечения экономической безопасности		
			Навыками организации защиты информации предприятия, организации, в том числе финансово-кредитной, на основе эффективного использования возможностей инфраструктуры рынка	ПР-10	ПР-1

Оценочные средства для текущей аттестации (типовые ОС по текущей аттестации и критерии оценки по каждому виду аттестации по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»)

Критерии оценки устного доклада (сообщения), в том числе выполненного в форме презентации (УО-4)

✓ 30баллов выставляется студенту, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно

✓ 25 баллов - доклад характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские

умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы

✓ 20 баллов - студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы/

✓ 10 балла - если доклад представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

✓ 5 баллов–в докладе допущено более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

✓ 0 баллов – доклад не представлен

Критерии оценки решения кейс-задачи (ПР-11)

20 баллов - выставляется, если студент выполнил все задания кейса, аргументировал свои выводы, проиллюстрировав их статистическими данными выразил своё мнение по сформулированной проблеме, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, информация нормативно-правового характера. Продемонстрировано знание и владение навыком самостоятельной работы; методами и приемами анализа. Фактических ошибок, связанных с пониманием проблемы, нет.

15 баллов– выполнено 80% задания кейса, работа студента характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания
заданий кейса. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки.
Фактических ошибок, связанных с пониманием проблемы, нет.

10 – выполнено не менее 50 заданий кейса, проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования результатов выполненных заданий. Привлечены основные источники по рассматриваемой теме кейса.

5 баллов – выполнено более 50% заданий кейса, допущено три ошибки смыслового содержание.

2 балла - выполнено менее 50% заданий кейса, допущено более трех ошибок смыслового содержание.

0 баллов – решение кейса не представлено.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

Текущая аттестация студентов. Текущая аттестация студентов по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» проводится в форме контрольных мероприятий (тестовые задания, контрольная работа) по оцениванию фактических результатов обучения студентов.

Объектами оценивания выступают:

− степень усвоения теоретических знаний (определяется по результатам на вопросы теста);

− уровень овладения практическими умениями и навыками по всем видам учебной работы (определяется по результатам решения кейс-задачи, участия в работе круглого стола, участия в деловой игре);

− результаты самостоятельной работы (задания и критерии оценки размещены в Приложении 1).

Промежуточная аттестация студентов. Промежуточная аттестация студентов по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения» проводится в соответствии с локальными нормативными актами ДВФУ.

Вид промежуточной аттестации –зачёт(1 семестр), состоящий из тестирования по вопросам, представленным в Приложении 1.

Краткая характеристика процедуры применения используемого оценочного средства. В результате посещения аудиторных занятий, выполнения практических заданий, самостоятельной работы студент последовательно осваивает материалы дисциплины и изучает материалы, необходимые для прохождения процедуры сдачи экзамена, представленные в структурном элементе Фонда оценочных средств (ФОС). В ходе промежуточной аттестации студент отвечает на вопросы преподавателя(перечень вопросов размещен в структурном элементе ФОС. Критерии оценки студента на зачётепредставлены в структурном элементе ФОС. Критерии оценки текущей аттестации – контрольная проверка знаний (тестовые задания, решения кейс-задачи, заданий контрольной работы, выступления с докладом) представлены в структурном элементе ФОС.

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**Критерии**	**Показатели**
ПК-11 Способность анализировать и использовать различные источники информации для проведения экономических расчетов	знает (порого-вый уровень)	Методы идентификации, оценки уровня рисков потери информации в распределённых финансовых системах	Знание методов, инструментов управления рисками потерь информации в распределённых финансовых системах, защиты информации предприятий, организаций, в том числе финансово-кредитных организаций, для обеспечения экономической безопасности	Формулирует экономическое содержание методов управления рисками потерь информации в распределённых финансовых системах

	умеет (продви-нутый)	Идентифицировать риски и рассчитывать уровень рисков потерь информации в распределённых финансовых системах	Умение идентифицировать риски потерь информации (в том числе кибер-рисками) в распределённых финансовых системах, выбрать наиболее эффективные способы защиты информации предприятий и организаций, в том числе финансово-кредитных организаций	Способен идентифицировать риски потерь информации, в том числе кибер-риски), исследовать причины-последствия реализации рисков, выбрать наиболее экономически эффективный способ защиты информации
	владеет (высокий)	Навыками идентификации и оценки уровня рисков потерь информации в распределенных финансовых системах	Владеет приёмами и инструментами защиты информации в финансовых системах предприятий и организаций, в том числе финансового-кредитного сектора	Способен организовать систему защиты финансовой информации предприятий и организаций, в том числе финансово-кредитного сектора
ПК-12 Способность составлять прогноз основных социально-экономических показателей деятельности предприятия, отрасли, региона и экономики в целом	знает (поро-говый уровень)	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	Знает методы, модели и инструменты прогнозированияпоказателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	Формулирует экономическое содержание показателей прогнозирования последствий утраты информации для хозяйствующих субъектов, субъектов финансового рынка, отрасли, экономики региона
	умеет (продви-нутый)	Составлять прогнозы показателей,	Умеет выбирать показатели для составления	Способен выбрать показатели, характеризующие

		характеризующихпоследствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	прогноза потерь от утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	уровень потерь от утраты информации, для составления прогноза
	владеет (высокий)	Методикой прогнозирования показателей, характеризующих последствия утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	Владеет навыками расчёта выбранных для составления прогноза показателей, характеризующих уровень потерь от утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом	Способен произвести расчёты показателей, характеризующих уровень потерь от утраты информации для предприятий, организаций, в том числе финансово-кредитного сектора, отрасли, региона и экономики в целом, для составления прогноза
ПК-14 Способность к применению теоретических знаний для решения практических проблем рационального и эффективного использования экономических ресурсов при осуществлении	знает (порого-вый уровень)	Методы и практики информационной защиты распределённых финансовых систем, вопросы нормативно-правового регулирования рисков потери информации и создания инфраструктуры	Знает методы и практики организации информационной защиты финансовой информации, основы нормативно-правового регулирования информационных рисков	Формулирует содержание и основные положения практик организации защиты финансовой информации, формулирует основные положения нормативного регулирования информационных рисков (в том числе отраслевого регулирования)

экономического выбора		рынка средств защиты информации		
	умеет (продви-нутый)	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	Способен применить на практике методы и возможности инфраструктуры рынка средств информационной защиты для защиты финансовой информации хозяйствующих субъектов, в том числе субъектов финансового рынка	Способен выбрать наиболее эффективные методы и лучшие практики, в том числе программное обеспечение, современные финансовые технологии для организации защиты финансовой информации хозяйствующих субъектов, в том числе субъектов финансового рынка
	владеет (высокий)	Навыками организации защиты информации предприятия, организации, в том числе финансово-кредитной, на основе эффективного использования возможностей инфраструктуры рынка	Владеет навыками использования возможностей инфраструктуры рынка средств информационной защиты для организации защиты информации хозяйствующих субъектов, в том числе субъектов финансового рынка	Способен организовать защиту информации хозяйствующих субъектов, в том числе субъектов финансового рынка, с использованием программного обеспечения, современные финансовые технологии

Комплект тестовых заданий для проведения текущей аттестации по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

(ПР-1)

Тестовое задание № 1.

1. Самым распространённым приёмами несанкционированного доступа к корпоративной финансовой информации являются:

а) использование резервных копий;

б) физический доступ к местам хранения и обработки корпоративной финансовой информации;

в) нарушение сотрудниками компаний регламентов доступа к информации;

г) действия инсайдеров.

2. Безопасность автоматизированных систем обработки информации (АСОИ) достигается:

а) обеспечением конфиденциальности информации;

б) ограничением доступа сотрудников к информации;

в) целостности компонентов и ресурсов системы;

г) доступности информации авторизованным субъектам системы.

3. К рискам, приводящим к потере целостности и доступности компонентов и ресурсов АСОИ, которые могут быть застрахованы, относятся:

а) стихийные бедствия: наводнения, ураганы и др.;

б) техногенные аварии: отключение электроэнергии, пожары и др.;

в) противоправные действия третьих лиц;

г) неумышленные действия персонала компании;

д) халатность сотрудников компании.

4. К аппаратным технологиям финансовой отрасли относят:

а) P2P-технологии.

б) технологии аутентификации.

в) блокчейн.

г) все варианты верные.

5. Среди программных технологий выделяют:

а) скоринг.

б) роботизацию.

в) блокчейн.

г) все варианты верные.

6. Верно ли утверждение: «При традиционной модели аутентификации достаточно было отпечатков пальцев для получения доступа ко всем счетам пользователя в одном банке»?

7. Новые модели аутентификации, использующие материальный носитель, делятся на:

а) основанные на пластиковых картах.

б) основанные на смартфонах как носителях информации.

в) основанные на биометрической аутентификации.

г) все варианты верные.

8.Неэкономические показатели эффективности информационных технологий характеризуют:

а) прирост благосостояния владельцев;

б) деятельность предприятия с точки зрения собственников;

в) аспекты деятельности проекта, не имеющие прямого денежного выражения;

г) деятельность предприятия с точки зрения внешних участников;

д) нет ответа.

9. Среди основных проблем законодательного регулирования финансово-технологической отрасли выделяют (выберите все верные ответы):

а) наличие жесткого законодательного регулирования.

б) пристальное внимание со стороны контролирующих органов.

в) отсутствие регулирования интернета и связи.

г) сложность защиты интересов инициаторов финтех-проектов в случае возникновения проблем.

10. С точки зрения готовности к инновационными форматам потребления информационных услуг в финансовой сфере наиболее передовыми в России являются:

а) сельские населенные пункты.

б) маленькие города.

в) мегаполисы.

г) города с населением до 100 тыс. жителей.

11.Страной-лидером в плане развития технологий и законодательного регулирования в сфере финтех-деятельности на постсоветском пространстве является:

а) Россия.

б) Белоруссия.

в) Эстония.

12. Согласно определению финтеха, интеграция финансовой деятельности с каким видом технологий лежит в его основе:

а) промышленных.

б) информационных.

в) медицинских.

г) нет верного ответа, т.е. ни одни из перечисленных выше технологий не подходят.

13. Для раннего этапа развития финтеха характерно внедрение именно такового вида банковского обслуживания:

а) персонального.

б) дистанционного.

в) вежливого.

г) доверительного.

14. К основным факторам развития финтеха не относится:

а) рост потенциала информационных технологий.

б) расширение применения информационных технологий.

в) формирование сравнительно конечного набора продуктов и сервисов.

15. Рост потенциала информационных технологий характеризуется возможностью:

а) аутентификации пользователя по карте и пин-коду.

б) аутентификации пользователя по его биометрическим характеристикам.

в) оба варианта верные.

8. К предпосылкам возникновения современного финтеха не относят:

а) консервацию потребительских привычек.

б) качественный и количественный рост информационных технологий.

в) потребность финансовых и нефинансовых организаций в повышении эффективности.

г) все варианты верные.

16. Неструктурированной информацией разного формата называются:

а) большие данные;

б) системы скоринга;

в) клиринговые системы;

г) факторинг.

17. Среди основных характеристик расширения доступа к финансовым услугам выделяют:

а) возможность получения всех необходимых услуг в одной точке благодаря интеграции сервисов;

б) круглосуточный доступ к финансовым услугам;

в) информационную прозрачность;

г) все варианты верные.

18. Верно ли данное утверждение: «Технологии аутентификации и P2P-технологии относят к группе аппаратных финансовых технологий»?

19. Ситуация, когда вся информация о сделках клиента становится известной банку и собирается и обрабатывается в автоматическом режиме, а банк может использовать эту информацию в своих интересах, является основой для такого недостатка виртуализации с точки зрения потребителей, как:

а) несоответствие привычкам отдельных групп потребителей.

б) рост контроля со стороны финансовых институтов.

в) рост информационных рисков.

20. Верно ли данное утверждение: «В Республике Корея со стороны регулятора рынка ценных бумаг фактически прозвучали рекомендации приравнять ICO к IPO, и ввести соответствующие требования к его проведению»?

Порядок формирования

оценкивыполнения тестовых задач и заданий

по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

За каждый правильно отвеченный вопрос студент получает **2,0 балла.**

Суммарное количество баллов за решённый тест определяется как сумма баллов, полученных за правильно отвеченные вопросы. Максимальная сумма баллов за один тест – **40 баллов**(2,0балла х 20 вопросов).

Кейс-задача (ПР-15)

по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

Гражданин С. работал в ООО «Региональная страховая компания» в должности директора Департамента продаж. Был уволен после того как переправил по корпоративной почте на свой личный почтовый адрес и адрес супруги файлы, содержащие информацию о страховых продуктах Общества. Этот факт, вскрытый сотрудниками Департамента информационных технологий, проводивших

контрольную проверку использования корпоративной почтовой системы, послужил основанием для проведения служебного расследования.

С. в объяснительной записке написал, что файлы ему были нужны для проведения презентации потенциальным партнерам продуктов и услуг Общества. По его мнению, среди пересланных документов не было секретных. Комиссия с доводами С. не согласилась и постановила применить к нему дисциплинарное взыскание в виде увольнения. Приказ об увольнении ссылался на пп. «в» п.6 ч.1 ст. 81 ТК РФ.

Первая судебная инстанция, куда обратился С., встала на сторону истца и признала увольнение незаконным. Основанием для такого судебного решения послужило непредоставление ответчиком трудового договора с С., нечеткие формулировки Правил внутреннего трудового распорядка и отсутствие Положения о коммерческой тайне или иных нормативных документов, регламентирующих данный вопрос.

Однако суд апелляционной инстанции более внимательно отнесся к тем мерам, которые ответчик предпринимает для защиты своей конфиденциальной информации, и счел их достаточными для того, чтобы считать С. виновным в разглашении коммерческой и служебной тайны.

Источник: Определение Московского городского суда по делу № 4г/9-9007/2014 от 20.10.2014

Порядок формирования оценки за решение кейс-задачи по дисциплине «Распределенные финансовые системы и экономическая безопасность: проблемы и пути решения»

20 баллов - выставляется, если студент выполнил все задания кейса, аргументировал свои выводы, проиллюстрировав их статистическими данными выразил своё мнение по сформулированной проблеме, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, информация нормативно-правового характера. Продемонстрировано

знание и владение навыком самостоятельной работы; методами и приемами анализа. Фактических ошибок, связанных с пониманием проблемы, нет.

15 баллов– выполнено 80% задания кейса, работа студента характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания
заданий кейса. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки.
Фактических ошибок, связанных с пониманием проблемы, нет.

10 – выполнено не менее 50 заданий кейса, проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования результатов выполненных заданий. Привлечены основные источники по рассматриваемой теме кейса.

5 баллов – выполнено более 50% заданий кейса, допущено три ошибки смыслового содержание.

2 балла - выполнено менее 50% заданий кейса, допущено более трех ошибок смыслового содержание.

0 баллов – решение кейса не представлено.

Темы докладов для участия в работе круглого стола «Информационная безопасность в финансово-кредитных организациях и предпринимательской деятельности»

1. Особенности формирования систем защиты информации традиционных финансовых компаний с инновационным продуктом
2. Матрица бизнес-моделей в эпоху внедрения современных финансовых технологий
3. Управление риском нарушения информационной безопасности коммерческого банка при аутсорсинге

4. Основные положения Доктрины информационной безопасности Российской Федерации в контексте экономической безопасности финансового сектора

5.Инструменты обеспечения конфиденциальности информации розничными операторами своих целей при внедрении финансовых технологий

6.Российская и зарубежная практика внедрения финансовых технологий операторами связи и социальными сетями

7.Модели сотрудничества в области защиты информации социальных сетей и финансовых институтов

8. Государственное регулирование вопросов информационной безопасности финансово-кредитных институтов: зарубежный опыт, российская практика

9. Особенностиформирования системы информационной защиты экосистемы Сбербанка

10. Экосистемы финансовых институтов: взгляд экспертов по информационной защите

11. Цифровизация российского страхового рынка: проблемы и перспективы развития

12. Особенности современного подхода к информационной защищённости нефинансовых компаний на рынке финансовых услуг

13. Страхование киберрисков в банковской деятельности: зарубежный опыт и российская практика.

14. Аудит информационной безопасности в финансово-кредитных организациях.

Порядок формирования
оценки за представление доклада для участия в работе круглого стола «Информационная безопасность в финансово-кредитных организациях и предпринимательской деятельности»

✓ 30 баллов выставляется студенту, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно

✓ 20 баллов - доклад характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы

✓ 10 баллов - студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы/

✓ 5 баллов - если доклад представляет собой пересказанный или полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

✓ 2 балла – в докладе допущено более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

✓ 0 баллов – доклад не представлен

Описание деловой игры «Уроки криптографии»

(ПР-10)

Цели проведения деловой игры:

1. Расширение кругозора и повышение интереса к изучению дисциплин в областиинформационной безопасности.

2. Развитие творческой инициативы и интереса к образовательному процессу, научной деятельности и исследовательской работе.

3. Внедрение игровых технологий в образовательный процесс.

4. Повышение качества образования.

5. Содействие в профессиональной ориентации

.

Порядок участия в деловой игре:

Для проведения деловой игре необходимо:

1.Зарегистрироваться на сайтепроекта:teachingame.ru/crypto

2.Скачать и изучить материалы: инструкция, презентация, правила игры.

3.Провести урок с помощью презентации и деловой игры.

4.Провести анонимный онлайн-опрос студентов после завершения игры, для этого:

а) попросить студентов перейти на сайт menti.comb.

б) ввестиключ: 40 11 42c.

в) ответитьна 7 вопросов

5.Пройтионлайн-опрос для преподавателейпо ссылке: goo.gl/forms/nvjVtCaxSYc3J6bK2

6.По возможности, прислать фотографии с занятия на почту info@teachingame.ru.

Образовательная игра показывает, как работает криптография,на каких принципах она построена, затрагивает область знаний о математических алгоритмах. Можно проводить на занятиях по вопросам организации защиты информации. Рекомендованное количество участников от 16 до 35.

Время проведения от 30 минут до 1 часа.

Необходимые знания: основы алгоритмического мышления. В игре используются простые шифры, имеющие свои исторические аналогии, на освоение которых требуется от 2 до 10 минут

Авторы: Караева Алина, Солдатов Иван, Иванов Максим

Правила игры.

Все игроки делятся на две команды: «Синие» и «Красные». Затем «Синие» еще раз делятся пополам на «Синие1» и «Синие2».

«Синие1», по условиямигры, должны будут передавать сообщения своим коллегам «Синим2», а «Красные»попытаться взломать как минимум два сообщения из пяти.

Перед началом игры «Синие1» и «Синие2» получают от ведущего ключи к шифрам (специально заполненную форму) и вместе держат их в секрете на протяжениивсей игры.

Рекомендуемый размер каждого зашифрованного сообщения –от 20 символов.

Каждый метод шифрования используется один разза игру.

Каждая команда имеет доступ к правилам игры и описанию шифров. Порядок использования шифров команда «Синие 1»определяет сама.

Побеждают синие или красные, возможно, чтообе команды проигрывают, если не выполняют условия.

Пользоватьсясредствами связи (телефон, компьютер и прочее) не допускается.

Порядок формирования

оценки за участие в деловой игре «Уроки криптографии»

За активное участие в работе команды, выполнение заданий по сценарию игры студент получает **10 баллов.**

Оценочные средства для проверки формированности компетенций

Код и формулировка компетенции	Задание
ПК-11 Способность анализировать и использовать различные источники информации для проведения экономических расчетов	**Кейс-задача 1.** Предприниматель А. зарегистрировался на одной из краудфандинговых платформ – «Новая Атлантида». Пролистывая список бизнес-проектов, А. выбрал перспективный проект по организации мобильного сервиса доставки свежих фермерских продуктов по ценам, доступным для широкого круга потребителей. Для реализации проекта необходимы инвестиции в размере 150 тысяч рублей. Условия, на которых осуществлялось привлечение денег: под 25% годовых сроком на год с равными выплатами раз в два месяца. Вскоре был заключен и заверен электронной подписью договор между предпринимателем А. и заемщиком Н. Первый платеж пришел в срок, второй платёж Н. задержал больше чем на месяц, сославшись на непредвиденные расходы, а после заемщик Н. вообще прекратил выплаты долга и процентов по нему. Предприниматель А. обратился к организаторам платформы, но выяснилось, что платформа ответственности по заключенным с ее помощью договорам не несет. Определите: 1) Какая информация о лицах, привлекающих инвестиции, и инвестиционных проектах должна предоставляться участникам платформы? Какую форму представления этой информации следует обеспечить организаторам платформы? 2) Кто и как должен проверять достоверность этой информации и нести ответственность в случае ее недостоверности? 3) Какие законодательные и регуляторные меры существуют для защиты интересов инвесторов при P2P-кредитовании? **Задача 2.** Страховая компания разработала страховой продукт по страхованию рисков, приводящих к потере целостности и доступности компонентов и ресурсов АСОИ. Страхователь, заполняя заявление на страхование, выделил следующие риски: а) стихийные бедствия: наводнения, ураганы и др.; б) техногенные аварии: отключение электроэнергии, пожары и др.; в) противоправные действия третьих лиц; г) неумышленные действия персонала компании. д) халатность сотрудников компании. Определите, какие риски не подлежат страхованию? Обоснуйте свой ответ, с использованием критериев страхуемости рисков. **Задача 3.** Вам необходимо принять решение о создании фермы для майнига криптовалют с учетом следующих параметров: стоимость майнига в Венесуэле ниже, чем в России, в свою очередь, в США она выше, чем в России, и ниже, чем в Норвегии. Какую страну Вы выберите?

Код и формулировка компетенции	Задание
ПК-12 Способность составлять прогноз основных социально-экономических показателей деятельности предприятия, отрасли, региона и экономики в целом	**Кейс-задача 1.** На одном из форумов размещена информация о недавно образовавшейся инициативе NewSilkRoadBit, которую основала группа инвесторов, вкладывающая деньги по всему миру в майнинг разнообразных криптовалют. Согласно сайту, NewSilkRoadBit – это группа компаний, зарегистрированных в нескольких странах, а большинство принадлежащих им криптоферм расположено в Европе и Азии, что позволяет получать дополнительную прибыль от колебаний цен на национальные валюты и льготных тарифов на электричество. NewSilkRoadBit планирует выпустить свою криптовалюту, чтобы еще больше увеличить возможности для заработка своих инвесторов и тем самым реализовать все возможности «Шелкового пути» в новой цифровой реальности. 1) На основании каких данных инвестор может принять решение о степени рискованности предложения NewSilkRoadBit, если он не является экспертом в отрасли, а срок возврата денег даже первым участникам еще не подошел? 2) Может ли регулятор (Банк России) предпринять какие-либо действия в отношении NewSilkRoadBit, и если да, то на каком основании, если никаких жалоб на компанию нет, а деятельность по использованию иностранных цифровых активов пока никак не регулируется? Как бы вы предложили регулировать такую деятельность? 3) Как добросовестные организаторы криптовалютного проекта могли бы сигнализировать потенциальным клиентам о своей добропорядочности и отсутствии «пирамидальности»? **Задача 2.** Собственник банка, в котором Вы работаете директором по развитию, предложил подумать над использованием комбинированной модели второго типа при разработке предложений по развитию кредитных сервисов. Идентифицируйте риски реализации следующих проектов? 1) Создание под брендом банка автономного подразделения, являющегося оператором краудлендинговой платформы. 2) Внедрение в клиентском онлайн-банке сервиса «Стакан кредитных предложений», куда будут включаться не только предложения по кредитам от банка, но и от других кредиторов с ним сотрудничающих. 3) Перевод всего кредитного бизнеса банка на краудлендинговую основу. Выберите проект по критерию минимизации рисков информационных потерь. **Задача 3.** Верно ли данное утверждение: «При принятии решения о создании краудлендинговой платформы Вы особое внимание уделите проработке такого фактора ее успеха, как обеспечение высокого уровня кибербезопасности»?. Обоснуйте свой ответ.

Код и формулировка компетенции	Задание
ПК-14 Способность к применению теоретических знаний для решения практических проблем рационального и эффективного использования экономических ресурсов при осуществлении экономического выбора	**Кейс-задача 1.** Гражданин В. при оплате приобретения на электронном сервисе авиакомпании авиабилета воспользовался кредитной картой с лимитом кредитования 110 тыс. рублей под 36% годовых. По условиям предоставления кредитной карты гражданин В. должен был получать уведомления обо всех операциях по карте, которые направлялись в личный кабинет пользователя. При приобретении авиабилета гражданин В. оформил заявку на приобретение платежа и был перенаправлен на страницу сайта, где открылось новое окно с формой оплаты и строчкой мелким шрифтом «совершается безопасный платеж». Оплата производилась на номер MANGO-кошелька. Как обычно при проведении онлайн платежа, гражданин В. получил смс-уведомление от банка с кодом, который нужно было ввести в соответствующую форму на сайте. После ввода гражданином В. кода подтверждения, на сайте отобразилось сообщение о сбое платежа. Гражданин В. запросил код еще раз и ввел его в форму на сайте. Таким образом, приобретаемые авиабилеты были оплачены дважды. Гражданин В. на следующий день обратился в банк с просьбой требованием блокировки транзакций и претензией по оспариванию операций. Банк отказал в удовлетворении требований гражданина В. Гражданин В. обратился в суд, и спустя 3 месяца после списания средств с карты, получил решение суда и законности отказа банка в блокировке транзакций и возврата излишне уплаченных денег. 1)Какова сумма долга, которую необходимо гражданину В. уплатить банку? 2) Как может потребитель финансовых услуг обезопасить себя от подобных ситуаций при покупке товаров и услуг в Интернете? Какими характеристиками должна обладать страница оплаты, поддерживаемая добросовестной организацией? **Задача 2.** Каким образом банки и регулятор могут содействовать повышению безопасности платежных операций в интернете (в том числе в ситуациях, когда внешние признаки сомнительных операций отсутствуют)? Нужны ли для этого какие-либо изменения в законодательстве? **Задача 3.** В проекте регулирования обращения криптоактивов от РАКИБ максимальный объем вложений, который может совершить в рамках ICO неквалифицированный инвестор, ограничивается суммой от 50 тыс. р. до 5 млн р. Обоснуйте вариант выбора объёма инвестиционных вложений инвестора.