МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.В.06 Информационная безопасность

Направление подготовки: 380401 "Экономика"
Профиль подготовки: Магистерская программа "Экономическая безопасность"
Квалификация (степень) выпускника: магистр

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

ПК-5 - способностью самостоятельно осуществлять подготовку заданий и разрабатывать проектные решения с учетом фактора неопределенности, разрабатывать соответствующие методические и нормативные документы, а также предложения и мероприятия по реализации разработанных проектов и программ

Знать:

Этап 1: методы оценки защищенности информационной системы предприятия;

Этап 2: методы поддержки принятия решения по обоснованию сер защиты информации на предприятии.

Уметь:

Этап 1: формировать комплекс мероприятий по снижению информационных рисков;

Этап 2: анализировать уровень защищенности ИС предприятия;

Владеть:

Этап 1: общего порядка организации защиты информации на предприятии.

Этап 2: методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.

ПК-7 - способностью разрабатывать стратегии поведения экономических агентов на различных рынках

Знать:

Этап 1: требования к системам информационной инфраструктуры предприятия и критически важным информационным системам.

Этап 2: расширенную структуру информационного законодательства по обеспечению информационной безопасности;

Уметь:

Этап 1: строить модель угроз и нарушителя;

Этап 2: рассчитывать вероятность реализации угроз.

Владеть:

Этап 1: общего порядка организации защиты информации на предприятии.

Этап 2: методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях..

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**	**Способы оценки**
ОПК-3 - способностью принимать организационно-управленческие решения	Этап 1: теоретические и практические основы обеспечения экономической безопасности различных экономических систем	Этап 1: выявлять, анализировать и оценивать угрозы экономической безопасности различных экономических систем	Этап 1: подходами к анализу экономических процессов и тенденций

ПК-9 – способностью анализировать и использовать различные источники информации для проведения экономических расчетов	Этап 1. требования к системам информационной инфраструктуры предприятия и критически важным информационным систем	Этап 1. строить модель угроз и нарушителя	Этап 1. общего порядка организации защиты информации на предприятии

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
ОПК-3 - способностью принимать организационно-управленческие решения	Этап 2: внешние и внутренние источники угроз экономической безопасности	Этап 2: определять взаимоотношение и взаимосвязь уровней системы экономической безопасности.	Этап 2: методами и подходами к формированию мероприятий по снижению угроз и разработке предложений по повышению уровня экономической безопасности различных экономических систем.
ПК-9 – способностью анализировать и использовать различные источники информации для проведения экономических расчетов	Этап 2.расширенную структуру информационного законодательства по обеспечению информационной безопасности.	Этап 2.рассчитывать вероятность реализации угроз.	Этап 2.методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.

2. Шкала оценивания.

Университет использует систему оценок соответствующего государственным регламентам в сфере образования и позволяющую обеспечивать интеграцию в международное образовательное пространство. Система оценок и описание систем оценок представлены в таблицах 2 и 3.

Таблица 3 –Система оценок

Диапазон	**Экзамен**	**Зачет**

оценки, в баллах	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)		Не зачтено
[33,3;50)	**FX** – (2+)	неудовлетворительно – (2)	
[0;33,3)	**F** – (2)		

Таблица 4 - Описание системы оценок.

ECTS	Описание оценок	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.	
C	**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)**
D	**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)**

E	**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.	**неудовлетворительно (незачтено)**
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.	

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.

Таблица 5 - ОПК-3 - способностью принимать организационно-управленческие решения
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: теоретические и практические основы обеспечения экономической безопасности различных экономических систем	1. Доступ к информации это: a)процесс сбора, накопления, обработки, хранения, распределения и поиска информации; b)преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; c)получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; d)совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям; e)деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

	2. Защита информации от утечки это деятельность по предотвращению: a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c)воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d)неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e)несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 3.Защита информации от несанкционированного воздействия это деятельность по предотвращению: a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c)воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d)неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e)несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
Уметь: выявлять, анализировать и оценивать угрозы экономической безопасности различных экономических систем	4.Защита информации от непреднамеренного воздействия это деятельность по предотвращению: a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c)воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

	d)неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e)несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 5.Защита информации от разглашения это деятельность по предотвращению: a)получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b)воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c)воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d)неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e)несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
Навыки: подходами к анализу экономических процессов и тенденций	6.Защита информации от несанкционированного доступа это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 7. Субъект доступа к информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установ-

	ленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах.

Таблица 6 - ОПК-3 - способностью принимать организационно-управленческие решения.
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: внешние и внутренние источники угроз экономической безопасности	1. Носитель информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 2. Собственник информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 3 Владелец информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и про-

	цессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах.
Уметь: определять взаимоотношение и взаимосвязь уровней системы экономической безопасности.	4. Пользователь (потребитель) информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 5. Естественные угрозы безопасности информации вызваны: a) деятельностью человека; b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; d) корыстными устремлениями злоумышленников; e) ошибками при действиях персонала. 6. Искусственные угрозы безопасности информации вызваны: a) деятельностью человека; b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; d) корыстными устремлениями злоумышленников; e) ошибками при действиях персонала.
Навыки: методами и подходами к формированию мероприятий по снижению угроз и разработке предложений по по-	7. К основным непреднамеренным искусственным угрозам АСОИ относится: a) физическое разрушение системы путем взрыва, поджога и т.п.; b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; c) изменение режимов работы устройств или программ, забастов-

вышению уровня экономической безопасности различных экономических систем.	ка, саботаж персонала, постановка мощных активных помех и т.п.; d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; e) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы. 8. К основным непреднамеренным искусственным угрозам АСОИ относится: a) физическое разрушение системы путем взрыва, поджога и т.п.; b) неправомерное отключение оборудования или изменение режимов работы устройств и программ; c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

Таблица 7 – ПК-9 способностью анализировать и использовать различные источники информации для проведения экономических расчетов. 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: требования к системам информационной инфраструктуры предприятия и критически важным информационным системам	1. Доступ к информации это: a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации; b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям; e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё. 2. Защита информации от утечки это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств инфор-

	мационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 3.Защита информации от несанкционированного воздействия это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
Уметь: строить модель угроз и нарушителя	4.Защита информации от непреднамеренного воздействия это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 5.Защита информации от разглашения это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а

	также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
Навыки: общего порядка организации защиты информации на предприятии	6.Защита информации от несанкционированного доступа это деятельность по предотвращению: a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации. 7. Субъект доступа к информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах.

Таблица 8 - ПК-9 способностью анализировать и использовать различные источники информации для проведения экономических расчетов. Этап 2

Наименование знаний, умений, навыков и (или) опыта дея-	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности

тельности	
Знать расширенную структуру информационного законодательства по обеспечению информационной безопасности	1. Носитель информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 2. Собственник информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 3 Владелец информации это: a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах.
Уметь: рассчитывать	4. Пользователь (потребитель) информации это:

вероятность реализации угроз	a) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов; b) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации; c) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением; d) субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами; e) участник правоотношений в информационных процессах. 5.Естественные угрозы безопасности информации вызваны: a) деятельностью человека; b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; d) корыстными устремлениями злоумышленников; e) ошибками при действиях персонала. 6. Искусственные угрозы безопасности информации вызваны: a) деятельностью человека; b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; d) корыстными устремлениями злоумышленников; e) ошибками при действиях персонала.
Навыки: методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.	7. К основным непреднамеренным искусственным угрозам АСОИ относится: a) физическое разрушение системы путем взрыва, поджога и т.п.; b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; e) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы. 8. К основным непреднамеренным искусственным угрозам АСОИ относится: a) физическое разрушение системы путем взрыва, поджога и т.п.; b) неправомерное отключение оборудования или изменение режимов работы устройств и программ; c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

	d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; e) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи.

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

В процессе изучения дисциплины предусмотрены следующие формы контроля: текущий, промежуточный контроль (*зачет, экзамен*), 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 аудиторные занятия.

Текущий контроль успеваемости может проводиться в следующих формах:

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

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

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 практические и семинарских занятий, выполнения лабораторных, расчетно-проектировочных и расчетно-графических работ, курсовых проектов (работ), а также проверку результатов учебной, производственной или преддипломной практик. В отдельных случаях зачеты могут устанавливаться по лекционным курсам, преимущественно описательного характера или тесно связанным с производственной практикой, или имеющим курсовые проекты и работы.

Экзамен, как правило, предполагает проверку учебных достижений обучаемы 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.

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.