

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Соловьев Дмитрий Александрович

Должность: ректор ФГБОУ ВО Вавиловский университет

Дата подписания: 12.03.2025 17:07:27

Уникальный программный ключ:

528682d78e671e5668b7f03fe1b3272f735a10

## 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	<b>УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИТ-ПРЕДПРИЯТИЯ</b>
Направление подготовки	<b>38.04.05 Бизнес-информатика</b>
Направленность (профиль)	<b>Управление бизнес-анализом</b>
Квалификация выпускника	<b>Магистр</b>
Нормативный срок обучения	<b>2 года</b>
Форма обучения	<b>Очная</b>
Кафедра-разработчик	<b>Цифровое управление процессами в АПК</b>
Ведущий преподаватель	<b>Розанов А.В., доцент</b>

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 .....	20

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

В результате изучения дисциплины «Управление безопасностью ИТ-предприятия» обучающиеся, в соответствии с ФГОС ВО по направлению подготовки 38.04.05 Бизнес-информатика, утвержденного приказом Министерства науки и высшего образования РФ от 12 августа 2020 г., № 973, формируют следующие компетенции, представленные в таблице 1.

Таблица 1

### Формирование компетенций в процессе изучения дисциплины «Управление безопасностью ИТ-предприятия»

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
ПК-2	способен собирать информацию, выбирать рациональные ИС и ИКТ-решения для управления бизнесом, разрабатывать стратегию развития архитектуры предприятия	ПК-2.2. выбирает рациональные ИС и ИКТ-решения для управления бизнесом	3 семестр	лекции, лабораторные занятия	лекции, лабораторные работы, тестовые задания, доклады, самостоятельная работа

#### Примечание.

Компетенция ПК-2 – также формируется в ходе освоения следующих дисциплин и практик: Прогнозирование бизнес-результатов деятельности предприятия на основе предиктивного моделирования с использованием IBM Watson, Электронные платежные системы, Информационно-аналитические системы управления корпоративной результативностью, Управление ценностью информационных систем, Ознакомительная практика, Научно-исследовательская работа, Проектно-технологическая практика, Подготовка к процедуре защиты 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 материала	Представление оценочного средства в ОМ
1	2	3	4
1	лабораторные занятия	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 публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы	темы устных докладов

### 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 отраслевых систем. Системный подход к обеспечению информационной безопасности. Средства обеспечения защиты информации в системах электронного документооборота.	ПК-2	Тестовые задания Лабораторная работа №1
2.	Основные принципы политики безопасности. Средства и способы анализа трафика на сетевых интерфейсах в ОС Windows.	ПК-2	Лабораторная работа №2 Самостоятельная работа
3.	Понятия состояния системы и потока информации. Правила разграничения доступа. Реализация моделей политики безопасности посредством управления доступом	ПК-2	Лабораторная работа №3 Самостоятельная работа
4.	Политика полномочного доступа. Метки секретности, уровень прозрачности. Изучение сетевых средств защиты операционной системы MS Windows.	ПК-2	Лабораторная работа №4 Самостоятельная работа
5.	Правовая защита на международном уровне и на уровне Российской Федерации. Диагностика защищенности информации в сети средствами операционной системы	ПК-2	Лабораторная работа №5 Самостоятельная работа
6.	Аппаратные, программные и криптографические средства защиты. Анализ защищенности от потери данных и отказов программно-аппаратных средств.	ПК-2	Лабораторная работа №6 Самостоятельная работа
7.	Классификация угроз информационным системам. Практика кодирования и шифрования информации.	ПК-2	Лабораторная работа №7 Самостоятельная работа
8	Криптографические методы защиты информации. Установка и настройка параметров антивирусных программ.	ПК-2	Лабораторная работа №8 Самостоятельная работа

**Описание показателей и критериев оценивания компетенций по дисциплине «Управление безопасностью ИТ-предприятия» на различных этапах их формирования, описание шкал оценивания**

Таблица 4

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
ПК-2, 3 семестр	ПК-2.2. выбирает рациональные ИС	обучающийся не знает значительной части	обучающийся демонстрирует	обучающийся демонстрирует	обучающийся демонстрирует

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
	и ИКТ-решения для управления бизнесом	программного материала, плохо ориентируется в ИС и ИКТ-решения для управления бизнесом, не знает практику применения материала, допускает существенные ошибки	знания только основного материала, но не знает деталей, допускает неточности, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала	знание ИС и ИКТ-решения для управления бизнесом, не допускает существенных неточностей	знание ИС и ИКТ-решения для управления бизнесом, практику применения материала, исчерпывающе и последовательно, четко и логично излагает материал, не затрудняется с ответом при видоизменении заданий
		не умеет применять рациональные ИС и ИКТ-решения для управления бизнесом, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено	в целом успешное, но не системное, умение применять рациональные ИС и ИКТ-решения для управления бизнесом	в целом успешное, но содержащее отдельные пробелы, умение применять рациональные ИС и ИКТ-решения для управления бизнесом	сформированное умение применять рациональные ИС и ИКТ-решения для управления бизнесом, используя современные методы и показатели

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
		обучающийся не владеет навыками рационального выбора ИС и ИКТ-решений для управления бизнесом, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины не выполнено	в целом успешное, но не системное владение навыками рационального выбора ИС и ИКТ-решений для управления бизнесом	в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками рационального выбора ИС и ИКТ-решений для управления бизнесом	успешное и системное владение навыками рационального выбора ИС и ИКТ-решений для управления бизнесом

### **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 стандартных курсов информатики и информационных технологий 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 одиночного или 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 документе 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 2.

Таблица 5

#### **Темы докладов, рекомендуемые к подготовке при изучении дисциплины «Управление безопасностью IT-предприятия»**

№ 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 бизнес-аналитики



№ п/п	Темы докладов
1	2
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 70,3% от общего объёма часов по дисциплине. Для самостоятельной работы отводится 75,9 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 «Управление безопасностью IT-предприятия» 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 Рубежный контроль успеваемости и проводится после изучения соответствующего раздела дисциплины.

## Пример письменного (бланкового) теста

### ТЕСТ № 1

Имитационная модель бизнес-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

Подбор параметра

Установить в ячейке: \$A\$2

Значение: 0

Изменяя значение ячейки: \$D\$1

OK Отмена

Вариант 2

Подбор параметра

Установить в ячейке: \$D\$1

Значение: 0

Изменяя значение ячейки: \$A\$2

OK Отмена

Вариант 3

Подбор параметра

Установить в ячейке: \$C\$1

Значение: -5

Изменяя значение ячейки: \$D\$1

OK Отмена

Вариант 4

Подбор параметра

Установить в ячейке: \$A\$2

Значение:

Изменяя значение ячейки: \$A\$1:\$C\$2

OK Отмена

Правильный ответ № \_\_\_\_\_

## Компьютерное тестирование

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

## Пример (фрагмент) компьютерного теста

**КОМПЬЮТЕРНЫЙ ТЕСТ**  
по дисциплине  
**«УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИТ-ПРЕДПРИЯТИЯ»**  
Направление подготовки:  
38.04.05 Бизнес-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. Лабораторные занятия**

Тематика 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 «Управление безопасностью IT-предприятия».

### **3.6. Рубежный контроль**

Рубежный контроль по дисциплине «Управление безопасностью IT-предприятия» позволяет оценить степень освоения учебного материала и проводится для оценки результатов изучения всех разделов дисциплины.

#### **Вопросы рубежного 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 рубежного контроля № 2**

*Вопросы, рассматриваемые на аудиторных занятиях*

1. Управление доступом в MS Windows.
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 рубежного 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.

### **3.7. Промежуточная аттестация**

В соответствии с учебным планом по направлению подготовки 38.04.05 Управление безопасностью IT-предприятия в качестве промежуточной аттестации предусмотрен зачет. Целью проведения промежуточной аттестации (зачета) является контроль за освоением дисциплины «Управление безопасностью IT-предприятия» и оценка степени формирования профессиональной компетенции,

предусмотренной ФГОС ВО по направлению подготовки 38.04.05 Управление безопасностью IT-предприятия, утвержденного приказом Министерства науки и высшего образования РФ от 12 августа 2020 г., № 973.

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 MS Windows.
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 «Управление безопасностью ИТ-предприятия» осуществляется через проведение входного, рубежного, выходного контролей и контроля самостоятельной работы.

Формы рубежного, промежуточного и итогового контроля и фонды контрольных заданий для рубежного 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
1	2	3
<b>высокий</b>	«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
1	2	3
		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
–	«не зачтено»	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:** рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы;

- **умения:** собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности;

- **владения навыками:** выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности

#### Критерии оценки



<b>отлично</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, тенденций и практики их применения, исчерпывающе и последовательно, четко и логично излагает материал, хорошо ориентируется в материале, не затрудняется с ответом при видоизменении заданий;</li> <li>- умение собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- успешное и системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>
<b>хорошо</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, тенденций и практики их применения,</li> <li>- в целом успешное, но содержащее отдельные пробелы, собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>

<b>удовлетворительно</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала;</li> <li>- в целом успешное, но не системное собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но не системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>
<b>неудовлетворительно</b>	<p>обучающийся:</p> <ul style="list-style-type: none"> <li>- не знает значительной части программного материала, плохо ориентируется в рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, не знает практику применения, допускает существенные ошибки;</li> <li>- не умеет собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено;</li> <li>- обучающийся не владеет навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено</li> </ul>

#### 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 ответе на вопрос обучающийся демонстрирует:

- **знания:** рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы;

- **умения:** собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности;

- **владения навыками:** выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности

### **Критерии оценки выполнения самостоятельной работы**

<b>отлично</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, тенденций и практики их применения, исчерпывающе и последовательно, четко и логично излагает материал, хорошо ориентируется в материале, не затрудняется с ответом при видоизменении заданий;</li> <li>- умение собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- успешное и системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>
<b>хорошо</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, тенденций и практики их применения,</li> <li>- в целом успешное, но содержащее отдельные пробелы, собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>

<b>удовлетворительно</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала;</li> <li>- в целом успешное, но не системное собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но не системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>
<b>неудовлетворительно</b>	<p>обучающийся:</p> <ul style="list-style-type: none"> <li>- не знает значительной части программного материала, плохо ориентируется в рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, не знает практику применения, допускает существенные ошибки;</li> <li>- не умеет собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено;</li> <li>- обучающийся не владеет навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено</li> </ul>

#### 4.2.5. Критерии оценки лабораторных работ

При ответе на вопрос обучающийся демонстрирует:

- **знания:** рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы;

- **умения:** собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности;

- **владения навыками:** выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности

### Критерии оценки выполнения лабораторных работ

<b>отлично</b>	обучающийся демонстрирует: - знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, 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 собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели; - успешное и системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий
----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p><b>хорошо</b></p>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, тенденции и практики их применения,</li> <li>- в целом успешное, но содержащее отдельные пробелы, собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но содержащее отдельные пробелы или сопровождающееся отдельными ошибками владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>
<p><b>удовлетворительно</b></p>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знания только основного материала, но не знает деталей, допускает неточности в формулировках, нарушает логическую последовательность в изложении программного материала;</li> <li>- в целом успешное, но не системное собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели;</li> <li>- в целом успешное, но не системное владение навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности с использованием перспективных цифровых и информационно-коммуникационных технологий</li> </ul>

<b>неудовлетворительно</b>	<p>обучающийся:</p> <ul style="list-style-type: none"> <li>- не знает значительной части программного материала, плохо ориентируется в рациональных информационных систем (ИС) и информационно-коммуникационных (ИКТ) решений для безопасного управления бизнесом; основные требования к информационным системам (ИС) предприятия, автоматизирующим задачи организационного управления и бизнес-процессы, не знает практику применения, допускает существенные ошибки;</li> <li>- не умеет собирать информацию, выделять и изучать отдельные объекты рынка ИС и ИКТ с учетом требований информационной безопасности; проводить обследование организаций и выявлять информационные потребности пользователей с точки зрения обеспечения информационной безопасности, используя современные методы и показатели; допускает существенные ошибки, неуверенно, с большими затруднениями выполняет самостоятельную работу, большинство заданий, предусмотренных программой дисциплины, не выполнено;</li> <li>- обучающийся не владеет навыками выбора рациональных ИС и ИКТ-решений для управления бизнесом и разработки стратегии развития архитектуры информационной безопасности предприятия; навыками технической поддержки процессов создания (модификации) и сопровождения ИС, автоматизирующих задачи организационного управления и бизнес-процессы с учетом требований информационной безопасности, допускает существенные ошибки, с большими затруднениями выполняет самостоятельную работу, большинство предусмотренных программой дисциплины не выполнено</li> </ul>
----------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### 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

<b>отлично</b>	<p>обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- 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)</li> <li>- грамотность и культура изложения;</li> <li>- дает правильные ответы на вопросы аудитории при презентации доклада</li> </ul>
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



<b>хорошо</b>	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)