МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
Директор института экономики
и управления АПК
_____ Бутырин В.В.
"19" декабря 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.01 «Организация и правовое обеспечение информационной безопасности»

для подготовки экономистов

ФГОС ВО

Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности

Курс 4
Семестр 7

Форма обучения - очная

Год начала подготовки 2019

Регистрационный номер _____

Москва, 2019

Разработчики:
Лосев А. Н.,
ст. преподаватель кафедры прикладной информатики _____

Катасонова Н.Л.,
доцент кафедры прикладной информатики _____

«_1_» _12_ 20_19_г.

Рецензент: Щедрина Е. В.,
доцент кафедры информационных
технологий в АПК, к.п.н. _____

«_2_» _12_ 20_19_г.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 38.05.01 «Экономическая безопасность» и учебного плана по данной специальности

Программа обсуждена на заседании кафедры прикладной информатики протокол № _4_ от «_3_» декабря 20_19_г.

Зав. кафедрой прикладной информатики
Худякова Е.В., д.э.н., профессор _____

«_3_» _12_ 20_19_г.

Согласовано:
Председатель учебно-методической
комиссии института экономики и управления АПК
Корольков А.Ф., к.э.н., доцент _____

«_11_» _12_ 20_19_г.

Заведующий выпускающей кафедрой
экономической безопасности, анализа и аудита
Карзаева Н.Н., д.э.н., профессор _____

«_2_» _12_ 20_19_г

Заведующий отделом комплектования ЦНБ _____

Бумажный экземпляр РПД, копии электронных вариантов РПД и оценочных материалов получены:
Методический отдел УМУ

_____ «___»_____20__г

Содержание

Аннотация

рабочей программы учебной дисциплины Б1.В.ДВ.03.01 «Организация и правовое обеспечение информационной безопасности» для подготовки экономистов по специальности 38.05.01 "Экономическая безопасность" специализации «Экономико-правовое обеспечение экономической безопасности»

Цель освоения дисциплины: формирование у студентов умений осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации и применять нормативные правовые акты и нормативные методические документы в области защиты информации

Место дисциплины в учебном плане: Дисциплина включена в вариативную часть дисциплин по выбору учебного плана по специальности 38.05.01 "Экономическая безопасность".

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции: ПСК-1; ПСК-3.

Краткое содержание дисциплины: Основные понятия. Актуальность. Законодательство РФ в области информационной безопасности. Объектно-ориентированный подход к ИБ. Изучение положений о государственном лицензировании деятельности в области защиты информации. Основные определения и критерии классификации угроз. Принципы построения систем защиты. Оценочные стандарты и технические спецификации. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации. Законодательный уровень ИБ. Административный уровень ИБ. Процедурный и программно-технические уровни ИБ. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации. Управление рисками. Типы вредоносного ПО. История компьютерных вирусов. Признаки присутствия на компьютере вредоносного ПО. Защита от вредоносного ПО. Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации. Атаки. Брандмауэр. Режим секретности. Криптоалгоритмы.

Общая трудоемкость дисциплины составляет: 3 зачётные единицы (108 часов)

Промежуточный контроль: зачет.

1. Цель освоения дисциплины

Целью освоения дисциплины «Организация и правовое обеспечение информационной безопасности» является: формирование у студентов умений осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации и применять нормативные правовые акты и нормативные методические документы в области защиты информации.

2. Место дисциплины в учебном процессе

Дисциплина «Организация и правовое обеспечение информационной безопасности» включена в вариативную часть дисциплин по выбору учебного плана. Дисциплина «Организация и правовое обеспечение информационной безопасности» реализуется в соответствии с требованиями ФГОС ВО и Учебного плана по специальности 38.05.01 "Экономическая безопасность".

Предшествующими курсами, на которых базируется дисциплина, являются: «Информационная безопасность», «Информационные системы в экономике».

Дисциплина «Организация и правовое обеспечение информационной безопасности» может быть использована при написании выпускной квалификационной работы.

Рабочая программа дисциплины «Организация и правовое обеспечение информационной безопасности» для инвалидов и лиц ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психологического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны:		
			знать	уметь	владеть
1.	ПСК-1	Способностью обеспечивать исполнение и соблюдение законодательства Российской Федерации участниками общественных отношений	- нормативно-правовые акты, регламентирующие деятельность по обеспечению экономической безопасности хозяйствующего субъекта; - положения нормативно-правовые акты, регламентирующие деятельность по обеспечению экономической безопасности хозяйствующего субъекта	- определять перечень нормативно-правовых актов, регламентирующих деятельность по обеспечению экономической безопасности хозяйствующего субъекта; - применять положения нормативно-правовых актов, регламентирующих деятельность по обеспечению экономической безопасности хозяйствующего субъекта	- положениями нормативно-правовых актов, регламентирующих деятельность по обеспечению экономической безопасности хозяйствующего субъекта
2.	ПСК-3	Способностью участвовать в разработке локальных нормативных правовых актов в соответствии с профилем своей профессиональной деятельности	- функционал субъектов экономической безопасности хозяйствующего субъекта; - права и обязанности субъектов экономической безопасности хозяйствующего субъекта; - структуру и содержание Положения службы экономической безопасности	- разрабатывать локальные нормативные акты, регламентирующие деятельность по обеспечению экономической безопасности хозяйствующего субъекта	- положениями нормативно-правовых актов, регламентирующих деятельность по обеспечению экономической безопасности хозяйствующего субъекта

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ семестрам представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	**7 семестр час.**
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**50,25**	**50,25**
Аудиторная работа	**50,25**	**50,25**
лекции (Л)	16	16
практические занятия (ПЗ)	30	30
Лабораторные работы(ЛР)	4	4
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**57,75**	**57,75**
самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям, лабораторным работам, тестированию и т.д.)	48,75	48,75
Подготовка к зачету (контроль)	9	9
Вид промежуточного контроля:	зачет	

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин	Всего	Аудиторная работа				Внеаудиторная работа СР
		Л	ПЗ	ЛР	ПКР	
Раздел 1 Правовое обеспечение информационной безопасности						
Тема № 1. Введение в правовое обеспечение информационной безопасности.	13	1	6			6
Тема № 2. Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты	13	1		4		8
Тема № 3. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации.	18	2	8			8
Тема № 4. Уровни информационной безопасности	19	3	8			8
Тема № 5. Управление рисками	9,75	1	2			6,75
Раздел 2. Организационное обеспечение информационной безопасности						
Тема № 1. Вредоносное программное обеспечение	14	2	6			6
Тема № 2. Организация средств защиты	12	6				6

Наименование разделов и тем дисциплин	Всего	Аудиторная работа				Внеаудиторная работа СР
		Л	ПЗ	ЛР	ПКР	
Контактная работа на промежуточном контроле (КРА)	0,25				0,25	
Подготовка к зачету (контроль)	9					9
Всего за 7 семестр	108	16	30	4	0,25	57,75
Итого по дисциплине	**108**	**16**	**30**	**4**	**0,25**	**57,75**

Раздел 1. Правовое обеспечение информационной безопасности

Тема № 1. Введение в правовое обеспечение информационной безопасности

Понятие ИБ. Основные составляющие. Актуальность проблемы ИБ.

Тема № 2. Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты

Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты. Сложные системы. Технические средства охраны. Основные принципы построения защиты. Классы каналов несанкционированного доступа. Основные задачи систем защиты. Стойкость алгоритма шифрования.

Тема № 3. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации

Основные определения и критерии классификации угроз. Меры противодействия угрозам. Принципы построения систем защиты. Классификация угроз. Целостность ПО. Оценочный стандарты и технические спецификации. Критерии оценки степени доверия. Политика безопасности. Уровень гарантированности. Механизм подотчетности (протоколирования). Доверенная вычислительная база. Механизмы безопасности. Виды гарантированности. Классы безопасности. Администрирование средств безопасности. Администрирование сервисов безопасности. Дискреционная политика безопасности. Мандатная политика безопасности.

Тема № 4. Уровни информационной безопасности

Уровни ИБ. Законодательный уровень ИБ. Законодательный. Административный. Процедурный. Программно-технический. Конституция РФ. Доктрина ИБ РФ. Основные принципы доктрины. Уголовный кодекс РФ. Закон "Об информации, информатизации и защите информации" Основные положения. Закон «О лицензировании отдельных видов деятельности». Закон "Об электронной цифровой подписи". Закон «О персональных данных». ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Единый реестр запрещенных сайтов. Административный уровень ИБ. Политика безопасности. Анализ рисков. Программа безопасности. Процедурный уровень ИБ. Программно-технический уровень ИБ.

Тема № 5. Управление рисками

Управление рисками. Система управления рисками. Риск-менеджер. Этапы управления рисками. Идентификация рисков. Категоризация рисков. Планирование мониторинга. Этап мониторинга анализа эффективности управления рисками. Обновление базы известных рисков. Паспортизация рисков. SWOT-анализ. Классификация рисков. Классификация проектов по рискам. Критерии риск-менеджера. Анализ эффективности управления рисками. Критерии эффективности управления рисками.

Раздел 2. Организационное обеспечение информационной безопасности

Тема № 1. Вредоносное программное обеспечение

Типы вредоносного ПО. История компьютерных вирусов. Признаки присутствия на компьютере вредоносного ПО. Грани вредоносного ПО. Классификация по вредоносной функции. Загрузочные вирусы. MBR вирусы. Файловые вирусы. Сетевые черви. Троянские программы. Макровирусы. Резидентные вирусы. Резидентные вирусы. Самошифрование и полиморфизм. Особенности современного вредоносного ПО. Хакерские утилиты и другое вредоносное ПО. Виды проявления вредоносного ПО. Сетевая активность. Защита от вредоносных программ. Методы защиты от вредоносных программ. Самозащита вредоносного ПО. Полиморфизм и обфускация. Борьба с антивирусами. Направления самозащиты. Типы антивирусов. Правила обработки информации.

Тема № 2. Организация средств защиты

Атаки. Виды атак. Локальные атаки. Средства аутентификации. Получение доступа на этапе загрузки ОС. Методы защиты. Социальная инженерия. Классификация удаленных атак. Межсетевой экран. Брандмауэры. Характеристики фаерволов. Управляемые коммутаторы канального уровня. Шлюзы сеансового уровня. Шлюзы прикладного уровня. Классификация по отслеживанию соединений. Режим секретности. Основные понятия. Государственная тайна. Признаки государственной тайны. Секретность. Элементы режима секретности. Грифы секретности и формы допуска. Защита государственной тайны. Порядок работы с секретными документами. Криптология. Криптоанализ. История криптографии. Полиалфавитные шифры. Шифр Виженера. Шифр Гронсфельда. Энигма. Современная криптография. Классификация криптоалгоритмов. Перестановочные алгоритмы. Потоковые шифры. Симметричные алгоритмы.

4.3 Лекции/ лабораторные/практические занятия

Таблица 4

Содержание лекций/лабораторных/практических занятий и контрольные мероприятия

№ п/п	№ раздела	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
1.	**Раздел 1.** Правовое обеспечение информационной безопасности				36
	Тема № 1. Введение в правовое	Лекция № 1. Основные понятия. Актуальность.	ПСК-3		1

№ п/п	№ раздела	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
	обеспечение информационной безопасности.	Практическая работа №1. Законодательство РФ в области информационной безопасности	ПСК-1	защита практической работы	6
	Тема № 2. Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты	Лекция № 2. Объектно-ориентированный подход к ИБ.	ПСК-1		1
		Лабораторная работа № 2. Изучение положений о государственном лицензировании деятельности в области защиты информации	ПСК-1	защита лабораторной работы	4
	Тема № 3. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации.	Лекция № 3. Основные определения и критерии классификации угроз. Принципы построения систем защиты.	ПСК-3		1
		Лекция № 4. Оценочные стандарты и технические спецификации	ПСК-1		1
		Практическая работа № 3. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	ПСК-1	защита практической работы	4
		Практическая работа № 4. Система сертификации средств криптографической защиты информации	ПСК-3	защита практической работы	2
		Практическая работа № 5. Изучение положения о сертификации средств вычислительной техники и связи	ПСК-1	защита практической работы	2
	Тема № 4. Уровни информационной безопасности	Лекция № 5. Законодательный уровень ИБ	ПСК-3		1
		Лекция № 6. Административный уровень ИБ	ПСК-3		1
		Лекция № 7. Процедурный и программно-технические уровни ИБ	ПСК-3		1
		Практическая работа № 6. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации	ПСК-3	защита практической работы, тестирование	6

№ п/п	№ раздела	№ и название лекций/ лабораторных/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов
		Практическая работа № 7. Изучение особенностей аттестации помещений по требованиям безопасности информации	ПСК-1	защита практической работы	2
	Тема № 5. Управление рисками	Лекция № 8. Управление рисками	ПСК-3		1
		Практическая работа № 8. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации	ПСК-3	защита практической работы	2
2.	**Раздел 2.** Организационное обеспечение информационной безопасности				14
	Тема №1. Вредоносное программное обеспечение	Лекция № 9. Типы вредоносного ПО. История компьютерных вирусов. Признаки присутствия на компьютере вредоносного ПО.	ПСК-1		1
		Лекция № 10. Защита от вредоносного ПО	ПСК-3		1
		Практическая работа № 9. Изучение типового положения об испытательной лаборатории	ПСК-1	защита практической работы	2
		Практическая работа № 10. Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации	ПСК-3	защита практической работы, тестирование	4
	Тема №2. Организация средств защиты	Лекция № 11. Атаки	ПСК-3		1
		Лекция № 12. Брандмауэр	ПСК-3		1
		Лекция № 13. Режим секретности	ПСК-3		2
		Лекция № 14. Криптоалгоритмы	ПСК-3		2

4.4 Перечень вопросов для самостоятельного изучения дисциплины

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов для самостоятельного изучения
Раздел 1. Правовое обеспечение информационной безопасности		

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема № 1. Введение в правовое обеспечение информационной безопасности.	1. Какие основные направления, принципы и условия организационной защиты информации Вам известны? ПСК-3 2. Какие основные определения организационной зашиты информации Вы можете назвать? ПСК-1 3. Какие основные принципы организационной защиты информации Вам известны? ПСК-1 4. Что такое система защиты информации? ПСК-1 5. Какие основные подходы к созданию системы защиты информации Вам известны? ПСК-1 6. Какие подразделения входят в службу безопасности предприятия? ПСК-3 7. Что относится к техническим средствам защиты информации? ПСК-1 8. Какие существуют методы защиты информации? ПСК-3
2.	Тема № 2. Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты	1. Перечислите основные понятия защиты информации. ПСК-3 2. Назовите основные принципы правового регулирования отношений, возникающих в сфере информации. ПСК-3 3. В чём заключается федеральный закон «Об информации, ин технологиях и защите информации»? ПСК-3 4. В чем заключается федеральный закон «О коммерческой тайне»? ПСК-3 5. Что обычно включают в перечень информации (сведений), составляющей коммерческую тайну? ПСК-1 6. Какие степени секретности установлены в РФ? ПСК-1
3.	Тема № 3. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации.	1. Каковы основные направления аналитической работы по предупреждению утечки конфиденциальной информации? ПСК-3 2. Назовите основные функции аналитического подразделения. ПСК-1 3. Какие этапы аналитической работы Вам известны? Опишите их. ПСК-3 4. Какие виды аналитических отчетов Вам известны? ПСК-3 5. В чём заключается классификация методов анализа информации? ПСК-3 6. Какие меры могут вырабатываться аналитическим подразделением с учетом результатов аналитической работы? ПСК-1 7. Какие разделы должна включать в себя типовая программа исследований? ПСК-1
4.	Тема № 4. Уровни информационной безопасности	1. В чём заключается контрольно-пропускной режим? ПСК-3 2. Каковы основные цели контольно-пропускного режима? ПСК-3

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов для самостоятельного изучения
		3. Какие исходные данные необходимы для разработки мероприятий и нормативных документов контольно-пропускного режима? ПСК-3 4. Что такое категории режимности? ПСК-3 5. Что должна включать в себя инструкция о пропускном режиме? ПСК-1 6. Какие виды пропусков существуют на предприятиях? ПСК-3 7. Каким требованиям должно отвечать оборудование КПП? ПСК-3 8. Какое оборудование КПП Вам известно? ПСК-3
5.	Тема № 5. Управление рисками	1. В чём заключается работа с персоналом предприятия, имеющим доступ к конфиденциальной информации? ПСК-3 2. Назовите основные причины разглашения конфиденциальной информации допущенным к ней персоналом предприятия. ПСК-3 3. Каковы обязанности работодателя по отношению к сотруднику предприятия в связи с охраной конфиденциальности информации? ПСК-3 4. Как проводится работа с сотрудниками предприятия, независимо от степени конфиденциальности информации? ПСК-3 5. На чём должны быть сосредоточены усилия руководства при работе с сотрудниками, допущенными к конфиденциальной информации? ПСК-1 6. Какие методы работы с персоналом предприятия, допущенным к конфиденциальной информации и работающим с носителями этой информации Вам известны? ПСК-3
Раздел 2. Организационное обеспечение информационной безопасности		
6.	Тема №1. Вредоносное программное обеспечение	1. В чём заключается допуск к конфиденциальной информации? ПСК-3 2. Какие меры по охране конфиденциальности информации признаются разумно достаточными? ПСК-1
7.	Тема №2. Организация средств защиты	1. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. ПСК-1 2. Контроль функционирования системы организационной защиты информации ПСК-1

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1	Раздел №1. Тема № 2. Объектно-ориентированный подход к ИБ. Физическая защита объектов. Концепция построения систем защиты	Л	Неимитационный метод (проблемная лекция)
2	Раздел №1. Тема № 4. Уровни информационной безопасности	Л	Неимитационный метод (проблемная лекция)
3	Раздел №1. Тема № 5. Управление рисками	Л	Неимитационный метод (проблемная лекция)
4	Раздел №2. Тема №1. Вредоносное программное обеспечение	Л	Неимитационный метод (проблемная лекция)

6. Текущий контроль успеваемости и промежуточная аттестация по итогам освоения дисциплины

6.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1)Примеры тестовых заданий

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...
   1) политическая разведка;
   2) промышленный шпионаж;
   3) добросовестная конкуренция;
   4) конфиденциальная информация;
   5) правильного ответа нет.
2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
   1) любая информация;
   2) только открытая информация;
   3) запатентованная информация;
   4) закрываемая собственником информация;
   5) коммерческая тайна.
3. Кто может быть владельцем защищаемой информации?
   1) только государство и его структуры;
   2) предприятия акционерные общества, фирмы;
   3) общественные организации;
   4) только вышеперечисленные;
   5) кто угодно.

4. Какие сведения на территории РФ могут составлять коммерческую тайну?
   1) учредительные документы и устав предприятия;
   2) сведенья о численности работающих, их заработной плате и условиях труда;
   3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
   4) другие;
   5) любые.
5. Какие секретные сведения входят в понятие «коммерческая тайна»?
   1) связанные с производством;
   2) связанные с планированием производства и сбытом продукции;
   3) технические и технологические решения предприятия;
   4) только 1 и 2 вариант ответа;
   5) три первых варианта ответа.
6. Что называют источником конфиденциальной информации?
   1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
   2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
   3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
   4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
   5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.
7. Как называют процессы обмена информацией с помощью официальных, деловых документов?
   1) непосредственные;
   2) межличностные;
   3) формальные;
   4) неформальные;
   5) конфиденциальные.

2) Примеры практических заданий или вопросов для их защиты

1. Законодательство РФ в области информационной безопасности
2. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации
3. Система сертификации средств криптографической защиты информации
4. Изучение положения о сертификации средств вычислительной техники и связи
5. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации

6. Изучение особенностей аттестации помещений по требованиям безопасности информации
7. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации
8. Изучение типового положения об испытательной лаборатории
9. Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации

3) Примеры лабораторных заданий или вопросов для их защиты

1. Изучение положений о государственном лицензировании деятельности в области защиты информации

4). Примерный перечень вопросов к зачету по дисциплине

1. Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам.
2. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
3. Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования.
4. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
5. Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса.
6. Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз.
7. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам.
8. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
9. Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности.
10. Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия».
11. Структура и содержание документа «Политика информационной безопасности предприятия».

6.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется **балльно-рейтинговая** система контроля и оценки успеваемости студентов.

В основу балльно-рейтинговой системы (БРС) положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего, промежуточного контроля и промежуточной аттестации знаний.

Таблица 7

Система рейтинговой оценки успеваемости

Баллы	Балльная оценка текущей успеваемости			
За тестирование	2	3	4	5
За практическую работу	2	4	5	6
За лабораторную работу	2	4	5	6
За зачет	2	3	4	5
Оценка	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично

Таблица 8

Итоговая сумма баллов

Виды контроля	Количество видов контроля	Максимальное возможное количество баллов за единицу	Количество баллов
Тестирование	2	5	10
Защита практической работы	9	6	54
Защита лабораторной работы	1	6	6
Зачет	1	30	30
Всего	-	-	100

Таблица 9

Балльно-рейтинговая система контроля успеваемости

Шкала оценивания	**Оценка**
85–100	Зачтено
70–84	
61-69	
0-60	Незачтено

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: учебное пособие / А.Е. Фаронов. — Электрон.

дан. — Москва: 2016. — 154 с. — Режим доступа: https://e.lanbook.com/book/100296 (открытый доступ)
2. Осавелюк, Е.А. Информационная безопасность государства и общества в контексте деятельности СМИ [Электронный ресурс]: монография / Е.А. Осавелюк. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 92 с. — Режим доступа: https://e.lanbook.com/book/107950. (открытый доступ)
3. Информационная безопасность [Электронный ресурс]: учебное пособие / сост. Е.Р. Кирколуп, Ю.Г. Скурыдин, Е.М. Скурыдина. — Электрон. дан. — Барнаул: АлтГПУ, 2017. — 316 с. — Режим доступа: https://e.lanbook.com/book/112164. (открытый доступ)

7.2 Дополнительная литература

1. Авдошин, С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]: учебное пособие / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. дан. — Москва:, 2016. — 432 с. — Режим доступа: https://e.lanbook.com/book/100514. (открытый доступ)
2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / В.А. Галатенко. — Электрон. дан. — Москва:, 2016. — 266 с. — Режим доступа: https://e.lanbook.com/book/100295. (открытый доступ)

7.3 Нормативные правовые акты

1. Конституция Российской Федерации. http://dehack.ru/intro/
2. Уголовный кодекс Российской федерации. http://dehack.ru/intro/
3. Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации». http://dehack.ru/intro/
4. Федеральный закон РФ 27.07.2006 г. N 152-ФЗ «О персональных данных». http://dehack.ru/intro/
5. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». http://dehack.ru/intro/
6. Руководящие документы ФСТЭК РФ: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty#
7. Доктрина информационной безопасности Российской Федерации http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=28679
8. BS ISO/IES 27005:20008 Ru. Информационные технологии - Методы обеспечения безопасности - Управление рисками информационной безопасности. http://gtrust.ru/show_good.php?idtov=1137 .

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

1. http://www.consultant.ru – сайт компании "КонсультантПлюс" (открытый доступ)
2. http://opdo.timacad.ru Система дистанционного обучения РГАУ МСХА им. К.А. Тимирязева (открытый доступ)

3. https://www.google.com/chrome Браузер Google Chrome (открытый доступ)
4. www.google.com – Поисковая система (открытый доступ)
5. https://ru.wikipedia.org/ – Общедоступная многоязычная универсальная интернет-энциклопедия со свободным контентом (открытый доступ)
6. http://www.rsl.ru/ - Российская государственная библиотека. (открытый доступ)
7. Зарубежные электронные научные информационные ресурсы: European Library.

9. Перечень программного обеспечения и информационных справочных систем

Таблица 9

Перечень программного обеспечения

№ п/п	Наименование раздела учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
1	Раздел №1-2	Microsoft Office 2007	демонстрирующая	Microsoft	2007
2	Раздел №1-2	Windows Server 2003R2	демонстрирующая	Microsoft	2003
3	Раздел №1-2	WinRAR 3.8	демонстрирующая	Евгений Рошал, Александр Рошал	2008
4	Раздел №1-2	Notepad++	демонстрирующая	Notepad++ Contributors	2018

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

Таблица 10

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. (26 учебный корпус, 416 аудитория)	видеопроектор, экран настенный, ноутбук
Учебные лаборатории, аудитории для проведения практических и лабораторных занятий, групповых и индивиду-	Экран настенный, видеопроектор, ноутбук, терминалы: ауд.408 – 15, ауд.409 – 15, ауд.411 – 17

альных консультаций, текущего контроля и промежуточной аттестации. (№ 408, 409,411, уч.корпус №26)	
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

В современных условиях творческая одаренность и нестандартная самостоятельная деятельность человека становятся основным ресурсом функционирования и развития общества. Процесс качественного обновления жизни в нашем обществе предполагает формирование устойчивого и долговременного спроса на творческую личность, яркую индивидуальность, на специалиста, свободно и критически мыслящего, самобытного и инициативного. Умение самостоятельно мыслить, свободно принимать решения, нести за них персональную ответственность необходимо молодежи еще и потому, что в современной жизни возросла автономия личности. И все же одним из важных требований социального заказа, предъявляемого выпускнику вуза в современных условиях, является умение самостоятельно пополнять свои знания, ориентироваться в стремительном потоке научной и культурной информации.

Промежуточным контролем по дисциплине является зачет.

Организация самостоятельной работы обучающихся является одним из важнейших вопросов в условиях реализации компетентностной модели образования. Это связано не только с увеличением доли самостоятельной работы при освоении учебных дисциплин, но, прежде всего, с современным пониманием образования как жизненной стратегии личности. Мотивация к непрерывному образованию, общекультурные и профессиональные компетенции становятся необходимым ресурсом личности для успешного включения в трудовую деятельность и реализации своих жизненных планов. Основная задача высшего образования заключается в формировании творческой личности специалиста, способного к саморазвитию, самообразованию, инновационной деятельности.

Под самостоятельной работой обучающихся сегодня понимается вид учебно-познавательной деятельности по освоению основной образовательной программы высшего профессионального образования, осуществляемой в определенной системе, при партнерском участии преподавателя в ее планировании и оценке достижения конкретного результата.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности;

- формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;

- формирования общих и профессиональных компетенций;

- развитию исследовательских умений.

При выполнении заданий, вынесенных на самостоятельное изучение, необходимо наряду с библиотечным фондом пользоваться различными базами знаний, размещенными в Интернет, к которым, в, частности, относятся: Научная электронная библиотека, Российская государственная библиотека и многие другие.

В подготовке к занятиям по дисциплине студенты должны активно использовать дополнительную литературу, поскольку именно с ее помощью можно получить наиболее полное и верное представление о происходящих в стране и в мире процессах. Для этих же целей необходимо шире использовать имеющиеся информационные технологии. Изучение литературы очень трудоемкая и ответственная часть подготовки к лабораторному занятию, написанию доклада и т.п. Она, как правило, сопровождается записями в той или иной форме. Конспектом называется краткая схематическая запись основного содержания научной работы. Желательно использование логических схем, делающих наглядным ход мысли конспектируемого автора.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятия обязан его отработать:

- лекцию отрабатывают путем индивидуальной проработки студентом лекционного материала по рекомендуемой литературе и устного ответа на вопросы преподавателя по пропущенной теме;

- практическое занятие путем выполнения практической работы, которая выполнялась на пропущенном практическом занятии, с разрешения преподавателя студент имеет право отработать пропущенное практическое задание самостоятельно и отчитаться по нему на ближайшем практическом занятии (если это не противоречит его плану) либо во время, назначенное преподавателем для индивидуальных консультаций.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

В процессе обучения по дисциплине «Организация и правовое обеспечение информационной безопасности» используются лекционно-практические занятия, деловые игры, разбор конкретных ситуаций, проводятся дискуссии по актуальным проблемам управления, организуется работа с методическими и справочными материалами, целесообразно применение современных технических средств обучения и информационных технологий. Освоение учебной дисциплины предполагает осмысление её разделов и тем на практических занятиях, в процессе которых специалист должен закрепить и углубить теоретические знания.

Своеобразие современной профессиональной деятельности преподавателя заключается в необходимости ведения, поддержки и сопровождения студентов, что позволит сформировать новое поколение специалистов, обладающих **современными компетенциями**.

В процессе изучения дисциплины «Организация и правовое обеспечение информационной безопасности» предусмотрены несколько форм контроля: текущий и промежуточный.

Текущий контроль предназначен для определения качества усвоения лекционного материала. В течение учебного семестра рекомендуется назначать контрольные точки для проверки качества усвоения изучаемого материала по определенным темам в форме опроса, тестирования и выполнения заданий практикума по дисциплине.

Рекомендуется определять сроки проведения контрольных мероприятий, максимальная оценка за каждое из них и правила перевода общего количества баллов, полученных при изучении дисциплины, в промежуточный результат (Зачет).

Выполнение практических заданий является обязательным для всех обучающихся. Студенты, не выполнившие в полном объеме работы, предусмотренные учебным планом, не допускаются к сдаче Зачета.

Самостоятельная работа студентов по курсу должна обязательно сопровождаться проработкой конспекта, выполнением заданий и упражнений.

Программу разработали:

Лосев А.Н., ст. преподаватель _____

Катасонова Н.Л., доцент _____

РЕЦЕНЗИЯ

на рабочую программу дисциплины
Б1.В.ДВ.03.01 «Организация и правовое обеспечение информационной безопасности»
ОПОП ВО по специальности 38.05.01 «Экономическая безопасность», специализации «Экономико-правовое обеспечение экономической безопасности» (квалификация выпускника – экономист)

Щедрина Елена Владимировна, доцент кафедры информационных технологий в АПК, ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева», кандидат педагогических наук (далее по тексту рецензент), проведено рецензирование рабочей программы дисциплины «**Организация и правовое обеспечение информационной безопасности**» ОПОП ВО по специальности **38.05.01 «Экономическая безопасность»,** специализации «**Экономико-правовое обеспечение экономической безопасности»** (специалитет) разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева», на кафедре прикладной информатики (разработчики – Лосев Алексей Николаевич, старший преподаватель и Катасонова Наталия Леонидовна, доцент).

Рассмотрев представленные на рецензирование материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Организация и правовое обеспечение информационной безопасности» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по специальности 38.05.01 «Экономическая безопасность». Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к дисциплинам по выбору вариативной части учебного цикла – Б1.В.ДВ.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО специальности 38.05.01 «Экономическая безопасность».

4. В соответствии с Программой за дисциплиной «Организация и правовое обеспечение информационной безопасности» закреплено 2 ***компетенции***. Дисциплина «Организация и правовое обеспечение информационной безопасности» и представленная Программа *способна реализовать* их в объявленных требованиях.

5. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

6. Общая трудоёмкость дисциплины «Организация и правовое обеспечение информационной безопасности» составляет 3 зачётные единицы (108 часов).

7. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Организация и правовое обеспечение информационной безопасности» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по специальности 38.05.01 «Экономическая безопасность» и возможность дублирования в содержании отсутствует.

8. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

9. Программа дисциплины «Организация и правовое обеспечение информационной безопасности» предполагает проведение занятий в интерактивной форме.

10. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО специальности 38.05.01 «Экономическая безопасность»**.**

11. Представленные и описанные в Программе формы *текущей* оценки знаний (участие в тестировании, выполнение практических заданий), *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в форме зачета, что *соответствует* статусу дисциплины, как дисциплины по выбору вариативной части учебного цикла – Б1.В.ДВ. ФГОС ВО специальности 38.05.01 «Экономическая безопасность»**.**

12. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

13. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 3 источник (базовый учебник), дополнительной литературой – 2 наименований, периодическими изданиями – 8 источников со ссылкой на электронные ресурсы, Интернет-ресурсы –7 источников и *соответствует* требованиям ФГОС ВО специальности 38.05.01 «Экономическая безопасность»**.**

14. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Организация и правовое обеспечение информационной безопасности» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

15. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Организация и правовое обеспечение информационной безопасности».

ОБЩИЕ ВЫВОДЫ

На основании проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Организация и правовое обеспечение информационной безопасности» ОПОП ВО по специальности 38.05.01 «Экономическая безопасность», специализации «Экономико-правовое обеспечение экономической безопасности» (квалификация выпускника – экономист), разработанная Лосевым А.Н., старшим преподавателем и Катасоновой Н.Л., доцентом кафедры прикладной информатики, соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Щедрина Е. В., доцент кафедры информационных технологий в АПК, ФГБОУ ВО РГАУ – МСХА имени К.А. Тимирязева», кандидат педагогических наук

_____ «___ » _____ 2019 г.


Пронумеровано, прошнуровано и
скреплено печатью
лист
Зам. директора
Нифонтова Е.А.
МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА ИМЕНИ К.А. ТИМИРЯЗЕВА»
ИНСТИТУТ ЭКОНОМИКИ И УПРАВЛЕНИЯ АПК