Министерство сельского хозяйства Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Вятский государственный агротехнологический университет"

УТВЕРЖДАЮ
Декан экономического факультета
_____ Т.Б. Шиврина
"15" апреля 2021 г.

Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **информационных технологий и статистики**

Учебный план Специальность 38.05.01 Экономическая безопасность
Специализация "Экономико-правовое обеспечение экономической безопасности"

Квалификация **экономист**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 64
самостоятельная работа 24
часов на контроль 36

Виды контроля в семестрах:
экзамены 9
курсовые работы 9

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	9 (5.1)		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	48	48	48	48
В том числе инт.	48	48	48	48
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	24	24	24	24
Часы на контроль	36	36	36	36
Курсовая работа	20	20	20	20
Итого	144	144	144	144

Киров 2021

Программу составил(и):

старший преподаватель кафедры информационных технологий и статистики, Ливанов Роман Витальевич

Рецензент(ы):

к.п.н., доцент кафедры информационных технологий и статистики, Дьячков Валерий Павлович

Рабочая программа дисциплины

Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования по специальности 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ (приказ Минобрнауки России от 16.01.2017 г. № 20)

составлена на основании Учебного плана:

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

одобренного и утвержденного Ученым советом университета от 15.04.2021 протокол № 5.

Рабочая программа дисциплины рассмотрена и одобрена учебно-методической комиссией

экономического факультета Протокол № от "15" апреля 2021 г.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры

информационных технологий и статистики

Протокол № от "15" апреля 2021 г.

Зав. кафедрой _____ к.э.н., доцент Козлова Лариса Алексеевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2022 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2025 г. № __

Зав. кафедрой _____

1. ЦЕЛЬ (ЦЕЛИ) ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	ознакомление студентов с тенденциями развития защиты информации, моделями возможных угроз, терминологией и основными понятиями теории защиты информации, ознакомление с нормативными документами и методами защиты компьютерной информации и формирование навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Обучающийся должен обладать знаниями, умениями, навыками не ниже 1 уровня (низкого), полученными при изучении следующих дисциплин:Информационные системы в экономике, Информатизация бизнес-процессов хозяйствующего субъекта в системе экономической безопасности, Компьютерные сети в системе экономической безопасности хозяйствующего субъекта, Программные средства обработки экономической информации в системе экономической безопасности, Электронный документооборот в системе экономической безопасности организации, Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика: Преддипломная практика, Государственная итоговая аттестация

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3: способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	
Знать:	
Уровень 1	иметь представление о знании закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 2	знать закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 3	интерпретировать знания о закономерностях создания и принципах функционирования систем информационной безопасности хозяйствующих субъектов
Уметь:	
Уровень 1	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на низком уровне
Уровень 2	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на среднем уровне
Уровень 3	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на высоком уровне
Владеть:	
Уровень 1	первичной способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 2	базовой способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 3	способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов

ПК-28: способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	
Знать:	
Уровень 1	иметь представление о знании критериев и показателей информационной безопасности
Уровень 2	знать критерии и показатели информационной безопасности
Уровень 3	интерпретировать знания о критериях и показателях информационной безопасности
Уметь:	
Уровень 1	определять первичные критерии информационной безопасности
Уровень 2	определять базовые критерии информационной безопасности
Уровень 3	определять критерии информационной безопасности
Владеть:	
Уровень 1	первичными критериями и показателями информационной безопасности
Уровень 2	базовыми критериями и показателями информационной безопасности

Уровень 3	критериями и показателями информационной безопасности

ПК-43: способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	
Знать:	
Уровень 1	иметь представление о знании методов принятия решений, критериев выбора оптимального решения по обеспечению информационной безопасности
Уровень 2	знать методы принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
Уровень 3	интерпретировать знания о методах принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
Уметь:	
Уровень 1	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на низком уровне
Уровень 2	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на среднем уровне
Уровень 3	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на высоком уровне
Владеть:	
Уровень 1	первичными навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности
Уровень 2	базовыми навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности
Уровень 3	навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.1.2	критерии и показатели информационной безопасности
3.1.3	методы принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
3.2	**Уметь:**
3.2.1	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.2.2	определять критерии информационной безопасности
3.2.3	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности
3.3	**Иметь навыки и (или) опыт деятельности (Владеть):**
3.3.1	способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.3.2	критериями и показателями информационной безопасности
3.3.3	навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1.						
1.1	Общие понятия и актуальность обеспечения информационной безопасности. /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.2	Менеджмент информационной безопасности в организации. /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	

1.3	Политика информационной безопасности в организации. Парольная политика /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.4	Разработка политики информационной безопасности организации /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.5	Анализ рисков и оценка затрат в системе информационной безопасности /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.6	Управление рисками в системе информационной безопасности /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.7	Угрозы информационной безопасности. Принципы и меры информационной безопасности /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.8	Менеджмент инцидентов информационной безопасности /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.9	Защита информации от несанкционированного доступа /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.10	Аудит информационной безопасности автоматизированной компьютерной системы /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.11	Криптографические методы защиты информации /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.12	Обеспечение безопасности автоматизированных компьютерных систем /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	
1.13	Эффективность защиты информации при помощи паролей /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1	6	
1.14	Криптографическое шифрование и кодирование данных /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.15	Организационно-правовое обеспечение информационной безопасности /Лек/	9	2	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	0	

1.16	Решение практических задач по обеспечению информационной безопасности /Лаб/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.1 Э2	6	
1.17	Подготовка к лекциям, лабораторным и практическим занятиям /Ср/	9	8	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.3 Л3.1 Э1 Э2	0	
1.18	Написание курсовой работы /КУРА/	9	20	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.3 Л3.1 Л3.2 Э1 Э2	0	
1.19	Самостоятельное изучение разделов и тем учебной дисциплины /Ср/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.3 Л3.1 Э1 Э2	0	
1.20	Текущий контроль успеваемости /Ср/	9	6	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.3 Л3.1 Э1 Э2	0	
1.21	Подготовка к экзамену /Ср/	9	4	ОПК-3 ПК-28 ПК-43	Л1.2 Л1.1Л2.3 Л2.2 Л2.1Л3.3 Л3.1 Э1 Э2	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля и промежуточной аттестации. Содержание фонда оценочных средств представлено в Приложении 1 и 2.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство,
Л1.1	Мельников, В. П	Информационная безопасность [Электронный ресурс]: учебник Режим доступа: https://book.ru/book/932908	Русайнс, 2020
Л1.2	О. В. Казарин, А. С. Забабурин	Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]: учебник и практикум для вузов Режим доступа: https://www.biblio-online.ru/bcode/452368	Юрайт, 2020

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство,
Л2.1	Крылов Г.О	Базовые понятия информационной безопасности [Электронный ресурс]: учебное пособие Режим доступа: https://book.ru/book/932492	Русайнс, 2020
Л2.2	под ред. В. В. Трофимова	Информатика в 2 т. Т. 1 [Электронный ресурс]: учебник для академического бакалавриата Режим доступа: https://www.biblio-online.ru/bcode/451824	Юрайт, 2020

	Авторы, составители	Заглавие	Издательство,
Л2.3	Сотов А. И.	Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации [Электронный ресурс]: монография Режим доступа: https://book.ru/book/920258	КноРус, 2020
6.1.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство,
Л3.1	Ливанов Р.В., Плотникова С.Н., Козлова Л.А	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие для лабораторных занятий, обучающихся по специальности 38.05.01 Экономическая безопасность Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров, 2021
Л3.2	Плотникова С.Н., Козлова Л.А., Ливанов Р.В.	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие по выполнению курсовой работы для обучающихся по специальности 38.05.01 Экономическая безопасность. Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров, 2021
Л3.3	Зонова Н.С., Ливанов Р.В	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие для самостоятельной работы обучающихся по специальности 38.05.01 Экономическая безопасность Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров: ВятГСХА, 2018
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"			
Э1	Научная электронная библиотека [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp		
Э2	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. - Режим доступа: https://digital.gov.ru/ru/ . - Загл. с экрана.		
6.3. Перечень информационных технологий			
6.3.1 Перечень программного обеспечения			
6.3.1.1	Операционная система семейства Windows (Windows Vista Business AO NL, MS Win Prof 7 AO NL, Win Prof 7 AOL NL, Win Home Bas 7 AOL NL LGG, Win Starter 7 AO NL LGG, Win SL 8 AOL NL LGG, Win Prof 8 AOL NL, Win Home 10 All Languages Online Product Key License)		
6.3.1.2	Приложения Office (MS Office Prof Plus 2007 AO NL, MS Office Prof Plus 2010 AO NL, MS Office 2013 OL NL, MS OfficeStd 2016 RUS OLP NL Acdmc)		
6.3.1.3	Антивирусное ПО Kaspersky Endpoint Security		
6.3.1.4	Free Commander 2009/02b		
6.3.1.5	Google Chrome 39/0/21/71/65		
6.3.1.6	Opera 26/0/1656/24		
6.3.1.7	Adobe Reader XI 11/0/09		
6.3.2 Перечень информационных справочных систем и современных профессиональных баз данных			
6.3.2.1	Информационная справочная система: КонсультантПлюс		
6.3.2.2	Информационная справочная система: Гарант Аэро		
6.3.2.3	Профессиональная база данных: Научная электронная библиотека elibrary.ru Режим доступа: http://elibrary.ru/defaultx.asp		
6.3.2.4	Профессиональная база данных: Электронный каталог ФГБОУ ВО Вятская ГСХА Режим доступа http://46.183.163.35/MarcWeb2		
6.3.2.5	Профессиональная база данных: Инспекция Федеральной налоговой службы по городу Кирову, Режим доступа: https://www.nalog.ru/rn43/ifns/imns43_17/		
6.3.2.6	Профессиональная база данных: Официальный сайт Министерства сельского хозяйства и продовольствия Кировской области, Режим доступа: http://www.dsx-kirov.ru/		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) представлено в Приложении 3 РПД.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение дисциплины проводится в форме аудиторных занятий и внеаудиторной самостоятельной работы обучающихся.

При проведении аудиторных занятий предусмотрено применение следующих инновационных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества: работа в малых группах, обсуждение и разрешение проблем, разбор конкретных ситуаций, встречи с представителями российских и зарубежных компаний. Количество часов занятий в интерактивных формах определено

учебным планом.
Практическая подготовка при реализации дисциплины организуется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.
Внеаудиторная самостоятельная работа осуществляется в следующих формах:
- самостоятельное изучение теоретического материала (тем дисциплины);
- подготовка к лабораторным занятиям;
- выполнение курсовых работ и иных индивидуальных заданий;
- подготовка к мероприятиям текущего контроля;
- подготовка к промежуточной аттестации.

При организации самостоятельной работы необходимо, прежде всего, обратить внимание на ключевые понятия, несущие основную смысловую нагрузку в том или ином разделе учебной дисциплины.

1. Самостоятельное изучение тем дисциплины

Для работы необходимо ознакомиться с учебным планом дисциплины и установить, какое количество часов отведено учебным планом в целом на изучение дисциплины, на аудиторную работу с преподавателем на лекционных и лабораторных занятиях, а также на самостоятельную работу. С целью оптимальной самоорганизации необходимо сопоставить эту информацию с графиком занятий и выявить наиболее затратные по времени и объему темы, чтобы заранее определить для себя
периоды объемных заданий. Целесообразно начать работу с изучения теоретического материала, основных терминов и понятий курса и с письменных ответов на индивидуальные и тестовые задания.

2. Подготовка к лекционным и лабораторным занятиям

Традиционной формой преподнесения материала является лекция. Курс лекций по предмету дает необходимую информацию по изучению закономерностей и тенденций развития объекта и предмета исследования изучаемой дисциплины. Лекционный материал рекомендуется конспектировать. Конспекты позволяют обучающемуся не только получить больше информации на лекции, но и правильно его структурировать, а в дальнейшем - лучше освоить.
Подготовка к лабораторным занятиям носит различный характер как по содержанию, так и по сложности исполнения. Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы. Прежде чем приступить к выполнению такой работы, обучающемуся необходимо ознакомиться обстоятельно с содержанием задания,
уяснить его, оценить с точки зрения восприятия и запоминания все составляющие его компоненты. Результаты эксперимента, графики и т.д. следует стремиться получить непосредственно при выполнении работы в лаборатории. Лабораторная работа считается выполненной только в том случае, когда отчет по ней принят. Чем скорее составлен отчет после проведения работы, тем меньше будет затрачено труда и времени на ее оформление.

3. Выполнение курсовой работы

Курсовая работа является одним из основных видов самостоятельной работы, направленной на закрепление, углубление и обобщение знаний по дисциплине. Целью выполнения курсовой работы является формирование навыков самостоятельного творческого решения профессиональных задач. Задачами выполнения курсовой работы являются систематизация, закрепление,углубление и расширение приобретенных обучающимся знаний, умений и навыков по дисциплине. Обучающийся выполняет курсовую работу по утвержденной теме под руководством преподавателя.

4. Подготовка к мероприятиям текущего контроля

В конце изучения каждой темы может проводиться тематическая контрольная работа, которая является средством промежуточного контроля оценки знаний. Подготовка к ней заключается в повторении пройденного материала и повторном решении заданий, которые рассматривались на занятиях, а также в выполнении заданий для самостоятельной работы.

5. Подготовка к промежуточной аттестации

Подготовка к экзамену является заключительным этапом изучения дисциплины и является средством промежуточного контроля. Подготовка к экзамену предполагает изучение конспектовлекций, рекомендуемой литературы и других источников, повторение материалов практических занятий. В процессе подготовки к экзамену выявляются вопросы, по которым нет уверенности в ответе либо ответ обучающемуся не ясен. Данные вопросы можно уточнить у преподавателя на консультации, которая проводится перед экзаменом.

Министерство сельского хозяйства Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Вятский государственный агротехнологический университет"

УТВЕРЖДАЮ

Декан экономического факультета

_____ Т.Б. Шиврина

_____ апреля 2021 г.

Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **информационных технологий и статистики**

Учебный план Специальность 38.05.01 Экономическая безопасность Специализация "Экономико-правовое обеспечение экономической безопасности"

Квалификация **экономист**

Форма обучения **заочная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 16
самостоятельная работа 99
часов на контроль 9

Виды контроля на курсах:
экзамены 5
курсовые работы 5

Распределение часов дисциплины по курсам

Курс	5		Итого	
Вид занятий	УП	РП		
Лекции	6	6	6	6
Лабораторные	10	10	10	10
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	99	99	99	99
Часы на контроль	9	9	9	9
Курсовая работа	20	20	20	20
Итого	144	144	144	144

Киров 2021

Программу составил(и):

старший преподаватель кафедры информационных технологий и статистики, Ливанов Роман Витальевич

Рецензент(ы):

к.п.н., доцент кафедры информационных технологий и статистики, Дьячков Валерий Павлович

Рабочая программа дисциплины

Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования по специальности 38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ (приказ Минобрнауки России от 16.02.2017 г. № 20)

составлена на основании Учебного плана:

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

одобренного и утвержденного Ученым советом университета от 15.04.2021 протокол № 5.

Рабочая программа дисциплины рассмотрена и одобрена учебно-методической комиссией

экономического факультета Протокол № 6 от "15" апреля 2021 г.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры

информационных технологий и статистики

Протокол № 12 от "15" апреля 2021 г.

Зав. кафедрой _____ к.э.н., доцент Козлова Лариса Алексеевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2022 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры

информационных технологий и статистики

Протокол от "__" _____ 2025 г. № __

Зав. кафедрой _____

1. ЦЕЛЬ (ЦЕЛИ) ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	ознакомление студентов с тенденциями развития защиты информации, моделями возможных угроз, терминологией и основными понятиями теории защиты информации, ознакомление с нормативными документами и методами защиты компьютерной информации и формирование навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Обучающийся должен обладать знаниями, умениями, навыками не ниже 1 уровня (низкого), полученными при изучении следующих дисциплин:Информационные системы в экономике, Информатизация бизнес-процессов хозяйствующего субъекта в системе экономической безопасности, Компьютерные сети в системе экономической безопасности хозяйствующего субъекта, Программные средства обработки экономической информации в системе экономической безопасности, Электронный документооборот в системе экономической безопасности организации, Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика: Преддипломная практика, Государственная итоговая аттестация

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3: способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	
Знать:	
Уровень 1	иметь представление о знании закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 2	знать закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 3	интерпретировать знания о закономерностях создания и принципах функционирования систем информационной безопасности хозяйствующих субъектов
Уметь:	
Уровень 1	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на низком уровне
Уровень 2	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на среднем уровне
Уровень 3	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на высоком уровне
Владеть:	
Уровень 1	первичной способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 2	базовой способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
Уровень 3	способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов

ПК-28: способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	
Знать:	
Уровень 1	иметь представление о знании критериев и показателей информационной безопасности
Уровень 2	знать критерии и показатели информационной безопасности
Уровень 3	интерпретировать знания о критериях и показателях информационной безопасности
Уметь:	
Уровень 1	определять первичные критерии информационной безопасности
Уровень 2	определять базовые критерии информационной безопасности
Уровень 3	определять критерии информационной безопасности
Владеть:	
Уровень 1	первичными критериями и показателями информационной безопасности
Уровень 2	базовыми критериями и показателями информационной безопасности

Уровень 3	критериями и показателями информационной безопасности

ПК-43: способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов	
Знать:	
Уровень 1	иметь представление о знании методов принятия решений, критериев выбора оптимального решения по обеспечению информационной безопасности
Уровень 2	знать методы принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
Уровень 3	интерпретировать знания о методах принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
Уметь:	
Уровень 1	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на низком уровне
Уровень 2	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на среднем уровне
Уровень 3	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на высоком уровне
Владеть:	
Уровень 1	первичными навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности
Уровень 2	базовыми навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности
Уровень 3	навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.1.2	критерии и показатели информационной безопасности
3.1.3	методы принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности
3.2	**Уметь:**
3.2.1	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.2.2	определять критерии информационной безопасности
3.2.3	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности
3.3	**Иметь навыки и (или) опыт деятельности (Владеть):**
3.3.1	способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов
3.3.2	критериями и показателями информационной безопасности
3.3.3	навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1.						
1.1	Общие понятия и актуальность обеспечения информационной безопасности. /Лек/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.2	Менеджмент информационной безопасности в организации. /Лаб/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	

1.3	Политика информационной безопасности в организации. Парольная политика /Лек/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.4	Разработка политики информационной безопасности организации /Лаб/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.5	Анализ рисков и оценка затрат в системе информационной безопасности. Обеспечение безопасности автоматизированных компьютерных систем /Лек/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.6	Управление рисками в системе информационной безопасности /Лаб/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.7	Аудит информационной безопасности автоматизированной компьютерной системы /Лаб/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.8	Криптографическое шифрование и кодирование данных /Лаб/	5	2	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.2 Э2	0	
1.9	Подготовка к лекциям, лабораторным и практическим занятиям /Ср/	5	20	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	
1.10	Написание курсовой работы /КУРА/	5	20	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Л3.3 Э1 Э2	0	
1.11	Самостоятельное изучение разделов и тем учебной дисциплины /Ср/	5	20	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	
1.12	Текущий контроль успеваемости /Ср/	5	35	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	
1.13	Подготовка к экзамену /Ср/	5	24	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	
1.14	Экзамен /Экзамен/	5	9	ОПК-3 ПК-28 ПК-43	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля и промежуточной аттестации. Содержание фонда оценочных средств представлено в Приложении 1 и 2.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство,
Л1.1	О. В. Казарин, А. С. Забабурин	Программно-аппаратные средства защиты информации. Защита программного обеспечения [Электронный ресурс]: учебник и практикум для вузов Режим доступа: https://www.biblio-online.ru/bcode/452368	Юрайт, 2020
Л1.2	Мельников, В. П	Информационная безопасность [Электронный ресурс]: учебник Режим доступа: https://book.ru/book/932908	Русайнс, 2020

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство,
Л2.1	Сотов А. И.	Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации [Электронный ресурс]: монография Режим доступа: https://book.ru/book/920258	КноРус, 2020
Л2.2	под ред. В. В. Трофимова	Информатика в 2 т. Т. 1 [Электронный ресурс]: учебник для академического бакалавриата Режим доступа: https://www.biblio-online.ru/bcode/451824	Юрайт, 2020
Л2.3	Крылов Г.О	Базовые понятия информационной безопасности [Электронный ресурс]: учебное пособие Режим доступа: https://book.ru/book/932492	Русайнс, 2020

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство,
Л3.1	Зонова Н.С., Ливанов Р.В	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие для самостоятельной работы обучающихся по специальности 38.05.01 Экономическая безопасность Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров: ВятГСХА, 2018
Л3.2	Ливанов Р.В., Плотникова С.Н., Козлова Л.А	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие для лабораторных занятий, обучающихся по специальности 38.05.01 Экономическая безопасность Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров, 2021
Л3.3	Плотникова С.Н., Козлова Л.А., Ливанов Р.В.	Информационная безопасность хозяйствующего субъекта в системе экономической безопасности [Электронный ресурс]: учебно-методическое пособие по выполнению курсовой работы для обучающихся по специальности 38.05.01 Экономическая безопасность. Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров, 2021

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp
Э2	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. - Режим доступа: https://digital.gov.ru/ru/ . - Загл. с экрана.

6.3. Перечень информационных технологий

6.3.1 Перечень программного обеспечения

6.3.1.1	Операционная система семейства Windows (Windows Vista Business AO NL, MS Win Prof 7 AO NL, Win Prof 7 AOL NL, Win Home Bas 7 AOL NL LGG, Win Starter 7 AO NL LGG, Win SL 8 AOL NL LGG, Win Prof 8 AOL NL, Win Home 10 All Languages Online Product Key License)
6.3.1.2	Приложения Office (MS Office Prof Plus 2007 AO NL, MS Office Prof Plus 2010 AO NL, MS Office 2013 OL NL, MS OfficeStd 2016 RUS OLP NL Acdmc)
6.3.1.3	Антивирусное ПО Kaspersky Endpoint Security
6.3.1.4	Free Commander 2009/02b
6.3.1.5	Google Chrome 39/0/21/71/65

6.3.1.6	Opera 26/0/1656/24
6.3.1.7	Adobe Reader XI 11/0/09
6.3.2 Перечень информационных справочных систем и современных профессиональных баз данных	
6.3.2.1	Информационная справочная система: КонсультантПлюс
6.3.2.2	Информационная справочная система: Гарант Аэро
6.3.2.3	Профессиональная база данных: Научная электронная библиотека elibrary.ru Режим доступа: http://elibrary.ru/defaultx.asp
6.3.2.4	Профессиональная база данных: Электронный каталог ФГБОУ ВО Вятская ГСХА Режим доступа http://46.183.163.35/MarcWeb2
6.3.2.5	Профессиональная база данных: Инспекция Федеральной налоговой службы по городу Кирову, Режим доступа: https://www.nalog.ru/rn43/ifns/imns43_17/
6.3.2.6	Профессиональная база данных: Официальный сайт Министерства сельского хозяйства и продовольствия Кировской области, Режим доступа: http://www.dsx-kirov.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) представлено в Приложении 3 РПД.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение дисциплины проводится в форме аудиторных занятий и внеаудиторной самостоятельной работы обучающихся.

При проведении аудиторных занятий предусмотрено применение следующих инновационных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества: работа в малых группах, обсуждение и разрешение проблем, разбор конкретных ситуаций, встречи с представителями российских и зарубежных компаний. Количество часов занятий в интерактивных формах определено учебным планом.

Практическая подготовка при реализации дисциплины организуется путем проведения лабораторных занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Внеаудиторная самостоятельная работа осуществляется в следующих формах:

- самостоятельное изучение теоретического материала (тем дисциплины);
- подготовка к лабораторным занятиям;
- выполнение курсовых работ и иных индивидуальных заданий;
- подготовка к мероприятиям текущего контроля;
- подготовка к промежуточной аттестации.

При организации самостоятельной работы необходимо, прежде всего, обратить внимание на ключевые понятия, несущие основную смысловую нагрузку в том или ином разделе учебной дисциплины.

1. Самостоятельное изучение тем дисциплины

Для работы необходимо ознакомиться с учебным планом дисциплины и установить, какое количество часов отведено учебным планом в целом на изучение дисциплины, на аудиторную работу с преподавателем на лекционных и лабораторных занятиях, а также на самостоятельную работу. С целью оптимальной самоорганизации необходимо сопоставить эту информацию с графиком занятий и выявить наиболее затратные по времени и объему темы, чтобы заранее определить для себя

периоды объемных заданий. Целесообразно начать работу с изучения теоретического материала, основных терминов и понятий курса и с письменных ответов на индивидуальные и тестовые задания.

2. Подготовка к лекционным и лабораторным занятиям

Традиционной формой преподнесения материала является лекция. Курс лекций по предмету дает необходимую информацию по изучению закономерностей и тенденций развития объекта и предмета исследования изучаемой дисциплины. Лекционный материал рекомендуется конспектировать. Конспекты позволяют обучающемуся не только получить больше информации на лекции, но и правильно его структурировать, а в дальнейшем - лучше освоить.

Подготовка к лабораторным занятиям носит различный характер как по содержанию, так и по сложности исполнения. Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы. Прежде чем приступить к выполнению такой работы, обучающемуся необходимо ознакомиться обстоятельно с содержанием задания,

уяснить его, оценить с точки зрения восприятия и запоминания все составляющие его компоненты. Результаты эксперимента, графики и т.д. следует стремиться получить непосредственно при выполнении работы в лаборатории. Лабораторная работа считается выполненной только в том случае, когда отчет по ней принят. Чем скорее составлен отчет после проведения работы, тем меньше будет затрачено труда и времени на ее оформление.

3. Выполнение курсовой работы

Курсовая работа является одним из основных видов самостоятельной работы, направленной на закрепление, углубление и обобщение знаний по дисциплине. Целью выполнения курсовой работы является формирование навыков самостоятельного творческого решения профессиональных задач. Задачами выполнения курсовой работы являются систематизация, закрепление,углубление и расширение приобретенных обучающимся знаний, умений и навыков по дисциплине. Обучающийся выполняет курсовую работу по утвержденной теме под руководством преподавателя.

4. Подготовка к мероприятиям текущего контроля

В конце изучения каждой темы может проводиться тематическая контрольная работа, которая является средством промежуточного контроля оценки знаний. Подготовка к ней заключается в повторении пройденного материала и повторном решении заданий, которые рассматривались на занятиях, а также в выполнении заданий для самостоятельной работы.

5. Подготовка к промежуточной аттестации

Подготовка к экзамену является заключительным этапом изучения дисциплины и является средством промежуточного контроля. Подготовка к экзамену предполагает изучение конспектовлекций, рекомендуемой литературы и других источников, повторение материалов практических занятий. В процессе подготовки к экзамену выявляются вопросы, по которым нет уверенности в ответе либо ответ обучающемуся не ясен. Данные вопросы можно уточнить у преподавателя на консультации, которая проводится перед экзаменом.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации по дисциплине
Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

Специальность 38.05.01 Экономическая безопасность
Специализация «Экономико-правовое обеспечение экономической безопасности»

Квалификация экономист

1. Описание назначения фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины/модуля «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»
и предназначен для оценки планируемых результатов обучения - знаний, умений, навыков, характеризующих этапы формирования компетенций (п.2) в процессе изучения данной дисциплины/модуля.

ФОС включает в себя оценочные материалы для проведения промежуточной аттестации в форме курсовой работы и экзамена.

ФОС разработан на основании:

федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета). Утвержден приказом Минобрнауки России от 16 января 2017 № 20;

основной профессиональной образовательной программы высшего образования по специальности 38.05.01 Экономическая безопасность специализация «Экономико-правовое обеспечение экономической безопасности»;

Положения «О формировании фонда оценочных средств для промежуточной и итоговой аттестации обучающихся по образовательным программам высшего образования».

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

Общепрофессиональные компетенции:

- способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов (ОПК-3)

Профессиональные компетенции:

- способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач (ПК-28);
- способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов (ПК-43).

Этапы формирования компетенции в процессе освоения образовательной программы

Код формируемой компетенции	Начальный	Основной	Заключительный
ОПК-3	• Экономическая безопасность • Учебная практика: практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-	• Оценка рисков • Информационная безопасность хозяйствующего субъекта в системе экономической безопасности • Практикум " Экономико-правовое обеспечение безопасности	• Производственная практика: преддипломная практика • Подготовка к государственной итоговой аттестации

	исследовательской деятельности	хозяйствующих субъектов" • Безопасность продовольственных рынков • Экономическая безопасность хозяйствующего субъекта в условиях глобализации экономики • Экономическая безопасность хозяйствующего субъекта в системе ВТО • Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности	
ПК-28	• Оценка и управление стоимостью предприятия в системе экономической безопасности • Программные средства обработки экономической информации в системе экономической безопасности • Финансовое право • Налоговое право • Информатизация бизнес-процессов хозяйствующего субъекта в системе экономической безопасности • Учебная практика: практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	• Основы оперативно-розыскной деятельности • Информационная безопасность хозяйствующего субъекта в системе экономической безопасности • Расследование и предупреждение экономических преступлений и правонарушений • Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности	• Производственная практика: преддипломная практика • Подготовка к государственной итоговой аттестации
ПК-43	• Превентивное антикризисное управление в системе обеспечения экономической	• Оценка рисков • Информационная безопасность хозяйствующего субъекта в системе экономической	• Производственная практика: преддипломная практика • Подготовка к

	безопасности организации • Экономика природопользования хозяйствующего субъекта • Экономическая оценка факторов и рисков воздействия хозяйствующего субъекта на окружающую среду • Оценка и управление инвестиционной и инновационной деятельностью организаций • • Внешнеэкономическая деятельность хозяйствующего субъекта в системе экономической безопасности • Прогнозирование национальной экономики и экономическая безопасность региона •	безопасности • Управление безопасностью производственных систем АПК • Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности	государственной итоговой аттестации

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

Планируемые результаты обучения по дисциплине - знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы

ОПК-3: Способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов		
Знать:		**Критерии оценивания**
Уровень 1	иметь представление о знании закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычислительной техники и современных информационных технологий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	знать закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов	
Уровень 3	интерпретировать знания о закономерностях создания и принципах функционирования систем информационной безопасности хозяйствующих субъектов	
Уметь:		**Критерии оценивания**
Уровень 1	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на низком уровне	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычислительной техники и современных информационных технологий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на среднем уровне	
Уровень 3	применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов на высоком уровне	
Владеть:		**Критерии оценивания**
Уровень 1	первичной способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычислительной
Уровень 2	базовой способностью применять основные закономерности создания и	

	принципы функционирования систем информационной безопасности хозяйствующих субъектов	техники и современных информационных технологий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 3	способностью применять основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов	
ПК-28: способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач		
Знать:		**Критерии оценивания**
Уровень 1	иметь представление о знании критериев и показателей информационной безопасности	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профес-сиональных задач; - правильность решения практического задания с использованием вычисли-тельной техники и современных информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	знать критерии и показатели информационной безопасности	
Уровень 3	интерпретировать знания о критериях и показателях информационной безопасности	
Уметь:		**Критерии оценивания**
Уровень 1	определять первичные критерии информационной безопасности	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профес-сиональных задач; - правильность решения практического задания с использованием вычисли-тельной техники и современных информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	определять базовые критерии информационной безопасности	
Уровень 3	определять критерии информационной безопасности	
Владеть:		**Критерии оценивания**
Уровень 1	первичными критериями и показателями информационной безопасности	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профес-сиональных задач; - правильность решения практического задания с использованием вычисли-тельной техники и современных
Уровень 2	базовыми критериями и показателями информационной безопасности	

		информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 3	критериями и показателями информационной безопасности	
ПК-43: способностью принимать оптимальные управленческие решения с учетом критериев социально- экономической эффективности, рисков и возможностей		
Знать:		**Критерии оценивания**
Уровень 1	иметь представление о знании методов принятия решений, критериев выбора оптимального решения по обеспечению информационной безопасности	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычисли-тельной техники и современных информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	знать методы принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности	
Уровень 3	интерпретировать знания о методах принятия решений, критерии выбора оптимального решения по обеспечению информационной безопасности	
Уметь:		**Критерии оценивания**
Уровень 1	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на низком уровне	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычисли-тельной техники и современных информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 2	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на среднем уровне	
Уровень 3	обосновывать выбор, оценивать условия и последствия принимаемых управленческих решений по обеспечению информационной безопасности на высоком уровне	
Владеть:		**Критерии оценивания**
Уровень 1	первичными навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности	- уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач; - правильность решения практического задания с использованием вычисли-тельной
Уровень 2	базовыми навыками обоснования выбора, оценки условий и последствий	

	принимаемых управленческих решений по обеспечению информационной безопасности	техники и современных информационных техно-логий; - логичность, обоснованность, четкость ответа, ответы на вопросы; - работа в течение семестра, наличие задолженности по текущему контролю успеваемости.
Уровень 3	навыками обоснования выбора, оценки условий и последствий принимаемых управленческих решений по обеспечению информационной безопасности	

Для оценки сформированности соответствующих компетенций по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности» применяется аналитическая шкала оценивания:

1.Форма промежуточной аттестации - курсовая работа

Критерии оценивания	Шкала оценивания			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	показатели			
Соответствие содержания теме работы и полнота ее раскрытия	содержание работы не соответствует теме	содержание работы соответствует не в полной мере теме, тема не полностью раскрыта	содержание соответствует теме работы, тема раскрыта не в полном объеме	содержание соответствует теме работы, тема раскрыта в полном объеме
Соответствие содержания требованиям методических указаний	полностью не соответствует	требования выполнены со значительными замечаниями	несоответствия носят незначительный характер	полностью соответствует требованиям
Требования к оформлению работы	требования не выполнены; имеются грубые стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены с незначительными замечаниями, имеются небольшие стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены с незначительными замечаниями, имеются небольшие стилистические, орфографические, пунктуационные и грамматические ошибки	требования выполнены полностью, отсутствуют стилистические, орфографические, пунктуационные и грамматические ошибки
Качество выполнения работы	имеются значительные логические нарушения в изложении	имеются незначительные логические нарушения в изложении	материал изложен логично; сделаны самостоятельн	материал изложен логично и доказательно; выводы

	материала; выводы не соответствуют фактическому материалу, либо носят необоснованный характер	материала; выводы не в полной мере соответствуют фактическому материалу	ые выводы, отвечающие фактическому материалу	самостоятельн ые, полные, соответствуют фактическому материалу
Качество защиты	обучающийся не владеет материалом, показывает неудовлетворитель ные знания, умения и навыки по применению показателей, методик; на поставленные вопросы дает неправильные ответы	обучающийся не в полной мере владеет материалом, показывает удовлетворительн ые знания, умения и навыки по применению показателей, методик; на большинство вопросов дает неправильные ответы	обучающийся владеет материалом, показывает хорошие знания, умения и навыки по применению показателей, методик; на большинство вопросов дает правильные ответы	обучающийся свободно владеет материалом, показывает отличные знания, умения и навыки по применению показателей, методик; правильно отвечает на вопросы по теме работы

2.Форма промежуточной аттестации - экзамен

№	Критерии оценивания	Шкала оценивания			
		неудовлетво-рительно	удовлетвори-тельно	хорошо	отлично
		Описание показателя			
1	Уровень усвоения обучающимся теоретических знаний и умение использовать их для решения профессиональных задач	Низкий уровень усвоения материала. Продемонстрировано незнание зна-чительной части программного материала	Представлены знания только основного материала, но не усвоены его деталей	Твердое знание материала	Высокий уровень усвоения материала, продемонстрировано умение тесно увязывать теорию с практикой
2	Правильность решения практического задания с использованием вычислительной техники и современных информационных технологий	Обучающийся неуверенно, с большими за-труднениями выполняет практические работы	Обучающийся испытывает затруднения при выполнении практических работ	Обучающийся правильно применяет тео-ретические по-ложения при решении прак-тических воп-росов и задач, владеет необ-ходимыми на-	Обучающийся свободно спра-вляется с зада-чами, вопросами и другими видами применения знаний, причем не

				выками и приемами их выполнения	затрудняется с ответом при видоизменении заданий,
3	Логичность, обоснованность, четкость ответа на вопросы	Существенные ошибки, нет ответов на дополнительные уточняющие вопросы	Неточности в ответах, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.	Грамотное и по существу изложение теоретического материала, не допуская существенных неточностей в ответе на вопрос	Исчерпывающе последовательно, четко и логически стройно излагается теоретический материал
4	Работа в течение семестра, наличие задолженности по текущему контролю успеваемости.	Имеются многочисленные пропуски занятий, задолженность по текущему контролю знаний	Имеются пропуски занятий, частичная задолженность по текущему контролю знаний	Активная, Задолженность отсутствует	Активная, Задолженность отсутствует

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

.Тематика курсовых работ
по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

1. Государственная система защиты информации РФ
2. Обеспечение информационной безопасности в банковских и финансовых структурах
3. Анализ мирового рынка антивирусного программного обеспечения
4. Концепция электронного документа и проблемы правового регулирования электронно-цифровой подписи
5. Анализ российских сетевых ресурсов, посвященных информационной безопасности
6. Безопасность электронной почты и Интернет
7. Методы и средства борьбы со спамом
8. Методы защиты аудио и визуальных документов
9. Аудит безопасности информационных систем
10. Компьютерная преступность в России
11. Выбор показателей защищенности от несанкционированного доступа к информации
12. Анализ рынка программного обеспечения используемого для обработки конфиденциальной информации
13. Проблемы внедрения электронной цифровой подписи в практику делопроизводства
14. Техническое, организационное и правовое обеспечение электронной цифровой подписи
15. Политика информационной безопасности в РФ

16. Использование количественных показателей для оценки информационной безопасности
17. Угрозы несанкционированного доступа к информации при помощи программных средств
18. Человеческий фактор с точки зрения информационной безопасности
19. Оценка эффективности систем защиты информации
20. Технологии, используемые при совершении компьютерных преступлений
21. Сравнительный анализ российского и американского законодательства в сфере ИБ.
22. Аудит безопасности корпоративных информационных систем
23. Правовые основы защиты конфиденциальной информации
24. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну
25. Обеспечение безопасности мобильных пользователей корпоративной сети
26. Классификация информационных преступлений
27. Криптографические системы защиты данных
28. Экономические основы защиты конфиденциальной информации
29. Управление безопасностью приложений (на примере компании….)
30. Современные технологии аутентификации и управления безопасностью компания
31. Нормативно-правовые аспекты обеспечения информационной безопасности
32. Анализ российского рынка биометрических систем, используемых в системах обеспечения информационной безопасности
33. Технологии хранения конфиденциальных документов
34. Методы перехвата и навязывания информации
35. Классификация и принципы оценивания безопасности компьютерных систем
36. Выбор качественных показателей для оценки информационной безопасности
37. Зарубежный рынок средств обеспечения информационной безопасности
38. Классификация угроз в сфере информационной безопасности
39. Анализ рынка аудита информационной безопасности
40. Основные направления профилактики и борьбы с компьютерными преступлениями в РФ
41. Технологии защиты Web-ресурсов от взлома и хакерских атак
42. Анализ рынка труда в сфере информационной безопасности
43. Технологии антивирусной защиты
44. Проблемы безопасности в глобальных сетях
45. Сравнительный анализ протоколов электронной подписи
46. Защита информации в рекламной и выставочной деятельности
47. Технологии обработки и хранения конфиденциальных документов
48. Экономические основы защиты конфиденциальной информации
49. Методы защиты документов на бумажных носителях
50. Методы защиты аудио и визуальных документов

Тестовые задания
по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»
для промежуточной аттестации в форме экзамена (62 задания)

1. ***Установите соответствие между составляющей информационной безопасности и её содержанием*** (***ОПК-3, ПК-28 Знания, уровень 1-Низкий***)

1. Доступность информации	А. Гарантия того, что информация сейчас

2. Целостность информации 3. Конфиденциальность информации	существует в её исходном виде Б. Гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена В. Гарантия получения требуемой информации или информационной услуги пользователем за определенное время
	1-В 2-А 3-Б

2. ***Установите соответствие между типом вируса и его определением*** (***ОПК-3, ПК-20, ПК-28 Знания, уровень 2-Базовый***)

1. Файловые вирусы 2. Загрузочные вирусы 3. Сетевые вирусы	А. Используют для своего распространения протоколы или команды компьютерных сетей Б. Записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жесткого диска В. Внедряются в выполняемые файлы
	1-В 2-Б 3-А

3. **Что из перечисленного являются составляющей информационной безопасности** (***ОПК-3, ПК-28, ПК-43 Знания, уровень 1-Низкий***)

   А. Нарушение целостности информации (-)
   Б. Проверка прав доступа к информации (-)
   В. *Доступность информации (+)*
   Г. Выявление нарушителей (-)

4. **Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией** (***ОПК-3, ПК-28, ПК-43 Знания, уровень 3-Продвинутый***)

   А. Законодательно-правовой (-)
   Б. Информационный (-)
   В. Административный (организационный) (-)
   Г. Программно-технический (+)

5. **Сколько категорий государственных информационных ресурсов определяет Закон «Об информации, информатизации и защите информации»** (***ОПК-3, ПК-28 Знания, уровень 2-Базовый***)

   А. Три (-)
   Б. Четыре (-)
   В. Два (-)
   Г. *Пять* (+)

6. **Что не рассматривается в политике безопасности** (***ОПК-3, ПК-28, ПК-43 Знания, уровень 3-Продвинутый***)

А. Требуемый уровень защиты данных (-)
Б. Роли субъектов информационных отношений (-)
В. Анализ рисков (-)
Г. *Защищенность механизмов безопасности (+)*

Практические задания по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности» для промежуточной аттестации в форме экзамена (15 вариантов)

Задача 1

Дайте описание документа «Политика информационной безопасности» (***ОПК-3, ПК-28, ПК-43 Умения, уровень 2-Базовый***)

Задача 2

Зашифровать с помощью криптографической системы Цезаря выражение «Пришел, увидел, победил» (***ОПК-3, ПК-28 Умения, уровень 2-Базовый***)

Задача 3

Выполнить резервное копирование и восстановление информационной базы предприятия в программе 1С:Бухгалтерия 8.3(***ОПК-3, ПК-28, ПК-43 Умения, уровень 3-Продвинутый***)

1. Выполнить операцию вручную, указав путь сохранения архива в папке Документы \1С.
2. Настроить автоматический режим копирования с периодичностью 2 дня.
3. Создать новый документ на выдачу денежных средств из кассы организации в подотчет.
4. Восстановить из архива информационную базу, убедиться в правильности выполнения операции.

Задача 4.

Настройка прав пользователей в программе 1С:Бухгалтерия 8.3 (***ОПК-3, ПК-28, ПК-43 Умения, уровень 2-Базовый***)

1. Создать список пользователей: Карамелькина Алевтина Ивановна - главный бухгалтер, Баринов Петр Николаевич – кладовщик, Автаномов Сегрей Сергеевич – программист администратор.
2. Каждому пользователю задать профили доступа.
3. Продемонстрировать результаты настроек.

Задача 5.

Технологии создания и работы с базами данных в 1С:Бухгалтерия 8.3 (***ОПК-3,ПК-28 Умения, уровень 3-Продвинутый***)

1. Запустите программу с информационной базой **Вятская молочная компания** в режиме **Конфигуратора 1С:Предприятие 8.**
2. Откройте окно конфигурации.
3. Создайте константу с общими свойствами:

Имя ДатаРегистрации
Синоним Дата регистрации
Комментарий Дата регистрации

4. Сохраните созданную константу.
5. Создайте константу с общими свойствами:

Имя НазваниеОрганизации
Синоним Наименование организации
Комментарий Наименование организации

6. Сохраните константу.
7. Создайте и сохраните константу:

Имя АдресОрганиэации
Синоним Юридический адрес
Комментарий Юридический адрес организации
Тип значения Строка
Длина **60**

6. Введите значения констант

Код	Наименование	Значение
Дата регистрации	Дата регистрации	15.06.16
Наименование организации	Полное наименование организации	ЗАО «Вятская молочная компания»
Юридический адрес	Юридический адрес организации	910017,Киров, Ленина, д.111
Телефоны организации	Телефоны организации	64-24-68
Основной вид деятельности	Основной вид деятельности	Производство молочной продукции

Вопросы к экзамену
по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

1. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
2. Международные стандарты информационного обмена.
3. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений.
4. Понятия и определения в информационной безопасности
5. Российское законодательство в области информационной безопасности. Правовые акты общего назначения. Закон «Об информации, информатизации и защите информации», Закон «О лицензировании отдельных видов деятельности», Закон «Об электронной цифровой подписи»,
6. Зарубежное законодательство в области информационной безопасности, стандарты и спецификации в области информационной безопасности, «Оранжевая книга», информационная безопасность распределенных систем, стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», методология оценки безопасности ИТ по общим критериям, общая методология оценки безопасности ИТ (ОМО).
7. Версии общей методологии оценки безопасности ИТ. Принципы разработки ОМО, содержание ОМО, процесс оценки.
8. Виды угроз информационной безопасности. Источники угроз информационной безопасности РФ.

9. Информационная безопасность в условиях функционирования в России глобальных сетей.
10. Виды возможных нарушений информационной системы.
11. Виды противников или «нарушителей». Удаленные атаки на интрасети.
12. Условия существования вредоносных программ. Понятия о видах вирусов.
13. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit.
14. Спам.
15. Признаки заражения компьютера. Источники компьютерных вирусов.
16. Защита от компьютерных вирусов. Основные правила защиты. Антивирусные программы.
    Основные положения теории информационной безопасности информационных систем.
17. Концепция информационной безопасности.
18. Модели безопасности и их применение.
19. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
20. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.
    Методы обеспечения информационной безопасности РФ.
21. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
22. Методы и средства защиты информации от случайных воздействий.
23. Методы защиты информации от аварийных ситуаций.
24. Организационные мероприятия по защите информации. Организация информационной Безопасности компании.
25. Выбор средств информационной информации.
26. Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности,
27. Планирование восстановительных работ, разделение обязанностей, минимизация привилегий, описание должности, обучение,
28. Непрерывность защиты в пространстве и времени, физическое управление доступом, периметр безопасности, контролируемая территория,
29. Защита поддерживающей инфраструктуры, защита от перехвата данных, защита мобильных систем,
30. Поддержка пользователей, поддержка программного обеспечения,
31. Конфигурационное управление, резервное копирование, управление носителями,
32. Документирование, регламентные работы,
33. Прослеживание нарушителя, предупреждение повторных нарушений, отслеживание новых уязвимых мест, критически важные функции, идентификация ресурсов, стратегия восстановительных работ.
34. Методы криптографии. Классификация криптографических методов.
35. Характеристики существующих шифров. Кодирование.
36. Электронная цифровая подпись.
37. Политика безопасности, программа безопасности, анализ рисков, уровень детализации, карта ИС,
38. Порядок разработки политики безопасности, непрерывная работа, оценка рисков, координация, стратегическое планирование, контроль, жизненный цикл, инициация, закупка, установка, эксплуатация, выведение из эксплуатации.

39. Практическое применение международного стандарта безопасности информационных систем ISO 17799. Типовые документы, основанные на стандарте безопасности.
40. Законодательство в области лицензирования и сертификации.
41. Правила функционирования системы лицензирования.
42. Основные нормативные руководящие документы, касающиеся государственной тайны,
43. Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux.
44. Администрирование прав пользователей.
45. Аппаратно-программные комплексы обеспечения безопасности ОС. Резервное копирование и восстановление данных.
46. Права доступа в БД. Использование процедур PL/SQL для повышения безопасности и быстродействия информационных систем.
47. Повышение надежности систем хранения данных. Сериализация транзакций. Журнализация.
48. Методика оценки совокупной стоимости владения для подсистемы ИБ.
49. Границы применения методики. Технология оценки затрат на ИБ. Идентификация затрат на безопасность. Внедрение системы учета затрат на ИБ.

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

Процедура оценивания знаний, умений и навыков при проведении промежуточной аттестации по дисциплине «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности» проводится в форме курсовой работы и экзамена.

Порядок организации и проведения промежуточной аттестации обучающегося, форма проведения, процедура сдачи экзамена, сроки и иные вопросы определены Положением о порядке организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Требования к организации выполнения, защиты и оценивания курсовой работы определены Положением по организации выполнения и защиты курсовой работы (проекта).

1 Этап: защита курсовой работы

Процедура оценивания знаний, умений и навыков при проведении защиты курсовой работы осуществляется путем выполнения обучающимся курсовой работы по выбранной теме с ее последующей защитой.

Процесс подготовки и защиты курсовой работы состоит из ряда последовательных этапов:

- выбор и согласование темы курсовой работы с преподавателем;
- подбор и изучение литературных источников, сбор и анализ практических материалов по конкретной отрасли и/или организации в соответствии с выбранной темой;
- изучение требований к оформлению работы;
- написание работы;
- предоставление готовой работы на проверку преподавателю;
- защита курсовой работы.

Требования к структуре, оформлению курсовой работы, критерии ее оценки, процедура защиты размещены в учебно-методическом пособии

По результатам проверки и защиты курсовой работы выставляется оценка в соответствии со шкалой оценивания.

2 Этап: экзамен

Практический:

Процедура оценивания знаний, умений и навыков при проведении практической части экзамена проводится путем выполнения индивидуального практического задания с использованием компьютерной техники и информационных технологий (ИТ):

- обучающемуся выдается вариант практического задания одного из разделов дисциплины;
- задание выполняется на персональном компьютере с использованием ИТ в течение ограниченного времени (не более 30 минут);
- выполненная работа поверяется преподавателем. Если замечаний по работе нет, то обучающийся переходит ко второму теоретическому этапу экзамена. Если замечания выявлены, то они озвучиваются обучающемуся, при этом предоставляется время для их устранения (не более 25 мин.)

Теоретический:

Процедура оценивания знаний, умений и навыков при проведении теоретической части экзамена проводится путем письменного или компьютерного тестирования обучающихся:

- обучающемуся выдается вариант письменного или компьютерного теста (система Moodle);
- по результатам тестирования выставляется оценка согласно установленной шкалы оценивания.
- Для подготовки к экзамену рекомендуется использовать лекционный и практический материал по дисциплине, литературные источники а также электронными ресурсами.

Приложение 2

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости по дисциплине
Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

Специальность 38.05.01 Экономическая безопасность

Специализация «Экономико-правовое обеспечение экономической безопасности»

Квалификация экономист

1. Описание назначения и состава фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности» и предназначен для оценки планируемых результатов обучения - знаний, умений, навыков в процессе изучения данной дисциплины.

2. Перечень компетенций, формируемых при изучении дисциплины

Общепрофессиональные компетенции:

- способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов (ОПК-3)

Профессиональные компетенции:

- способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач (ПК-28);

- способностью принимать оптимальные управленческие решения с учетом критериев социально-экономической эффективности, рисков и возможностей использования имеющихся ресурсов (ПК-43).

3. Банк оценочных средств

Для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности» используются следующие оценочные средства:

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства
1	Тестовые задания	Тестовые задания содержат теоретические вопросы и практические задания, позволяющие определить уровень подготовки обучающегося
2	Кейс-задачи	Практические задания, позволяющее оценить умения и навыки, которыми овладел обучающийся при формировании соответствующих компетенций

Тестовые задания
для проведения текущего контроля успеваемости по дисциплине
«Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

Текущий контроль в форме тестирования предназначен для закрепления и поверки теоретических и практических знаний по отдельным темам дисциплины.

Результаты текущего контроля в форме тестирования оцениваются посредством интегральной (целостной) шкалы.

Шкала оценивания:

Критерии оценивания	Шкала оценивания			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	показатели			
Правильность ответов на вопросы теста	обучающийся дал менее 50% правильных ответов на вопросы теста	обучающийся дал 51-70% правильных ответов на вопросы теста	обучающийся дал менее 71-90% правильных ответов на вопросы теста	обучающийся дал более 90% правильных ответов на вопросы теста

Типовые тестовые задания
для проведения текущего контроля успеваемости по дисциплине
«Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

1.Кто является основным ответственным за определение уровня классификации информации?
1.Руководитель среднего звена
2.Высшее руководство
3.Владелец
4.Пользователь

2.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
1.Сотрудники
2.Хакеры
3.Атакующие
4.Контрагенты (лица, работающие по договору)

3.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. Улучшить контроль за безопасностью этой информации
4 Снизить уровень классификации этой информации

4.Что самое главное должно продумать руководство при классификации данных?
1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. Необходимый уровень доступности, целостности и конфиденциальности
3. Оценить уровень риска и отменить контрмеры
4. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
1.Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

6. Что такое процедура?
1.Правила использования программного и аппаратного обеспечения в компании
2. Пошаговая инструкция по выполнению задачи
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
1. Поддержка высшего руководства
2. Эффективные защитные меры и методы их внедрения
3. Актуальные и адекватные политики и процедуры безопасности
4. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2. Когда риски не могут быть приняты во внимание по политическим соображениям
3.Когда необходимые защитные меры слишком сложны
4.Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?
1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. Совокупность правил, процедур, практических методов и руководящих принципов в области ИБ, используемых организацией в своей деятельности
4.Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4. . Выявление уязвимостей и угроз, являющихся причиной риска

Методические материалы, определяющие процедуру оценивания

Процедура оценивания знаний, умений и навыков при проведении текущего контроля успеваемости по дисциплине в форме тестирования определяется следующими методическими указаниями:

- тестирование проводится после изучения соответствующей темы дисциплины
- при подготовке к тестированию обучающимся рекомендуется использовать практический материал по дисциплине, литературные источники и электронные ресурсы
- обучающемуся выдается вариант письменного или компьютерного теста (система

Moodle), тестирование выполняется в течение ограниченного времени (не более 1 академического часа)

- по результатам тестирования выставляется оценка согласно установленной шкалы оценивания

кейс-задачи
для проведения текущего контроля успеваемости по дисциплине
«Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

Текущий контроль в форме кейс-задачи предназначен для закрепления и проверки умений и навыков, которыми овладел обучающийся при формировании соответствующих компетенций в ходе освоения дисциплины «Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

Результаты текущего контроля в форме **кейс-задачи** оцениваются посредством интегральной (целостной) шкалы:

Шкала оценивания:

Шкала оценивания	Показатели оценивания
Зачтено	Обучающийся овладел элементами дескрипторов компетенций в рамках определенного уровня. Решил кейс-задачу методически верно, не допуская грубых методических ошибок, грамотно представил вывод (отчет) по итогам решения поставленной задачи.
Не зачтено	Обучающийся не овладел элементами дескрипторов компетенций в рамках определенного уровня, обнаружил существенные пробелы в знании теоретического и практического материала, не справился с решением кейс - задачи или решил кейс-задачу методически не верно, допуская грубые ошибки

Кейс-задачи
для проведения текущего контроля успеваемости по дисциплине
«Информационная безопасность хозяйствующего субъекта в системе экономической безопасности»

Тема № 1. Понятие информационной безопасности по законодательству РФ.

1.Обзор законодательства в информационной сфере. Знакомство с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Работа с нормами права регулирующими вопросы защиты информации с ограниченным доступом, государственной тайны и система ее защиты, а также конфиденциальной информации и ее защите.

3. Работа с Федеральным законом «Об электронной цифровой подписи» и его краткая характеристика

4. Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны.

5. Изучение порядка осуществления лицензирование и сертификации в области защиты информации.

Тема № 2. Преступления в сфере компьютерной информации.

1.Изучите вопросы защиты интеллектуальной собственности в Российской Федерации

2. Сравните определение киберпреступности, содержащиеся в отечественном законодательстве и международных нормативных актах, а также в научной литературе.

3. Какие из них кажутся вам наиболее удачными?

4. Проанализируйте судебную практику Кировской области по рассмотрению уголовных дел о преступлениях в сфере информационной безопасности.

5. Используя свою ЭВМ, Сивков "на спор" сумел подключиться к сети ЭВМ Госгидромета и для доказательства того, что это ему удалось, скопировал информацию о параметрах метеоусловий в центральных районах страны и изменил пароль для доступа к этой информации работников Госгидромета.

6. Выполняя работу по наладке компьютера в соответствии с указанием начальника лаборатории, Ложкин скопировал для себя несколько отсутствующих у него программ и таким образом модифицировал команды загрузочного файла, что в результате отдельные из программ перестали запускаться. О том, что он снял копии с некоторых программ, Ложкин по окончании работы поставил в известность своего начальника. Спустя некоторое время, ввиду жалоб пользователей ЭВМ тот сам был вынужден устранить сбой в ее работе.

7. В целях защиты разработанной им программы от несанкционированного копирования и одновременно наказания за это Шишкин предусмотрел, что всякая попытка "взлома" оригинальной программы приведет к автоматическому блокированию важнейших файлов программ- оболочек компьютера. Предупреждение о последствиях несанкционированного копирования было указано на дискете.

8. Дударов приобрел в магазине "Компьютеры" комплект дискет с игровой программой и, проверив ее на наличие "вирусов" (они обнаружены не были), установил на свой персональный компьютер. Спустя некоторое время, работа компьютера была полностью заблокировала. Придя к выводу, что причиной тому – новейший "вирус", которым поражена купленная им программа, Дударов продал комплект дискет с ней своему знакомому, утаив от него о некачественности "игрушки".

Тема № 3. Криминологическая характеристика компьютерной преступности.

1. Проиллюстрируйте с помощью графиков и диаграмм изменение уровня киберпреступности в РФ за последние 20 лет.

2. Приведите данные эмпирических исследований о распространенности киберпреступности в разных странах

Тема № 4. Правоохранительные органы РФ, осуществляющие борьбу с преступлениями в сфере высоких технологий.

1.Разработка должностной инструкции сотрудника подразделения информационной безопасности.

2. Изучение полномочий ФСБ в области обеспечения информационной безопасности

3. Изучение полномочий МВД РФ в области обеспечения информационной безопасности.

4. Изучение полномочий СК РФ в области обеспечения информационной безопасности.

Тема № 5. Расследование преступлений в сфере компьютерной информации.

1. Сравните ФЗ "Об Оперативно-розыскной деятельности" и нормативно-правовых актов об ОРМ и Закона "О частной детективной и охранной деятельности".

2. По предложенным примерам из следственной практике составить план расследования.

3. По предложенным примерам из следственной практики составить процессуальные документы: a. План следственных мероприятий b. Постановление о ВУД c. Обвинительное заключение d. Постановление о признании и приобщении вещественных доказательств.

Тема № 6. Предупреждение киберпреступности.

1. Проведите сравнительный анализ законодательства и правоприменительной практики США, Великобритании, Германии, Франции, Финляндии, Японии, КНР и других зарубежных стран о профилактике и пресечении киберпреступности.

Методические материалы, определяющие процедуру оценивания

Процедура оценивания знаний, умений и навыков при проведении текущего контроля успеваемости по дисциплине в форме кейс-задачи определяется следующими методическими указаниями:

- выполнение кейс-задачи проводится в аудиториях, отведенных для практических занятий;
- обучающийся должен представить развернутый вывод по итогам решения кейс-задачи.

Приложение 3

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ПО ДИСЦИПЛИНЕ

Информационная безопасность хозяйствующего субъекта в системе экономической безопасности

Наименование специальных помещений	Оснащенность специальных помещений
Учебная аудитория для проведения занятий лекционного типа	Д115 Рабочее место преподавателя, комплект столов и стульев для обучающихся, доска белая магнитная, 3 компьютера, комплект мультимедийного оборудования с экраном, муляж кассы банка, 2 телевизора, 2 рабочих места операциониста банка. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus и свободно распространяемое программное обеспечение
Учебная аудитория для занятий семинарского типа	Д106 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, 9 принтеров. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение Д113 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1СПредприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Помещение для самостоятельной работы	Б202 Рабочее место администратора, компьютерная мебель, компьютер администратора, 11 персональных компьютеров, 3 принтера, видеоувеличитель. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus и свободно распространяемое программное обеспечение С возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации
Учебная аудитория для групповых и индивидуальных консультаций.	Д106 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, 9 принтеров. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение Д113 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1СПредприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Учебная аудитория для текущего контроля и промежуточной аттестации.	Д106 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, 9 принтеров. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение Д113 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1СПредприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Лаборатория информационных технологий	Д106 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, 9 принтеров. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Помещение для хранения и	Д128 3 рабочих места, 2 персональных компьютера, принтер, 2 пылесоса, фотоаппарат, мультиметр, 2 паяльника, комплект ручного инструмента, 4 телефонных аппарата

профилактического обслуживания учебного оборудования	Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus и свободно распространяемое программное обеспечение Д216 Мебель, 2 сканера, копировальный аппарат, 2 ноутбука, 2 принтера, персональный компьютер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus и свободно распространяемое программное обеспечение Д221 Мебель, 6 калькуляторов, 5 персональных компьютеров, 2 принтера. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus и свободно распространяемое программное обеспечение
Учебная аудитория для курсового проектирования (выполнения курсовых работ)	Д106 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, 9 принтеров. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение Д113 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, 9 персональных компьютеров, принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, 1СПредприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение

Приложение 4

Перечень

периодических изданий, рекомендуемых по дисциплине

Информационная безопасность хозяйствующего субъекта в системе экономической безопсности

Наименование	Наличие доступа
Информационная безопасность [Электронный ресурс]: науч. журн./ Воронежский государственный политехнический университет ISSN:1682-7813	Режим доступа: http://elibrary.ru/item.asp?id=24957242
Современные информационные технологии и IT-образование [Электронный ресурс]: журн. / Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала Лига интернет-медиа	Режим доступа: http://elibrary.ru/defaultx.asp
Информационное общество [Электронный ресурс]: журн. / Автономная некоммерческая организация Институт развития информационного общества	Режим доступа: http://elibrary.ru/defaultx.asp