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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.В.09 – **Информационная безопасность**

Специальность: 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Квалификация выпускника: экономист

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

Наименование и содержание компетенции

ОК-12:
способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

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: навыками 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.

ПСК-1:
способностью осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению

Знать:
Этап 1: методы оценки защищенности информационной системы предприятия;
Этап 2: методы поддержки принятия решения по обоснованию 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-27:
способностью анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение;

Знать:
Этап 1: методы анализа результатов контроля, методы исследований причин и последствий выявленных отклонений, нарушений и недостатков;
Этап 2: методики подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.

Уметь:
Этап 1: анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков;
Этап 2: готовить предложения, направленные на устранение выявленных отклонений, нарушений и недостатков.

Владеть:

Этап 1: методами анализа результатов контроля, исследования и обобщения причин и последствий выявленных отклонений, нарушений и недостатков;
Этап 2: навыками подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.

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-12	способен работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	**Знания:** требования к системам информационной инфраструктуры предприятия и критически важным информационным системам. **Умения:** строить модель угроз и выявлять нарушителя; **Навыки:** общего порядка организации защиты информации на предприятии	Устный опрос
ПСК-1	способен осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению	**Знания:** методы оценки защищенности информационной системы предприятия; **Умения:** формировать комплекс мероприятий по снижению информационных рисков; **Навыки:** организации общего порядка защиты информации на предприятии	Устный опрос
ПК-27	способен анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить	**Знания:** методы анализа результатов контроля, методы исследований причин и последствий выявленных отклонений, нарушений и недостатков;	Устный опрос

	предложения, направленные на их устранение	**Умения** анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков; **Навыки:** подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.	

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Процедура оценивания**
1	2	3	4
ОК-12	способен работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	**Знания:** расширенную структуру информационного законодательства по обеспечению информационной безопасности; **Умения:** рассчитывать вероятность реализации угроз **Навыки:** решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.	Устный опрос
ПСК-1	способен осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению	**Знания:** методы поддержки принятия решения по обоснованию мер защиты информации на предприятии. **Умения:** анализировать уровень защищенности ИС предприятия; **Навыки:** решения задач, связанных с организацией защиты данных на	Устный опрос

		предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.	
ПК-27	способен анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение	**Знания:** методики подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков. **Умения:** готовить предложения, направленные на устранение выявленных отклонений, нарушений и недостатков. **Навыки:** подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.	Устный опрос

3. Шкалы оценивания

Университет использует шкалы оценивания, соответствующие государственным регламентам в сфере образования и позволяющие 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)		незачтено
[33,3;50)	**FX** – (2+)	неудовлетворительно – (2)	
[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.	
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.	

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 5 - ОК-12**: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации**
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. Содержанием информационной безопасности являются:** А) целостность, доступность и конфиденциальность информации Б) конфиденциальность информации В) целостность, доступность информации Г) доступность информации Д) доступность и конфиденциальность информации **2. Компьютерная безопасность НЕ зависит:** А) только от компьютеров Б) от поддерживающей инфраструктуры В) от обслуживающего персонала Г) от средства коммуникаций Д) от системы электроснабжения Е) от вентиляции **3. Доступность - это** А) гарантия получения требуемой информации или информационной услуги пользователем за определенное время Б) фактор времени в определении получения информации В) гарантия доступности конкретной информации только

	тому кругу лиц, для кого она предназначена Г) ошибка в управляющей программе Д) информационная система для получения определенных информационных услуг
Уметь: строить модель угроз и выявлять нарушителя;	4. Приведите определение целостности информации. 5. Приведите определение конфиденциальности информации. 6. Перечислите уровни формирования режима информационной безопасности.
Навыки: общего порядка организации защиты информации на предприятии.	7. Перечислите задачи информационной безопасности общества. 8. Перечислите уровни формирования режима информационной безопасности. 9. Перечислите классы угроз информационной безопасности.

Таблица 6 - ОК-12**: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации**

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: расширенную структуру информационного законодательства по обеспечению информационной безопасности;	**1. Случайные и преднамеренные воздействия относятся к угрозам ИБ по ...** А) по характеру воздействия Б) по расположению источника угроз В) по компонентам информационных систем Г) по составляющим информационной безопасности Д) по составу ПК **2. Угрозы, классифицируемые по расположению источника угроз, бывают …** А) внутренние и внешние Б) горизонтальные и вертикальные В) опасные и неопасные Г) государственные и негосударственные Д) вменяемые и невменяемые **3. Что НЕ относится к мотивам действия нарушителя?** А) отказы и сбои аппаратуры Б) положением В) любопытство Г) конкурентная борьба Д) уязвленное самолюбие
Уметь: рассчитывать вероятность реализации угроз.	4. Перечислите основные механизмы безопасности. 5.Дайте краткую характеристику законодательно-правового уровня. 6.Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.

Навыки: методами и навыками решения задач, связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях	7. Назовите основные принципы засекречивания информации. 8. Приведите определение конфиденциальности информации. 9. Назовите причины и источники случайных воздействий на информационные системы.

Таблица 7 - ПСК-1 - способностью осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению
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: методы оценки защищенности информационной системы	**1. Угрозы, классифицируемые по расположению источника угроз, бывают …** А) внутренние и внешние Б) горизонтальные и вертикальные В) опасные и неопасные Г) государственные и негосударственные Д) вменяемые и невменяемые 2. **Кто НЕ может выступать в качестве злоумышленника?** А) аппаратура Б) служащий В) посетитель Г) конкурент Д) наемник 3. **Что значит признак Угрозы ИБ по характеру…** А) случайные или преднамеренные, действия природного или техногенного характера Б) доступность, целостность В) целостность, конфиденциальность Г) данные, программы Д) внутри или вне рассматриваемой информационной системы
Уметь: формировать комплекс мероприятий по снижению информационных рисков.	4.Назовите причины и источники случайных воздействий на информационные системы. 5. Дайте характеристику преднамеренным угрозам. 6. Перечислите каналы несанкционированного доступа
Навыки: общего порядка организации защиты информации на предприятии.	7. Перечислите классификационные признаки компьютерных вирусов. 8. Назовите когда появился первый вирус, который самостоятельно дописывал себя в файлы? 9. Назовите характерные черты компьютерных вирусов.

Таблица 8 - ПСК-1 - способностью осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению
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: методы поддержки принятия решения по обоснованию мер защиты информации на предприятии.	**1.Конфиденциальность трафика** А) это защита информации, которую можно получить, анализируя сетевые потоки данных Б) обеспечивает защиту от несанкционированного получения информации В) подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры Г) обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети Д) используется при установлении соединения и периодически во время сеанса 2. **Конфиденциальность данных ...** А) обеспечивает защиту от несанкционированного получения информации. Б) используется при установлении соединения и периодически во время сеанса В) обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных Г) обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети Д) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки 3. **Средства защиты информации это ...** А) технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну. Б) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него В) санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну Г) совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну Д) совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей
Уметь: анализировать уровень защищенности ИС предприятия;	4.Назовите цели и задачи административного уровня обеспечения информационной безопасности. 5.Перечислите содержание административного уровня. 6.Назовите существующие показатели защищенности межсетевых экранов?
Навыки: методами и навыками решения задач,	7. Приведите основную классификацию информации. 8.Назовите признаки защищаемой информации.

связанных с организацией защиты данных на предприятиях и в организациях различных форм хозяйствования, в современных экономических условиях.	9. Перечислите классы защищенности межсетевых экранов

Таблица 9 - ПК-27 -способностью анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение;

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: методы анализа результатов контроля, методы исследований причин и последствий выявленных отклонений, нарушений и недостатков;	**1. Носители сведений, составляющих государственную тайну это ...** А) материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов Б) совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну В) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него Г) технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну Д) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности 2. **Основополагающими документами по информационной безопасности в РФ являются ..** А) конституция РФ и Концепция национальной безопасности Б) конституция РФ и Уголовный кодекс Российской Федерации В) конституция РФ и Доктрина Информационной безопасности Г) конституция РФ и Закон "Об информации, информатизации и защите информации" Д) конституция РФ 3. **Законодательно-правовой, административный (организационный), программно-технический уровни являются?**

	А) Режимами информационной безопасности. Б) Задачами информационной безопасности В) Уровнями средства защиты Г) Уровнями компьютерной безопасности Д) Уровнями информационной безопасности
Уметь: анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков;	4. Укажите какие сведения относят к сведениям особой важности»? 5.Укажите какие сведения относят к сведениям с грифом «совершенно секретно»? 6.Назовите кто может быть владельцем защищаемой информации
Навыки: анализа результатов контроля, исследования и обобщения причин и последствий выявленных отклонений, нарушений и недостатков	7.Перечислите виды ущерба при утечке сведений, составляющих государственную тайну. 8.Дайте определение понятию «государственная тайна». 9.Сформулируйте признаки стелс-вирусов.

Таблица 10 - ПК-27 -способностью анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение;

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: методики подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.	1. **К этапам жизненного цикла структурных элементов систем обработки данных относят:** А)эксплуатация Б) строительство помещений В) проектирование системы Г) монтаж и наладка оборудования Д) испытания и проверки Е) все варианты верны 2. **Формирование режима информационной безопасности зависит от таких факторов, как** А) традиций и норм поведения Б) научный потенциал страны В) степень внедрения средств информатизации в жизнь общества и экономику Г) степень внедрения средств информатизации в жизнь общества и экономику Д) общей культуры общества Е) все варианты верны 3. **Программы защиты могут быть** А) отдельные и встроенные. Б) отдельные В) встроенные Г) загружаемые и встроенные Д) загружаемые

	Е) подключаемые Ж) подключаемые и загружаемые
Уметь: готовить предложения, направленные на устранение выявленных отклонений, нарушений и недостатков.	4. Укажите структуру государственной системы информационной безопасности. 5. Перечислите основные задачи государственной системы защиты информации. 6. Дайте определение понятию «засекречивание информации».
Навыки: подготовки предложений, направленных на устранение выявленных отклонений, нарушений и недостатков.	7. Назовите службу, которая ведет общую организацию и координации работ в стране по защите информации, обрабатываемой техническими средствами. 8. Назовите субъекты информационных отношений и их роли при обеспечении информационной безопасности 9. Перечислите основные принципы засекречивания информации

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.

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 аудиторные 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.

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.

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.

Расчетно-графическая работа - средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю.

Критерии оценки:

–понимание методики и умение ее правильно применить;

–качество оформления (аккуратность, логичность, для чертежно-графических работ соответствие требованиям единой системы конструкторской документации);

–достаточность пояснений.

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	45 мин.
Предлагаемое количество заданий из одного контролируемого подэлемента	30, 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. 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 квалитативного типа (по шкале наименований «зачтено»/ «не зачтено»), так и квантитативного (т.н. дифференцированный зачет с выставлением отметки по шкале порядка - «отлично, «хорошо» и т.д.)

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.

6.1. Тестовые задания

1. Содержанием информационной безопасности являются:

А) конфиденциальность информации
Б) целостность, доступность и конфиденциальность информации
В) целостность, доступность информации
Г) доступность информации
Д) доступность и конфиденциальность информации

2. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации называют

А) конфиденциальностью информации
Б) защитой информации
В) информационной безопасностью
Г) доступностью информации
Д) содержанием информационной безопасности

3. Какое определение информационной безопасности дано НЕ верно?

А) информационная безопасность характеризует состояние конфиденциальности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства

Б) свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя

В) информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства

Г) это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации

4. Решение проблемы информационной безопасности начинается с..

А) выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем

Б) выявления объектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем

В) выявления конфиденциальной информации
Г) выявления ценной информации для субъектов информационных отношений
Д) выявления интересов владельца информации

5. Какое из высказываний НЕ верно?

А) задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться

Б) задачи по обеспечению информационной безопасности для разных категорий субъектов одинаковы

В) информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации - это принципиально более широкое понятие

Г) информационная безопасность есть составная часть информационных технологий - области, развивающейся беспрецедентно высокими темпами

Д) в области информационной безопасности важны не столько отдельные решения, сколько механизмы генерации новых решений

6. Компьютерная безопасность НЕ зависит:

А) от поддерживающей инфраструктуры
Б) только от компьютеров
В) от обслуживающего персонала
Г) от средства коммуникаций
Д) от системы электроснабжения
Е) от вентиляции

7. Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением задачи:

А) Обеспечением конфиденциальности информации
Б) Обеспечением доступности информации
В) Обеспечением доступности информации, целостности информации и конфиденциальности информации
Г) Обеспечением целостности, конфиденциальности информации
Д) Обеспечением доступности

8. Доступность - это

А) гарантия получения требуемой информации или информационной услуги пользователем за определенное время
Б) фактор времени в определении получения информации
В) гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена
Г) ошибка в управляющей программе
Д) информационная система для получения определенных информационных услуг

9. Что является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.?

А) Доступность и целостность
Б) Безопасность
В) Конфиденциальность
Г) Целостность
Д) Конфиденциальность и доступность

10. Целостность - это

А) гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений
Б) предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации
В) включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др
Г) гарантия получения требуемой информации или информационной услуги пользователем за определенное время
Д) самый проработанный у нас в стране аспект информационной безопасности

11. Конфиденциальной информацией в организациях может быть…

А) юридические сведения об организации
Б) программный продукт
В) анкетные данные сотрудников

Г) анкетные данные клиентов

Д) технология производства, программный продукт, анкетные данные сотрудников и др.

12. Какое из высказываний НЕ верно?

А) нарушение конфиденциальности приводит к раскрытию информации

Б) нарушение доступности приводит к отказу в доступе к информации

В) нарушение целостности приводит к фальсификации информации

Г) нарушение любой из трех категорий не приводит к нарушению информационной безопасности в целом

Д) нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом.

13. Что является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств обработки информации?

А) информационная безопасность.

Б) нарушитель информационной безопасности

В) защита конфиденциальной информации

Г) целостность информации

Д) доступность информации

14. В каком документе не дается определение информационной безопасности?

А) Закон РФ "Об информации, информационных технологиях и о защите информации".

Б) Закон РФ "Об участии в международном информационном обмене"

В) Доктрина информационной безопасности Российской Федерации

Г) Концепция информационной безопасности сетей связи общего пользования Российской Федерации

Д) Закон РФ "Об участии в международном информационном обмене" и Концепция информационной безопасности сетей связи общего пользования Российской Федерации

15. Какое из высказываний НЕ верно?

А) Под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности

Б) Понятие "информационная безопасность" можно заменять термином "компьютерная безопасность"

В) Роль доступности информации особенно проявляется в разного рода системах управления

Г) Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками

Д) Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени

16. Какое из высказываний НЕ верно?

А) Конфиденциальная информация есть только в государственных организациях

Б) Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т. д.

В) Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности

Г) Нарушение конфиденциальности приводит к раскрытию информации

Д) Современное общество все более приобретает черты информационного общества

17. Какое из высказываний НЕ верно?

А) практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями

Б) выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности

В) нарушение целостности приводит к отказу в доступе к информации

Г) статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации

Д) доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности

18. Какое из высказываний НЕ верно?

А) Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем

Б) В ряде случаев понятие "информационная безопасность" подменяется термином "компьютерная безопасность". В этом случае информационная безопасность рассматривается очень узко

В) Согласно определению, компьютерная безопасность зависит только от компьютеров

Г) Согласно ГОСТу 350922-96 защита информации - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Д) Нарушение доступности приводит к отказу в доступе к информации

19. Целостность информации условно подразделяется на:

А) статическую и динамическую

Б) первичную и вторичную

В) полную и частичную

Г) частную и общую

Д) государственную и индивидуальную

20. Основной задачей информационной безопасности НЕ является:

А) защита конституционных прав граждан на тайну переписки, переговоров, личную тайну

Б) защита государственной тайны

В) защита прав граждан на владение, распоряжение и управление принадлежащей им информацией

Г) защита прав предпринимателей при осуществлении ими коммерческой деятельности

Д) защита прав граждан на владение, распоряжение и управление не принадлежащей им информацией

21. Выделяют уровни формирования режима информационной безопасности:

А) законодательный, правовой, технический

Б) организационный, програмно-технический

В) законодательно-правовой, административный, программно-технический

Г) административный и законодательный

Д) законодательно-правовой и програмно-технический

22. Программно-технический уровень включает подуровни:

А) физический, аппаратный и программный

Б) физический и программный

В) физический, технический

Г) физический, технический и аппаратный

Д) аппаратный и программный

23. Средства защиты каких подуровней непосредственно связаны с системой обработки информации?

А) физического и технического

Б) аппаратного и программного

В) физического и аппаратного

Г) технического и аппаратного

Д) физического, технического и программного

24. Программы защиты могут быть

А) загружаемые

Б) отдельные

В) встроенные

Г) загружаемые и встроенные

Д) отдельные и встроенные

Е) подключаемые

Ж) подключаемые и загружаемые

25. Формирование режима информационной безопасности зависит от таких факторов, как

А) традиций и норм поведения

Б) научный потенциал страны

В) степень внедрения средств информатизации в жизнь общества и экономику

Г) степень внедрения средств информатизации в жизнь общества и экономику

Д) общей культуры общества

Е) все варианты верны

26. Какое утверждение НЕ верно?

А) информационная безопасность предполагает, как минимум, обеспечение одной ее составляющей

Б) административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации

В) программно-технический уровень включает три подуровня

Г) законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных от-

ношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус

Д) понятие "компьютерная безопасность" подходит под определение информационной безопасности в узком смысле

27. Какое утверждение НЕ верно?

А) Программно-технический уровень включает комплекс взаимокоординируемых мероприятий и технических мер

Б) Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов

В) Одна из основных задач информационной безопасности это защита государственной тайны

Г) Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации

Д) Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний

28. Какое из утверждений НЕ верно?

А) Выделяют пять уровней формирования режима информационной безопасности

Б) Задачей информационной безопасности является защита технических и программных средств информатизации от преднамеренных воздействий

В) Рассматривая проблему информационной безопасности в широком смысле речь идет об информационной безопасности всего общества и его жизнедеятельности

Г) Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной

Д) Информационная безопасность предполагает обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных

29. Задачами информационной безопасности в узком смысле являются:

А) защита конституционных прав граждан на тайну переписки, переговоров, личную тайну

Б) защита государственной тайны

В) защита прав граждан на владение, распоряжение и управление принадлежащей им информацией

Г) защита прав предпринимателей при осуществлении ими коммерческой деятельности

Д) нет верного ответа

30. Какое из утверждений НЕ верно?

А) информационная безопасность = компьютерная безопасность

Б) выделяют три уровня формирования режима информационной безопасности

В) примером морально-этических норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США

Г) организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла

Д) физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам

6.2 Типовые контрольные задания

1. Приведите определение целостности информации.

2. Приведите определение конфиденциальности информации.

3. Перечислите задачи информационной безопасности общества.

4. Перечислите уровни формирования режима информационной безопасности.

5. Дайте краткую характеристику законодательно-правового уровня.

6. Укажите, какие подуровни включает программно-технический уровень?

7. Перечислите, что включает административный уровень.

8. Перечислите основные механизмы безопасности.

9. Перечислите и охарактеризуйте межсетевые экраны

10. Перечислите классы удаленных угроз

Разработал(а): _____ О.Я. Набокина