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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.В.11 Технические средства безопасности объектов

Направление подготовки 27.03.04 Управление в технических системах

Профиль подготовки Интеллектуальные системы обработки информации и управления

Квалификация 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 жизнедеятельности
Знать:
Этап 1: Принципы действия основных применяемых средств охраны
Этап 2: Структура систем документационного обеспечения;
Уметь:
Этап 1: Умения освоения новых образцов программных, технических средств и информационных технологий
Этап 2: Анализировать и оценивать угрозы безопасности объекта
Владеть:
Этап 1: Навыки работы с новой литературой по освоению новых образцов программных, технических средств
Этап 2: Типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования

Наименование и содержание компетенции
ОПК-8 - способностью использовать нормативные документы в своей деятельности
Знать:
Этап 1: Структуру систем документационного обеспечения
Этап 2: Новые образцы технических средств информационных технологий
Уметь:
Этап 1: Пользоваться научно-технической и справочной литературой для решения прикладных задач,
Этап 2: Умения классификации новых образцов программных, технических средств и информационных технологий
Владеть:
Этап 1: Поиском информации и выполнять аналитического исследования по определенной теме.
Этап 2: Навыками внедрения полученных знаний в профессиональной деятельности.

Наименование и содержание компетенции
ПК-21 - способностью выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов
Знать:
Этап 1: Основные руководящие документы в области технических средств охраны объектов
Этап 2: Основные понятия и методы в области управления службой безопасности предприятия
Уметь:
Этап 1: Организовывать работу по техническим средствам охраны объектов
Этап 2: Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Владеть:
Этап 1: Рассчитывать необходимое количество и расположение средств охранной сигнализации
Этап 2: Навыками анализа методов и средств передачи, хранения и обработки данных, применения средств охраны от негативных воздействий.

1. 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
1	2	3	4
ОК-4 - способностью использовать основы правовых знаний в различных сферах жизнедеятельности	способность использовать основы правовых знаний в различных сферах жизнедеятельности	**Знать:** Принципы действия основных применяемых средств охраны **Уметь:** Умения освоения новых образцов программных, технических средств и информационных технологий **Владеть:** Навыками работы с новой литературой по освоению новых образцов программных, технических средств	индивидуальный устный опрос, практическое решение задач, тестирование.
ОПК-8 - способностью использовать нормативные документы в своей деятельности	способность использовать нормативные документы в своей деятельности	**Знать:** Структуру систем документационного обеспечения **Уметь:** Пользоваться научно-технической и справочной литературой для решения прикладных задач, **Владеть:** Навыки внедрения полученных знаний в профессиональной деятельности	индивидуальный устный опрос, практическое решение задач, тестирование.
ПК-21 - способностью выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов	способность выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов	**Знать:** Основные понятия и методы в области управления службой безопасности предприятия **Уметь:** Организовывать работу по техническим средствам охраны объектов **Владеть:** Рассчитывать необходимое количество и расположение средств охранной сигнализации	индивидуальный устный опрос, практическое решение задач, тестирование.

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
1	2	3	4
ОК-4 - способностью использовать основы правовых знаний в различных сферах жизнедеятельности	способность использовать основы правовых знаний в различных сферах жизнедеятельности	**Знать:** Структура систем документационного обеспечения **Уметь:** Анализировать и оценивать угрозы безопасности объекта **Владеть:** Типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования	индивидуальный устный опрос, практическое решение задач, тестирование.
ОПК-8 - способностью использовать нормативные документы в своей деятельности	способность использовать нормативные документы в своей деятельности	**Знать:** Новые образцы технических средств информационных технологий **Уметь:** Умения классификации новых образцов программных, технических средств и информационных технологий **Владеть:** Поиском информации и выполнять аналитического исследования по определенной теме.	индивидуальный устный опрос, практическое решение задач, тестирование.
ПК-21 - способностью выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов	способность выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов	**Знать:** Основные руководящие документы в области технических средств охраны объектов **Уметь:** Организовывать работу по техническим средствам охраны объектов **Владеть:** Навыками анализа методов и	индивидуальный устный опрос, практическое решение задач, тестирование.

		средств передачи, хранения и обработки данных, применения средств охраны от негативных воздействий.	

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 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	**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 - ОК-4 - способностью использовать основы правовых знаний в различных сферах жизнедеятельности. 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: Принципы действия основных применяемых средств охраны	1. Комплексная система безопасности объекта 2. Структура технических средств охраны 3. Категорирование объектов охраны
Уметь: Навыками работы с новой литературой по освоению новых образцов программных, технических средств	4. Требования и нормы, используемые при организации охраны объекта. 5. Укрепленность зданий и помещений
Навыки: Умения освоения новых образцов программных, технических средств и информационных технологий	6. Линейные характеристики звукового поля 7. Энергетические характеристики звукового поля

Таблица 6 - ОПК-8 - способностью использовать нормативные документы в своей 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: Структуру систем документационного обеспечения	1.Структура технических средств охраны
Уметь: Навыки внедрения полученных знаний в профессиональной деятельности	1.Категорирование объектов охраны
Навыки: Пользоваться научно-технической и справочной литературой для решения прикладных задач	1. Требования и нормы, используемые при организации охраны объекта

Таблица 7 - ПК-21 - способностью выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов. 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: Рассчитывать необходимое количество и расположение средств охранной сигнализации	1. Характеристики помещения 2. Технические средства охранной и тревожной сигнализации 3. Извещатели охраны периметра. 4. Извещатели охраны помещений
Уметь: Организовывать работу по техническим средствам охраны объектов	7. Радиоволновые извещатели. 8. Извещатели разбития стекла
Навыки: Основные понятия и методы в области управления службой безопасности предприятия	9. Приемно-контрольные приборы 10. Системы охранного телевидения

Таблица 8 - ОК-4 - способностью использовать основы правовых знаний в различных сферах жизнедеятельности. 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: Типовыми приемами проектирования, инструментарием для документирования проектных решений, методами прямого и обратного проектирования	1. Скрытые проявлениям вирусного заражения: 1. Наличие на рабочем столе подозрительных ярлыков 2. Наличие в оперативной памяти подозрительных процессов 3. Наличие на компьютере подозрительных файлов 4. Подозрительная сетевая активность 5. Неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт 6. Неожиданное уведомление антивирусной программы об обнаружении вируса
Уметь: Анализировать и оценивать угрозы безопасности объекта .	2. К классу условно опасных относятся программы … 1. О которых нельзя однозначно сказать, что они вредоносны 2. Последствия выполнения которых нельзя предугадать 3. Которые можно выполнять только при наличии установленного антивирусного программного обеспечения 4. Характеризующиеся способностью при срабатывании заложенных в них выполнять какоелибо действие, например, удаление файлов, в остальное время они безвредны.
Навыки: Структура	3. Документ, определивший важнейшие сервисы безопасности и

систем документационного обеспечения .	предложивший метод классификации информационных систем по требованиям безопасности 1. Рекомендации X.800 2. Оранжевая книга Закону «Об информации, информационных технологиях и о защите информации»

Таблица 9 - ОПК-8 - способностью использовать нормативные документы в своей 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
Знать: Новые образцы технических средств информационных технологий	1. Технические средства охранной и тревожной сигнализации 2. Определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Уметь: Поиском информации и выполнять аналитического исследования по определенной теме.	3. Частотный диапазон и спектры 4. Определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения безопасности
Навыки: Умения классификации новых образцов программных, технических средств и информационных технологий	5. Навыками проведения экспертной оценки уровня безопасности систем; 6. Современным аппаратом для количественной и качественной оценки результатов аудита, комплексами средств

Таблица 10 - ПК-21 - способностью выполнять задания в области сертификации технических средств, систем, процессов, оборудования и материалов. 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: Основные руководящие документы в области технических средств охраны объектов	1. Содержание управленческой работы руководителя подразделения службы безопасности предприятия; 2. Организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты технических средств;
Уметь: Организовывать работу по техническим средствам охраны объектов .	3. Формулировать и настраивать политику безопасности 4. Анализировать и оценивать безопасности объекта, применять отечественные и зарубежные стандарты в области безопасности объекта
Навыки: Навыками анализа методов и средств передачи, хранения и обработки данных, применения средств охра-	5. Методами расчета и инструментального контроля показателей технической защиты 6. Применять действующую законодательную базу в области обеспечения безопасности

ны от негативных воздействий.	

4. 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 9. 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
1	**2**	**3**
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Проверка конспектов лекций, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Проверка: устных ответов на вопросы в ходе семинарских занятий; тестирование; индивидуальное собеседование, письменных ответов на вопросы, контрольных тестовых заданий
Самостоятельная работа (выполнение индивидуальных, дополнительных и творческих заданий)	Знания, умения и навыки, сформированные во время самоподготовки	Проверка индивидуальных домашних заданий, вопросов, выносимых на самостоятельное изучение, тестирование,

Таблица 10. 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
1	**2**	**3**
Лекционное занятие (посещение лекций)	Знание теоретического материала по пройденным темам	Проверка конспектов лекций, тестирование
Выполнение практических (лабораторных) работ	Основные умения и навыки, соответствующие теме работы	Проверка: устных ответов на вопросы в ходе семинарских занятий; тестирование; индивидуальное собеседование, письменных ответов на вопросы, контрольных тестовых заданий
Самостоятельная работа	Знания, умения и навыки,	Проверка индивидуальных

(выполнение индивидуальных, дополнительных и творческих заданий)	сформированные во время самоподготовки	домашних заданий, вопросов, выносимых на самостоятельное изучение, тестирование,
Промежуточная аттестация	Знания, умения и навыки соответствующие изученной дисциплине	Экзамен или зачет с учетом результатов текущего контроля, в традиционной форме или компьютерное тестирование

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, доклад по результатам самостоятельной работы и т.д.);
- письменная (письменный опрос, выполнение письменных работ, запланированных в РПД и т.д.);
- тестовая (письменное или 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 систематизированно 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 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 препо-

давателей/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 написание конспектов семинарских занятий, вопросов, выносимых на самостоятельное изучение, выполнение индивидуальных домашних заданий.

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.

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.

Тестовая форма - позволяет охватить большое количество критериев оценки и допускает компьютерную обработку данных. Как правило, предлагаемые тесты делятся на тесты открытого и закрытого типов, на определение соответствия и выявление хронологической последовательности.

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

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.

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

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

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).

Тестовые задания

№1 Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, нежелательных программ вообще и восстановления зараженных такими программами файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

1. Antivirus Kaspersky
2. DrWeb
3. Avast Nod 32

№2 Сервисы безопасности это

1. Обеспечение безопасного восстановления
2. Инверсия паролей
3. Контроль целостности
4. Регулирование конфликтов
5. Шифрование
6. Кэширование записей
7. Экранирование

№3 Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на еѐ функционирование

1. Активная
2. Умышленная
3. Пассивная

№4 Основные угрозы конфиденциальности информации

1. Блокирование
2. Маскарад
3. Злоупотребления полномочиями
4. Переадресовка
5. Перехват данных

№5 Элементы знака охраны авторского права

1. Года первого выпуска программы
2. Наименование охраняемого объекта
3. Наименования (имени) правообладателя

№6 Суть компрометации информации

1. Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
2. Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
3. Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неѐ , либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений в начало

№7 Преднамеренная угроза безопасности информации

1. Ошибка разработчика
2. Наводнение
3. Повреждение кабеля, по которому идет передача,
4. В связи с погодными условиями
5. Кража

№8 Основные угрозы доступности информации

1. Отказ программного и аппаратно обеспечения
2. Перехват данных
3. Непреднамеренные ошибки пользователей
4. Злонамеренное изменение данных
5. Разрушение или повреждение помещений

№9 Причины возникновения ошибки в данных

1. Использование недопустимых методов анализа данных
2. Ошибка при записи результатов измерений в промежуточный документ
3. Ошибки при переносе данных с промежуточного документа в компьютер
4. Неустранимые причины природного характера
5. Преднамеренное искажение данных

№10 Под угрозой удаленного администрирования в компьютерной сети понимается угроза

1. Несанкционированного управления удаленным компьютером
2. Внедрения агрессивного программного кода в рамках активных объектов Web-страниц
3. Вмешательства в личную жизнь
4. Перехвата или подмены данных на путях транспортировки
5. Поставки неприемлемого содержания

№11 Защита информации обеспечивается применением антивирусных средств?

1. Да

2. Не всегда
3. Нет

№12 Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

1. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом
2. МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
3. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

№13 Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она

1. Способна противостоять только информационным угрозам, как внешним так и внутренним
2. Способна противостоять только внешним информационным угрозам
3. С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на еè функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
4. С одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

№14 Наиболее эффективное средство для защиты от сетевых атак

1. Посещение только «надè жных» Интернет-узлов
2. Использование антивирусных программ
3. Использование только сертифицированных программ-броузеров при доступе к сети Интернет
4. Использование сетевых экранов или «firewall»

№15 RAID-массив это

1. Набор жестких дисков, подключенных особым образом
2. Антивирусная программа
3. Вид хакерской утилиты
4. База защищенных данных Брандмауэр

№16 Отметьте составные части современного

1. Модем
2. Принтер
3. Сканер
4. Межсетевой экран
5. Монитор

№17 Вредоносные программы – это

1. Шпионские программы
2. Программы, наносящие вред данным и программам, находящимся на компьютере
3. Антивирусные программы
4. Программы, наносящие вред пользователю, работающему на зараженном компьютере
5. Троянские утилиты и сетевые черви

№18 К вредоносным программам относятся

1. Потенциально опасные программы
2. Вирусы, черви, трояны
3. Шпионские и рекламмные программы
4. Вирусы, программы-шутки, антивирусное программное обеспечение
5. Межсетевой экран, брандмауэр

№19 Сетевые черви это

1. Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
2. Вирусы, которые проникнув на компьютер, блокируют работу сети
3. Вирусы, которые внедряются в документы под видом макросов
4. Хакерские утилиты управляющие удаленным доступом компьютера
5. Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

№20 Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется

1. Загрузочный вирус
2. Макровирус
3. Троян
4. Сетевой червь
5. Файловый вирус

№21 Руткит – это Вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю Разновидность межсетевого экрана

1. Программа использующая для распространения Рунет (Российскую часть Интернета)
2. Вредоносная программа, маскирующаяся под макрокоманду
3. Программа для скрытого взятия под контроль взломанной системы

№22 Компьютерные вирусы это

1. Вредоносные программы, наносящие вред данным.
2. Программы, уничтожающие данные на жестком диске
3. Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.
4. Программы, заражающие загрузочный сектор дисков и препядствующие загрузке компьютера
5. Это скрипты, помещенные на зараженных интернет-страничках

№2 3 Вирус внедряется в исполняемые файлы и при их запуске активируется- это.

1. Загрузочный вирус
2. Макровирус
3. Файловый вирус
4. Сетевой червь
5. Троян

№2 4 Вирус поражающий документы называется

1. Троян
2. Файловый вирус
3. Макровирус

4. Загрузочный вирус
5. Сетевой червь

№25 Суть компрометации информации

1. Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
2. Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
3. Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неѐ , либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

№26 Методы повышения достоверности входных данных

1. Замена процесса ввода значения процессом выбора значения из предлагаемого множества
2. Отказ от использования данных
3. Проведение комплекса регламентных работ
4. Использование вместо ввода значения его считывание с машиночитаемого носителя
5. Введение избыточности в документ первоисточник
6. Многократный ввод данных и сличение введенных значений

№27 К формам защиты информации не относится…

1. Аналитическая
2. Правовая
3. Организационно-техническая
4. Страховая

№28 Информация, составляющая государственную тайну не может иметь гриф…

1. «для служебного пользования»
2. «секретно»
3. «совершенно секретно»
4. «особой важности»

№29 Разделы современной криптографии:

1. Симметричные криптосистемы
2. Криптосистемы с открытым ключом
3. Системы электронной подписи
4. Управление паролями
5. Управление ключами

№30 Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности

3. Рекомендации X.800
4. Оранжевая книга Закону «Об информации, информационных технологиях и о защите информации»

№31 Утечка информации – это …

1. Несанкционированный процесс переноса информации от источника к злоумышленнику
2. Процесс раскрытия секретной информации

3. Процесс уничтожения информации
4. Непреднамеренная утрата носителя информации

№32 Концепция системы защиты от информационного оружия не должна включать…

1. Средства нанесения контратаки с помощью информационного оружия
2. Механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
3. Признаки, сигнализирующие о возможном нападении
4. Процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

№33 В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации реализацию права на доступ к информации»
2. Соблюдение норм международного права в сфере информационной безопасности выявление нарушителей и привлечение их к ответственности
3. Соблюдение конфиденциальности информации ограниченного доступа разработку методов и усовершенствование средств информационной безопасности

№34 Сигнатурный метод антивирусной проверки заключается в …

1. Анализе поведения файла в разных условиях сравнении файла с известными образцами вирусов
2. Отправке файлов на экспертизу в компанию-производителя антивирусного средства
3. Анализе кода на предмет наличия подозрительных команд

№35 Косвенное проявление наличия вредоносной программы на компьютере

1. Неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
2. Неожиданно появляющееся всплывающее окно с текстом порнографического содержания
3. Неожиданное отключение электроэнергии
4. Неожиданное уведомление антивирусной программы об обнаружении вируса Неожиданное самопроизвольное завершение работы почтового агента

№36 Антиспамовая программа, установленная на домашнем компьютере, служит для …

1. Корректной установки и удаления прикладных программ
2. Обеспечения регулярной доставки антивирусной программе новых антивирусных баз
3. Защиты компьютера от хакерских атак
4. Защиты компьютера от нежелательной и/или незапрошенной корреспонденции

№37 Положения, которые целесообразно вынести в инструкцию по работе за компьютером, разрабатываемую для компьютерного класса средней школы

1. Не открывать почтовые сообщения от незнакомых отправителей
2. Перед работой (копированием, открытие, запуском) с файлами, размещенными на внешнем носителе (компакт-диск, дискета, флеш-накопитель) нужно проверить их на отсутствие вирусов
3. Перед работой с любым объектом, загруженным из Интернета, его следует проверить на вирусы
4. При работе в Интернет не соглашаться на предложения загрузить и/или установить неизвестную программу
5. Не открывать почтовые сообщения, содержащие вложения
6. Не пользоваться определенными видами браузеров

№38 Цель создания анонимного SMTP-сервера – для …

1. Размещения на них сайтов с порнографической или другой запрещенной информацией
2. Рассылки спама
3. Создания ботнета
4. Распределенных вычислений сложных математических задач

№39 Метаморфизм – это …

1. Метод маскировки от антивирусов с помощью шифрования
2. Метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки
3. Создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд
4. Создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд

№40 Деятельность клавиатурных шпионов

1. Находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают своему хозяину
2. Находясь в оперативной памяти следят за вводимой информацией. Как только пользователь вводит некое кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
3. Находясь в оперативной памяти следят за вводимой пользователем информацией и по команде хозяина производят нужную ему замену одних символов (или групп символов) другими Передают хозяину марку и тип используемой пользователем клавиатуры

№41 Обязательные свойства любого современного антивирусного комплекса

1. Не мешать выполнению основных функций компьютера
2. Не занимать много системных ресурсов
3. Не занимать канал Интернет
4. Надежно защищать от вирусов
5. Быть кроссплатформенным (работать под управлением любой операционной системы)
6. Интегрироваться в браузер

№42 Задача, выполняющая модуль планирования, входящий в антивирусный комплекс

1. Настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)
2. Определения параметров взаимодействия различных компонентов антивирусного комплекса
3. Определения областей работы различных задач поиска вирусов
4. Настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса

№43 Логические бомбы относятся к классу …

1. Файловых вирусов
2. Макровирусов
3. Сетевых червей
4. Троянов
5. Условно опасных программ

№44 К какому типу использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к методам антивирусной защиты.

1. Теоретическим
2. Практическим
3. Организационным
4. Техническим

№45 Использование брандмауэров относят к методам антивирусной защиты.

1. Теоретическим
2. Практическим
3. Организационным
4. Техническим

№46 Свойство вируса, позволяющее называться ему загрузочным – способность

1. Заражать загрузочные сектора жестких дисков
2. Заражать загрузочные дискеты и компакт-диски
3. Вызывать перезагрузку компьютера-жертвы
4. Подсвечивать кнопку Пуск на системном блоке

№47 К классу условно опасных относятся программы …

5. О которых нельзя однозначно сказать, что они вредоносны
6. Последствия выполнения которых нельзя предугадать
7. Которые можно выполнять только при наличии установленного антивирусного программного обеспечения
8. Характеризующиеся способностью при срабатывании заложенных в них выполнять какоелибо действие, например, удаление файлов, в остальное время они безвредны.

№48 Типы методов антивирусной защиты

1. Теоретические
2. Практические
3. Организационные
4. Технические

5. Программные

№49 Главное преимущество встроенного в Microsoft Windows брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами

1. Более ясный и интуитивно понятный интерфейс
2. Отсутствие необходимости отдельно покупать его и устанавливать
3. Наличие более полного функционала
4. Возможность более точно задавать исключения

№50 Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет

1. Трудности с регулярным автоматическим получением новых антивирусных баз Невозможность использовать антиспамовую программу в режиме реального времени
2. Ложные срабатывания в работе персонального брандмауэра
3. Невозможность запуска антивирусной проверки в режиме реального времени

№51 Брандмауэр (firewall) – это программа, …

1. Которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
2. Которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
3. На основе которой строится система кэширования загружаемых веб-страниц
4. Реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов

№52 Преимущества сигнатурного метода антивирусной проверки над эвристическим

1. Более надежный
2. Существенно менее требователен к ресурсам
3. Не требует регулярного обновления антивирусных баз
4. Позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

№ 53 Типы троянов:

1. Клавиатурные шпионы
2. Похитители паролей
3. Дефрагментаторы дисков
4. Утилиты скрытого удаленного управления
5. Логические бомбы
6. Вирусные мистификации

№54 Вирус – это программа, способная…

1. Создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению
2. Нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети

3. Нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

№25 Стадии жизненного цикла классического трояна

1. Проникновение на чужой компьютер
2. Активация
3. Поиск объектов для заражения
4. Подготовка копий
5. Внедрение копий
6. Выполнение вредоносных действий

№56 Трояны классифицируются по …

1. Методу размножения
2. Методу распространения
3. Методу маскировки
4. Типу вредоносной нагрузки

№57 Основная задача, которую решает антивирусная проверка в режиме реального времени

1. Обеспечение непрерывности антивирусной проверки
2. Обеспечение невмешательства в процесс деятельности других программ
3. Обеспечение взаимодействия между пользователем и антивирусной программой
4. Предоставление возможности глубокой проверки заданных объектов

№58 Скрытые проявлениям вирусного заражения:

7. Наличие на рабочем столе подозрительных ярлыков
8. Наличие в оперативной памяти подозрительных процессов
9. Наличие на компьютере подозрительных файлов
10. Подозрительная сетевая активность
11. Неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
12. Неожиданное уведомление антивирусной программы об обнаружении вируса

№59 Преимущества эвристического метода антивирусной проверки над сигнатурным

1. Более надежный
2. Существенно менее требователен к ресурсам
3. Не требует регулярного обновления антивирусных баз
4. Позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

№60 Подозрительная сетевая активность может быть вызвана …

1. Сетевым червем
2. P2P-червем
3. Трояном
4. Логической бомбой

Перечень вопросов для самоподготовки

1. Компьютерная информация: определение, основные категории с точки зрения безопасности
2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.
3. Политика безопасности информационных систем и ее основные элементы
4. Обзор нормативных правовых актов РФ в области информационной защиты.
5. Дискреционный и мандатный доступ к ресурсам информационных систем.
6. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы
7. Атаки типа переполнения стека
8. Основные услуги безопасности, предоставляемые информационными системами
9. Механизмы реализации услуг безопасности в информационных системах
10. Классификация криптографических алгоритмов
11. Структурная схема симметричной криптосистемы
12. Структурная схема асимметричной криптосистемы
13. Математические определения шифра, процедур шифрования и дешифрации
14. История развития криптоалгоритмов: шифр Цезаря, афинная криптосистема, шифры Виженера и Вернома
15. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы
16. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования
17. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля
18. Алгоритм шифрования TEA: структура, достоинства и недостатки
19. Алгоритм шифрования DES: структура, достоинства и недостатки
20. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB
21. Поточные шифры: принципы функционирования, структура
22. Криптоатаки на поточные шифры, построение ЛРС с последовательностями наибольшей длины
23. Методы построения нелинейных поточных шифров
24. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов
25. RSA: математические основы криптоалгоритма
26. RSA: структура криптоалгоритма
27. RSA: возможные криптоатаки и криптостойкость алгоритма
28. Алгоритм асимметричного шифрования Рабина
29. Криптосистема ЭльГемаля: структура, криптостойкость
30. Метод ключевого обмена Диффи-Хелмана
31. Асимметричные криптоалгоритмы рюкзачного типа
32. Алгоритмы генерации случайных чисел для криптоарлгоритмов,
33. Алгоритмы генерации и поверки простых чисел в современных криптосистемах

34. Хэш-функции: назначение и основные свойства
35. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров
36. Электронная цифровая подпись: назначения, структура системы ЭЦП на основе алгоритма RSA
37. Система ЭЦП на основе алгоритма ЭльГемаля
38. Система ЭЦП на основе эллиптических кривых
39. Криптосистема: структура, основные функции
40. Современные схемы разделения ключей
41. Сертификация открытых ключей. Структура сертификата. Инфраструструктура PKI.
42. Иерархическая и сетевая модели сертификации открытых ключей.
43. Роль сжатия информации в криптосистемах. Алгоритм сжатия Хаффмана
44. Роль сжатия информации в криптосистемах. Алгоритм сжатия Лемпела-Зива
45. Аутентификация в информационных системах: назначение, разновидности, угрозы подсистемам аутентификации
46. Системы аутентификации с защищенными паролями и с проверкой на стороне сервера
47. Система аутентификации по схеме «запрос-ответ»
48. Обзор современных протоколов аутентификации.
49. Обзор современных защищенных сетевых протоколов.
50. Угрозы безопасности в глобальных сетях
51. Межсетевые экраны: назначение, основные функции, состав
52. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки
53. Proxy-сервера : назначение, основные функции, достоинства и недостатки
54. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона
55. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.
56. Модель безопасности ОС Windows. Реализация дискреционной модели защиты доступа к ресурсам системы.
57. Модель безопасности ОС Windows: политика аудита.
58. Модель безопасности ОС Windows. Файловая система EFS.
59. Вредоносные программы: определение, классификация
60. Эксплойты: определение. Атаки на переполнение буфера и методы защиты от них.
61. Эксплойты: определение. SQL-инъекции и методы .защиты от них
62. Компьютерные вирусы: определение, методы заражения и маскировки. Методы защиты от вирусов.