Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

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

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«УПРАВЛЕНИЕ РИСКАМИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Информационно-аналитические системы финансового мониторинга
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

Королев
2020

Автор: профессор Шихнабиева Т.Ш. Рабочая программа дисциплины: «Управление рисками». – Королев МО: «Технологический университет», 2020.

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

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

Рабочая программа рассмотрена и одобрена на заседании кафедры:

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

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

Рабочая программа рекомендована на заседании УМС:

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

2

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

Целью изучения дисциплины является:

– получение обучаемыми достаточно полного представления о понятиях «информационных рисков», «оценке информационных рисков», «анализе информационных рисков» и «управлении информационными рисками», целях, задачах, методах управления информационными рисками при обеспечении комплексной безопасности предприятия;

– формирование профессиональных компетенций в сфере управления информационными рисками с использованием передового отечественного и мирового опыта в области обеспечения информационной безопасности современных предприятий.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
- ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности.

Профессиональные компетенции:

- ПК-9: способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
- ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Основными **задачами** дисциплины являются:

- определение основных понятий, связанных с экономическим обоснованием мероприятий при обеспечении информационной безопасности на современных предприятиях;

- раскрытие базовых составляющих экономической деятельности по обеспечению комплексной безопасности;
- ознакомление с основными подходами экономического обоснования разрабатываемых и существующих мер по информационной безопасности в государственных и коммерческих организациях;
- раскрытие базового уровня нормативно-законодательных и административно-технических направлений при экономическом обосновании мер по обеспечению комплексной безопасности;
- ознакомление с практическими вопросами по использованию современных технологий и средств экономического обоснования мер по обеспечения информационной безопасности на предприятии.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные подходы к процессу управления информационными рисками;
- организацию процесса риск-менеджмента в области информационной безопасности и его место в системе управления предприятием;
- требования к информационно-аналитическим документам в основных стандартах по управлению информационными рисками;
- сущность и виды рисков предприятия;
- формы отчетности в системе риск-менеджмента по защите информации;
- сущность и классификацию информационных рисков предприятия;
- показатели деятельности по информационной безопасности предприятия, учитывающие риски;
- алгоритмы управления информационными рисками корпорации;
- основные страховые информационные риски предприятия и способы защиты от них;
- основные виды страхования для покрытия информационных рисков предприятия.

Уметь:

- управлять работой по оценке и анализу информационных рисков;
- идентифицировать, оценивать, измерять, диагностировать информационные риски;
- представлять информацию об информационных рисках;
- проводить анализ эффективности деятельности по защите информации с учетом факторов риска в области информационной безопасности;
- оценивать рискованность проектов и вложений в активы по защите информации;

- управлять информационными рисками на основе инжиниринга по защите информации;
- использовать страховые продукты как способ снижения информационных рисков.

Владеть:

- основными методами организации работы при внедрении систем управления информационными рисками;
- математическим аппаратом анализа информационных рисков;
- методами защиты от информационных рисков;
- моделями оценки и анализа информационных рисков;
- способами защиты от информационных рисков с помощью страхования.

2. Место дисциплины в структуре ОПОП ВО

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

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы исследований информационной безопасности», «Основы управленческой деятельности» «Организационное и правовое обеспечение информационной безопасности», «Финансовое моделирование» и компетенциях: ОК-4,5,6,8, ОПК-2,3,4,5, ПК-3,6,8,9,10,11,12,13,14,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин «Информационная безопасность автоматизированных систем», «Актуальные проблемы финансов», «Мониторинг рынка страхования», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Организация информационно-аналитического обеспечения финансового мониторинга», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3.Объем дисциплины (модуля) и виды учебной работы

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

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр …	Семестр …	Семестр …
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
КСР	-	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час. Очное	Код компетенций
Шестой семестр				
Раздел (модуль) 1. Базовые основы по управлению информационными рисками				
Тема 1. Сущность и место управления информационными рисками в системе безопасности предприятия	2	2	2	ОПК-4,5; ПК-9,15.
Тема 2. Нормативно-правовые основы управления информационными рисками (отечественные	2	6	4	ОПК-4,5; ПК-9,15.

стандарты)				
Тема 3. Нормативно-правовые основы управления информационными рисками (международные стандарты)	2	6	2	ОПК-4,5; ПК-9,15.
Раздел (модуль) 2. Технологии управления информационными рисками				
Тема 4. Частные методики оценки и анализа информационных рисков	2	6	4	ОПК-4,5; ПК-9,15.
Тема 5. Корпоративные методики управления информационными рисками	4	6	4	ОПК-4,5; ПК-9,15.
Тема 6. Инструментальные средства анализа информационных рисков	4	6	2	ОПК-4,5; ПК-9,15.
Итого:	**16**	**32**	**18**	

4.2. Содержание тем дисциплины

Раздел 1. Базовые основы по управлению информационными рисками

Тема 1. Сущность и место управления информационными рисками в системе безопасности предприятия

Основы информационной безопасности бизнес-процессов. Информация и информационные процессы как ключевые элементы безопасного бизнеса. Существующие подходы обоснования стоимости систем защиты информации на предприятии: теоретико-прикладной и эмпирико-практический. Анализ использования на предприятиях теоретико-прикладного и эмпирико-практического подходов.

Тенденции развития служб информационной безопасности предприятий в области экономической оценки деятельности по защите информации: российская и международная практика управления информационными рисками.

Тема 2. Нормативно-правовые основы управления информационными рисками (отечественные стандарты)

Сущность, содержания и актуальность отечественного процесса управления информационными рисками при обеспечении информационной безопасности современных предприятий. Ключевые понятия: риск, уязвимость, угроза и ущерб; оценка риска.

Существующие требования, рекомендации и руководящие документы ФСТЭК и ФСБ России по управлению информационными рисками. Количественный и качественный анализ, экспертная и аналитическая оценка информационных рисков. Снижение (парирование) информационных рисков: активные и пассивные действия.

Тема 3. Нормативно-правовые основы управления информационными рисками (международные стандарты)

Особенности организации информационной безопасности современных предприятий, на основе существующей международной практики (стандартов): наличие систем управления информационной безопасностью и управления информационными рисками.

Общая характеристика международного стандарта ISO/IES 27002:2005(17799), часть 1 и 2 и содержание их разделов. Роль и место процессов по управлению информационными рисками.

Германский стандарт BSI: общая характеристика и структура. Сравнение стандартов ISO 17799 и BSI по вопросам управления информационными рисками.

Стандарт США NIST 800-30: вопросы управления информационными рисками. Технологии управления рисками: стадии, исходная информация и выходные документы. Уровни оценки рисков. Итоговые отчетные документы.

Ведомственные и корпоративные стандарты по управлению информационной безопасностью: XBSS - спецификации сервисов безопасности уровня ИБ для консорциума X/Open; Стандарт NASA «Безопасность информационных технологий»; Концепция управления рисками для организации MITRE.

Уровни зрелости предприятий с позиции информационной безопасности и их характеристика.

Раздел 2. Технологии управления информационными рисками

Тема 4. Частные методики оценки и анализа информационных рисков

Особенности разработки частных (отдельных) методик управления информационными рисками с учетом специфики функционирования предприятий.

Технологии анализа и управления рисками: 1. Идентификация рисков (угроз и уязвимостей); 2.Оценивание рисков (шкалы и критерии,

вероятностные оценки событий, технологии измерения рисков); 3. Измерение рисков (по двум и трем факторам); 4. Оценки угроз и уязвимостей (экспертные и статистические оценки, учет влияния различных факторов, анкетные вопросники); 5. Выбор допустимого уровня риска (базовый и повышенный уровень, обоснование требуемого уровня на основе критерия «стоимость/эффективность»); 6. Выбор контрмер и их эффективности: комплексно с учетом разных уровней: административного, организационного, программно-технического; количественные и качественные оценки эффективности предлагаемых мероприятий.

Тема 5. Корпоративные методики управления информационными рисками

Особенности разработки корпоративной методики управления информационными рисками с учетом специфики функционирования предприятия: 1. Постановка задачи (сущность анализа информационных рисков и типовой сценарий анализа информационных рисков); 2. Методы оценивания информационных рисков (идентификация и оценка информационного ресурса, оценка угроз и уязвимостей, оценка эффективности информационной безопасности); 3. Табличные методы оценки рисков (двух и трехфакторные); 4.Методика анализа рисков Microsoft.

Тема 6. Инструментальные средства анализа информационных рисков

Виды возможных инструментальных средств анализа рисков: «бумажные» и программные методики. Требования к инструментальным средствам анализа рисков.

Классификация специализированных программных методик: базовый уровень и уровень полного анализа рисков. Инструментарий базового уровня: справочные и методические материалы; программное обеспечение анализа рисков и аудита (COBRA). Инструментальные средства повышенного уровня (с полным анализом рисков): метод CRAMM; средства компании MethodWare; экспертная система АванГард; средства компании RiskWatch и др.

Разработка модели управления рисками при обеспечении информационной безопасности типового предприятия: общая характеристика; основные этапы реализации и возможности модели.

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

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

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Управление рисками» приведена в Приложении 1.

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

Основная литература:

1. Воробьёв С.Н., Балдин К.В. Управление рисками в предпринимательстве. Учебное пособие. – М.: Дашков и К°, 2013.
2. Гринев М.В. Риск-менеджмент инвестиционного проекта. Учебник для вузов. М.: ЮНИТА-ДАНА, 2008.
3. Мамаева Л.Н. Управление рисками. Учебное пособие. – М.: Дашков и К°, 2013.
4. Страхование. Учебник. Под ред. Л.А.Орланюк-Малицкого. М.: Юрайт, 2011.

Дополнительная литература:

1. Балдин К.В., Передеряев И.И., Голов С.С. Управление рисками в инновационно-инвестиционной деятельности предприятия. Учебное пособие. – М.: Дашков и К°, 2012.
2. Плошкин В.В. Оценка и управление рисками на предприятиях. Учебное пособие. – Ст. Оскол: ТНТ, 2013.
3. Уродовских В.Н. Управление рисками предприятия. Учебное пособие. – М.: Инфра-М, 2011.

Рекомендуемая литература:

1. Королёв В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска. Учебное пособие. – М.: Физматлит, 2011.
2. Ляпина С.Ю., Грачёва М.В. Управление рисками в инновационной деятельности. Учебное пособие. – М.: Юнити-Дана, 2012.
3. Нестеров С.А., Петренко С.А. Программные средства анализа информационных рисков компании // Экспресс-электроника. - № 10. - 2002.
4. Петренко С.А. Управление информационными рисками компании // Экспресс-электроника. - № 2-3. - 2002.
5. Никитин И.А., Цулая М.Т. Процессы анализа и управления рисками в области информационных технологий. Учебное пособие. – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
6. Симонов С.В. Методология анализа рисков в информационных системах // Конфидент. Защита информации. - № 1. - 2001.
7. Симонов С.В. Технологии и инструментарий для управления рисками //Jet Info. - № 1.-2003.

Электронные книги:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.Технические средства и методы защиты информации. Учебное пособие для вузов: - 4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012. **http://biblioclub.ru/index.php?page=book&id=253208&sr=1**

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **http://www.academy.it.ru/ –** академия АЙТИ.

9. Методические указания для обучающихся, по освоению дисциплины

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

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

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

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Управление рисками»

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

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

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

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«УПРАВЛЕНИЕ РИСКАМИ»
(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тема: 1,2,3	основные подходы к процессу управления информационными рисками; организацию процесса риск-менеджмента в области информационной безопасности и его место в системе управления предприятием; требования к информационно-аналитическим документам в основных стандартах по управлению информационными рисками сущность и виды рисков предприятия; формы отчетности в системе риск-менеджмента по защите информации; сущность и классификацию информационных рисков предприятия;	управлять работой по оценке и анализу информационных рисков; идентифицировать, оценивать, измерять, диагностировать информационные риски; представлять информацию об информационных рисках; проводить анализ эффективности деятельности по защите информации с учетом факторов риска в области информационной безопасности;	основными методами организации работы при внедрении систем управления информационными рисками; математическим аппаратом анализа информационных рисков;
2.	ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Тема:4,5,6	сущность и виды рисков предприятия; формы отчетности в системе риск-менеджмента по защите информации;	представлять информацию об информационных рисках; проводить анализ эффективности деятельности	методами защиты от информационных рисков;

				сущность и классификацию информационных рисков предприятия;	по защите информации с учетом факторов риска в области информационной безопасности;	
3.	ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Тема:4,5,6	показатели деятельности по информационной безопасности предприятия, учитывающие риски; алгоритмы управления информационными рисками корпорации; основные страховые информационные риски предприятия и способы защиты от них; основные виды страхования для покрытия информационных рисков предприятия.	оценивать рискованность проектов и вложений в активы по защите информации; управлять информационными рисками на основе инжиниринга по защите информации; использовать страховые продукты как способ снижения информационных рисков.	моделями оценки и анализа информационных рисков;
4.	ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Тема:4,5,6	показатели деятельности по информационной безопасности предприятия, учитывающие риски; алгоритмы управления информационными рисками корпорации; основные страховые информационные риски предприятия и способы защиты от них; основные виды страхования для покрытия информационных рисков	оценивать рискованность проектов и вложений в активы по защите информации; управлять информационными рисками на основе инжиниринга по защите информации; использовать страховые продукты как способ снижения информационных рисков.	способами защиты от информационных рисков с помощью страхования.

				предприятия.		

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

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

			4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-9	Доклад в форме презентации	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-15	Контрольная работа	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл).

			2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

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

Примерная тематика докладов в презентационной форме / рефератов:

1. Объективное и субъективное понимание информационных рисков.
2. Структурные характеристики информационных рисков.
3. Классификация информационных рисков предприятия.
4. Развитие концепции управления информационными рисками на предприятии.
5. Системы управления информационными рисками на предприятии.
6. Основные принципы управления информационными рисками.
7. Управление информационными рисками как часть менеджмента информационной безопасности фирмы.
8. Управление информационными рисками и стратегия информационной безопасности фирмы.
9. Управление информационными рисками и организационная структура службы информационной безопасности фирмы.
10. Аутсорсинг управления информационными рисками современного предприятия.
11. Методы финансирования информационных рисков на уровне фирмы.

12. Оценки эффективности программы управления информационными рисками.

13. Основные этапы управления информационными рисками.

14. Общая характеристика идентификации и анализа информационных рисков.

15. Характеристика информации, необходимой для управления рисками.

16. Основные принципы оценки информационных рисков.

17. Методы управления информационными рисками.

18. Метод управления информационными рисками: отказ от риска.

19. Метод управления информационными рисками: снижение риска.

20. Метод управления информационными рисками: разделение риска.

21. Метод управления информационными рисками: аутсорсинг риска.

22. Метод управления информационными рисками: сохранение риска.

23. Метод управления информационными рисками: избежание риска.

24. Метод управления информационными рисками: передача риска.

25. Построение организационной структуры системы управления информационными рисками.

26. Выбор механизмов защиты от информационных рисков на предприятии.

27. Виды страхования информационных рисков.

28. Управление информационными рисками хранения закрытых данных.

29. Требования по обеспечению информационной безопасности при управлении информационными рисками.

30. Документационное обеспечение управления информационными рисками.

Примерная тематика заданий на контрольную работу:

1. Информационные риски, породившие мировой финансовый кризис.
2. Информационные риски киберпространства.
3. Информационные риски кибертерроризма.
4. Информационные риски современного предприятия.
6. Риски утечки информации на типовой фирме.
7. Информационные риски систем электронного бизнеса.
8. Оценка информационных рисков как основа корпоративного управления.
9. Отечественный подход оценки информационных рисков.
10. Основные элементы управления рисками информационной безопасности.
11. Стандарты в области управления информационными рисками.
12. Количественное определение величины информационных рисков.
13. Качественное определение величины информационных рисков.
14. Информационная составляющая бизнес-рисков.
15. Активы предприятия как ключевые факторы информационных рисков.

16. Подходы к управлению информационными рисками.
17. Системный подход к управлению информационными рисками.
18. Политика управления информационными рисками на типовом предприятии.
19.Процессорная модель управления информационными рисками.
20. Организационная деятельность по управлению информационными рисками.
21. Обоснование и распределение ответственности за управление информационными рисками.
22. Оценка рисков информационной безопасности.
23. Определение величины информационных рисков.
24. Обработка рисков информационной безопасности.
25. Оценка возврата инвестиций в информационную безопасность.
26. План обработки информационных рисков.
27. Выбор инструментов для оценки информационных рисков.
28. Реализация проектов по оценке информационных рисков.
29. Внедрение системы управления информационными рисками.
30. Жизненный цикл управления информационными рисками.

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

Формой контроля знаний по дисциплине «Управление рисками» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-4; ПК-9.	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%.

						Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-4; ПК-9; ПК-15.	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-4; ОПК-5; ПК-9; ПК-15	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы

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

						рирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

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

1. Какие наиболее общие закономерности присущи информационным процессам?

– постоянный рост количества информации, ее кругооборот,
– рассеяние и старение информации.
– все вышеперечисленное

2. К факторам, приводящим к информационным потерям и, как следствие, к различным видам убытков или ущерба можно отнести следующие причины и действия…

– материальный ущерб, связанный с несчастными случаями, кража и преднамеренная порча материальных средств, аварии и выход из строя аппаратуры, программ и баз данных, убытки, связанные с ошибками накопления, хранения, передачи и использования информации
– ошибки эксплуатации, концептуальные ошибки и ошибки внедрения, убытки от злонамеренных действий в нематериальной сфере, болтливость и разглашение, убытки социального характера
– все вышеперечисленное

3. Какие потери можно отнести к категории эксплуатационных?

– потеря клиентуры;
– расходы на анализ и исследование причин и величины ущерба;
– все вышеперечисленное

4. Выберите приемлемые единицы измерения энтропии дискретного сигнала:

– биты;
– ваты;
– ниты;
– диты.

5. Где используют понятие условная энтропия?

– при определении взаимозависимости между символами кодируемого алфавита;
– при ранжировании символов в кодовом сообщении;
– при определении метода сжатия информации для размещения её в памяти ПК.
– для определения потерь при передаче информации по каналам связи;

6. Что такое энтропия объединения сообщений?

– это среднее количество информации, приходящееся на каждый символ отправляемого сообщения ансамбля «А» или ансамбля «В»;
– это среднее значение полученных адресатом сообщений ансамбля «В», при условии, что передавались сообщения ансамбля «А»;
– это среднее количество информации при совместном появлении символов ансамблей «А» и «В» в принятом сообщении.

7. Выберите типы источников информации, рассматривающиеся в управлении рисками:

– марковские;
– резидентурные;
– бернуллиевские;
– комбинаторные.

8. Что понимается под сообщением в теории рисков?

– форма представления элемента с помощью физической величины;
– информационный процесс, в отношении которого необходимо обеспечить соответствующую защиту;
– порция информации, передаваемой в системе с коммутацией данных;
– совокупность элементов, узлов и блоков, объединённых в общую законченную конструкцию.

9. Выберите типы сигналов, рассматриваемые в теории рисков:

– аналоговые;
– дискретизированные;
– квантованные;
– генетические.

10. Существует ли эргодический источник информации?

– да;

– нет.

11. Чем можно измерить количество информации, содержащееся в дискретном сообщении по Шеннону?

– произведением длительности сигнала, полосы пропускания и логарифма уровня помех;

– суммой логарифмов априорной и апостериорной вероятностей того, что принятый сигнал содержит передаваемое сообщение;

– произведением объёма импульсов, способных принимать некоторое значение и градации уровня передаваемого сигнала;

– разностью логарифмов апостериорной и априорной вероятностей того, что принятый сигнал содержит передаваемое сообщение.

12. Что показывает искусственно созданная избыточность информации для источника сообщений?

– сколько дополнительных компонентов источника может быть задействовано с целью повышения надёжности и работоспособности системы;

– каково максимальное число символов кода в сообщениях источника;

– какую долю максимально возможной неопределённости символов при заданном объёме алфавита не использует источник сообщений;

– какова степень близости неравномерных состояний источника к оптимальному значению.

13. Первая теорема Шеннона рассматривает кодирование информации и передачу сообщений в канале связи с помехами?

– да;

– нет.

14. Что понимается под эффективностью кода?

– величина, характеризующая среднюю избыточность кода по отношению к передаваемому сообщению;

– величина, характеризующая абсолютную недогруженность источника на каждый символ кодируемого сообщения;

– величина, характеризующая разрешённые кодовые комбинации с постоянным соотношением символов в передаваемом сообщении.

– величина, характеризующая степень близости неравномерного статистического кода к оптимальному;

15. Учитывает ли вторая теорема Шеннона вероятность ошибки кодирования информации при передаче сообщений по дискретному постоянному каналу?

– да;

– нет.

16. На какие типы делят каналы связи в зависимости от характера сигналов, передаваемых по ним?

– статистические;

– дискретные;
– комбинаторные;
– аналоговые.

17. Каковы пределы полосы пропускания частот, воспринимаемые человеческим ухом?

– 300 – 3400 Гц;
– 16 Гц – 20 КГц;
– 50 – 300 Гц;
– 100 Гц – 10 КГц.

18. Полоса пропускания является характеристикой непрерывных каналов связи?

– да;
– нет.

19. Что понимают под белым шумом в каналах связи?

– если мощность помех в канале является непрерывной случайной величиной, подчиняющаяся нормальному статистическому распределению;
– если отношение средних мощностей помехи и сигнала в канале связи является величиной неизменной при передаче сигнала;
– если в пределах полосы пропускания канала средняя мощность помех оказывается одинаковой на всех её частотах, а вне этой полосы она равна нулю;
– если средняя мощность помех в канале связи оказывается достаточно мала и стремится к нулю, а вне полосы пропускания она максимальна.

20. Что понимается под пропускной способностью Гауссовского канала передачи информации?

– удельная скорость передачи информации в нормированной полосе пропускания канала;
– максимально достижимая скорость передачи информации при заданном качестве;
– среднее количество передаваемой информации на одно сообщение;
– отношение энергии передаваемого сигнала к спектральной плотности некоторого порогового нормального шума сигнала.

21. Когда дискретный канал называют однородным каналом?

– когда влияние помех всё время одинаково;
– когда отсутствует корреляция знаков в сообщении;
– когда задано время одного элементарного сигнала;
– когда пропускная способность канала не изменяется.

22. Как определить степень загрузки канала связи с помехами?

– вычислением логарифма количества элементарных сигналов в сообщении;
– вычислением разности числа контрольных разрядов и числа информационных знаков в сообщении;
– вычислением отношения количества информации в сообщении к длительности сигнала в канале связи;

– вычислением отношения производительности источника сообщений к пропускной способности канала связи.

23. Используется ли операция контроля по модулю для обнаружения ошибок в циклических кодах?

– да;

– нет;

24. Выберите приемлемые модификации операции контроль по модулю:

– контроль по сумме;

– контроль по разности;

– контроль по частному;

– контроль по произведению.

25. Выберите применяемые методы сжатия информации:

– делением кода на части;

– выбором образующих многочленов;

– применяя побуквенный сдвиг;

– на основе исключения повторений.

26. Метод Лавинского используется для сжатия информации?

– да;

– нет;

27. В чём суть структурного кодирования данных?

– когда данные представляются в виде матрицы кодов;

– когда данные разбиваются на составные части с последующим их сжатием;

– когда данные представляются определённым макетом в памяти ПК;

– когда данные представляются в виде семантической модели в памяти ПК.

28. Выберите структуры данных, которые применяют при статическом и динамическом распределении памяти ПК:

– последовательная структура данных;

– фреймовая структура данных;

– списковая структура данных;

– генетическая структура данных.

29. Что называют терминатором в структурном кодировании данных?

– специальный знак для обозначения конца массива;

– способ организации данных в памяти ПК;

– адрес ячейки памяти ПК;

– граница между кодовыми комбинациями.

30. Что понимается под списковой структурой данных в структурном кодировании?

– это способ организации данных в памяти ПК, при котором последовательности предварительно упорядоченных чисел разбиваются на ряд равных отрезков, внутри которых отсчёт ведётся от границ очередной структуры;

– это способ организации данных в памяти ПК, при котором в массивах повторяющиеся единичные элементы старших разрядов заменяются некоторыми условными символами;

– это способ организации данных в памяти ПК, при котором каждой строке матрицы значений соответствует код с числом двоичных знаков, равных числу клеток самой матрицы;

– это способ организации данных в памяти ПК, при котором физически разбросанные элементы объединяют в логически упорядоченную совокупность при помощи звеньев связи.

31. Понятие звено связи в структурном кодировании информации включает в себя минимальное кодовое расстояние?

– да;

– нет;

32. Что представляют собой двунаправленные строки в структурном кодировании информации?

– это структуры, в которых элементы списка и подсписков просматриваются как в прямом, так и в обратном направлениях;

– это структуры, в которых переход от одного элемента к другому может осуществляться как в прямом, так и в обратном направлениях;

– это структуры, в которых элементы списка и подсписков просматриваются только в одном направлении;

– это структуры, в которых переход от одного элемента к другому может осуществляться только в одном направлении;

33. Для задания двунаправленного списка необходимо, чтобы указатель списка содержал адрес первого и последнего элемента списка, а каждый элемент списка содержал адреса как последующих, так и предыдущих элементов?

– да;

– нет;

34. Что такое бинарные деревья в структурном кодировании информации?

– это структуры данных не имеющие контуров и петель;

– это структуры, в которых наименования качественных признаков, характеризующих данные выносятся отдельным списком в шапку массива и являются общими для всех характеризуемых объектов;

– это структуры, в которых считывание данных с одного или группы элементов происходит до тех пор, пока не выполнится условие перехода к следующему элементу, либо группе элементов;

– это структуры, в которых узел любого уровня может быть соединён не более чем с двумя узлами более низкого уровня.

35. Выберите приемлемые способы представления данных в памяти компьютера:

– с помощью способа логических шкал;

– с помощью азбуки Морзе;

– с помощью кольцевой структуры данных;
– с помощью типичных последовательностей.

4.2. Типовые вопросы, выносимые на экзамен

1. Основы информационной безопасности бизнес-процессов.
2. Информация и информационные процессы как ключевые элементы безопасного бизнеса.
3. Общая характеристика существующих подходов по обоснованию стоимости систем защиты информации на предприятии: теоретико-прикладной и эмпирико-практический.
4. Характеристика существующего подхода по обоснованию стоимости систем защиты информации на предприятии: теоретико-прикладной аспект.
5. Характеристика существующего подхода по обоснованию стоимости систем защиты информации на предприятии: эмпирико-практический аспект.
6. Анализ использования на предприятиях теоретико-прикладного и эмпирико-практического подходов.
7. Анализ использования на предприятиях теоретико-прикладного подхода по обоснованию стоимости системы информационной безопасности.
8. Анализ использования на предприятиях эмпирико-практического подхода по обоснованию стоимости системы информационной безопасности.
9. Тенденции развития служб информационной безопасности предприятий в области экономической оценки деятельности по защите информации: российская практика управления информационными рисками.
10. Тенденции развития служб информационной безопасности предприятий в области экономической оценки деятельности по защите информации: международная практика управления информационными рисками.
11. Сущность, содержания и актуальность отечественного процесса управления информационными рисками при обеспечении информационной безопасности современных предприятий.
12. Ключевые понятия: риск, уязвимость, угроза и ущерб, оценка риска.
13. Существующие требования, рекомендации (руководящие документы ФСТЭК и ФСБ России) по управлению информационными рисками.
14. Сравнительная характеристика количественной и качественной, экспертной и аналитической оценки и анализа информационных рисков.
15. Характеристика количественной оценки и анализа информационных рисков.
16. Характеристика качественной оценки и анализа информационных рисков.
17. Характеристика экспертной оценки и анализа информационных рисков.

18. Характеристика аналитической оценки и анализа информационных рисков.

19. Снижение (парирование) информационных рисков: активные и пассивные действия.

20. Организация информационной безопасности современных предприятий (на основе существующей международной практике (стандартов)) при наличие систем управления защитой информации.

21. Организация информационной безопасности современных предприятий (на основе существующей международной практике (стандартов)) при наличие систем управления информационными рисками.

22. Общая характеристика международного стандарта ISO/IES 27002:2005(17799), часть 1 и 2 (роль и место процессам по управлению информационных рисков).

23. Германский стандарт BSI: общая характеристика и структура.

24. Сравнение стандартов ISO 17799 и BSI по вопросам управления информационными рисками.

25. Стандарт США NIST 800-30: вопросы управления информационными рисками.

26. Общая характеристика технологии управления информационными рисками: стадии, исходная информация и выходные документы.

27. Определение возможных уровней по оценке информационных рисков.

28. Итоговые отчетные документы по оценке информационных рисков.

29. Общая характеристика ведомственных и корпоративных стандартов по управлению информационной безопасностью: XBSS - спецификации сервисов безопасности уровня ИБ для консорциума X/Open; Стандарт NASA «Безопасность информационных технологий»; Концепция управления рисками для организации MITRE.

30. Сравнительная характеристика ведомственных и корпоративных международных стандартов по управлению информационной безопасностью (XBSS; Стандарт NASA «Безопасность информационных технологий»; Концепция управления рисками для организации MITRE).

31. Характеристика ведомственных и корпоративных стандартов по управлению информационной безопасностью: XBSS - спецификации сервисов безопасности уровня ИБ для консорциума X/Open.

32. Характеристика ведомственных и корпоративных стандартов по управлению информационной безопасностью: Стандарт NASA «Безопасность информационных технологий».

33. Характеристика ведомственных и корпоративных международных стандартов по управлению информационной безопасностью: Концепция управления рисками для организации MITRE.

34. Уровни зрелости предприятий с позиции информационной безопасности (оценки информационных рисков).

35. Особенности разработки частных (отдельных) методик управления информационными рисками с учетом специфики функционирования предприятий.

36. Содержание (этапы) технологии анализа и управления информационными рисками: 1. 2. 3. 4. 5. 6. Выбор контрмер и их эффективности: комплексно с учетом разных уровней: административного, организационного, программно-технического; количественные и качественные оценки эффективности предлагаемых мероприятий.

37. Содержание и характеристика этапа идентификация информационных рисков (угроз и уязвимостей).

38. Содержание и характеристика этапа оценивание информационных рисков (шкалы и критерии, вероятностные оценки событий, технологии измерения рисков).

39. Содержание и характеристика этапа измерение информационных рисков по двум факторам.

40. Содержание и характеристика этапа измерение информационных рисков по трем факторам.

41. Содержание и характеристика этапа управления информационными рисками: оценка угроз и уязвимостей (экспертные и статистические оценки, учет влияния различных факторов, анкетные вопросники).

42. Содержание и характеристика этапа оценки информационных рисков: выбор допустимого уровня риска (базовый и повышенный уровень).

43. Содержание и характеристика этапа оценки информационных рисков: обоснование требуемого уровня на основе критерия «стоимость/эффективность».

44. Общий алгоритм разработки корпоративной методики управления информационными рисками с учетом специфики функционирования предприятия.

45. Этап разработки корпоративной методики управления информационными рисками предприятия: постановка задачи (сущность анализа информационных рисков и типовой сценарий анализа информационных рисков).

46. Этап разработки корпоративной методики управления информационными рисками предприятия: выбор методов оценивания информационных рисков (идентификация и оценка информационного ресурса, оценка угроз и уязвимостей, оценка эффективности информационной безопасности).

47. Этап разработки корпоративной методики управления информационными рисками предприятия: выбор табличных методов оценки рисков (двух и трехфакторные).

48. Этап разработки корпоративной методики управления информационными рисками предприятия: целесообразность использования методика анализа рисков фирмы Microsoft.

49. Виды возможных инструментальных средств анализа информационных рисков: «бумажные» и программные методики.

50. Требования к инструментальным средствам анализа информационных рисков.

51. Классификация специализированных программных методик управления информационными рисками: базовый уровень и уровень полного анализа.

52. «Бумажный» инструментарий управления информационными рисками базового уровня: справочные и методические материалы.

53. Программный инструментарий анализа рисков и аудита: COBRA.

54. Инструментальные средства оценки информационных рисков повышенного уровня (с полным анализом рисков): метод CRAMM.

55. Инструментальные средства оценки информационных рисков повышенного уровня (с полным анализом рисков): средства компании MethodWare.

56. Инструментальные средства оценки информационных рисков повышенного уровня (с полным анализом рисков): экспертная система АванГард.

57. Инструментальные средства оценки информационных рисков повышенного уровня (с полным анализом рисков): средства компании RiskWatch.

58. Разработка модели управления рисками при обеспечении информационной безопасности типового предприятия: общая характеристика.

59. Разработка модели управления рисками при обеспечении информационной безопасности типового предприятия: основные этапы реализации.

60. Разработка модели управления рисками при обеспечении информационной безопасности типового предприятия: возможности использования модели (полученных результатов моделирования).

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«УПРАВЛЕНИЕ РИСКАМИ»
(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

- Сформировать представление в сфере управления информационными рисками с использованием передового отечественного и мирового опыта в области обеспечения информационной безопасности современных предприятий.
- Получение студентами основ понимания и формирования целей, задач и методов управления информационными рисками при обеспечении комплексной безопасности предприятий;

Задачи дисциплины:

- Ознакомление студентов с основными подходами экономического обоснования разрабатываемых и существующих мер по информационной безопасности с учётом управления рисками в государственных и коммерческих организациях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области управления рисками и экономического обоснования мер по обеспечению информационной безопасности предприятий.

2. Указания по проведению практических занятий

Раздел 1. Базовые основы по управлению информационными рисками

Тема 1. Сущность и место управления информационными рисками в системе безопасности предприятия

Практическое занятие 1.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по определению сущности управления информационными рисками в системе безопасности предприятий.

Основные положения темы занятия:

- анализ использования на предприятиях теоретико-прикладного и эмпирико-практического подходов исследований;
- существующие подходы обоснования стоимости систем защиты информации на предприятии.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Понятие и содержание процесса управления информационными рисками.

2. Цель и задачи управления информационными рисками.

3. Основные этапы процесса управления информационными рисками.

Продолжительность занятия – 2 ч.

Тема 2. Нормативно-правовые основы управления информационными рисками (отечественные стандарты)

Практическое занятие 2.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по применению нормативно-правовых основ управления информационными рисками с использованием отечественных стандартов и требований.

Основные положения темы занятия:

- существующие требования, рекомендации и руководящие документы ФСТЭК и ФСБ России по управлению информационными рисками.
- количественный и качественный анализ, экспертная и аналитическая оценка информационных рисков.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Содержание отечественного процесса управления информационными рисками при обеспечении информационной безопасности современных предприятий.
2. Количественная и качественная оценка и анализ информационных рисков.
3. Экспертная оценка и анализ информационных рисков.
4. Аналитическая оценка и анализ информационных рисков
5. Снижение (парирование) информационных рисков: активные действия.
6. Снижение (парирование) информационных рисков: пассивные действия.

Продолжительность занятия – 6 ч.

Тема 3. Нормативно-правовые основы управления информационными рисками (международные стандарты)

Практическое занятие 3.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по применению нормативно-правовых основ управления информационными рисками с использованием международных стандартов и требований.

Основные положения темы занятия:

- особенности организации информационной безопасности современных предприятий, на основе существующей международной практики (стандартов).
- ведомственные и корпоративные стандарты по управлению информационной безопасностью.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Германский стандарт BSI: общая характеристика и структура.
2. Сравнение стандартов ISO 17799 и BSI по вопросам управления информационными рисками.
3. Стандарт США NIST 800-30: вопросы управления информационными рисками.
4. Общая характеристика ведомственных и корпоративных стандартов по управлению информационной безопасностью.
5. Характеристика стандарта XBSS - спецификации сервисов безопасности уровня ИБ для консорциума X/Open;
6. Стандарт NASA «Безопасность информационных технологий».
7. Концепция управления рисками для организации MITRE.

Продолжительность занятия – 6 ч.

Раздел 2. Технологии управления информационными рисками

Тема 4. Частные методики оценки и анализа информационных рисков

Практическое занятие 4.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки в применении частных методик оценки и анализа информационных рисков.

Основные положения темы занятия:

- особенности разработки частных (отдельных) методик управления информационными рисками с учетом специфики функционирования предприятий;
- выбор допустимого уровня риска (базовый и повышенный уровень, обоснование требуемого уровня на основе критерия «стоимость/эффективность»).

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Оценивание рисков (шкалы и критерии, вероятностные оценки событий, технологии измерения рисков).
2. Измерение рисков (по двум и трем факторам).

3. Оценки угроз и уязвимостей (экспертные и статистические оценки, учет влияния различных факторов, анкетные вопросники).
4. Выбор контрмер по снижению рисков и комплексная оценка их эффективности.

Продолжительность занятия – 6 ч.

Тема 5. Корпоративные методики управления информационными рисками

Практическое занятие 5.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки в применении корпоративных методик управления информационными рисками.

Основные положения темы занятия:

- методы оценивания информационных рисков (идентификация и оценка информационного ресурса, оценка угроз и уязвимостей, оценка эффективности информационной безопасности).
- табличные методы оценки рисков (двух и трехфакторные), методика анализа рисков Microsoft.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Особенности разработки корпоративной методики управления информационными рисками с учетом специфики функционирования предприятия.

2. Постановка задачи (сущность анализа информационных рисков и типовой сценарий анализа информационных рисков).

3. Двух и трехфакторные табличные методы оценки рисков.

Продолжительность занятия – 6 ч.

Тема 6. Инструментальные средства анализа информационных рисков

Практическое занятие 6.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки в применении инструментальных средств анализа информационных рисков.

Основные положения темы занятия:

- классификация специализированных программных методик: базовый уровень и уровень полного анализа рисков.
- инструментальные средства повышенного уровня с полным анализом рисков.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Виды и требования к инструментальным средств анализа рисков: «бумажные» и программные методики.

2. Инструментарий базового уровня: справочные и методические материалы; программное обеспечение анализа рисков и аудита (COBRA).

3. Инструментальные средства повышенного уровня: метод CRAMM; средства компании MethodWare; экспертная система АванГард; средства компании RiskWatch и др.

4. Разработка модели управления рисками при обеспечении информационной безопасности типового предприятия: основные этапы реализации.

Продолжительность занятия – 6 ч.

3. Указания по проведению лабораторных работ

Лабораторные работы не предусмотрены учебным планом

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных методик оценки и управления рисками;

2) привить навыки самостоятельного решения нестандартных задач в области управления рисками на предприятиях.

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

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**60**
Вопросы, выносимые на самостоятельное изучение	12
Подготовка к практическим занятиям	32
Подготовка к лабораторным занятиям	-
Подготовка докладов	8
Выполнение практических заданий	8

Вопросы, выносимые на самостоятельное изучение: для очной формы обучения:

1. Информационные риски, породившие мировой финансовый кризис.
2. Информационные риски киберпространства.

3. Информационные риски кибертерроризма.
4. Информационные риски современного предприятия.
6. Риски утечки информации на типовой фирме.
7. Информационные риски систем электронного бизнеса.
8. Оценка информационных рисков как основа корпоративного управления.
9. Отечественный подход оценки информационных рисков.
10.Основные элементы управления рисками информационной безопасности.
11. Стандарты в области управления информационными рисками.
12. Количественное определение величины информационных рисков.
13. Качественное определение величины информационных рисков.
14. Информационная составляющая бизнес-рисков.
15. Активы предприятия как ключевые факторы информационных рисков.
16. Подходы к управлению информационными рисками.
17. Системный подход к управлению информационными рисками.
18. Политика управления информационными рисками на типовом предприятии.
19.Процессорная модель управления информационными рисками.
20. Организационная деятельность по управлению информационными рисками.
21. Обоснование и распределение ответственности за управление информационными рисками.
22. Оценка рисков информационной безопасности.
23. Определение величины информационных рисков.
24. Обработка рисков информационной безопасности.
25. Оценка возврата инвестиций в информационную безопасность.
26. План обработки информационных рисков.
27. Выбор инструментов для оценки информационных рисков.
28. Реализация проектов по оценке информационных рисков.
29.Внедрение системы управления информационными рисками.
30. Жизненный цикл управления информационными рисками.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	12	Изучение открытых источников
2.	Подготовка к практическим занятиям	32	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	

4.	Тематика докладов	8	1. Оценки эффективности программы управления информационными рисками. 2. Основные принципы управления информационными рисками.
5.	Выполнение практических заданий	8	Разработка модели управления риском на предприятии.

Примерные темы докладов

1. Информационные риски, породившие мировой финансовый кризис.
2. Информационные риски киберпространства.
3. Информационные риски кибертерроризма.
4. Информационные риски современного предприятия.
6. Риски утечки информации на типовой фирме.
7. Информационные риски систем электронного бизнеса.
8. Оценка информационных рисков как основа корпоративного управления.
9. Отечественный подход оценки информационных рисков.
10. Основные элементы управления рисками информационной безопасности.
11. Стандарты в области управления информационными рисками.
12. Количественное определение величины информационных рисков.
13. Качественное определение величины информационных рисков.
14. Информационная составляющая бизнес-рисков.
15. Активы предприятия как ключевые факторы информационных рисков.
16. Подходы к управлению информационными рисками.
17. Системный подход к управлению информационными рисками.
18. Политика управления информационными рисками на типовом предприятии.
19. Процессорная модель управления информационными рисками.
20. Организационная деятельность по управлению информационными рисками.
21. Обоснование и распределение ответственности за управление информационными рисками.
22. Оценка рисков информационной безопасности.
23. Определение величины информационных рисков.
24. Обработка рисков информационной безопасности.
25. Оценка возврата инвестиций в информационную безопасность.
26. План обработки информационных рисков.
27. Выбор инструментов для оценки информационных рисков.
28. Реализация проектов по оценке информационных рисков.
29. Внедрение системы управления информационными рисками.
30. Жизненный цикл управления информационными рисками.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

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

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

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

6. Перечень основной и дополнительной учебной литературы

Основная:

1. Воробьёв С.Н., Балдин К.В. Управление рисками в предпринимательстве. Учебное пособие. – М.: Дашков и К°, 2013.
2. Гринев М.В. Риск-менеджмент инвестиционного проекта. Учебник для вузов. М.: ЮНИТА-ДАНА, 2008.
3. Мамаева Л.Н. Управление рисками. Учебное пособие. – М.: Дашков и К°, 2013.
4. Страхование. Учебник. Под ред. Л.А.Орланюк-Малицкого. М.: Юрайт, 2011.

Дополнительная:

1. Балдин К.В., Передеряев И.И., Голов С.С. Управление рисками в инновационно-инвестиционной деятельности предприятия. Учебное пособие. – М.: Дашков и К°, 2012.
2. Плошкин В.В. Оценка и управление рисками на предприятиях. Учебное пособие. – Ст. Оскол: ТНТ, 2013.

3. Уродовских В.Н. Управление рисками предприятия. Учебное пособие. – М.: Инфра-М, 2011.

Рекомендуемая:

1. Королёв В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска. Учебное пособие. – М.: Физматлит, 2011.
2. Ляпина С.Ю., Грачёва М.В. Управление рисками в инновационной деятельности. Учебное пособие. – М.: Юнити-Дана, 2012.
3. Нестеров С.А., Петренко С.А. Программные средства анализа информационных рисков компании // Экспресс-электроника. - № 10. - 2002.
4. Петренко С.А. Управление информационными рисками компании // Экспресс-электроника. - № 2-3. - 2002.
5. Никитин И.А., Цулая М.Т. Процессы анализа и управления рисками в области информационных технологий. Учебное пособие. – М.: Национальный Открытый Университет «ИНТУИТ», 2016.
6. Симонов С.В. Методология анализа рисков в информационных системах // Конфидент. Защита информации. - № 1. - 2001.
7. Симонов С.В. Технологии и инструментарий для управления рисками //Jet Info.-№ 1.-2003.

Электронные книги:

1. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.Технические средства и методы защиты информации. Учебное пособие для вузов: - 4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.
http://biblioclub.ru/index.php?page=book&id=253208&sr=1

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по

Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*
Информационные справочные системы:
1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Управление рисками».