МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Экономические вопросы обеспечения информационной безопасности

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью курса «**Экономические вопросы обеспечения информационной безопасности»** является ознакомление студентов с методами защиты информации в бизнесе и примерами реализации этих методов на практике. Дисциплина направлена на формирование практических навыков построения модели защиты информационной безопасности электронного бизнеса.

2. Место дисциплины в структуре ОП магистратуры

Данная дисциплина относится к обязательной части (Б1.О.05). Она является частью ядра образования в системе обучения методам защиты информации, состоящего из дисциплин экономического профиля.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП специалитета

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	И-УК-1_1 Осуществляет системный анализ задачи, выделяя ее базовые составляющие И_УК-1_2 Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	**Знать:** - связи и элементы различных структур управления в направлении информационной безопасности; - методы управленческой деятельности; - основы корпоративной культуры организации; - типы поведения людей в организации; **Уметь:** - принимать организационно-управленческие решения по совершенствованию системы управления информационной безопасностью - работать в коллективе и кооперироваться с коллегами для

		выполнения заданий; - формировать цели команды **Владеть:** - навыками расчета и анализа показателей процесса управления с целью совершенствования системы управления информационной безопасностью - умениями руководства подразделениями и фирмой, - способами предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности
УК – 2 Способен управлять проектом на всех этапах его жизненного цикла	И-УК-2_3 Знает виды ресурсов и ограничений для реализации проекта; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность И-УК-2_4 Формулирует цели, задачи, ожидаемые результаты проекта; разрабатывать план реализации проекта; использовать нормативно-правовую документацию в сфере профессиональной деятельности	**Знать:** - виды ресурсов и ограничений для реализации проекта по информационной безопасности; -основные методы оценки разных способов решения задач при разработке проекта по информационной безопасности; - действующее законодательство и правовые нормы, регулирующие профессиональную деятельность в области информационной безопасности **Уметь:** - формулировать цели, задачи, ожидаемые результаты проекта по разработке системы информационной безопасности бизнеса; - разрабатывать план реализации проекта по информационной безопасности **Владеть:** -навыками работы в коллективе и кооперирования с коллегами для выполнения заданий по информационной безопасности; -способами предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности по информационной безопасности
УК - 3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	И-УК-3_1 Уметь учитывать в совместной деятельности особенности поведения и общения разных людей; устанавливать различные виды	**Знать :** -основные приемы и нормы социального взаимодействия при разработке проектов по информационной безопасности; -основные понятия и методы конфликтологии, технологии межличностной и деловой коммуникации, принципы командной работы как основы организации и руководства работой команды, способы мотивации членов

	коммуникации (невербальную, вербальную, устную, письменную, виртуальную, реальную и т.п.) для руководства командой и достижения поставленной цели И-УК-3_2 Владеть соблюдением этических норм взаимодействия	команды с учетом организационных возможностей и личностных особенностей членов команды при разработке проектов по информационной безопасности. **Уметь**: - устанавливать и поддерживать контакты, обеспечивающие успешную работу в команде; - разрабатывать цели команды в соответствии с целями проекта; выбирать стратегию формирования команды и определять функциональные и ролевые критерии отбора участников. **Владеть:** - навыками организации и руководства работой команды, презентации результатов собственной и командной работы.

4. Объем, структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 акад. часов.

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)*** ***Формы ЭО и ДОТ (при наличии)***
			Контактная работа						
		2	лекции	практические	Лабораторные	Консультации	аттестационные испытания	самостоятельная работа	
1	Теоретические основы управления информационной безопасности бизнеса	2	4	4				3	Вопросы по теме 1
	в том числе с ЭО и ДОТ							4	Материалы в LMS Moodle: - презентация; - конспект лекций; -Вопросы по теме 1 -
2	Модель информационной безопасности бизнеса	2	4	4		2		3	Вопросы по теме 2 практическая работа № 1

	в том числе с ЭО и ДОТ							6	Материалы в LMS Moodle: - презентация; - конспект лекций; -Вопросы по теме 2 -текст практической работы № 1
3	Модели управления для обеспечения информационной безопасности бизнеса	2	8	8				3	**Тест**
	в том числе с ЭО и ДОТ							6	Материалы в LMS Moodle: - Тест для самоподготовки
4	Оценка информационной безопасности бизнеса	2	6	8		2		3	практическая работа №2
5	Роль персонала в задачах обеспечения информационной безопасности бизнеса	2	10	8				2	Задания для самостоятельной работы, практическая работа № 3
	в том числе с ЭО и ДОТ							6	Материалы в LMS Moodle: - презентация; - конспект лекций; -текст самостоятельной работы -текст практической работы № 3
							0.3	3.7	зачет
	Итого		32	32		4	0.3	39.7	
	в том числе с ЭО и ДОТ							22	

Содержание разделов дисциплины

1.Теоретические основы управления информационной безопасностью бизнеса
Бизнес, электронный бизнес. Стандарты и модели. Определение информационной безопасности. Доктрина национальной безопасности. Информационная сущность бизнеса. Информационные характеристики бизнеса. Правовая среда бизнеса и ее свойства. Информационная сфера —главный источник рисков бизнеса.

2.Модель информационной безопасности бизнеса
Риски, рисковые события, ущербы и уязвимости. Обобщенная модель распределения ресурсов организации в условиях рисков. Риск-ориентированный подход к обеспечению ИБ. Интерпретация характеристик риска для управления ИБ. Общая модель обеспечения ИБ бизнеса. Проблемы практической реализации модели обеспечения ИБ организации.

3.Модели управления для обеспечения информационной безопасности бизнеса.

Модели непрерывного совершенствования: корпоративное управление и международные стандарты. Стандартизированные модели менеджмента. Аспекты контроля и совершенствования.

4.Оценка информационной безопасности электронного бизнеса.
Проблема измерения и оценивания информационной безопасности бизнеса. Способы оценки информационной. Процесс оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Риск-ориентированная оценка информационной безопасности.

5.Роль персонала в задачах обеспечения информационной безопасности бизнеса.
Формализованное представление угроз ИБ от персонала. Внешние сообщники внутреннего злоумышленника. Типология мотивов. Деятельность внутреннего злоумышленника с точки зрения формальных полномочий. Управление идентификационными данными и доступом (IBM Восточная Европа/Азия) Противодействие угрозам ИБ от персонала Общий подход к противодействию Обеспечение осведомленности персонала в области ИБ Получение информации от сотрудников организации. Программно-технические средства защиты от утечек информации.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

1) **Академическая лекция** (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

2) Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

3) вступление (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.

4) Изложение является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые

формулировки и определения должны быть четкими, насыщенными глубоким содержанием.

Заключение обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Лекция с разбором конкретных ситуаций – это по форме та же лекция - дискуссия, но на обсуждение преподаватель ставит не вопрос, а конкретную ситуацию. Как правило, такая ситуация представляется устно или в очень короткой видеозаписи, поэтому изложение ее должно быть очень кратким, но содержать достаточную информацию для оценки характерного явления и обсуждения. Это, так называемая, микроситуация. Слушатели анализируют и обсуждают ее сообща, всей аудиторией. Преподаватель старается активизировать участие в обсуждении отдельными вопросами, обращенными к отдельным слушателям, выясняет их оценку суждениям коллег, предлагает сопоставить с собственной практикой, «сталкивает» между собой различные мнения и тем развивает дискуссию, стремясь направить ее в нужное русло. Затем, опираясь на правильные высказывания и анализируя неправильные, ненавязчиво, но убедительно подводит аудиторию к коллективному выводу или обобщению.

Обобщающая лекция – проводится в завершение изучения раздела или темы для закрепления знаний. На лекции вновь выделяются основные вопросы, используются обобщающие таблицы, схемы, алгоритмы, позволяющие включить усвоенные знания в новые связи и зависимости, переводя их на более высокие уровни усвоения.

Обзорная лекция – проводится обычно перед государственными или курсовыми экзаменами. В лекции излагаются лишь отдельные, наиболее крупные вопросы дисциплины. Материал лекции представляет конспективный обзор полного учебного курса. Проводится такая лекция с целью систематизации знаний студентов, полученных ими в ходе изучения (в том числе самостоятельного) учебного материала.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Для выработки системного видения ситуаций в процессе изучения дисциплины необходимо использовать интерактивные формы обучения, которые направлены на стимулирование познавательного интереса. С этой целью будет использоваться метод разбора конкретных ситуаций.

Метод разбора конкретных ситуаций предполагает переход от метода накопления знаний к практико-ориентированному обучению специалиста-менеджера. В результате проведения индивидуального анализа, обсуждения в группе, определения проблем, нахождения альтернатив, выбора действий и плана их выполнения обучающиеся получают возможность развивать навыки маркетингового анализа и планирования.

Разработка практических ситуаций может происходить двумя путями: на основе описания реальных событий и действий или на базе искусственно сконструированных ситуаций. Слушатели намного более заинтересованы в анализе практических ситуаций, учитывающих специфику управления в нашей стране. Сюда можно отнести проблемы, с которыми сталкиваются начинающие руководители в современных условиях нестабильной экономической обстановки, а также типичные проблемы, решаемые руководящими работниками разных уровней

При проведении практических занятий используются такие *инновационные методы* обучения, как диалог-собеседование, коллективное обсуждение тематических вопросов, разбор практических ситуаций (метод кейсов), нормативных документов, теоретических и методических аспектов по темам дисциплины.

Обсуждение и оценка правильности выполненных различного типа заданий, указанных в фонде оценочных средств рабочей программы, производится коллективно студентами под руководством преподавателя.

Консультации – групповые занятия, являющиеся одной из форм контроля самостоятельной работы студентов в течение семестра. На консультациях по инициативе студентов рассматриваются и обсуждаются различные вопросы тематики дисциплины, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

LMS Электронный университет Moodle ЯрГУ, в котором размещен электронный учебный курс - онлайн-курс «**Экономические вопросы обеспечения информационной безопасности**», разработанный доцентом кафедры мировой экономики и статистики, кэн Зеткиной О.В., который расположен по адресу: https://moodle.uniyar.ac.ru/course/view.php?id=15162

Данный курс содержит:

- задания для самостоятельной работы обучающихся по темам дисциплины;
- средства текущего контроля успеваемости студентов (тестирование);
- презентации и тексты лекций по темам дисциплины;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:
1)для формирования текстов материалов для промежуточной и текущей аттестации – программы:
- Microsoft Office, Adobe Acrobat Reader DC.
-электронный университет Moodle
2)для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").
3) информационные справочные системы, в т.ч. профессиональные базы данных:
- справочная правовая система ГАРАНТ;
- справочная правовая система КонсультантПлюс
3) Программные продукты
- электронные таблицы Excel MS Office,
- ППП «1С: Предприятие»

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература:

1. Бусов, В. И. Управленческие решения : учебник для вузов / В. И. Бусов. — Москва : Издательство Юрайт, 2020. — 254 с. — (Высшее образование). — ISBN 978-5-534-01436-5. - Текст : электронный // Образовательная платформа Юрайт [сайт]. — Режим доступа: URL: https://urait.ru/bcode/449843

2.Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. Текст : электронный // Образовательная платформа Юрайт [сайт]. — Режим доступа: URL: https://urait.ru/bcode/454453

б) дополнительная литература

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. - Текст : электронный // Образовательная платформа Юрайт [сайт]. — Режим доступа: URL: https://urait.ru/bcode/468273

2.Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1 Текст : электронный // Образовательная платформа Юрайт [сайт]. — Режим доступа: URL: https://urait.ru/bcode/468273

3.Сковиков, А. Г. Цифровая экономика. Электронный бизнес и электронная коммерция : учебное пособие для вузов / А. Г. Сковиков. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 260 с. — ISBN 978-5-8114-6857-7.- Текст : электронный - Режим доступа: URL: https://e.lanbook.com/book/152653

в) ресурсы сети «Интернет»

1. Аналитический обзор систем электронного документооборота, http://www.cio-world.ru/analytics/34692/
2. Анташов В. и др. Разработка систем документооборота для корпорации, http://citforum.ru
3. Электронный каталог Научной библиотеки ЯрГУ (https://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
4. Электронная библиотечная система (ЭБС) издательства «Юрайт» (https://www.urait.ru).
5. Электронная библиотечная система (ЭБС) издательства «Проспект» (http://ebs.prospekt.org/).
6. Научная электронная библиотека (НЭБ) (http://elibrary.ru)
7. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).
8. https://exportcenter76.ru/ - Центр экспорта ярославской области официальный сайт
9. Экономико-статистические ресурсы Internet:
   - www.gks.ru – Госкомстат РФ.
   - www.cbr.ru – Центральный банк Российской Федерации.
   - www.cea.gov.ru – Аналитический центр при правительстве Российской Федерации.
   - www.fcsm.ru – Федеральная служба по финансовым рынкам.
   - www.rbk.ru – РБК (РосБизнесКонсалтинг).
   - www.stat.hse.ru – Статистическая база данных НИУ ВШЭ.

- http://prognoz.org – Прогнозы и прогнозирование. Методы прогнозирования. Технологии.
- repec.org – RePEc (Research Papers in Economics) – база данных, содержащая статьи, различные материалы по экономике (на англ. яз.).
- www.cemi.rssi.ru – Центральный экономико-математический институт РАН (ЦЭМИ).
- www.forecast.ru/mainframe.asp – Центр макроэкономического анализа и прогнозирования.
- www. ecfor.ru – Институт народнохозяйственного прогнозирования РАН.
- www.rtsnet.ru – Российская торговая система.
- www.micex.ru – Московская межбанковская валютная биржа.
- Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
- - учебные аудитории для проведения занятий лекционного типа;
- - учебные аудитории для проведения практических занятий (семинаров);
- - учебные аудитории для проведения групповых и индивидуальных консультаций;
- - учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- - помещения для самостоятельной работы;
- - помещения для хранения и профилактического обслуживания технических средств обучения.
- Специальные помещения укомплектованы средствами обучения, служащими для представления учебной информации большой аудитории.
- Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, хранящиеся на электронных носителях и обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплин.
- Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.
- Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор:

доцент, к. э. н. Зеткина О.В.

Приложение №1 к рабочей программе дисциплины
«Экономические вопросы обеспечения информационной безопасности»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Список вопросов и (или) заданий для проведения текущей аттестации

1.Контрольные задания и иные материалы. Задания для самостоятельной работы, используемые в процессе текущей аттестации (И-УК-1_1, И-УК-1_2, И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)

*Практическая работа №1.Рассмотрение и анализ Доктрины информационной безопасности Российской Федерации***(И-УК-1_1, И-УК-1_2, И-УК-2_3, И-УК-2_4)**

Проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности; определить положения государственной политики в области обеспечения ИБ, выделить первоочередные мероприятия по обеспечению ИБ, дать им оценку.

Практическая работа №2 Определение целей защиты информации на предприятии регионального уровня **(И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)**

Проанализировать структуру местного предприятия, рассмотреть виды информации и носители, используемые в его подразделениях. Сформулировать цели защиты информации на данном предприятии. Составить программу информационной безопасности.

Практическая работа №3 Рассмотрение особенностей объекта защиты информации
Используя данные предыдущей практической работы, рассмотреть особенности каждого типа носителей информации, отметить плюсы и минусы каждого типа, условия хранения и обработки. **(И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)**

2. Критерии оценки форм текущего контроля

Критерии оценки теста

Тест – инструмент оценивания уровня знаний студентов, состоящий из системы тестовых заданий, стандартизованной процедуры проведения, обработки и анализа результатов.

Оценка «отлично» выставляется при условии правильного ответа студента на более чем 85 % тестовых заданий.

Оценка «хорошо» выставляется при условии правильного ответа студента на 71-85 % тестовых заданий.

Оценка «удовлетворительно» выставляется при условии правильного ответа на 56-70 % тестовых заданий.

Оценка «неудовлетворительно» выставляется при условии правильного ответа на 55 % тестовых заданий и менее.

Критерии оценки устного опроса (диалога-собеседования) по конкретным ситуациям

Опрос – метод контроля знаний, заключающийся в осуществлении взаимодействия между преподавателем и студентом посредством получения от студента ответов на заранее сформулированные вопросы.

Оценка «отлично» выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.

Оценка «хорошо» выставляется за полный ответ на поставленный в опрос в объеме лекции с включением в содержание ответа материалов учебников с четкими ответами на наводящие вопросы преподавателя.

Оценка «удовлетворительно» выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.

Оценка «неудовлетворительно» выставляется за ответ, в котором озвучено менее половины требуемого материала или не озвучено главное в содержании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Критерии оценки практического задания

Выполнение практических заданий – метод контроля знаний, заключающийся в осуществлении взаимодействия между преподавателем и студентом посредством получения от студента ответов на заранее сформулированные вопросы.

Оценка «отлично» выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.

Оценка «хорошо» выставляется за полный ответ на поставленный в опрос в объеме лекции с включением в содержание ответа материалов учебников с четкими ответами на наводящие вопросы преподавателя.

Оценка «удовлетворительно» выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.

Оценка «неудовлетворительно» выставляется за ответ, в котором озвучено менее половины требуемого материала или не озвучено главное в содержании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Критерии оценки вопросов для самостоятельного изучения по шкале зачтено / не зачтено

Вопросы для самостоятельного изучения – метод контроля знаний, заключающийся в предварительном изучении заранее сформулированных вопросов по темам дисциплины с последующим ответом на них во время индивидуальных или групповых консультаций. Критерии оценки: правильность ответа на предложенный для самостоятельного изучения вопрос; культура речи.

Оценка «зачтено» – полное или частичное соответствие критериям.

Оценка «не зачтено» – несоответствие критериям.

1.2. Список вопросов и (или) заданий для проведения промежуточной аттестации
1. Вопросы (И-УК-1_1, И-УК-1_2, И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)

Вопросы к теме 1

1. Проведите анализ существующих толкований понятий "электронная коммерция", "электронный бизнес".
2. Раскройте специфику организации бизнеса в условиях интернет-среды.
3. Раскройте состав организационных, правовых, технологических вопросов, требующих обязательного рассмотрения при организации бизнеса на рынке электронной коммерции.
4. Какие изменения претерпевает система маркетинга фирмы, функционирующей в интернет-среде?
5. Дайте характеристику основных моделей электронной коммерции (B2C, B2B).
6. В чём состоят основные признаки интернет-экономики?
7. Каковы тенденции развития мирового рынка информационных технологий и их влияние на экономический рост, эффективность бизнес-процессов, рынок труда, финансовые рынки?
8. Дайте определение конкурентной среды фирмы. Назовите основные методы конкуренции, раскройте возможность их действия на рынке электронной коммерции.
9. В чём специфика интернет-среды как основы рынка электронной коммерции?
10. Раскройте характеристики основных конкурентных сил на рынке электронной коммерции.

Вопросы к теме 2

1. Сформулируйте основные цели и задачи, связанные с обеспечением безопасности электронной коммерции, прокомментируйте на примерах.
2. Какие основные стандарты, связанные с обеспечением безопасности информации Вы знаете?
3. Какие протоколы передачи информации наиболее безопасны?
4. Прокомментируйте основные этапы использования электронно-цифровой подписи.
5. Какие типовые ошибки, связанные с безопасностью электронной коммерции Вы знаете?

Практические задания (И-УК-1_1, И-УК-1_2, И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)

2.

На зачете предполагается ответ студента на вопрос из предложенной базы Выполнение заданий предполагает их представление в форме **презентации** (общие правила представления проектов).

1. **Практическое задание 1. (И-УК-1_1, И-УК-1_2)**

   Задание 1. Выполнить оценку информационной безопасности ИС «1С: Предприятие» на основе выбора критериев и показателей. Представить отчет, указав цель, методы и результаты.

   Задание 2. Сравнить информационную безопасность системы «1С: Предприятие» с любой на выбор.

3. **Практическое задание 2. (И-УК-2_3, И-УК-2_4, И-УК-3_1, И-УК-3_2)**

   Выполнить указанные НИЖЕ В ТЕКСТЕ задания.

Как показывает опыт, одной из наиболее сложных проблем обеспечения информационной безопасности является объяснение руководителю организации в доходчивой форме, чем именно занимается коллектив специалистов по информационной безопасности, почему на

эту работу нужно тратить значительные финансовые и иные ресурсы, чего именно можно ожидать в результате этих затрат и как он лично может убедиться в том,что выделенные ресурсы не потрачены впустую. Подобные вопросы возникают не только на уровне руководства организации, но и на уровне многих руководителей федерального, регионального и местного масштаба предприняли попытку поставить и решить задачу развития стандартов обеспечения информационной безопасности применительно к деятельности коммерческой организации, увязать связанные с этим вопросы с бизнес-процессами, которые для любой коммерческой организации являются приоритетными. (Примеры процессов из 1С в задании 1 и для выбранной системы в задании 2)

Нередко подход к стандартизации процессов обеспечения информационной безопасности организации базируется на результатах философского осмысления проблемы, ее сущности, а кроме того, на возможных проявлениях в реальной жизни и на разработке структурированных описаний (схем-моделей) стандартизируемых процессов (Пример подхода 1С в задании 1 и для выбранной системы в задании 2).

На основе изучения роли и места информации в бизнес-процессах, а также анализа видов информации, в которых данные процессы проявляются (учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы и т. п.), требуется разработать обобщенную схему — модель информационной безопасности бизнеса. Данная модель должна быть основана на анализе источников возникновения рисков снижения эффективности бизнеса, возникающих в информационной сфере организации. На основе анализа известных схем — моделей осуществления менеджмента разработать схему — модель управления процессами обеспечения информационной безопасности организации или управления рисками нарушения ее информационной безопасности. С учетом устоявшегося подхода к унификации описаний процессов менеджмента можно предложить стандартизованное описание системы менеджмента информационной безопасности организации, а также реализацию ее отдельных составляющих (менеджмента рисков, инцидентов, активов, документов и т. п.).

Рассмотреть возможные методики оценки уровня информационной безопасности организации и примеры их использования. (Примеры на основе 1С в задании 1 и на основе выбранной системы в задании 2)

Для общего рассмотрения проблемы.

В середине 1970-х гг. в связи с созданием крупных баз данных и переводом все больших объемов информационных ресурсов в цифровую форму в проблеме защиты информации наметился сдвиг от инженерного подхода к вопросам информатики в область управления доступом к вычислительным и информационным ресурсам, что нашло отражение в итоге в создании в США знаменитой Оранжевой книги, использованной впоследствии для разработки отечественных требований по защите информации в автоматизированных системах Гостехкомиссии СССР (позднее ГТК России, сейчас ФСТЭК).

Но потенциал этой идеи в силу ее статичности был достаточно быстро исчерпан, в середине 1990-х гг. Оранжевая книга, как отжившая идея, была публично сожжена, а международными экспертами в области безопасности в примерно в одно время было сформировано два направления развития — создание технических стандартов по обеспечению безопасности продуктов информационных технологий под общим названием «Общие критерии» (Дополнить своими дом работами) и создание семейства стандартов качества, а в последнее время — управления, под обобщенным названием «Стандарты аудита безопасности» (Дополнить своими дом работами). Стало очевидно, что «Общие критерии» не получили широкого распространения в силу ряда причин (ограниченность сферы применения, сложность и ограниченность используемых

механизмов оценок), поэтому началась их активная доработка в направлении второй группы стандартов,
а сама группа стандартов аудита обогатилась концепцией «риск-ориентированного подхода», что означало фундаментальные изменения в концептуальных взглядах на проблему безопасности в целом и сдвиг проблемы защиты информации, а если точнее — информационной безопасности в сферу управления сложными техническими системами и коллективами, как эксплуатационного персонала, так и пользователей. В последнее время в теории и практике управления возникло еще одно направление — создание стандартов управления организациями, имеющее своей целью оптимизацию внутренней структуры организации для получения максимального результата от их деятельности (реинжиниринг). Появились «Стандарты управления деятельностью организаций», которые рассматривают общие вопросы управления сложно организованными коллективами людей.

Безопасность как самостоятельный объект исследования также имеет некоторые фундаментальные свойства:
— безопасность никогда не бывает абсолютной — всегда есть некий риск ее нарушения, таким образом, усилия по обеспечению безопасности реально сводятся к задаче понижения уровня риска до приемлемого уровня, не более; (Какой % приемлем? Как определяют? Согласно Стандартам или эмпирически?)
— измерить уровень безопасности невозможно, можно лишь косвенно его оценить, измерив соответствующие показатели, характеризующие состояние безопасности системы; в связи с этим можно говорить только о вероятности наступления того или иного события и степени его последствий, т. е. использовать для оценок уровня безопасности рисковый подход;
— наступление рискового события в общем случае предотвратить невозможно, можно лишь понизить вероятность его наступления, т. е. добиться того, что такие события будут наступать реже;
— можно также понизить степень ущерба от наступления такого события, но при этом чем реже наступает рисковое событие, тем сильнее ущерб от них;
— при любом вмешательстве в систему в первую очередь страдает ее безопасность.

Оказалось, что для анализа свойств безопасности сложных систем,состоящих из технических компонент людей, взаимодействующих друг с другом, в полной мере могут быть применены некоторые социологические и психологические правила, выведенные на основе наблюдения за развитием процессов и событий:
-Закон Парето(универсальный закон неравенства), сформулированный итальянским экономистом и социологом Вильфредо Паретов соответствии с которым первые 20% усилий дают 80% результатов или 80% всех проблем порождаются человеком (персоналом) и лишь 20% приходится на долю технического оборудования (по оценкам специалистов, эта доля может доходить до соотношения 94:6%). (Ваш пример из теории или, возможно , практики)
-Методологический принцип, получивший название по имени английского философа-номиналиста Уильяма Оккама (Ockham, ок. 1285–1349), гласящий: «То, что можно объяснить посредством меньшего, не следует выражать посредством большего» (В соответствии с ним при равной вероятности событий с различной степенью тяжести последствий, как правило, первым случается событие, степень тяжести последствий которого меньше. Из этого также следует, что злоумышленник, планируя атаку на ресурс, из всех воз-
можных будет выбирать наиболее простой способ осуществления своих целей, а вирусы будут попадать в систему наиболее простым способом. Этот принцип следует дополнить следующим наблюдением: степень тяжести последствий растет обратно пропорционально частоте их возникновения. (Ваш пример из теории или, возможно , практики)

-Правило связиста: связиста замечают только тогда, когда пропадает связь. (Ваш пример из теории или, возможно , практики)
-Парадокс «крысиного короля», хорошо знакомый морякам: можно избавиться от крыс на корабле, заведя крысу — ≪крысоеда≫, но через некоторое время он даст потомство, бороться с которым будет еще сложнее. (Ваш пример из теории или, возможно , практики)

Аспектов обеспечения информационной безопасности бизнеса достаточно много, но в целом есть и ряд общих моментов,на которых следует коротко остановиться.
-Ведение бизнеса всегда предполагает наличие некого первоначального капитала, актива, который вкладывается в некое ≪дело≫ с целью получения прибыли. Все остальное, не имеющее актива, к бизнесу не относится и не рассматривается.
-Эффективность бизнеса тем выше, чем выше прибыль — это аксиома.
-На величину прибыли влияет несколько факторов, среди них выделяются наиболее существенные:
— величина внутренних издержек, в том числе на содержание коллектива и затрат на обеспечение безопасности в том числе. В результате задания неправильных требований по безопасности, величина издержек может стать настолько обременительной, что сделает бизнес не эффективным;
— качество управления собственным активом. Если кроме собственника актива или его представителя активом может управлять еще кто-то в собственных интересах, то актив может разворовываться, а бизнес — существенно ухудшаться. Пример— хищение средств в карточных платежных системах и в системах дистанционного банковского обслуживания;
— качество работы коллектива, обеспечивающего бизнес; (Ваш пример из теории или, возможно , практики)
— скорость реакции коллектива на внешние факторы, влияющиена бизнес, или на управляющие воздействия; (Ваш пример из теории или, возможно , практики)
— стратегия и качество ведения самого бизнеса;
— выбранная стратегия управления рисками, в том числе экономическими рисками и рисками информационной безопасности. (Ваш пример из теории или, возможно , практики)

Следует также отметить, что бизнес ведется, как правило, во враждебной среде, в условиях конкурентной борьбы, неблагоприятного законодательства, риска рейдерства, часто нескоординированной деятельности различных надзорных органов. Особое место в этом списке занимает криминал, стремящийся отнять или поставить под контроль прибыль от вло-
жения активов. Наиболее в острой форме это появляется в банковском бизнесе, поскольку банки работают с самой сублимированной формой активов — деньгами, а атака на них наиболее результативна, потому что приносит быстрые и ощутимые результаты.

Поэтому все большее значение приобретает прогноз, то есть модели-
рование возможных рисковых ситуаций и разработка превентивных защитных мер, позволяющих избежать (отразить, уклониться) последствий от атак на бизнес или на среду, обеспечивающую использование активов,составляющих основной элемент бизнеса.(Какие математические методы используют для прогнозирования?)
Также следует отметить, что среди всего набора угроз и рисков существует определенная иерархия, по силе воздействия и уровню катастрофичности для бизнеса угрозы серьезно различаются. Так, политические риски или риски несоответствия законодательству являются для бизнеса определяющими, так как способны вне зависимости, насколько качественно осуществляется работа по минимизации рисков информационной безопасности физически уничтожить бизнес (лишение лицензии, налоговые штрафы и т. д.). К сожалению, следует говорить и о рисках, возникавших и при взаимодействии с

правоохранительными органами, например, когда в ходе расследования изымались оригиналы документов или сервера с базами данных, что неминуемо ведет к катастрофическим последствиям для организации. С другой стороны, при абсолютно благоприятном внешнем политическом, законодательном и экономическом фоне, реализация рисков информационной безопасности может нанести субъекту бизнеса ущерб такого размера, от которого оправиться крайне сложно.

Таким образом, существует ряд рисков, включая риски информационной безопасности, ущерб от которых может быть неприемлем для субъекта бизнеса. В то же время некоторые общие риски политического, экономического и правового характера обладают ≪кумулятивным≫ эффектом и способны нанести системный ущерб, затрагивающий практически все сферы деятельности организации.

Что касается угроз информационной безопасности бизнеса, то их условно тоже можно разделить на две группы:

— традиционные угрозы безопасности информации, такие как нарушение конфиденциальности или неправомерное использование информации, реализуемые через новые механизмы, возникшие в результате использования информационных систем; (Примеры на основе 1С в задании 1 и на основе выбранной системы в задании 2)

— новые угрозы, порожденные спецификой информационных систем — вирусы, сетевые атаки, нарушения функционирования и отказы разного рода, всевозможные нарушения персоналом установленных регламентов, инструкций и предписаний по эксплуатациии обслуживанию информационных систем.

Целью информационных воздействий является в первую очередь ослабление контроля за счет создания иллюзии, что бизнес-процесс идет нормально и эффективно. (Примеры на основе 1С в задании 1 и на основе выбранной системы в задании 2) Наиболее характерные примеры: искажение отчетности и лоббирование при принятии решений. В обоих случаях результатом, как правило, являются необоснованное увеличение (раздувание) активов и выделение (≪выколачивание≫) для ≪своего≫ подразделения организации избыточного ресурса. Избыточные активы и ресурс затем используются в своих интересах. Это всем известная схема превращения информации в материальную выгоду. Ущерб от конфликта интересов может значительно превосходить потери от злоумышленных действий, и, что страшнее, конфликт интересов реально приводит к потере управления. Тенденции современного мира таковы, что бизнес, стремясь уменьшить издержки за счет ускорения процессов, все больше уходит в информационный мир, действия над материальными объектами во все большей степени замещаются действиями над их описаниями, т. е. над информацией. Эта тенденция и есть главный источник проблем информационной безопасности, поскольку в результате не только становятся возможными атаки с очень низким ресурсным и психологическим порогом их осуществления, но даже при отсутствии злоумышленных действий просто негативные свойства самой информационной сферы начинают отрицательно воздействовать на бизнес и приводить к серьезным потерям.

3.Критерии оценки форм текущего контроля

1. Критерии оценки по практическим заданиям

Оценивается по 2 балльной системе: ***«зачтено», «не зачтено».***

Оценка ***«зачтено»*** ставится, если:

- демонстрируемые студентом знания отличаются достаточной глубиной и содержательностью,
- дается достаточно полный ответ, как на основные вопросы, так и на дополнительные;
- студент достаточно свободно владеет терминологией;
- ответ студента не содержит принципиальных ошибок.

-практическое задание выполнено в целом успешно не менее, чем на 90%, но, возможно, содержит неполные ответы.

Оценка ***«не зачтено»*** ставится, если:

- обнаружено незнание или непонимание студентом основных разделов дисциплины;
- студент допускает существенные фактические ошибки, которые он не может исправить самостоятельно;
- на значительную часть дополнительных вопросов студент затрудняется дать правильный ответ;
- практическое задание выполнено менее, чем на 90% или содержит существенные ошибки.

2. Критерии ответа по вопросы к зачету

Оценка проводится по 10 балльной системе.

Баллы по ответу на зачете

- 10 баллов выставляется за полный ответ на поставленный вопрос с включением в содержание ответа лекции, материалов учебников, дополнительной литературы без наводящих вопросов.
- 8-9 баллов выставляется за полный ответ на поставленный вопрос в объеме лекции с включением в содержание ответа материалов учебников с четкими ответами на наводящие вопросы преподавателя.
-6-7 баллов выставляется за ответ, в котором озвучено более половины требуемого материала, с положительным ответом на большую часть наводящих вопросов.
4-5 баллов выставляется за ответ, в котором озвучено менее половины требуемого материала, с положительным ответом на половину наводящих вопросов.
Менее 4 баллов выставляется за ответ, в котором озвучено менее половины требуемого материала, не озвучено главное в содержании вопроса с отрицательными ответами на наводящие вопросы или студент отказался от ответа без предварительного объяснения уважительных причин.

Описание процедуры выставления оценки

Оценка на зачете оценивается по 2 балльной системе: ***«зачтено», «незачтено».***

Оценка на зачета складывается из 2х видов работ: практического задания и устного ответа. На зачете предполагается ответ студента на вопрос из предложенной базы и выполнение практического задания. Выполнение заданий предполагает их представление в форме **презентации** (общие правила представления проектов).

Оценка ***«зачтено»*** ставится, если студентом успешно выполнено практическое задание (оценка «зачтено») и по ответу на вопрос получено не менее 6 баллов из 10 (60%).

Приложение №2 к рабочей программе дисциплины
«Экономические вопросы обеспечения информационной безопасности»
Методические указания для студентов по освоению дисциплины

Успешное овладение дисциплиной «**Экономические вопросы обеспечения информационной безопасности»** предусмотренное рабочей программой, предполагает выполнение ряда рекомендаций.

1. Следует внимательно изучить материалы, характеризующие курс «**Экономические вопросы обеспечения информационной безопасности»** и определяющие целевую установку. Это поможет четко представить круг изучаемых проблем и глубину их постижения.

2. Необходимо знать подборку литературы, достаточную и необходимую для изучения предлагаемого курса. При этом следует иметь в виду, что нужна литература различных видов:

а) учебники, учебные и учебно-методические пособия.

б) монографии, сборники научных статей, публикаций в экономических журналах, представляющие эмпирический материал, а также многообразные аспекты анализа современного развития организаций;

в) справочная литература – энциклопедии, экономические словари, раскрывающие категориально понятийный аппарат.

г) аналитические материалы.

3. По ряду тем предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем устного опроса и решения практических задач. Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы механизма внешнеэкономической деятельности предприятий и фирм. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

4. Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

5. Для проверки и контроля усвоения теоретического материала и приобретенных практических навыков в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса и контрольных работ. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

6. В конце курса студенты сдают зачет. Вопросы к зачету представлены в программе. На самостоятельную подготовку к зачету выделяется 3 дня