Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Экономический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«_29_» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.13 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БИЗНЕСА

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки 38.03.05 Бизнес-информатика
(код и наименование направления подготовки)

Направленность (профиль) Электронный бизнес
(наименование направленности (профиля))

Программа подготовки Академическая
(академическая /прикладная)

Форма обучения Очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника Бакалавр
(бакалавр, магистр)

Краснодар 2020

1. Цели и задачи изучения дисциплины

1.1. Цель дисциплины

Дисциплина «Обеспечение безопасности электронного бизнеса» изучается в соответствии с Государственным образовательным стандартом высшего образования РФ и является одной из базовых дисциплин, изучаемых студентами специальности 38.03.05 - Бизнес информатика.

1.2 Задачи дисциплины

Задача курса состоит в получении представления о концепции информационной безопасности на основе информационных технологий и использования системного подхода для обеспечения безопасности электронного бизнеса. Существенное значение имеет изучение основных методов, протоколов и алгоритмов, реализующих защиту информации в сетях, получение навыков оценки существующих угроз информации для электронного бизнеса.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина входит в блок Б3.В.ОД.13 - вариативную часть обязательных дисциплин профессионального цикла учебного плана подготовки бакалавров направления 38.03.05 Бизнес-информатика, профиль подготовки «Электронный бизнес». Логически дисциплина увязана с такими основными базовыми курсами как «Общая экономическая теория», «Основы бизнеса», «Теоретические основы информатики», «Экономика фирмы», «Институциональная экономика», «Информационная безопасность», «Вычислительные системы», «Эффективность ИТ», «Анализ экономических систем», «Базы данных», «Менеджмент», «Общая теория систем», «Теория вероятностей и математическая статистика» и является дальнейшим развитием прикладных аспектов названных дисциплин.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате обучения выпускник приобретает профессиональные компетенции ПК-9 (организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия), ПК-27 (способность использовать лучшие

практики продвижения инновационных программно-информационных продуктов и услуг).

Изучение данной учебной дисциплины направлено на формирование у обучающихся *профессиональных* компетенций (*ПК)*

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Основные определения причин нарушения целостности информации, каналов несанкционированного получения информации, каналов копирования информации	Проводить анализ архитектуры предприятия на уязвимость	Методологией математического моделирования в прикладных областях; Элементами структурно-функционального мышления при решении задач формализации и алгоритмизации в конкретных областях деятельности.
2	ПК-27	способность использовать лучшие практики продвижения инновационных программно-информационных продуктов и услуг	современные стандарты де-юро, де-факто в области организации безопасности электронного бизнеса	использовать современные стандарты и методики, разрабатывать регламенты для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий	методиками оценки затрат ресурсов, методов их оптимизации и распределения

2. Структура и содержание дисциплины

2.1. Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице (*для студентов ОФО*).

Вид учебной работы	Всего часов	Семестры			
		VII	___ _		
Аудиторные занятия (всего)	50.2	50.2	-/-		
В том числе:					
Занятия лекционного типа	18	18	-/-		
Занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32	32	-/-		
КСР	6	6			
Самостоятельная работа (всего)	51.8	51.8	-/-		
В том числе:					
Курсовая работа	-/-	-/-	-/-		
Другие виды самостоятельной работы (выполнение домашних заданий)	-/-	-/-			
Вид промежуточной аттестации (зачет)	7	7	-/-		
Общая трудоемкость час	108	108	__		
зач. ед.	3	3	__		

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в VII семестре

№ раздела	Наименование раздела	Количество часов				
		Всего	Аудиторная работа			Самостоятельная работа
			Л.	П.з.	Л.р.	
1	2	3	4	5	6	7
1	Общее понятие безопасности и система мер по её обеспечению	10	2	2		6
2	Правовые аспекты и диагностические параметры экономической безопасности	12	2	4		6
3	Экономические разведка и контрразведка	10	2	2		6
4	Экономическая безопасность предприятия и основные её критерии и показатели	11	2	6		9
5	Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения.	10	2	6		4
6	Проблемы обеспечения безопасности предпринимательской деятельности в России.	6.8	2	4		4.8
7	Методы информационно-аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании	18	2	4		6
8	Защита компании от экономических рисков, связанных с участием компании в гражданско-правовых отношениях	16	2	2		6
9	Зарубежный опыт обеспечения безопасности предпринимательской деятельности	8	2	2		4
	Итого	101.8	18	32		51.8

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Общее понятие безопасности и система мер по её обеспечению	Категории «опасность» и «безопасность»: генезис и диалектика развития. Национальная безопасность государства. Основные определения экономической безопасности Роль и место экономической безопасности в системе национальной безопасности. Угрозы информации. Классификация угроз по видам, по природе происхождения, по предпосылкам появления, по источникам. Взаимодействие угроз информации .	Консультации Обсуждение.
2	Правовые аспекты и диагностические параметры экономической безопасности	Основные положения, концепции и Государственной стратегии экономической безопасности России. Критерии и индикаторы экономической безопасности страны. Основные понятия и определения. Классификация показателей экономической безопасности. Методы оценки экономической безопасности страны. Критерии базовых показателей экономической безопасности. Методы экспертной оценки. Доктрина информационной безопасности РФ. Закон о Государственной Тайне. Закон об информации, информационных технологиях и защите информации.	Консультации Обсуждение.
3	Экономические разведка и контрразведка	Причины возникновения и дальнейшего развития экономической разведки. Основные области интересов экономической разведки Внутренние угрозы безопасности объектов экономики Цель и задачи системы криминологической безопасности объекта. Организационно-управленческие аспекты функционирования системы обеспечения криминологической безопасности на специальном уровне. Политико-правовые проблемы обеспечения безопасности негосударственных объектов экономики.	Консультации Промежуточная аттестация
4	Экономическая безопасность предприятия и основные её критерии и показатели	Необходимость обеспечения экономической безопасности предприятия. «Экономическая безопасность предприятия» как экономическая категория. Основные направления и принципы обеспечения экономической безопасности	Консультации Обсуждение

		предприятия. Стратегическое планирование и прогнозирование экономической безопасности предприятия.	
5	Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения.	Функциональный анализ. Алгоритм анализа. Основные направления обеспечения экономической безопасности предприятия. Финансовая составляющая и её сущность. Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия. Интеллектуальная и кадровая составляющая(ИКС) экономической безопасности предприятия. Технико-технологическая составляющая(ТТС) экономической безопасности предприятия. Политико-правовая составляющая(ППС) экономической безопасности предприятия. Информационная составляющая(ИС) экономической безопасности предприятия.	Консультации Обсуждение
6	Проблемы обеспечения безопасности предпринимательской деятельности в России.	Деятельность коммерческих банков и компаний в условиях роста террористической угрозы Принципы организации профессионального отбора персонала в коммерческие предприятия. Увольнение кадров из коммерческих организаций. Проблемы защиты коммерческой тайны при увольнении персонала. Проблемы и перспективы развития частной правоохранительной деятельности в России.	Консультации
7	Методы информационно-аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании	Классификация информации и информационных ресурсов, применяемые информационные технологии, способы оценки информации, виды оперативного представления информационных услуг. Методы сбора информации, оценка информации и перевод её в сведения. Получение информации из «открытых источников» (из ресурсов Интернета, баз данных, средств массовой информации и т.д.). Методы анализа информации (SWOT-анализ, анализ конкурентной среды методом 5 сил Майкла Портера, диверсионный анализ, метод аналогии, метод исключения, анализ причинно-следственных связей, экспертные методы анализа и т.д.) Обзор автоматизированных информационно-аналитических систем, представленных на рынке	Консультации Обсуждение
8	Защита компании от экономических рисков, связанных с участием	Проверка надёжности организации перед заключением гражданско-правовых отношений.	Консультации Обсуждение

	компании в гражданско-правовых отношениях	Направления анализа предполагаемого контрагента. Определение безопасности предложений и коммерческих проектов. Растровые признаки опасности при определении надёжности контрагентов и коммерческих проектов Защита компании от внешнего мошенничества. Защита компании от рейдерства.	
9	Зарубежный опыт обеспечения безопасности предпринимательской деятельности	Частная правоохранительная деятельность в США. Проблемы взаимодействия правоохранительных органов с общественными организациями и частнопредпринимательскими структурами. Великобритания. Частные детективные агентства. Специфика законодательства и основные направления работы. Германия. Задачи и направления деятельности частных охранно-сыскных бюро. Особенности работы их сотрудников. Франция. Деятельность частных охранно-сыскных бюро. Основные направления работы частных служб промышленной и коммерческой безопасности. Япония. Борьба общественных организаций с преступностью. Динамика криминогенной обстановки в Японии и формы участия общественности в борьбе с преступностью.	Консультации Обсуждение

2.3.2 Занятия семинарского типа

№ раздела	**Наименование раздела**	**Содержание раздела**	**Форма текущего контроля**
1	**2**	**3**	**4**
1	Коммерческая тайна	Понятие "коммерческой тайны" в предпринимательской деятельности. Законодательство РФ в области защиты коммерческой тайны. Организации защиты коммерческой тайны в компании. Методика составления Перечня сведений, содержащих коммерческую тайну Внутренние нормативные документы, регламентирующие деятельность компании в области защиты коммерческой тайны. Положение об организации защиты сведений конфиденциального характера, составляющих коммерческую тайну Примерный договор об оформлении допуска сотрудников к коммерческой тайне. Примерная инструкция о порядке проведения внутреннего расследования по фактам незаконного получения и разглашения сведений, составляющих коммерческую	Консультации Обсуждение.

		тайну, нарушения порядка конфиденциального делопроизводства Организация конфиденциального делопроизводства в компании	
2	Конкурентная разведка. Стратегическое и оперативное направление информационно-аналитической работы	Основные задачи конкурентной разведки. Законодательство Российской Федерации об информации, информационных технологиях и защите информации. Законные способы сбора и анализа информации. Конкурентная разведка, бизнес разведка. Создание службы конкурентной разведки. Этапы конкурентной разведки. Понятие разведывательного цикла. Использование конкурентной разведки в инновационной деятельности компании, а также в бенчмаркинге.	Консультации Контрольная работа
3	Методы сбора информации, применяемые в конкурентной разведке	Классификация информации и информационных ресурсов. Первичная и вторичная информация. Влияние субъективных факторов на достоверность информации. Релевантность информации. Создание рубрикатора тем по основным направлениям сбора и анализа информации. Способы оценки информации. Процедура перевода информации в сведения. Виды оперативного представления информационных услуг. Получение информации из баз данных. Специализированные ресурсы с базами данных по отраслям бизнеса и территориям. Использование информационных ресурсов Интернета для задач конкурентной разведки. Работа в чатах, блогах, живых журналах и иных информационных массивах	Консультации Промежуточная аттестация
4	Аналитические методы, применяемые в конкурентной разведке	Методы анализа информации: SWOT-анализ, анализ конкурентной среды методом 5 сил Майкла Портера, диверсионный анализ, метод аналогии, метод исключения, анализ причинно-следственных связей, экспертные методы анализа и т.д. Обзор автоматизированных информационных систем, применяемых на рынке. Что может и для чего используются АИС. Обработка больших массивов информации, выстраивание связей между объектами учёта и работа по сценариям, а также иные алгоритмы, заложенные в АИС. Применение АИС для финансового анализа компании. Формирование корпоративных баз данных	Консультации Коллоквиум
5	Анализ надёжности контрагентов и безопасности коммерческих	Алгоритм определения надёжности партнёров – юридических лиц. Алгоритм определения надёжности партнёров – физических лиц. Формирование матрицы	Консультации Коллоквиум

	предложений	действий по проверке компании в зависимости от суммы сделки, предоплаты и иных условий. Применение метода Due Diligence в анализе компании. Анализ финансовой устойчивости компании по представленным финансовым отчётным документам - баланс, отчет о прибылях и убытках, отчёт о движении капитала и т.д. Анализ платёжеспособности клиента. Анализ возможных кризисных ситуаций в деятельности компании на основе статистических методов, использующих информацию о времени деятельности компании, её обороте и количестве работающих сотрудников. Применение на практикеэмпирического закона больших чисел Бенфорда. Анализ учредительных документов компании с позиции безопасности. Анализ атрибутов компании и фирменного стиля компании	
6	Практика решения информационно-аналитических задач службы безопасности компании	Формирование информационно-аналитического поля службы безопасности компании. Нормативные документы, регламентирующие цели, источники, порядок получения и использования информации для задач службы безопасности. Подготовка аналитических документов (досье, отчёт, справка, доклад). Применение методов деловой разведки при решении стратегических и тактических задач службы безопасности. Работа с источниками текстовой информации. Методы анализа документов. Сценарные методы прогнозирования	Консультации
7	Организация корпоративной системы противодействия промышленному шпионажу	Элементы контрразведывательной деятельности в работе службы безопасности предприятия. Координация деятельности структурных подразделений предприятия по выявлению агентуры конкурента, «агентов влияния» и т.д. Привлечение сотрудников своего предприятия к участию в работе службы безопасности Инсайдеры. Методы борьбы с инсайдерами	Консультации Контрольная работа
8	Организация режима и охраны предприятия	Режим охраны негосударственных предприятий. Классификация видов режима охраны Пропускной режим. Внутриобъектовый режим. Режим конфиденциальности. Правовые основы охранно-пропускного режима. Технические средства	Консультации Промежуточная аттестация
9	Обзор российского рынка средств безопасности. Тактико-технические и	Системы инженерно-технического обеспечения. Охрана периметра. Системы охранной сигнализации. Системы видеонаблюдения. Технические средства	Аналитический обзор по проблеме.

	стоимостные характеристики. Компании-производители технических средств	противодействия промышленному шпионажу. Программно-аппаратные средства защиты информации	
10	Экономические аспекты обеспечения безопасности предприятия	Оценка эффективности безопасности предприятия. Методика оценки стоимости методов обеспечения безопасности предприятия. Организационные, технические и прочие методы	Консультации
11	Цели и задачи системы безопасности на объектах коммерческой недвижимости	Определение угроз безопасности коммерческой недвижимости. Цели и содержание угроз внешней и внутренней среды. Прогнозирование возможных негативных последствий от рисков и угроз. Классификация рисков и угроз объектам недвижимости. Категории объектов и классификация основных зон/помещений объектов коммерческой недвижимости в зависимости от уровня рисков и угроз. Цели и задачи организации системы внутриобъектового и пропускного режимов на объектах	Аналитический обзор по проблеме.
12	Хозяйственные риски объектов коммерческой недвижимости	Система хозяйственных рисков объекта. Виды и функции. Методы прогнозирования хозяйственных рисков. Оценка и минимизация хозяйственных рисков для объектов коммерческой недвижимости. Рекомендации по организации внутренних контрольных мероприятий и проведению инвентаризаций	Консультации
13	Методы сокращения потерь для объектов коммерческой недвижимости	Элементы системы предотвращения потерь для объектов недвижимости. Специфика и назначение основных субъектов предотвращения потерь. Типовые решения организации системы предотвращения потерь. Предотвращение потерь без службы безопасности. Предотвращение потерь с использованием службы безопасности	Консультации Контрольная работа
14	Мероприятия по обеспечению безопасности объекта коммерческой недвижимости	Разработка мероприятий по решению задач безопасности. Организация противодействия рискам и угрозам с позиции системы безопасности. Необходимые документы, регламентирующие деятельность Службы Безопасности (СБ) на объектах коммерческой недвижимости. Правовые и организационные вопросы обеспечения информационной безопасности и сохранности коммерческой тайны. Пути совершенствования структуры и организации СБ на объекте коммерческой недвижимости	Консультации Промежуточная аттестация
15	Методика разработки концепции безопасности	Цели, задачи и принципы политики безопасности. Взаимосвязь и интеграция в технологии, осуществляемые на объекте коммерческой недвижимости. Организация системы защиты объекта коммерческой	Подготовка рефератов, презентаций, выступлений. Резюме,

		недвижимости. Систематизация управления безопасностью. Особенности системного подхода к безопасности	аналитический обзор по проблеме.
16	Проведение аудита безопасности на объектах коммерческой недвижимости	Необходимость, содержание и периодичность проведения аудита безопасности на объектах коммерческой недвижимости. Алгоритм проведения аудита безопасности объекта. Как правильно определить объекты, сроки и направления аудита безопасности. Проведение аудита безопасности собственными силами или с использованием аутсорсеров. Преимущества и недостатки. Критерии выбора сторонней организации для проведения аудита и разработки концепции безопасности. Планирование аудиторских мероприятий. Применение полученных итогов аудита в целях усиления защиты объектов коммерческой недвижимости	Подготовка рефератов, презентаций, выступлений.
17	Конфиденциальная информация в компании	Законодательство Российской Федерации в области защиты информации. Правовые основы наличия в компании конфиденциальной информации. Информация, доступ к которой не может быть ограничен. Структура конфиденциальных информационных массивов. Источники конфиденциальной информации. Виды и формы представления конфиденциальной информации. Коммерческая тайна как составная часть конфиденциальной информации. Законодательство Российской Федерации в области коммерческой тайны. Процедуры создания в компании режима коммерческой тайны. Персональные данные как составная часть конфиденциальной информации.	Консультации Контрольная работа
18	Основные направления защиты конфиденциальной информации в компании	Организационные мероприятия по защите конфиденциальной информации. Анализ информационных ресурсов компании. Определение информации, подлежащей обязательной защите и информации, которая может быть защищена. Оптимизация информационных потоков в компании. Определение формы представления информационных ресурсов, подлежащих защите. Дробление информации на части, как эффективный организационный способ защиты информации. Режимные мероприятия по защите конфиденциальной информации. Создание внутриобъектного и контрольно-пропускного режимов в компании. Физическая защита охраняемых информационных ресурсов. Способы хранения информации вне территории компании. Кадровые мероприятия по защите конфиденциальной информации.	

		Распределение прав доступа к информации. Разглашение информации через «человеческий фактор», как основной канал утечки конфиденциальной информации. Процедура проведения внутрикорпоративного расследования по факту разглашения конфиденциальной информации. Инженерно-технические мероприятия по защите конфиденциальной информации. Применение систем видеонаблюдения для защиты материальных носителей информации. Возможность использовать видеозаписи как доказательства противоправных действий с защищаемыми информационными ресурсами	

2.3.3 Лабораторные занятия

Лабораторные занятия – не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Наименование раздела	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Общее понятие безопасности и система мер по её обеспечению	Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 Иванов М.А. Криптографические методы зашиты информаци в компьютерных системах и сетях / Иванов М.А.
2.	Правовые аспекты и диагностические параметры экономической безопасности	Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422 Иванов М.А. Криптографические методы зашиты

		информаци в компьютерных системах и сетях / Иванов М.А.
3.	Экономические разведка и контрразведка	Информационная безопасность : учебник для студентов вузов / Ярочкин, Владимир Иванович ; В. И. Ярочкин Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. — Электрон. дан. — Минск : "Вышэйшая школа", 2017. — 324 с. — Режим доступа: https://e.lanbook.com/book/75150. — Загл. с экрана.
4.	Экономическая безопасность предприятия и основные её критерии и показатели	Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 Иванов М.А. Криптографические методы зашиты информаци в компьютерных системах и сетях / Иванов М.А.
5.	Анализ уровня экономической безопасности предприятия(ЭБП) и основные направления её обеспечения.	Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422 В. П. Мельников, С. А. Клейменов, А. М. Петраков; Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков
6.	Проблемы обеспечения безопасности предпринимательской деятельности в России.	Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 Информационная безопасность : учебник для студентов вузов / Ярочкин, Владимир Иванович ; В. И. Ярочкин
7.	Методы информационно-аналитической работы (конкурентной разведки),	Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-

	применяемые для определения и оценки экономических рисков компании	68E0EF829422 Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков.
8.	Защита компании от экономических рисков, связанных с участием компании в гражданско-правовых отношениях	Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. — Электрон. дан. — Минск : "Вышэйшая школа", 2017. — 324 с. — Режим доступа: https://e.lanbook.com/book/75150. — Загл. с экрана. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков
9.	Зарубежный опыт обеспечения безопасности предпринимательской деятельности	Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. — Электрон. дан. — Минск : "Вышэйшая школа", 2017. — 324 с. — Режим доступа: https://e.lanbook.com/book/75150. — Загл. с экрана. В. П. Мельников, С. А. Клейменов, А. М. Петраков Информационная безопасность : учебник для студентов вузов / Ярочкин, Владимир Иванович ; В. И. Ярочкин

3. Образовательные технологии

В процессе обучения используются технологии личностно-ориентированного обучения, а также построения индивидуальных образовательных траекторий.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущей аттестации

Перечень примерных заданий

Тема: Общее понятие безопасности и система мер по её обеспечению

1. Как трактуется политика безопасности в Документах Гостехкомиссии России?
2. Аналогичны ли термины квалификационный анализ и сертификационные испытания?
3. Верно ли, что дискреционное управление доступом основывается на заданном множестве разрешенных отношений доступа?

4. Какое управление доступа определяется множеством атрибутов безопасности субъектов и объектов?
5. Какое понятие, используемое в стандартах, гарантирует, что передаваемая информация не подвергается искажению?
6. Верно ли, что угрозы конфиденциальности включают в себя угрозы целостности?
7. Каким требованиям обязательно противоречат требования безопасности?
8. Что позволяет экспертам по квалификационному анализу оценить уровень безопасности, обеспечиваемый продуктами информационных технологий?
9. В каком документе были впервые нормативно определены такие понятия, как ТСВ и и политика безопасности?
10. Какие базовые требования безопасности "Оранжевой книги" направлены на качество безопасности?
11. Действительно ли, что системы класса А1 ("Оранжевая книга") функционально эквивалентны системам класса В2?
12. Чем вызвана потеря актуальности рядом положений "Оранжевой книги"?
13. Как отражают критерии адекватности реализацию средств защиты в "Оранжевой книге"?
14. Какие аспекты включает в себя требование адекватности в "Европейских критериях безопасности информационных технологий"?
15. Какому классу по стандарту "Оранжевой книги" соответствует класс F-DI?
16. Какие фазы жизненного цикла системы анализируются припроверке уровня адекватности согласно требованиям "Европейских критериев безопасности информационных технологий"?

Тема: Правовые аспекты и диагностические параметры экономической безопасности

1. Главное достижение "Европейских критериев безопасности информационных технологий"?
2. Какая мера защиты от угроз работоспособности вообще не упоминается в документах Гостехкомиссии России?
3. Чем отличаются группы классов защищенности АС от НСД согласно документам Гостехкомиссии России?
4. Основное достоинство стандарта "Документы Гостехкомиссии России"?
5. Какое понятие концепции информационной безопастности "Федеральных критериев безопастности информационных технологий" является ключевым?
6. Идентичны ли назначение и структура Профиля защиты в "Федеральных критериях безопастности информационных технологий" и в "Единых критериях безопастности информационных технологий"?
7. Что может выступать в качестве тега пользователя в "Канадских критериях безопастности информационных технологий"?
8. Что входит в политику аудита в "Федеральных критериях безопастности информационных технологий"?
9. Что называется независимым ранжированием требований в каждой группе?

10. Какое понятие "Оранжевой книги" заменено понятием "процесс" в "Канадских критериях безопастности информационных технологий"?
11. Чем отличается Профиль защиты от Проекта защиты?
12. Какие категории требований безопастности есть в "Единых критериях безопастности информационных технологий"?
13. Что отражает уровни безопастности внутри каждой группы функциональных требований в "Канадских критериях безопастности информационных технологий"?
14. Какой показатель стандарта отражает возможность адекватной реализации требований?
15. Что отражает гарантированность стандарта?

Тема: Экономические разведка и контрразведка

1. Как классифицируются угрозы по природе происхождения?
2. Что представляют собой объективные предпосылки угроз информации?
3. Перечислите источники угроз информации?
4. Причиной чего являются угрозы информации?
5. Что входит в систему показателей уязвимости информации?
6. Что есть ПНЦИ?
7. Является ли агрегиронной группа ПНЦИ "Отказ системы передачи данных?" Почему?
8. Как получили 6 классов КНПИ?
9. К какому классу КНПИ относится подмена аппаратуры?
10. Какие компоненты требуют защиты от несанкционированного размножения информации?
11. Совокупность каких факторов определяет конкретные требования к защите системы обработки данных?
12. Какие требования к защите обусловлены территориально - распределенностью АСОД?
13. Требования к защите, обусловленные продолжительностью пребывания защищаемой информации в АСОД?
14. Требования к защите, обусловленные различными режимами функционирования АСОД?
15. Какие функции обеспечивает защита информации?
16. Чем отличается избыточность от резервирования?

Тема: Проблемы обеспечения безопасности предпринимательской деятельности в России

1. Какой может быть избыточность?
2. Разница между холодным и горячим резервированием?
3. Перечислите классы задач, обеспечивающие реализацию функций защиты?
4. Перечислите классы задач, обеспечивающие реализацию функций активной защиты?
5. Регламентация как средство защиты? Какими средствами может быть

6. реализована?
7. Разница между физическими и аппаратными средствами защиты?
8. Побуждение и принуждение? Сходства и различия.
9. Средства защиты, используемые при побуждении?
10. Почему анализируют и акцентируют внимание обычно только на технических, программных, криптографических и организационных средствах защиты?
11. Недостатки организационных средств защиты?
12. Избыточность организационная.
13. Программное регулирование доступа к элементам системы.
14. Технические средства реагирования?
15. Почему имеется 160 различных подклассов средств защиты?
16. Почему криптографические средства защиты выделены в отдельный класс?

Тема: Методы информационно-аналитической работы (конкурентной разведки), применяемые для определения и оценки экономических рисков компании

1. Перечислить функциональное назначение программных средств защиты.
2. Перечислить функциональное назначение технических средств защиты.
3. По каким критериям производится классификация технических средств защиты.
4. Структура критерия, "сопряженность с основными средствами АСОД" при классификации технических средств защиты.
5. Структура критерия "выполняемые функции защиты" при классификации технических средств защиты.
6. Структура критерия "сложность устройства" при классификации технических средств защиты.
7. Как получили 27 самостоятельных групп технических средств защиты.
8. Что входит в технические средства охранной сигнализации.
9. Перечислите важнейшие элементы ОПС.
10. Какими бывают датчики по функциональному назначению.
11. Перечислите наиболее распространенные типы датчиков.

Тема: Защита компании от экономических рисков, связанных с участием компании в гражданско-правовых отношениях

1. Перечислить средства оповещения, связи.
2. Функции охранного телевидения.
3. Перечислите некоторые из функций, выполняемых аппаратным комплексом защиты.
4. Перечислите некоторые функции защиты, выполняемых средствами программной защиты.
5. Перечислить некоторые функции защиты, выполняемые с помощью организации средств защиты.

6. Почему и какие организационные средства защиты обязательны на любом предприятии.

7. Виды преобразования, используемые при криптографическом закрытии данных.

8. Способы преобразования, используемые при шифровании.

9. Способы преобразования, используемые в кодировании и других видах закрытия информации.

10. Перечислить разновидности преобразования с заменой.

11. Перечислить различные преобразования при перестановке.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Перечень примерных контрольных вопросов к промежуточной аттестации и зачету по учебной дисциплине

1. Доктрина информационной безопасности РФ. Ее содержание и назначение.
2. Федеральный закон об информации, информатизации и защите информации. Назначение и содержание.
3. Закон о Государственной тайне. Назначение и содержание.
4. Закон о цифровой подписи.
5. Определение и содержание понятия угрозы информации в современных системах ее обработки.
6. Классификация и содержание угроз информации.
7. Методы и модели оценки уязвимости информации.
8. Постановка задачи определения требований к защите информации.
9. Роль стандартов информационной безопасности.
10. Критерии безопасности компьютерных систем министерства обороны США.
11. Европейские критерии безопасности информационных систем.
12. Руководящие документы Гостехкомиссии России.
13. Федеральные критерии безопасности информационных технологий.
14. Канадские критерии безопасности компьютерных систем.
15. Единые критерии безопасности информационных технологий.
16. Анализ стандартов информационной безопасности.
17. Постановка задачи определения требований к защите информации.
18. Криптографические протоколы аутентификации.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература:

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия : Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа : www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422

3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. — Электрон. дан. — Минск : "Вышэйшая школа", 2017. — 324 с. — Режим доступа: https://e.lanbook.com/book/75150. — Загл. с экрана.

4. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2017. - 295 с.

5. Информационная безопасность : учебник для студентов вузов / Ярочкин, Владимир Иванович ; В. И. Ярочкин ; [отв. ред. Л. И. Филиппенко]. - [5-е изд.]. - М. : Академический Проект, 2016. - 543 с. : ил. - (Gaudeamus) (Учебник для вузов). - Библиогр. : с. 534-539. - ISBN 9785829109875.

5.2 Дополнительная литература:

1. Столлингс В. Криптография и защита сетей: принципы и практика, / Столлингс В. – М.: Издательский дом «Вильямс», 2017. – 672 с.
2. Иванов М.А. Криптографические методы зашиты информаци в компьютерных системах и сетях / Иванов М.А. - М.:КУДИЦ-ОБРАЗ, 2016. – 220 с.
3. Молдовян А.А. Криптография / Молдовян А.А., Молдовян Н.А., Советов Б.Я. – СПб.: Издательство «Лань», 2016. – 224 с.

5.3. Периодические издания:

Периодические издания не предусмотрены

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Попов, В.Б. Основы информационных и телекоммуникационных технологий. Часть 2. Основы информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : Финансы и статистика, 2016. — 174 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=65922

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учебное пособие / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2016. — 552 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5114
3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учебное пособие / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. — Электрон. дан. — Спб. : НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики), 2016. — 149 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=43579

7. Методические указания для обучающихся по освоению дисциплины (модуля)

Для успешного освоения дисциплины необходимо своевременно и полностью выполнять домашние задания. Теоретические основы и список задач можно найти в указанных ниже источниках.

1. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2015. - 295 с.
2. Информационная безопасность и защита информации : учебное пособие для студентов вузов / Мельников, Владимир Павлович, С. А. Клейменов, А. М. Петраков ; В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2016. - 331 с. : ил. - (Высшее профессиональное образование , Информатика и вычислительная техника) (Учебное пособие). - Библиогр.: с. 327-328. – ISBN 9785769577383.

7.1 Методические рекомендации по организации изучения дисциплины

Контрольная работа представляет собой самостоятельную реферативную работу студентов. Каждый студент выполняет работу по одной теме.

Для написания реферата необходимо подобрать литературу. Общее количество литературных источников, включая тексты из Интернета, (публикации в журналах), должно составлять не менее 10 наименований. Учебники, как правило, в литературные источники не входят.

Рефераты выполняют на листах формата А4. Страницы текста, рисунки, формулы нумеруют, рисунки снабжают порисуночными надписями. Текст следует печатать шрифтом №14 с интервалом между строками в 1,5 интервала, без недопустимых сокращений. В конце реферата должны быть сделаны выводы.

В конце работы приводят список использованных источников. Реферат должен быть подписан студентом с указанием даты ее оформления. Работы,

выполненные без соблюдения перечисленных требований, возвращаются на доработку.

Выполненная студентом работа определяется на проверку преподавателю в установленные сроки. Если у преподавателя есть замечания, работа возвращается и после исправлений либо вновь отправляется на проверку, если исправления существенные, либо предъявляется на зачете, где происходит ее защита.

Темы для рефератов:

1. Блочное шифрование (стандарт шифрования DES).
2. Шифр Файстейля.
3. Международный алгоритм шифрования IDEA.
4. Традиционное шифрование. Алгоритм Blo Fish.
5. Традиционное шифрование. Алгоритм RC5.
6. Традиционное шифрование. Алгоритм CAST-128.
7. Традиционное шифрование. Алгоритм RC2.
8. Традиционное шифрование и конфиденциальность. Распределение ключей.
9. Криптография с открытым ключом.
10. Алгоритм RSA.
11. Криптография с использованием эллиптических кривых.
12. Отечественный стандарт криптографии защиты ГОСТ 28149-89.
13. Криптосистемы с открытым ключом. Электронная подпись.
14. Криптосистема, основанная на задаче об укладке рюкзака.
15. Гибридные криптосистемы.
16. Криптографический протокол. Протокол подбрасывания монеты.
17. Протокол битовых обязательств.
18. Протокол разделения секрета.
19. Контроль целостности информации. Задача аутентификации.
20. Контроль целостности информации. Имитозащита информации.
21. Симметричные методы аутентификации информации.
22. Схема Kerberos.
23. Несимметричные методы аутентификации. (протокол Диффи-Желлмона).
24. Протокол Шнорра.
25. Протокол Фиата-Шамира.
26. Протокол электронной подписи. Схема RSA.
27. Схема Шнорра.
28. Отечественный стандарт электронной подписи ГОСТ Р34.10-84.
29. Поточные шифры AS и RC4.
30. Поточные шифры ORYX CHAMELEON, COLITAIRE.
31. Самосинхронизирующиеся поточные шифры.
32. Стандарт AES.
33. Вероятностное шифрование.
34. Криптография с временным распознаванием
35. Квантовая криптография.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

8.1 Перечень необходимого программного обеспечения

Применение специализированного программного обеспечения при изучении данной дисциплины не предусмотрено.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

По всем изучаемым темам студентам предоставляется раздаточный материал, обеспечивающий информационную поддержку теоретического и практического курсов.

В качестве материально-технического обеспечения дисциплины используются - проекционное оборудование (цифровой проектор, экран, ноутбук).

Перечень необходимых информационных справочных систем и профессиональных баз данных

Обучающимся обеспечен доступ к современным профессиональным базам данных, профессиональным справочным и поисковым системам:

1. Консультант Плюс - справочная правовая система http://www.consultant.ru;
2. База данных международных индексов научного цитирования Web of Science (WoS) http://webofscience.com/;
3. База данных рефератов и цитирования Scopus http://www.scopus.com/;
4. Базы данных компании «Ист Вью» http://dlib.eastview.com;
5. База открытых данных Росфинмониторинга http://fedsfm.ru/opendata;
6. База открытых данных Росстата http://www.gks.ru/opendata/dataset;
7. База открытых данных Управления Федеральной службы государственной статистики по Краснодарскому краю и Республике Адыгея http://krsdstat.gks.ru/wps/wcm/connect/rosstat_ts/krsdstat/ru/statistics/krsndStat/db/;
8. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/;
9. Электронная Библиотека Диссертаций https://dvs.rsl.ru;
10. Научная электронная библиотека КиберЛенинка http://cyberleninka.ru/

РЕЦЕНЗИЯ
на рабочую программу учебной дисциплины «Обеспечение безопасности электронного бизнеса» направления подготовки 38.03.05 Бизнес-информатика (бакалавриат)

Рабочая программа по дисциплине «Обеспечение безопасности электронного бизнеса» составлена преподавателем кафедры теоретической экономики экономического факультета Кубанского государственного университета Пономаренко Т.Н. Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению 38.03.05 Бизнес информатика, профиль: Электронный бизнес очной формы обучения. Программа одобрена на заседании кафедры теоретической экономики и на заседании учебно-методического совета экономического факультета.

Целью освоения учебной дисциплины «Обеспечение безопасности электронного бизнеса» является развитие профессиональных компетентностей приобретения практических навыков разработки и использования знаний основных концепций и технологий компьютерных сетей и коммуникаций.

Рабочая программа дисциплины «Обеспечение безопасности электронного бизнеса» составлена логично. Последовательность тем, предлагаемых к изучению, направлена на качественное усвоение учебного материала.

Считаю, что рабочая программа по дисциплине «Обеспечение безопасности электронного бизнеса» может быть рекомендована для внедрения при подготовке бакалавров по направлению 38.03.05 Бизнес информатика, профиль: Электронный бизнес очной формы обучения.

Рецензент:

Доктор физико-математических наук,
Профессор кафедры математического
моделирования ФГБОУ ВО КубГУ

Павлова А.В.

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины «Обеспечение безопасности электронного бизнеса» направления подготовки 38.03.05 Бизнес-информатика (бакалавриат)

Рабочая программа по дисциплине «Обеспечение безопасности электронного бизнеса» составлена преподавателем кафедры теоретической экономики Пономаренко Т.Н.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.03.05 бизнес-информатика (бакалавриат) и одобрена на заседании кафедры теоретической экономики и на заседании учебно-методического совета экономического факультета.

Рабочая программа дисциплины «Обеспечение безопасности электронного бизнеса» составлена логично. Последовательность тем, предлагаемых к изучению, направлена на качественное усвоение учебного материала. Лабораторные задания разнообразны, позволяют адекватно оценивать уровень знаний студентов по дисциплине. Методические рекомендации по лабораторным занятиям обеспечивают формирование базовых умений для выполнения исследований в процессе научного познания и теоретического обоснования профессиональных задач. Методические рекомендации по организации самостоятельной работы направлены на закрепление умения поиска, накопления и обработки научной информации. Мультимедийное сопровождение лекционного материала и лабораторных работ отличается точностью и конкретностью, способствует лучшему усвоению дисциплины.

Структура программы включает в себя: учебно-тематический план занятий, планы лекций, семинарских занятий, примерную тематику лабораторных работ, список основной и дополнительной литературы по дисциплине. Рецензируемая программа формируют развитие профессиональных компетентностей приобретения практических навыков использования для решения задач бизнес-информатики.

Программа может быть рекомендована для использования в процессе реализации дисциплины «Обеспечение безопасности электронного бизнеса» в Кубанском государственном университете.

Рецензент:

заместитель директора
по информационной
безопасности
ООО «Экс-Торг»

Гузенко В.М.