

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ
АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ
Б1.Б.13 Основы информационной безопасности**

Направление подготовки (специальность)

09.03.01 Информатика и вычислительная техника

Профиль подготовки (специализация)

“Автоматизированные системы обработки информации и управления”

Квалификация (степень) выпускника бакалавр

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

Наименование и содержание компетенции

ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности

Знать:

Этап 1: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства

Этап 2: основные правила разработки политики безопасности организации. Компоненты политики безопасности

Уметь:

Этап 1: выявлять угрозы системе информационной безопасности

Этап 2: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю

Владеть:

Этап 1: оценки эффективности систем защиты информации автоматизированных систем

Этап 2: навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем

Наименование и содержание компетенции

ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

Этап 1: знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ

Этап 2: знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ

Уметь:

Этап 1: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю

Этап 2: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Владеть:

Этап 1: внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю

Этап 2: навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты

2. Показатели и критерии оценивания компетенций на различных этапах их формирования.

Таблица 1 - Показатели и критерии оценивания компетенций на 1 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	владеет способностью использовать основы правовых знаний в различных сферах деятельности	Знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства Уметь: выявлять угрозы системе информационной безопасности Владеть: оценки эффективности систем защиты информации автоматизированных систем	индивидуальный устный опрос, письменный опрос, тестирование.
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: знать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ Уметь: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю Владеть: внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации	индивидуальный устный опрос, устная (письменная) защита практической работы, тестирование.

		Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю	
--	--	---	--

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	Критерии сформированности компетенции	Показатели	Процедура оценивания
1	2	3	4
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	владеет способностью использовать основы правовых знаний в различных сферах деятельности	Знать: основные правила разработки политики безопасности организации. Компоненты политики безопасности Уметь: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю Владеть: навыки применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем	индивидуальный устный опрос, письменный опрос, тестирование.
ОПК-5 способностью решать стандартные задачи	владеет способностью решать стандартные задачи	Знать: знать цели и задачи, решаемые разрабатываемыми процессами управления	устная (письменная) защита практической

профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИБ Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Владеть: навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты	работы, экзамен с учетом результатов текущего контроля
--	--	--	--

3. Шкала оценивания.

Университет использует шкалы оценивания соответствующего государственным регламентам в сфере образования и позволяющую обеспечивать интеграцию в международное образовательное пространство. Шкалы оценивания и описание шкал оценивания представлены в таблицах 3 и 4.

Таблица 3 - Шкалы оценивания

Диапазон оценки, в баллах	Экзамен		Зачет
	европейская шкала (ECTS)	традиционная шкала	
[95;100]	A – (5+)	отлично – (5)	зачтено
[85;95)	B – (5)		
[70;85)	C – (4)	хорошо – (4)	
[60;70)	D – (3+)	удовлетворительно – (3)	
[50;60)	E – (3)		
[33,3;50)	FX – (2+)	неудовлетворительно – (2)	незачтено
[0;33,3)	F – (2)		

Таблица 4 - Описание шкал оценивания

ECTS	Критерии оценивания	Традиционная шкала
A	Превосходно – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.	отлично (зачтено)
B	Отлично – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным	

	материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.	
С	Хорошо – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено максимальным числом баллов, некоторые виды заданий выполнены с ошибками.	хорошо (зачтено)
Д	Удовлетворительно – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.	удовлетворительно (зачтено)
Е	Посредственно – теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	удовлетворительно (незачтено)
FX	Условно неудовлетворительно – теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.	
F	Безусловно неудовлетворительно – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.	неудовлетворительно (незачтено)

Таблица 5 – Формирование шкалы оценивания компетенций на различных этапах

Этапы формирования компетенций	Формирование оценки						
	незачтено			зачтено			
	неудовлетворительно		удовлетворительно	хорошо	отлично		
	F(2)	FX(2+)	E(3)*	D(3+)	C(4)	B(5)	A(5+)
	[0;33,3)	[33,3;50)	[50;60)	[60;70)	[70;85)	[85;95)	[95;100)
Этап-1	0-13	13-19,5	19,5-23,4	23,4-27,3	27,3-33,2	33,2-37,5	37,5-39
Этап 2	0-25	25-37	37-45	45-52	52-63,5	63,5-71,5	71,5-75

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

Таблица 6 - ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности. Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства	<p>1. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь</p> <p>2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)</p> <p>3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации +в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации</p> <p>4. Что самое главное должно продумать руководство при</p>

	<p>классификации данных?</p> <p>+а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным</p> <p>б) Необходимый уровень доступности, целостности и конфиденциальности</p> <p>в) Оценить уровень риска и отменить контрмеры</p> <p>г) Управление доступом, которое должно защищать данные</p> <p>5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?</p> <p>а) Владельцы данных</p> <p>б) Пользователи</p> <p>в) Администраторы</p> <p>+г) Руководство</p>
<p>Уметь: выявлять угрозы системе информационной безопасности</p>	<p>6. Что такое процедура?</p> <p>А) Правила использования программного и аппаратного обеспечения в компании</p> <p>+Б) Пошаговая инструкция по выполнению задачи</p> <p>С) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах</p> <p>Г) Обязательные действия</p> <p>7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?</p> <p>+А) Поддержка высшего руководства</p> <p>Б) Эффективные защитные меры и методы их внедрения</p> <p>С) Актуальные и адекватные политики и процедуры безопасности</p> <p>Г) Проведение тренингов по безопасности для всех сотрудников</p> <p>8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?</p> <p>А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски</p> <p>Б) Когда риски не могут быть приняты во внимание по политическим соображениям</p> <p>С) Когда необходимые защитные меры слишком сложны</p> <p>+Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери</p> <p>9. Что такое политики безопасности?</p> <p>А) Пошаговые инструкции по выполнению задач безопасности</p> <p>Б) Общие руководящие требования по достижению определенного уровня безопасности</p> <p>+С) Широкие, высокоуровневые заявления руководства</p> <p>Г) Детализированные документы по обработке инцидентов безопасности</p> <p>10. Какая из приведенных техник является самой важной при</p>

	<p>выборе конкретных защитных мер?</p> <p>А) Анализ рисков +Б) Анализ затрат / выгоды С) Результаты ALE Г) Выявление уязвимостей и угроз, являющихся причиной риска</p>
<p>Навыки: оценки эффективности систем защиты информации автоматизированных систем</p>	<p>11.Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем +б)объективных проблем современной технологии программирования в)происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы</p> <p>12.В число универсальных сервисов безопасности входят: +a) шифрование б) средства построения виртуальных частных сетей +в) туннелирование</p> <p>13.В число принципов управления персоналом входят: а)"разделяй и властвуй" +б)разделение обязанностей в)инкапсуляция наследования</p> <p>14.Комплексное экранирование может обеспечить: +a) разграничение доступа по сетевым адресам +б) выборочное выполнение команд прикладного протокола +в) контроль объема данных, переданных по TCP-соединению</p> <p>15.Уровень безопасности С, согласно "Оранжевой книге", характеризуется: а) Основы информационной безопасности +б) произвольным управлением доступом в) принудительным управлением доступом г) верифицируемой безопасностью</p>

Таблица 7 ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности - Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
<p>Знать: основные правила разработки политики безопасности организации. Компоненты политики</p>	<p>1.Перехват данных является угрозой: а)доступности +б)конфиденциальности в)целостности</p> <p>2.Что из перечисленного не относится к числу основных аспектов информационной безопасности:</p>

<p>безопасности</p>	<p>а)доступность б)целостность +в)защита от копирования г)конфиденциальность</p> <p>3.В число целей политики безопасности верхнего уровня входят: +а)формулировка административных решений по важнейшим аспектам б)реализации программы безопасности в)выбор методов аутентификации пользователей +г)обеспечение базы для соблюдения законов и правил</p> <p>4.В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: +а)законодательные меры б)меры обеспечения доступности в)профилактические меры</p> <p>5.Оценка рисков позволяет ответить на следующие вопросы: +а)существующие риски приемлемы? б)кто виноват в том, что риски неприемлемы? +в)что делать, чтобы риски стали приемлемыми?</p>
<p>Уметь: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю</p>	<p>6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников</p> <p>7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери</p> <p>8. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности</p> <p>9. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец</p>

	<p>г) Пользователь</p> <p>10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?</p> <p>+а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)</p>
<p>Навыки: применения комплексного подхода к обеспечению информационной безопасности автоматизированных систем</p>	<p>11. В число этапов управления рисками входят:</p> <p>+а) анализ угроз б) угрозы проведения анализа +в) выявление уязвимых мест</p> <p>12. Агрессивное потребление ресурсов является угрозой:</p> <p>+а) доступности б) конфиденциальности в) целостности</p> <p>13. В рамках программы безопасности нижнего уровня определяются:</p> <p>а) совокупность целей безопасности +б) набор используемых механизмов безопасности в) наиболее вероятные угрозы безопасности</p> <p>14. "Общие критерии" содержат следующие виды требований:</p> <p>+а) функциональные +б) доверия безопасности в) экономической целесообразности</p> <p>15. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на:</p> <p>а) системы электронной коммерции б) инфраструктуру для электронных цифровых подписей +в) средства электронной аутентификации</p>

Таблица 8 ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности - Этап 1

<p>Наименование знаний, умений, навыков и (или) опыта деятельности</p>	<p>Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности</p>
<p>Знать: текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления</p>	<p>1. Кто является основным ответственным за определение уровня классификации информации?</p> <p>а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь</p>

<p>ИБ</p>	<p>2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?</p> <p>+а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)</p> <p>3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?</p> <p>а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации +в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации</p> <p>4. Что самое главное должно продумать руководство при классификации данных?</p> <p>+а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) Необходимый уровень доступности, целостности и конфиденциальности в) Оценить уровень риска и отменить контрмеры г) Управление доступом, которое должно защищать данные</p> <p>5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?</p> <p>а) Владельцы данных б) Пользователи в) Администраторы +г) Руководство</p>
<p>Уметь: умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю</p>	<p>6. Что такое процедура?</p> <p>А) Правила использования программного и аппаратного обеспечения в компании +Б) Пошаговая инструкция по выполнению задачи С) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах Г) Обязательные действия</p> <p>7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?</p> <p>+А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех</p>

	<p>сотрудников</p> <p>8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери</p> <p>9. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности</p> <p>10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер? А) Анализ рисков +Б) Анализ затрат / выгоды С) Результаты ALE Г) Выявление уязвимостей и угроз, являющихся причиной риска</p>
<p>Навыки: внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой</p>	<p>11.Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем +б)объективных проблем современной технологии программирования в)происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы</p> <p>12.В число универсальных сервисов безопасности входят: +а) шифрование б) средства построения виртуальных частных сетей +в) туннелирование</p> <p>13.В число принципов управления персоналом входят: а)"разделяй и властвуй" +б)разделение обязанностей в)инкапсуляция наследования</p> <p>14.Комплексное экранирование может обеспечить: +а) разграничение доступа по сетевым адресам +б) выборочное выполнение команд прикладного протокола +в) контроль объема данных, переданных по ТСР-соединению</p> <p>15.Уровень безопасности С, согласно "Оранжевой книге",</p>

по техническому и экспортному контролю	характеризуется: а) Основы информационной безопасности +б) произвольным управлением доступом в) принудительным управлением доступом г) верифицируемой безопасностью
--	---

Таблица 9 ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности - Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: знать цели и задачи, решаемые разрабатываемыми процессами управления ИБ	<p>1. Перехват данных является угрозой: а) доступности +б) конфиденциальности в) целостности</p> <p>2. Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) целостность +в) защита от копирования г) конфиденциальность</p> <p>3. В число целей политики безопасности верхнего уровня входят: +а) формулировка административных решений по важнейшим аспектам б) реализации программы безопасности в) выбор методов аутентификации пользователей +г) обеспечение базы для соблюдения законов и правил</p> <p>4. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: +а) законодательные меры б) меры обеспечения доступности в) профилактические меры</p> <p>5. Оценка рисков позволяет ответить на следующие вопросы: +а) существующие риски приемлемы? б) кто виноват в том, что риски неприемлемы? +в) что делать, чтобы риски стали приемлемыми?</p>
Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных	<p>6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников</p>

<p>программных и аппаратных средств защиты</p>	<p>7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери</p> <p>8. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности</p> <p>9. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь</p> <p>10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +a) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)</p>
<p>Навыки: применения комплексного подхода к обеспечению информационной безопасности объекта защиты</p>	<p>11. В число этапов управления рисками входят: +a) анализ угроз б) угрозы проведения анализа +в) выявление уязвимых мест</p> <p>12. Агрессивное потребление ресурсов является угрозой: +a) доступности б) конфиденциальности в) целостности</p> <p>13. В рамках программы безопасности нижнего уровня определяются: а) совокупность целей безопасности +б) набор используемых механизмов безопасности в) наиболее вероятные угрозы безопасности</p> <p>14. "Общие критерии" содержат следующие виды требований: +a) функциональные</p>

	+б)доверия безопасности в)экономической целесообразности 15.В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на: а)системы электронной коммерции б)инфраструктуру для электронных цифровых подписей +в)средства электронной аутентификации
--	---

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

Многообразие изучаемых тем, видов занятий, индивидуальных способностей студентов, обуславливает необходимость оценивания знаний, умений, навыков с помощью системы процедур, контрольных мероприятий, различных технологий и оценочных средств.

Таблица 10 - Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на 1 этапе формирования компетенции

Виды занятий и контрольных мероприятий	Оцениваемые результаты обучения	Описание процедуры оценивания
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Индивидуальный устный опрос, письменный опрос, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Устная (письменная) защита практической работы, тестирование
Самостоятельная работа (выполнение индивидуальных, дополнительных и творческих заданий)	Знания, умения и навыки, сформированные во время самоподготовки	Индивидуальный устный опрос, письменный опрос, тестирование

Таблица 11 - Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на 2 этапе формирования компетенции

Виды занятий и контрольных мероприятий	Оцениваемые результаты обучения	Описание процедуры оценивания
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Индивидуальный устный опрос, письменный опрос, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Устная (письменная) защита практической работы, тестирование
Самостоятельная работа	Знания, умения и навыки,	Индивидуальный устный

(выполнение индивидуальных, дополнительных и творческих заданий)	сформированные во время самоподготовки	опрос, письменный опрос, тестирование
Промежуточная аттестация	Знания, умения и навыки соответствующие изученной дисциплине	Экзамен с учетом результатов текущего контроля

В процессе изучения дисциплины предусмотрены следующие формы контроля: текущий, промежуточный контроль, контроль самостоятельной работы студентов.

Текущий контроль успеваемости обучающихся осуществляется по всем видам контактной и самостоятельной работы, предусмотренным рабочей программой дисциплины. Текущий контроль успеваемости осуществляется преподавателем, ведущим аудиторские занятия.

Текущий контроль успеваемости может проводиться в следующих формах:

- устная (устный опрос, собеседование, публичная защита, защита письменной работы, доклад по результатам самостоятельной работы и т.д.);
- письменная (письменный опрос, выполнение, расчетно-проектировочной и расчетно-графической работ и т.д.);
- тестовая (устное, письменное, компьютерное тестирование).

Результаты текущего контроля успеваемости фиксируются в журнале занятий с соблюдением требований по его ведению.

Устная форма позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. Проводятся преподавателем с обучающимся на темы, связанные с изучаемой дисциплиной, рассчитана на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Уровень знаний, умений и навыков обучающегося при устном ответе во время промежуточной аттестации определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» по следующим критериям:

Оценка «5» (отлично) ставится, если:

- полно раскрыто содержание материала;
- материал изложен грамотно, в определенной логической последовательности;
- продемонстрировано системное и глубокое знание программного материала;
- точно используется терминология;
- показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации;
- продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков;
- ответ прозвучал самостоятельно, без наводящих вопросов;
- продемонстрирована способность творчески применять знание теории к решению профессиональных задач;
- продемонстрировано знание современной учебной и научной литературы;
- допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию.

Оценка «4» (хорошо) ставится, если:

- вопросы излагаются систематизировано и последовательно;
- продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер;
- продемонстрировано усвоение основной литературы.
- ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

–в изложении допущены небольшие пробелы, не исказившие содержание ответа;
–допущены один–два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;

–допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.

Оценка «3» (удовлетворительно) ставится, если:

–неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала;

–усвоены основные категории по рассматриваемому и дополнительным вопросам;

–имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов;

–при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации;

–продемонстрировано усвоение основной литературы

Оценка «2» (неудовлетворительно) ставится, если:

–не раскрыто основное содержание учебного материала;

–обнаружено незнание или непонимание большей или наиболее важной части учебного материала;

–допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов;

–не сформированы компетенции, умения и навыки.

Доклад–подготовленное студентом самостоятельно публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной проблемы.

Количество и вес критериев оценки доклада зависят от того, является ли доклад единственным объектом оценивания или он представляет собой только его часть.

Доклад как единственное средство оценивания эффективен, прежде всего, тогда, когда студент представляет результаты своей собственной учебно/научно-исследовательской деятельности, и важным является именно содержание и владение представленной информацией. В этом случае при оценке доклада может быть использована любая совокупность из следующих критериев:

–соответствие выступления теме, поставленным целям и задачам;

–проблемность / актуальность;

–новизна / оригинальность полученных результатов;

–глубина / полнота рассмотрения темы;

–доказательная база / аргументированность / убедительность / обоснованность

выводов;

–логичность / структурированность / целостность выступления;

–речевая культура (стиль изложения, ясность, четкость, лаконичность, красота языка, учет аудитории, эмоциональный рисунок речи, доходчивость, пунктуальность, невербальное сопровождение, оживление речи афоризмами, примерами, цитатами и т.д.);

–используются ссылки на информационные ресурсы (сайты, литература);

–наглядность / презентабельность (если требуется);

–самостоятельность суждений / владение материалом / компетентность.

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Для повышения объективности оценки собеседование может проводиться группой преподавателей/экспертов. Критерии оценки результатов

собеседования зависят от того, каковы цели поставлены перед ним и, соответственно, бывают разных видов:

- индивидуальное (проводит преподаватель);
- групповое (проводит группа экспертов);
- ориентировано на оценку знаний
- ситуационное, построенное по принципу решения ситуаций.

Критерии оценки при собеседовании:

- глубина и систематичность знаний;
- адекватность применяемых знаний ситуации;
- рациональность используемых подходов;
- степень проявления необходимых качеств;
- умение поддерживать и активизировать беседу;
- проявленное отношение к определенным.

Письменная форма приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе. Письменные работы могут включать: диктанты, контрольные работы, эссе, рефераты, курсовые работы, отчеты по практикам, отчеты по научно-исследовательской работе студентов.

Контрольная работа - средство проверки умений применять полученные знания для решения задач определенного типа по теме, разделу или всей дисциплины. Контрольная работа – письменное задание, выполняемое в течение заданного времени (в условиях аудиторной работы – от 30 минут до 2 часов, от одного дня до нескольких недель в случае внеаудиторного задания). Как правило, контрольная работа предполагает наличие определенных ответов и решение задач.

Критерии оценки выполнения контрольной работы:

- соответствие предполагаемым ответам;
- правильное использование алгоритма выполнения действий (методики, технологии и т.д.);
- логика рассуждений;
- неординарность подхода к решению;
- правильность оформления работы.

Реферат–продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения.

Критерии оценки (собственно текста реферата и защиты):

- информационная достаточность;
- соответствие материала теме и плану;
- стиль и язык изложения (целесообразное использование терминологии, пояснение новых понятий, лаконичность, логичность, правильность применения и оформления цитат и др.);
- наличие выраженной собственной позиции;
- адекватность и количество использованных источников (7 –10);
- владение материалом.

Эссе-средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме. Особенность эссе от реферата в том, что это – самостоятельное сочинение-размышление студента над научной проблемой, при использовании идей, концепций, ассоциативных образов из других областей наук и, искусства, собственного опыта,

общественной практики и др. Эссе может использоваться на занятиях (тогда его время ограничено в зависимости от целей от 5 минут до 45 минут) или внеаудиторно.

Критерии оценки:

–наличие логической структуры построения текста (вступление с постановкой проблемы; основная часть, разделенная по основным идеям; заключение с выводами, полученными в результате рассуждения);

–наличие четко определенной личной позиции по теме эссе;

–адекватность аргументов при обосновании личной позиции;

–стиль изложения (использование профессиональных терминов, цитат, стилистическое построение фраз, и т.д.);

–эстетическое оформление работы (аккуратность, форматирование текста, выделение и т.д.).

Курсовой проект/работа является важным средством обучения и оценивания образовательных результатов. Выполнение курсового проекта/работы требует не только знаний, но и многих умений, являющихся компонентами как профессиональных, так и общекультурных компетенций (самоорганизации, умений работать с информацией (в том числе, когнитивных умений анализировать, обобщать, синтезировать новую информацию), работать сообща, оценивать, рефлексировать).

Критерии оценки содержания и результатов курсовой работы могут различаться в зависимости от ее характера:

–реферативно-теоретические работы – на основе сравнительного анализа изученной литературы рассматриваются теоретические аспекты по теме, история вопроса, уровень разработанности проблемы в теории и практике, анализ подходов к решению проблемы с позиции различных теорий и т.д.;

–практические работы – кроме обоснований решения проблемы в теоретической части необходимо привести данные, иллюстрацию практической реализации теоретических положений на практике (проектные, методические, дидактические и иные разработки);

–опытно-экспериментальные работы – предполагается проведение эксперимента и обязательный анализ результатов, их интерпретации, рекомендации по практическому применению.

Примерные критерии оценивания курсовых работ/проектов складываются из трех составных частей:

1)оценка процесса выполнения проекта, осуществляемая по контрольным точкам, распределенным по времени выполнения проекта (четыре контрольные точки или еженедельно), проводится по критериям:

–умение самоорганизации, в том числе, систематичность работы в соответствии с планом,

–самостоятельность,

–активность интеллектуальной деятельности,

–творческий подход к выполнению поставленных задач,

–умение работать с информацией,

–умение работать в команде (в групповых проектах);

2) оценка полученного результата (представленного в пояснительной записке):

–конкретность и ясность формулировки цели и задач проекта, их соответствие теме;

–обоснованность выбора источников (полнота для раскрытия темы, наличие новейших работ

–журнальных публикаций, материалов сборников научных трудов и т.п.);

–глубина/полнота/обоснованность раскрытия проблемы и ее решений;

–соответствие содержания выводов заявленным в проекте целям и задачам;

–наличие элементов новизны теоретического или практического характера;

–практическая значимость; оформление работы (стиль изложения, логичность, грамотность, наглядность представления информации

–графики, диаграммы, схемы, рисунки, соответствие стандартам по оформлению текстовых и графических документов);

3) оценки выступления на защите проекта, процедура которой имитирует процесс профессиональной экспертизы:

–соответствие выступления заявленной теме, структурированность, логичность, доступность, минимальная достаточность;

–уровень владения исследуемой темой (владение терминологией, ориентация в материале, понимание закономерностей, взаимосвязей и т.д.);

–аргументированность, четкость, полнота ответов на вопросы;

–культура выступления (свободное выступление, чтение с листа, стиль подачи материала и т.д.).

Тестовая форма - позволяет охватить большое количество критериев оценки и допускает компьютерную обработку данных. Как правило, предлагаемые тесты оценки компетенций делятся на психологические, квалификационные (в учебном процессе эту роль частично выполняет педагогический тест) и физиологические.

Современный тест, разработанный в соответствии со всеми требованиями теории педагогических измерений, может включать задания различных типов (например, эссе или сочинения), а также задания, оценивающие различные виды деятельности учащихся (например, коммуникативные умения, практические умения).

В обычной практике применения тестов для упрощения процедуры оценивания как правило используется простая схема:

–отметка «3», если правильно выполнено 50 –70% тестовых заданий;

–«4», если правильно выполнено 70 –85 % тестовых заданий;

–«5», если правильно выполнено 85 –100 % тестовых заданий.

Параметры оценочного средства

Предел длительности контроля	30 мин.
Предлагаемое количество заданий из одного контролируемого подэлемента	40, согласно плана
Последовательность выборки вопросов из каждого раздела	Определенная по разделам, случайная внутри раздела
Критерии оценки:	Выполнено верно заданий
«5», если	(85-100)% правильных ответов
«4», если	(70-85)% правильных ответов
«3», если	(50-70)% правильных ответов

Промежуточная аттестация – это элемент образовательного процесса, призванный определить соответствие уровня и качества знаний, умений и навыков обучающихся, установленным требованиям согласно рабочей программе дисциплины. Промежуточная аттестация осуществляется по результатам текущего контроля.

Конкретный вид промежуточной аттестации по дисциплине определяется рабочим учебным планом и рабочей программой дисциплины.

Зачет, как правило, предполагает проверку усвоения учебного материала практических и семинарских занятий, выполнения лабораторных, расчетно-проектировочных и расчетно-графических работ, курсовых проектов (работ), а также проверку результатов учебной, производственной или преддипломной практик. Зачет, как правило, выставляется без опроса студентов по результатам контрольных работ, рефератов, других работ выполненных студентами в течение семестра, а также по результатам текущей успеваемости на семинарских занятиях, при условии, что итоговая

оценка студента за работу в течение семестра (по результатам контроля знаний) больше или равна 60%. Оценка, выставляемая за зачет, может быть как качественной типа (по шкале наименований «зачтено»/ «не зачтено»), так и количественной (т.е. дифференцированный зачет с выставлением отметки по шкале порядка - «отлично», «хорошо» и т.д.).

Экзамен, как правило, предполагает проверку учебных достижений обучаемых по всей программе дисциплины и преследует цель оценить полученные теоретические знания, навыки самостоятельной работы, развитие творческого мышления, умения синтезировать полученные знания и их практического применения.

Экзамен в устной форме предполагает выдачу списка вопросов, выносимых на экзамен, заранее (в самом начале обучения или в конце обучения перед сессией). Экзамен включает, как правило, две части: теоретическую (вопросы) и практическую (задачи, практические задания, кейсы и т.д.). Для подготовки к ответу на вопросы и задания билета, который студент вытаскивает случайным образом, отводится время в пределах 30 минут. После ответа на теоретические вопросы билета, как правило, ему преподаватель задает дополнительные вопросы. Компетентностный подход ориентирует на то, чтобы экзамен обязательно включал деятельностный компонент в виде задачи/ситуации/кейса для решения.

В традиционной системе оценивания именно экзамен является наиболее значимым оценочным средством и решающим в итоговой отметке учебных достижений студента. В условиях балльно-рейтинговой системы балльный вес экзамена составляет 25 баллов.

По итогам экзамена, как правило, выставляется оценка по шкале порядка: «отлично»- 21-25 баллов; «хорошо»- 17,5-21 балл; «удовлетворительно»- 12,5-17,5 баллов; «неудовлетворительно»- 0-12,5 баллов.

6. Материалы для оценки знаний, умений, навыков и (или) опыта деятельности

Полный комплект оценочных средств для оценки знаний, умений и навыков находится у ведущего преподавателя.

1. Тестовые задания (предоставляются в полном объеме).

2. Типовые контрольные задания (предоставляются варианты заданий контрольных работ, расчетно-графических работ, индивидуальных домашних заданий, курсовых работ и проектов, темы эссе, докладов, рефератов).

3. Комплект билетов (предусматриваются для дисциплин формой промежуточной аттестации которых является экзамен).