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 и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **информационных технологий и статистики**

Учебный план

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144

в том числе:

аудиторные занятия 52

самостоятельная работа 92

Виды контроля в семестрах:

зачеты с оценкой 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**			
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	34	34	34	34
В том числе инт.	4	4	4	4
Итого ауд.	52	52	52	52
Контактная работа	52	52	52	52
Сам. работа	92	92	92	92
Итого	144	144	14	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 и защита информации
разработана в соответствии с ФГОС:

ФГОС ВО - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании Учебного плана:

09.03.02 Информационные системы и технологии
одобренного и утвержденного Ученым советом университета от 15.04.2021 протокол № 5.

Рабочая программа дисциплины рассмотрена и одобрена учебно-методической комиссией

Протокол № 8 от "15" апреля 2021 г.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры

информационных технологий и статистики

Протокол № 8 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

Протокол от "__" _____ 2022 г. № __

Зав. кафедрой _____

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 _____

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 _____

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.О

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-3.1	Понимает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информаци-онно-коммуникационных технологий и с учетом основных требований информационной безопасности
ОПК-3.2	Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной без-опасности
ОПК-3.3	Использует методы поиска, обработки и адаптации информации для подготовки научно-технических документов на основе информационной и библиографической культуры, с соблюдением требований авторского права и 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	Инте ракт.	Примечание
	Раздел 1.				
1.1	Общие понятия и актуальность обеспечения информационной безопасности. /Лек/	7	2	0	
1.2	Менеджмент информационной безопасности в организации. /Лаб/	7	2	0	
1.3	Политика информационной безопасности в организации. Парольная политика /Лек/	7	2	0	
1.4	Разработка политики информационной безопасности организации /Лаб/	7	4	0	

1.5	Анализ рисков и оценка затрат в системе информационной безопасности /Лек/	7	2	0	
1.6	Управление рисками в системе информационной безопасности /Лаб/	7	4	0	
1.7	Угрозы информационной безопасности. Принципы и меры информационной безопасности /Лек/	7	2	0	
1.8	Менеджмент инцидентов информационной безопасности /Лаб/	7	4	0	
1.9	Защита информации от несанкционированного доступа /Лек/	7	2	0	
1.10	Аудит информационной безопасности автоматизированной компьютерной системы /Лаб/	7	4	0	
1.11	Криптографические методы защиты информации /Лек/	7	2	0	
1.12	Обеспечение безопасности автоматизированных компьютерных систем /Лек/	7	2	0	
1.13	Эффективность защиты информации при помощи паролей /Лаб/	7	6	2	
1.14	Криптографическое шифрование и кодирование данных /Лаб/	7	6	2	
1.15	Организационно-правовое обеспечение информационной безопасности /Лек/	7	4	0	
1.16	Решение практических задач по обеспечению информационной безопасности /Лаб/	7	4	0	
1.17	Подготовка к лекциям, лабораторным и практическим занятиям	7	23	0	
1.18	Самостоятельное изучение разделов и тем учебной дисциплины	7	23	0	
1.19	Текущий контроль успеваемости /Ср/	7	24	0	
1.20	Подготовка к зачету с оценкой /Ср/	7	22	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.

	Авторы, составители	Заглавие	Издательство,
Л.1	Ливанов Р.В	Информационная безопасность и защита информации [Электронный ресурс]: : учебно-методическое пособие для самостоятельной работы обучающихся по направлению 09.03.02 Информационные системы и технологии Режим доступа: http://90.156.226.97/MarcWeb2/Default.asp	Киров: ФГБОУ ВО Вятский ГАТУ, 2022
Л.2	Ливанов Р.В	Информационная безопасность и защита информации [Электронный ресурс] : учебно-методическое пособие для лабораторных занятий Режим доступа: http://90.156.226.97/MarcWeb2/Default.asp	Киров, 2022
Л.3	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов Режим доступа: https://urait.ru/bcode/450371	Издательство Юрайт, 2020
Л.4	Суворова, Г. М.	Информационная безопасность [Электронный ресурс]: учебное пособие для вузов Режим доступа: https://urait.ru/bcode/467370	Издательство Юрайт, 2021
Л.5	Чернова, Е. В.	Информационная безопасность человека [Электронный ресурс]: учебное пособие для вузов Режим доступа: https://urait.ru/bcode/449350	Издательство Юрайт, 2020
Л.6	Зенков, А. В.	Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие для вузов Режим доступа: https://urait.ru/bcode/477968	Издательство Юрайт, 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 Вятский ГАТУ Режим доступа http://90.156.226.97/MarcWeb2/Default.asp
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;

□ 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. 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.

4. Подготовка к промежуточной аттестации

Подготовка к зачету с оценкой является заключительным этапом изучения дисциплины и является средством промежуточного контроля. Подготовка к зачету с оценкой предполагает изучение конспектовлекций, рекомендуемой литературы и других источников, повторение материалов практических занятий.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации по дисциплине
Информационная безопасность и защита информации
Направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) программы бакалавриата «Проектирование, разработка и сопровождение информационных систем в АПК»
Квалификация бакалавр

1. Описание назначения и состава фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины «Информационная безопасность и защита информации» и предназначен для оценки планируемых результатов обучения - сформированности индикаторов достижения компетенций и опыта деятельности, характеризующих этапы формирования компетенций (п.2) в процессе изучения данной дисциплины.

ФОС включает в себя оценочные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

ФОС разработан на основании:

- Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 922);
- основной профессиональной образовательной программы высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии направленности (профилю) программы бакалавриата « Проектирование, разработка и сопровождение информационных систем в АПК»;
- 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

- Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

Код формируемой компетенции	Этапы формирования компетенции в процессе освоения образовательной программы		
	Начальный этап	**Основной этап**	**Заключительный этап**
ОПК-3	• Технологии обработки информации	• Информационная безопасность и защита информации	• Учебная практика: эксплуатационная практика • Подготовка к государственной итоговой аттестации

3. Планируемые результаты освоения образовательной программы по дисциплине, выраженные через компетенции и индикаторы их достижений, описание шкал оценивания

Код и наименование формируемых компетенций	Код и наименование индикатора достижения формируемой компетенции		Наименование контролируемых разделов и тем	Наименование оценочного средства промежуточной аттестации
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Понимает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Раздел 4 рабочей программы дисциплины	Тестовые вопросы и практические задания к дифференцированному зачету по дисциплине
	ОПК-3.2	Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
	ОПК-3.3	Использует методы поиска, обработки и адаптации информации для подготовки научно-технических документов на основе информационной и библиографической культуры, с соблюдением требований авторского права и информационной безопасности		

Для оценки сформированности соответствующих компетенций по дисциплине «**Информационная безопасность и защита информации**» при проведении промежуточной аттестации в форме дифференцированного зачета применяется следующая шкала оценивания:

Критерии оценивания	Шкала оценивания			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	Описание показателя			
Полнота знаний контролируемого материала	Низкий уровень усвоения материала. Продемонстрировано незнание значительной части программного материала – менее 60% правильных ответов	Представлены знания только основного материала, но не усвоены его детали – 60 - 74% правильных ответов	Твердое знание материала – 75 - 90% правильных ответов	Высокий уровень усвоения материала – более 90% правильных ответов
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 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
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 сформированности компетенций в процессе освоения образовательной программы

Тестовые задания
по дисциплине «Информационная безопасность и защита информации»
для промежуточной аттестации в форме дифференцированного зачета

1. Установите соответствие между составляющей информационной безопасности и её содержанием (ОПК-3)

1. Доступность информации 2. Целостность информации 3. Конфиденциальность информации	А. Гарантия того, что информация сейчас 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

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)

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)

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)

А. Три)
Б. Четыре
В. Два
Г. Пять

6. Что не рассматривается в политике безопасности (ОПК-3)

А. Требуемый уровень защиты данных
Б. Роли субъектов информационных отношений
В. Анализ рисков
Г. Защищенность механизмов безопасности

7.Кто является основным ответственным за определение уровня классификации информации (ОПК-3)?

1.Руководитель среднего звена
2.Высшее руководство
3.Владелец
4.Пользователь

8.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности (ОПК-3)?

1.Сотрудники
2.Хакеры
3.Атакующие
4.Контрагенты (лица, работающие по договору)

9.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству (ОПК-3)?

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

10.Что самое главное должно продумать руководство при классификации данных (ОПК-3)?

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

11 Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены (ОПК-3)?

1.Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

12. Что такое процедура (ОПК-3)?

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

13 Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании (ОПК-3)?

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

14. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков (ОПК-3)?

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

15. Что такое политики безопасности (ОПК-3)?

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

16. Какая из приведенных техник является самой важной при выборе конкретных защитных мер (ОПК-3)?

1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4.Выявление уязвимостей и угроз, являющихся причиной риска

Практические задания по дисциплине «Информационная безопасность и защита информации» для промежуточной аттестации в форме дифференцированного зачета

Задача 1

Дайте описание документа «Политика информационной безопасности» (ОПК-3)

Задача 2

Зашифровать с помощью криптографической системы Цезаря выражение «Пришел, увидел, победил» (ОПК-3)

Задача 3

Выполнить резервное копирование и восстановление информационной базы предприятия в программе 1С:Бухгалтерия 8.3 (ОПК-3)

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)

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)

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

Задача 6
Дайте описание внутренним рискам организации (ОПК-3)

Задача 7
Дайте описание внешним рискам организации (ОПК-3)

Задача 8
Зашифровать с помощью криптографической системы выражении «О спорт –ты мир» (ОПК-3)

Задача 9
Установите права доступа к общей папке на сервере (ОПК-3)

Задача 10
Дайте описание как устанавливаются права доступа пользователей к системе (ОПК-3)

Вопросы для подготовки к дифференцированному зачету по дисциплине «Информационная безопасность и защита информации»

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 сформированности индикаторов достижения компетенций и опыта деятельности, характеризующих этапы формирования компетенций.

Процедура оценивания сформированности индикаторов достижения компетенций при проведении промежуточной аттестации по дисциплине «Информационная безопасность и защита информации» проводится в форме дифференцированного зачета.

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

Процедура оценивания сформированности индикаторов достижения компетенций при проведении дифференцированного зачета теоретической части дифференцированного зачета проводится путем письменного или

компьютерного тестирования обучающихся и (или) устного ответа на вопросы к зачету:

- обучающемуся выдается вариант письменного или компьютерного теста;
- в определенное время (в среднем 2 минуты на 1 тестовое задание) обучающийся отвечает на 20 вопросов теста, в котором представлены все изучаемые темы дисциплины;
- по результатам тестирования выставляется оценка, согласно установленной шкалы оценивания.

Процедура оценивания сформированности индикаторов достижения компетенций при проведении дифференцированного зачета практической части дифференцированного зачета 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.)

Для подготовки к дифференцированному зачету рекомендуется использовать лекционный и практический материал по дисциплине, литературные источники, рекомендованные в рабочей программе дисциплины.

Приложение 2

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости по дисциплине
Информационная безопасность и защита информации

Направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) программы бакалавриата «Проектирование, разработка и сопровождение информационных систем в АПК»
Квалификация бакалавр

1. Описание назначения и состава фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины «Информационная безопасность и защита информации» и предназначен для оценки планируемых результатов обучения - сформированности индикаторов достижения компетенций и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

2. Перечень компетенций, формируемых при изучении дисциплины

- Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3).

3. Банк оценочных средств

Для оценки сформированности индикаторов достижения компетенций и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины «Информационная безопасность и защита информации» используются следующие оценочные средства:

Код и наименование формируемых компетенций	Код и наименование индикатора достижения формируемой компетенции		Критерии оценивания	Наименование контролируемых разделов и тем	Наименование оценочного средства текущей аттестации
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1	Понимает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Полнота знаний контролируемого материала - Логичность, обоснованность, четкость ответа на вопросы	Раздел 4 рабочей программы дисциплины.	Кейс- задачи
	ОПК-3.2	Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
	ОПК-3.3	Использует методы поиска, обработки и адаптации информации для подготовки научно-технических документов на основе информационной и библиографической культуры, с соблюдением требований авторского права и информационной безопасности			

Кейс-задачи
для проведения текущего контроля знаний
по дисциплине «Информационная безопасность и защита информации»

Текущий контроль в форме кейс-задач предназначен определения уровня оценки сформированности индикаторов достижения компетенций и опыта деятельности в процессе изучения дисциплины обучающимися очной, очно-заочной и заочной формы обучения.

Результаты текущего контроля оцениваются посредством шкалы:

Шкала оценивания	Показатели оценивания
Не 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.
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

Типовые кейс-задачи

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 сформированности индикаторов достижения компетенций и опыта деятельности в процессе изучения дисциплины при проведении текущего контроля знаний проводится путем выполнения кейс-задач на практических занятиях. Обучающийся должен представить развернутый вывод по итогам решения кейс-задачи. Оценка проводится посредством шкалы оценивания.

Приложение 3

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ПО ДИСЦИПЛИНЕ

Информационная безопасность

Наименование специальных помещений	Оснащенность специальных помещений
Учебная аудитория для проведения занятий лекционного типа	Д304 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, комплект мультимедийного оборудования с экраном. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirusи свободно распространяемое программное обеспечение Д122 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, мультимедийное оборудование с экраном, 12 персональных компьютеров, 1 принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, IBMSPSSStatisticsBase, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Учебная аудитория для занятий семинарского типа	Д122 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, мультимедийное оборудование с экраном, 12 персональных компьютеров, 1 принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, IBMSPSSStatisticsBase, 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 групповых и индивидуальных консультаций.	Д122 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, мультимедийное оборудование с экраном, 12 персональных компьютеров, 1 принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, IBMSPSSStatisticsBase, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Учебная аудитория для текущего контроля и промежуточной аттестации.	Д122 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, мультимедийное оборудование с экраном, 12 персональных компьютеров, 1 принтер. Список ПО: Windows, MicrosoftOffice, KasperskyAntivirus, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSiSWOT – Analysis, KonSiAnketter, IBMSPSSStatisticsBase, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Помещение для самостоятельной работы	Б202 Рабочее место администратора, компьютерная мебель, компьютер администратора, 5 персональных компьютеров, 3 принтера, видеоувеличитель. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus и свободно распространяемое программное обеспечение С возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации

Приложение 4

Перечень

периодических изданий, рекомендуемых по дисциплине

Информационная безопасность

Наименование	Наличие доступа
Информационные технологии в проектировании и производстве [Электронный ресурс]: журн. / ФГУП «НТЦ оборонного комплекса «Компас» (Москва)	Режим доступа: https://elibrary.ru/query_results.asp
Информационное общество [Электронный ресурс]: журн. / Автономная некоммерческая организация Институт развития информационного общества	Режим доступа: http://elibrary.ru/defaultx.asp
Вычислительные технологии [Электронный ресурс]: журн. /Институт вычислительных технологий СО РАН (Новосибирск)	Режим доступа: https://elibrary.ru/query_results.asp
Вычислительные методы и программирование [Электронный ресурс]: журн. / Московский государственный университет им. М.В. Ломоносова (Москва)	Режим доступа: https://elibrary.ru/query_results.asp
Модели, системы, сети в экономике, технике, природе и обществе [Электронный ресурс]: журн./ Пензенский государственный университет (Пенза)	Режим доступа: https://elibrary.ru/query_results.asp
Научный сервис в сети интернет[Электронный ресурс]: журн./Институт прикладной математики им. М.В. Келдыша РАН (Москва)	Режим доступа: https://elibrary.ru/query_results.asp
Вестник южно-уральского государственного университета. серия: компьютерные технологии, управление, радиоэлектроника [Электронный ресурс]: журн./ Южно-Уральский государственный университет (национальный исследовательский университет) (Челябинск)	Режим доступа: https://elibrary.ru/query_results.asp?pagenum=10
Вестник удмуртского университета. математика. механика. компьютерные науки [Электронный ресурс]: журн./ Удмуртский государственный университет (Ижевск)	Режим доступа: https://elibrary.ru/query_results.asp