

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Соловьев Дмитрий Александрович
Должность: ректор ФГБОУ ВО Вавиловский университет
Дата подписания: 08.09.2025 17:14:17
Уникальный программный ключ:
528682d78e671e565a10c691fe17c02f735a12



МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Саратовский государственный университет генетики,
биотехнологии и инженерии имени Н.И. Вавилова»**

УТВЕРЖДАЮ

И.о. заведующего кафедрой

 / Ключиков А.В. /
« 12 » 04 2024 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Дисциплина

**ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ
БЕЗОПАСНОСТЬ**

Направление
подготовки

09.03.03 Прикладная информатика

Направленность
(профиль)

Проектирование информационных систем

Квалификация
выпускника

Бакалавр

Нормативный срок
обучения

4 года

Форма обучения

Заочная

Кафедра-разработчик

Цифровое управление процессами в АПК

Ведущий преподаватель

Розанов А.В., доцент

Разработчик: доцент, Розанов А.В.


(подпись)

Саратов 2024

Содержание

1	Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП	3
2	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания	6
3	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.....	12
4	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы их формирования	19

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

В результате изучения дисциплины «Введение в информационную безопасность» обучающиеся, в соответствии с ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства науки и высшего образования РФ от 19 сентября 2017 г., № 922, формируют следующие компетенции, представленные в таблице 1.

Формирование компетенций в процессе изучения дисциплины «Введение в информационную безопасность»

Таблица 1

Компетенция		Индикаторы достижения компетенций	Этапы формирования компетенции в процессе освоения ОПОП (семестр)*	Виды занятий для формирования компетенции	Оценочные средства для оценки уровня сформированности компетенции
Код	Наименование				
1	2	3	4	5	6
ОПК-2	способен понимать принципы работы современных информационных технологий и программных средств, в том числе, отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.2. понимает принципы работы в информационной среде и решает типовые задачи управления бизнес-процессами с применением цифровых технологий	1 курс	лекции, лабораторные занятия	лекции, лабораторная работа, тестовые задания, доклады, самостоятельная работа

Компетенция		Индикаторы достижения компетенций	Этапы формирования компетенции в процессе освоения ОПОП (семестр)*	Виды занятий для формирования компетенции	Оценочные средства для оценки уровня сформированности компетенции
Код	Наименование				
1	2	3	4	5	6
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. применяет информационно-коммуникационные технологии с учетом основных требований информационной безопасности для решения стандартных задач в области прикладной информатики	1 курс	лекции, лабораторные занятия	лекции, лабораторная работа, тестовые задания, доклады, самостоятельная работа
		ОПК-3.2.разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы	1 курс	лекции, лабораторные занятия	лекции, лабораторная работа, тестовые задания, доклады, самостоятельная работа

Примечание

Компетенция ОПК-2 – также формируется в ходе освоения дисциплин: Информатика; Введение в информационную безопасность; Цифровые технологии в системе управления предприятий; Архитектура компьютера и операционные системы; Базы данных; Автоматическое управление системами в АПК; Микроконтроллеры и микропроцессоры; Ознакомительная практика; Выполнение и защита выпускной квалификационной работы.

Компетенция ОПК-3 – также формируется в ходе освоения дисциплин: Введение в информационную безопасность; Выполнение и защита выпускной квалификационной работы.

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

Перечень оценочных материалов

Таблица 2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ОМ
1	2	3	4
1	лабораторная работа	средство, направленное на изучение практического хода тех или иных процессов, исследование явления в рамках заданной темы с применением методов, освоенных на лекциях, сопоставление полученных результатов с теоретическими концепциями, осуществление интерпретации полученных результатов, оценивание применимости полученных результатов на практике	Лабораторные работы
2	тестирование	метод, который позволяет выявить уровень знаний, умений и навыков, способностей и других качеств личности, а также их соответствие определенным нормам путем анализа способов выполнения обучающимися ряда специальных заданий	банк тестовых заданий
3	собеседование	средство контроля, организованное как специальная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной и рассчитанной на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.	задания для самостоятельной работы
4	доклад	продукт самостоятельной работы обучающегося, представляющий собой публич-	темы устных докладов

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ОМ
1	2	3	4
		ное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы	

Программа оценивания контролируемой дисциплины

Таблица 3

№ п/п	Контролируемые разделы (темы дисциплины)	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	2	3	4
1.	Основные понятия информационной безопасности. Системный подход к обеспечению информационной безопасности. Средства обеспечения защиты информации.	ОПК-2.2	Тестовые задания Лабораторная работа №1
2.	Основные принципы политики безопасности. Средства обеспечения защиты информации в системах электронного документооборота.	ОПК-2.2	Лабораторная работа №2 Самостоятельная работа
3.	Понятия состояния системы и потока информации. Правила разграничения доступа. Средства и способы анализа трафика на сетевых интерфейсах в ОС Windows. Изучение настроек Ethernet для повышения безопасности	ОПК-3.1	Лабораторная работа №3 Самостоятельная работа
4.	Программные средства информационной безопасности. Антивирусные программные системы Касперского и Dr.WEB	ОПК-3.2	Лабораторная работа №4 Самостоятельная работа

Описание показателей и критериев оценивания компетенций по дисциплине «Введение в информационную безопасность» на различных этапах их формирования, описание шкал оценивания

Таблица 4

Код компетенции, эта-	Индикаторы достижения	Показатели и критерии оценивания результатов обучения
-----------------------	-----------------------	---

пы освоения ком- петенции	компетенций	ниже поро- вого уровня (неудовлетво- рительно)	пороговый уровень (удовлетво- рительно)	продвинутый уровень (хо- рошо)	высокий уровень (от- лично)
1	2	3	4	5	6
ОПК-2, 1 курс	ОПК-2.2. по- нимает прин- ципы работы в информаци- онной среде и решает типо- вые задачи управления бизнес- процессами с применением цифровых технологий	обучающийся не знает значи- тельной части программного материала, пло- хо понимает принципы рабо- ты в информа- ционной среде и решает типовые задачи управле- ния бизнес- процессами с применением цифровых тех- нологий, не зна- ет практику применения ма- териала, допус- кает существен- ные ошибки	обучаю- щийся де- монстрирует знания толь- ко основного материала, но не знает деталей, до- пускает не- точности, до- пускает не- точности в формулиров- ках, нару- шает логиче- скую после- дователь- ность в из- ложении программ- ного мате- риала	обучаю- щийся де- монстрирует знаниеprin- ципов рабо- ты в инфор- мационной среде и ре- шает типо- вые задачи управления бизнес- процессами с применением цифровых технологий, не допускает существен- ных неточ- ностей	обучаю- щийся де- монстрирует знаниеprin- ципов рабо- ты в инфор- мационной среде и ре- шает типо- вые задачи управления бизнес- процессами с применением цифровых технологий, практику применения материала, исчерпы- вающе и по- следова- тельно, четко и логично излагает ма- териал, не затрудняется с ответом при видоиз- менении за- даний
		не умеетисполь- зовать про- граммные сред- ства, в том чис- ле отечествен- ного производ- ства, при реше- нии задач проф- фессиональной деятельности, допускает су- щественные ошибки, неуве- ренно, с боль- шими затрудне- ниями выпол-	в целом ус- пешное, но не систем- ное, умение использовать программные средства, в том числе отечествен- ного произ- водства, при решении за- дач профес- сиональной деятельности	в целом ус- пешное, но содержащие отдельные пробелы, умениеис- пользовать программные средства, в том числе отечествен- ного произ- водства, при решении за- дач профес- сиональной	сформиро- ванное уме- ниеисполь- зовать про- граммные средства, в том числе отечествен- ного произ- водства, при решении за- дач профес- сиональной деятельно- сти, исполь- зуя совре-

Код компетенции, этапы освоения компетенции	Индикаторы достижения компетенций	Показатели и критерии оценивания результатов обучения			
		ниже порогового уровня (неудовлетворительно)	пороговый уровень (удовлетворительно)	продвинутый уровень (хорошо)	высокий уровень (отлично)
1	2	3	4	5	6
		не выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено		деятельности	методы и показатели
		обучающийся не владеет навыками решения типовых задач управления бизнес-процессами с применением цифровых технологий, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины не выполнено	в целом успешное, но не системное владение навыками решения типовых задач управления бизнес-процессами с применением цифровых технологий	в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками решения типовых задач управления бизнес-процессами с применением цифровых технологий	успешное и системное владение навыками решения типовых задач управления бизнес-процессами с применением цифровых технологий
ОПК-3, 1 курс	ОПК-3.1. применяет информационно-коммуникационные технологии с учетом основных требований информационной безопасности для решения	обучающийся не знает основы информационной и библиографической культуры в области прикладной информатики, не знает практику применения материала, допускает существенные ошибки	обучающийся демонстрирует знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность	обучающийся демонстрирует знание основ информационной и библиографической культуры в области прикладной информатики, не допускает существенных неточностей	обучающийся демонстрирует знание основ информационной и библиографической культуры в области прикладной информатики, практику применения

Код компетенции, этапы освоения компетенции	Индикаторы достижения компетенций	Показатели и критерии оценивания результатов обучения			
		ниже порогового уровня (неудовлетворительно)	пороговый уровень (удовлетворительно)	продвинутый уровень (хорошо)	высокий уровень (отлично)
1	2	3	4	5	6
	стандартных задач в области прикладной информатики		довательность в изложении программного материала	точностей	материала, исчерпывающе и последовательно, четко и логично излагает материал, не затрудняется с ответом при видоизменении заданий
		не умеет решать стандартные задачи в области прикладной информатики, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено	в целом успешное, но не системное умение решать стандартные задачи в области прикладной информатики, использовать современные информационно-коммуникационные технологии	в целом успешное, но содержащие отдельные пробелы, умение решать стандартные задачи в области прикладной информатики, современные информационно-коммуникационные технологии	демонстрирует сформированное умение решать стандартные задачи в области прикладной информатики, используя современные и перспективные информационно-коммуникационные технологии, методы и показатели
		обучающийся не владеет навыками решения стандартных задач в области прикладной информатики с учетом основных требований информационной безопасности, до-	в целом успешное, но не системное владение навыками решения стандартных задач в области прикладной информатики с учетом ос-	в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками ре-	успешное и системное владение навыками решения стандартных задач в области прикладной информатики с учетом основных тре-

Код компетенции, этапы освоения компетенции	Индикаторы достижения компетенций	Показатели и критерии оценивания результатов обучения			
		ниже порогового уровня (неудовлетворительно)	пороговый уровень (удовлетворительно)	продвинутый уровень (хорошо)	высокий уровень (отлично)
1	2	3	4	5	6
		пускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины не выполнено	новых требований информационной безопасности	шения стандартных задач в области прикладной информатики с учетом основных требований информационной безопасности	бований информационной безопасности с использованием современных и перспективных информационно-коммуникационных технологий
ОПК-3, 1 курс	ОПК-3.2. разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы	обучающийся не знает значительной части программного материала, плохо ориентируется в нормах и правилах обеспечения информационной безопасности в сфере своей профессиональной деятельности, не знает практику применения материала, допускает существенные ошибки	обучающийся демонстрирует знания только основного материала, но не знает деталей, допускает неточности, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала	обучающийся демонстрирует знание норм и правил обеспечения информационной безопасности в сфере своей профессиональной деятельности, не допускает существенных неточностей	обучающийся демонстрирует знание норм и правил обеспечения информационной безопасности в сфере своей профессиональной деятельности, практику применения материала, исчерпывающе и последовательно, четко и логично излагает материал, не затрудняется с ответом при видоизменении заданий
		не умеет разрабатывать техническую документацию, свя-	в целом успешное, но не системное, умение	в целом успешное, но содержащие отдельные	сформированное умение разрабатывать тех-

Код компетенции, этапы освоения компетенции	Индикаторы достижения компетенций	Показатели и критерии оценивания результатов обучения			
		ниже порогового уровня (неудовлетворительно)	пороговый уровень (удовлетворительно)	продвинутый уровень (хорошо)	высокий уровень (отлично)
1	2	3	4	5	6
		занную с информационной безопасностью в области прикладной информатики, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено	разрабатывать техническую документацию, связанную с информационной безопасностью в области прикладной информатики	пробелы, умение разрабатывать техническую документацию, связанную с информационной безопасностью в области прикладной информатики	ническую документацию, связанную с информационной безопасностью в области прикладной информатики, используя современные методы и показатели
		обучающийся не владеет навыками разработки мер защиты информации на основе требований информационной безопасности и нормативно-правовой базы, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины не выполнено	в целом успешное, но не системное владение навыками разработки мер защиты информации на основе требований информационной безопасности и нормативно-правовой базы	в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками разработки мер защиты информации на основе требований информационной безопасности и нормативно-правовой базы	успешное и системное владение навыками разработки мер защиты информации на основе требований информационной безопасности и нормативно-правовой базы

3. 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

3.1. Входной контроль

Входной контроль проводится перед изучением первого раздела с целью проверки исходного уровня знания стандартного курса информатики и готовности обучаемого к изучению данной дисциплины. Входной контроль проводится на первом практическом занятии в форме устного опроса или автоматизированного опроса на основе компьютерных тестов множественного выбора, реализованных на ПЭВМ. Оценка результатов входного контроля проводится в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования.

Вопросы входного контроля

1. В чём отличие персональных ЭВМ от универсальных ЭВМ?
2. Правила запуска и завершения работы в операционной системе Windows?
3. Каковы основные элементы типового окна Windows?
4. Какие приложения входят в стандартную поставку ОС Windows?
5. Назначение “быстрых” и “горячих” клавиш?
6. Как в текстовом процессоре MS Word выполняется ввод и форматирование специальных символов?
7. Как в документ MS Word вставить рисунок, спецсимвол, диаграмму?
8. Как вызвать редактор формул Microsoft Equation?
9. Для каких целей применяется надстройка «Поиск решения» MS Excel?
10. Как в MS Excel построить столбиковую и круговую диаграмму?
11. Что называют базами данных?
12. Что называют записями и полями данных?
13. Какова специфика ввода данных в электронных таблицах?
14. Что называют сетями ЭВМ?
15. В чем отличие сетей Internet и Intranet?

3.2 Доклады

Выполнение устного доклада в полной мере раскрывает творческий подход обучающихся к самостоятельной проработке нового материала, позволяет оценить степень готовности учащихся к самостоятельному выбору актуальных проблем дисциплины. Данный вид творческой работы позволяет обучающимся овладеть навыками систематизации материала, развивает умение конкретизировать и обобщать проблемы и перспективы развития цифровых технологий на основе анализа массива

научной и периодической литературы по выбранной теме.

Рекомендуемая тематика устных докладов по дисциплине приведена в таблице 5.

Таблица 5

**Темы докладов, рекомендуемые к подготовке при изучении дисциплины
«Введение в информационную безопасность»**

№ п/п	Темы докладов
1	2
1	Информация как стратегический ресурс цифровой трансформации
2	Перспективные применения цифровых технологий в киберпространстве
3	Цифровые технологии структурного анализа и проектирования
4	Оптимизация затрат на обеспечение информационной безопасности
5	Модели безопасного управления финансовыми потоками
6	Минимизация угроз для беспилотных транспортных средств
7	Передовые системы безопасности в сфере перерабатывающих производств
8	Системный подход и системный анализ в сфере АПК
9	Сетевые мультимедиа-энциклопедии и справочные издания
10	Свободное программное обеспечение в сфере кибербезопасности
11	Организация информационной защиты поставок сельхозпродукции
12	Облачные информационные технологии – тенденции развития
13	Новейшие программно-аппаратные средства защиты информации
14	Концептуальное программирование и системы искусственного интеллекта
15	Компьютерные технологии защиты с точки зрения системного анализа
16	Планирование кампании по продвижению передовых технологий
17	Интернет – информационная гиперсреда для ведения эффективного бизнеса
18	GPL-лицензии в рамках Российского законодательства
19	CRM-системы. Виды, назначение и средства защиты

3.3. Самостоятельная работа

Самостоятельная работа составляет 88,8% от общего объёма часов по дисциплине. Для самостоятельной работы отводится 95,9 часа.

Для обеспечения необходимого уровня мотивации обучающихся к выполнению самостоятельной работы, вопросы по темам, вынесенным на самостоятельное изучение, используются при проведении рубежных и выходного контролей.

Тематика самостоятельных работ определяется основными темами и разделами рабочей программы. Обучающимся предлагается 10 вариантов заданий.

3.4. Тестовые задания

По дисциплине «Введение в информационную безопасность» предусмотрено проведение двух видов тестирования: письменное или компьютерное тестирование. Каждый тест содержит 20 – 30 вопросов, выбираемых по случайному закону из базы данных объёмом 120 вопросов.

Письменное тестирование

Письменное тестирование рассматривается как Текущий контроль успеваемости и проводится после изучения соответствующего раздела дисциплины.

Пример письменного (бланкового) теста

ТЕСТ № 1

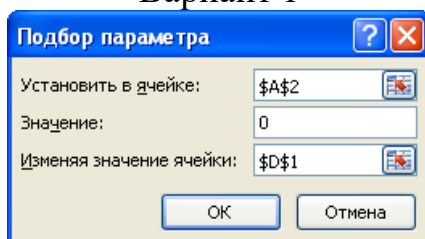
Имитационная модель технологического процесса в сфере АПК опирается на уравнение:

$$3x^4 + 5x^2 - 4x - 5 = 0$$

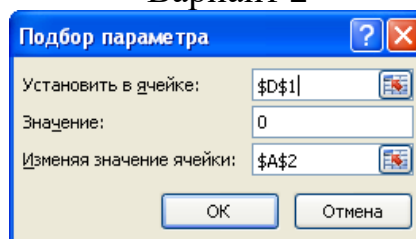
Используя средство «Подбор параметра» табличного процессора MS Excel, необходимо найти все корни уравнения. Формула вводится в ячейку D1 электронной таблицы. Для получения правильного решения окно надстройки «Подбор параметра» должно иметь следующий вид.

Укажите номер правильного варианта ответа.

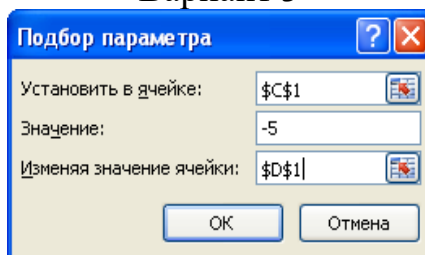
Вариант 1



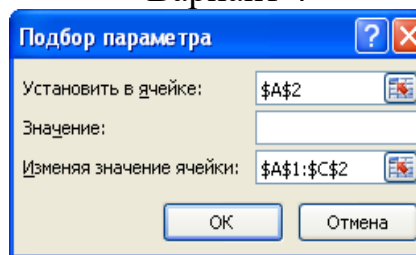
Вариант 2



Вариант 3



Вариант 4



Правильный ответ № ____

Компьютерное тестирование

Компьютерное тестирование, как и письменное тестирование, проводится после изучения определенного раздела дисциплины.

Пример(фрагмент) компьютерного теста

КОМПЬЮТЕРНЫЙ ТЕСТ
 по дисциплине
«ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ»
 Направление подготовки:
 09.03.03 Прикладная информатика

I: Задание в закрытой форме на один выбор ответа

Q: Выберите правильное определение

S: Информационной безопасностью называют:

- : знания, подготовленные людьми для социального использования в обществе и зафиксированные законодательными актами
- : умение целенаправленно работать с информацией и использовать для ее получения, обработки и передачи компьютерную информационную технологию
- +: меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
- : социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан и органов государственной власти

I: Задание в закрытой форме на один выбор ответа

Q: Выберите правильное определение

S: Эмерджентностью системы называют:

- : степень упорядоченности отношений между элементами системы.
- : степень разветвленности взаимосвязей элементов системы.
- +: проявление качественно новых свойств, не присущих отдельным элементам системы.
- : особый характер взаимосвязей между элементами системы.
- : целенаправленное взаимодействие элементов системы.

I: Задание в закрытой форме на один выбор ответа

Q: Выберите правильное определение

S: Целостностью системы безопасности называют:

- : степень упорядоченности отношений между элементами системы.
- +: взаимодействие элементов в соответствии с общей целью ее функционирования
- : степень разветвленности взаимосвязей элементов системы.
- : проявление качественно новых свойств, не присущих отдельным элементам системы.
- : особый характер взаимосвязей между элементами системы.

3.5. Лабораторная работа

Тематика лабораторных работ определяется основными темами и разделами рабочей программы. Обучающимся предлагается 10 вариантов заданий.

Лабораторные работы выполняются в соответствии с Методическими указаниями по выполнению лабораторных работ по дисциплине «Введение в информационную безопасность».

3.6. Текущий контроль

Текущий контроль по дисциплине «Введение в информационную безопасность» позволяет оценить степень освоения учебного материала и проводится для оценки результатов изучения всех разделов дисциплины.

Вопросы текущего контроля № 1

Вопросы, рассматриваемые на аудиторных занятиях

1. Основные области применения цифровых технологий в сфере АПК?
2. Что называют системным подходом в сфере информационной безопасности?
3. Проблемы разработки и выбора методики использования информационной системы.
4. Принципы применения средств информационной безопасности в системах организационно-технического типа.
5. Формирование безопасного информационного пространства пользователя.
6. Информационная модель организации. Информационное обслуживание (сервис) производственных и бизнес-процессов
7. Модели взаимодействия информационных систем

Вопросы для самостоятельного изучения

1. Особенности функционирования распределенных информационных систем управления деятельностью
2. Понятие защищенной информационной системы.
3. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.

Вопросы текущего контроля № 2

Вопросы, рассматриваемые на аудиторных занятиях

1. Управление доступом в MSWindows.
2. Управление средствами аутентификации, идентификации и аудита
3. Назначение атрибутов защиты вновь создаваемым объектам, наследование дескрипторов защиты.

4. Средства минимизации полномочий пользователей
5. Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия скриптовым вирусам.
6. Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.
7. Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.

Вопросы для самостоятельного изучения

1. Стелс-технологии: назначение, методы противодействия
2. Сетевые атаки и защита от них
3. Адаптивная безопасность в вычислительных сетях.

Вопросы текущего контроля № 3

Вопросы, рассматриваемые на аудиторных занятиях

1. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения.
2. Виртуальные частные сети. Применение служб и технологии обеспечения безопасности в Internet/Intranet сетях
3. Электронные таблицы, базы и банки данных, их использование в информационно-коммуникационных системах.
4. Основные принципы шифрования данных в информационных сетях.
5. Доступность, целостность, конфиденциальность информационных ресурсов в локальных и общемировых информационных сетях.
6. Защита проблемно-ориентированных пакетов прикладных программ (управление материальными запасами, управление производством, управление персоналом и т. п.)

Вопросы для самостоятельного изучения

1. Автоматизации управления на основе информационных технологий.
2. Проблемы безопасности в информационной инфраструктуре РФ.
3. Правовые основы защиты информации в сфере электронного документооборота.

1. 7. Промежуточная аттестация

В соответствии с учебным планом по направлению подготовки 09.03.03 Прикладная информатика для дисциплины «Введение в информационную безопасность» в качестве промежуточной аттестации предусмотрен зачет. Целью проведения промежуточной аттестации (зачета) является контроль за освоением дисциплины «Введение в информационную безопасность» и оценка степени фор-

мирования профессиональных компетенций, предусмотренных ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства науки и высшего образования РФ от 19 сентября 2017 г., № 922.

Вопросы зачета формируются на основе вопросов рубежного контроля по разделам. Зачет проводится в форме письменного опроса или компьютерного тестирования.

Вопросы, выносимые на зачет

1. Основные области применения цифровых технологий в сфере АПК?
2. Что называют системным подходом в сфере информационной безопасности?
3. Проблемы разработки и выбора методики использования информационной системы.
4. Принципы применения средств информационной безопасности в системах организационно-технического типа.
5. Формирование безопасного информационного пространства пользователя.
6. Информационная модель организации. Информационное обслуживание (сервис) производственных и бизнес-процессов
7. Модели взаимодействия информационных систем
8. Особенности функционирования распределенных информационных систем управления деятельностью
9. Понятие защищенной информационной системы.
10. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
11. Управление доступом в MSWindows.
12. Управление средствами аутентификации, идентификации и аудита
13. Назначение атрибутов защиты вновь создаваемым объектам, наследование дескрипторов защиты.
14. Средства минимизации полномочий пользователей
15. Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия скриптовым вирусам.
16. Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.
17. Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.
18. Стелс-технологии: назначение, методы противодействия
19. Сетевые атаки и защита от них
20. Адаптивная безопасность в вычислительных сетях.
21. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения.
22. Виртуальные частные сети. Применение служб и технологии обеспечения безопасности в Internet/Intranet сетях
23. Электронные таблицы, базы и банки данных, их использование в информационно-коммуникационных системах.
24. Основные принципы шифрования данных в информационных сетях.

25. Доступность, целостность, конфиденциальность информационных ресурсов в локальных и общемировых информационных сетях.
26. Защита проблемно–ориентированных пакетов прикладных программ (управление материальными запасами, управление производством, управление персоналом и т. п.)
27. Методо-ориентированные пакеты прикладных программ (математическое программирование, статистическая обработка данных)
28. Системы искусственного интеллекта для защиты информации
29. Структурные методологии и CASE-средства.
30. Автоматизации управления на основе информационных технологий.
31. Проблемы безопасности в информационной инфраструктуре РФ.
32. Правовые основы защиты информации в сфере электронного документооборота.

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

4.1 Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Контроль результатов обучения обучающихся, этапов и уровня формирования компетенций по дисциплине «Введение в информационную безопасность» осуществляется через проведение входного, текущего и выходного контролей и контроля самостоятельной работы.

Формы текущего, промежуточного и итогового контроля и фонды контрольных заданий для соответствующего контроля разрабатываются кафедрой исходя из специфики дисциплины, и утверждаются на заседании кафедры.

4.2 Критерии оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Описание шкалы оценивания достижения компетенций по дисциплине приведено в таблице 6.

Таблица 6

Уровень освоения компетенции	Отметка по пяти-балльной системе (промежуточная аттестация)	Описание
высокий	«зачтено»	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебного материала, умеет свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литера-

Уровень освоения компетенции	Отметка по пяти-балльной системе (промежуточная аттестация)	Описание
		турой, рекомендованной программой. Как правило, обучающийся проявляет творческие способности в понимании, изложении и использовании материала
<i>базовый</i>	«зачтено»	Обучающийся обнаружил полное знание учебного материала, успешно выполняет предусмотренные в программе задания, усвоил основную литературу, рекомендованную в программе
<i>пороговый</i>	«зачтено»	Обучающийся обнаружил знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляется с выполнением практических заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой, допустил погрешности в ответе на экзамене и при выполнении заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя
—	«незачтено»	Обучающийся обнаружил пробелы в знаниях основного учебного материала, допустил принципиальные ошибки в выполнении предусмотренных программой практических заданий, не может продолжить обучение или приступить к профессиональной деятельности по окончании образовательной организации без дополнительных занятий

4.2.1. Критерии оценки устного ответа при промежуточной аттестации

При ответе на вопрос обучающийся демонстрирует:

- **знания:** понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространенных угроз;
- **умения:** пользоваться информационными системами для анализа уровня информационной безопасности;
- **владения навыками:** применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности.

Критерии оценки

отлично	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, исчерпывающе и последовательно, четко и логично излагает материал, хорошо ориентируется в материале, не затрудняется с ответом при видоизменении заданий; - умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - успешное и системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
хорошо	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, - в целом успешное, но содержащие отдельные пробелы, умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
удовлетворительно	обучающийся демонстрирует: - знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала; - в целом успешное, но не системное умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но не системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий

неудовлетворительно	обучающийся: - не знает значительной части программного материала, плохо ориентируется в понятиях информационной безопасности, системного и объектно-ориентированного подходах к обеспечению информационной безопасности, в наиболее распространённых угрозах, не знает практику применения, допускает существенные ошибки; - не умеет пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено; - обучающийся не владеет навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено
----------------------------	--

4.3.2. Критерии оценки тестовых заданий

Критерии оценки письменного или компьютерного тестирования

1. Оценка 5 «отлично» - выставляется, если обучающийся правильно ответил более, чем на 86% вопросов теста.
2. Оценка 4 «хорошо» -выставляется, если обучающийся правильно ответил на 73% - 85% вопросов теста.
3. Оценка 3 «удовлетворительно» -выставляется, если обучающийся правильно ответил на 60% - 72% вопросов теста.
4. Оценка 2 «неудовлетворительно» - выставляется, если обучающийся правильно ответил на менее, чем 60% вопросов теста.

4.2.3 Критерии оценки самостоятельной работы

При выполнении самостоятельных работ обучающийся демонстрирует:

- **знания:** понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз;
- **умения:** пользоваться информационными системами для анализа уровня информационной безопасности;
- **владения навыками:** применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности.

Критерии оценки выполнения самостоятельной работы

отлично	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, исчерпывающе и последовательно, четко и логично излагает материал, хорошо ориентируется в материале, не затрудняется с ответом при видоизменении заданий; - умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - успешное и системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
хорошо	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, - в целом успешное, но содержащие отдельные пробелы, умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
удовлетворительно	обучающийся демонстрирует: - знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала; - в целом успешное, но не системное умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но не системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий

неудовлетворительно	обучающийся: - не знает значительной части программного материала, плохо ориентируется в понятиях информационной безопасности, системного и объектно-ориентированного подходах к обеспечению информационной безопасности, в наиболее распространённых угрозах, не знает практику применения, допускает существенные ошибки; - не умеет пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено; - обучающийся не владеет навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено
----------------------------	--

4.2.5. Критерии оценки лабораторных работ

При выполнении лабораторных работ обучающийся демонстрирует:

- **знания:** понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз;

- **умения:** пользоваться информационными системами для анализа уровня информационной безопасности;

- **владения навыками:** применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности.

Критерии оценки выполнения лабораторных работ

отлично	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, исчерпывающе и последовательно, четко и логично излагает материал, хорошо ориентируется в материале, не затрудняется с ответом при видеоизменении заданий; - умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - успешное и системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и инфор-
----------------	--

	мационно-коммуникационных технологий
хорошо	обучающийся демонстрирует: - знание понятий информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, наиболее распространённых угроз, тенденций и практики их применения, - в целом успешное, но содержащие отдельные пробелы, умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
удовлетворительно	обучающийся демонстрирует: - знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала; - в целом успешное, но не системное умение пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; - в целом успешное, но не системное владение навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
неудовлетворительно	обучающийся: - не знает значительной части программного материала, плохо ориентируется в понятиях информационной безопасности, системного и объектно-ориентированного подходов к обеспечению информационной безопасности, в наиболее распространённых угрозах, не знает практику применения, допускает существенные ошибки; - не умеет пользоваться информационными системами для анализа уровня информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено; - обучающийся не владеет навыками применения стандартов и спецификаций в области сетевой безопасности данных, использования законодательной базы информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено

4.2.6 Критерии оценки доклада

При подготовки устного доклада обучающийся демонстрирует:

- **знания:** основных понятий проблемы доклада;
- **умения:** систематизировать и структурировать материал; делать обобщения и сопоставления различных точек зрения по рассматриваемому вопросу, делать и аргументировать основные выводы

Критерии оценки устного доклада

отлично	обучающийся демонстрирует: - знание материала (материал систематизирован и структурирован; сделаны обобщения и сопоставления различных точек зрения по рассматриваемому вопросу, сделаны и аргументированы основные выводы, отчетливо видна самостоятельность суждений, основные понятия проблемы изложены полно и глубоко) - грамотность и культура изложения; - дает правильные ответы на вопросы аудитории при презентации доклада
хорошо	обучающийся демонстрирует: - знание материала (материал систематизирован и структурирован; сделаны обобщения и сопоставления различных точек зрения по рассматриваемому вопросу, сделаны и аргументированы основные выводы) - дает неточные ответы на вопросы аудитории при презентации доклада

Разработчик: доцент, Розанов А.В.


(подпись)