МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Экономическая безопасность, анализ и учет»

«СОГЛАСОВАНО»
Декан факультета _____
_____/ Е.Н. Евдокимова
«28» июня 2019 г

Заведующий кафедрой_____
_____/ С.Г. Чеглакова
«28» июня 2019 г

«УТВЕРЖДАЮ»
Проректор РОПиМД
_____/А.В.Корячко
«___» _____ 2019 г

РАБОЧАЯ ПРОГРАММА

дисциплины

Б1.В.ДВ.04.01 «ЗАЩИТА ИНФОРМАЦИИ НА РЕЖИМНЫХ ОБЪЕКТАХ»

Специальность
38.05.01 Экономическая безопасность

Специализация № 2
Экономика и организация производства на режимных объектах

Уровень подготовки
специалитет

Квалификация выпускника – экономист

Формы обучения – заочная

Рязань 2019 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования

по специальности 38.05.01 Экономическая безопасность (уровень специалитета)

утвержденного Приказом Минобрнауки России от 16.01.2017 г. № 20

Разработчики

доцент кафедры ИБ  Ю.В. Конкин

Программа обсуждена и одобрена на заседании кафедры информационной безопасности «14» 06 2019 г. протокол № 12.

Зав. кафедрой ИБ
к.т.н., доцент  В.Н. Пржегорлинский

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ СПЕЦИАЛИТЕТА

Рабочая программа дисциплины «Защита информации на режимных объектах» является составной частью основной профессиональной образовательной программы (далее – ОПОП), реализуемой по специальности 38.05.01 Экономическая безопасность (уровень специалитета).

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета) [утв. Приказом Министерства образования и науки Российской Федерации от 16.01.2017 г. № 20].

Рабочая программа дисциплины предназначена для студентов, обучающихся по специализации №2 «Экономика и организация производства на режимных объектах», реализуемой по специальности 38.05.01 Экономическая безопасность (уровень специалитета).

Целью освоения дисциплины «Защита информации на режимных объектах» является формирование комплекса знаний законодательства об информатизации и защите информации, практических навыков обеспечения информационной безопасности хозяйствующих субъектов, изучение комплекса проблем информационной безопасности компьютерных систем различных типов, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны их информационных ресурсов и приобретение компетенций, необходимых выпускнику специальности 38.05.01 «Экономическая безопасность» специализации №2«Экономика и организация производства на режимных объектах» для его профессиональной деятельности и (или) обучения в аспирантуре.

Для решения поставленной цели определены следующие задачи:

- получение знаний по правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- изучение процессов сбора, передачи и накопления информации;
- ознакомление с угрозами информационной безопасности, правилами их выявления, анализа и требованиями к различным уровням обеспечения информационной безопасности.

Перечень планируемых результатов обучения по дисциплине

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ПСК-1	способность применять в профессиональной деятельности в сфере экономики и организации производства на режимных объектах знание технологий промышленного производства, а также технологий обеспечения информационной безопасности,защиты информации и секретности	Знать: основные методы, способы и средства хранения, систематизации, обработки, передачи информации; методы, средства обеспечения и стандарты защиты информации на режимных объектах. Уметь: проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач, обеспечивать защиту источников информации. Владеть: навыками работы с различными источниками информации, информационными ресурсами и технологиями, навыками обеспечения защиты источников информации.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации на режимных объектах» относится к вариативной части блока Б1 (Б1.В.ДВ.04.01) дисциплин по выбору ОПОП по специальности 38.05.01 «Экономическая безопасность».

Дисциплина изучается по заочной форме обучения на 2-м курсе.

Пререквизиты дисциплины. Для изучения дисциплины обучаемый должен

знать:

- основы алгебры, математического анализа, дискретной математики, теории вероятностей и математической статистики, информатики;

уметь:

- использовать современные технические средства и информационные технологии для решения аналитических и исследовательских задач;

владеть:

- навыками научного познания применительно к постановке и решению задач информационной безопасности.

Взаимосвязь с другими дисциплинами. Дисциплина «Защита информации на режимных объеках» логически взаимосвязана с дисциплиной Б1.Б.05 «Современные информационные системы и ресурсы в экономике.

Программа дисциплины ориентирована на возможность расширения и углубления знаний, умений и навыков студентов специалитета для успешной профессиональной деятельности.

Постреквизиты дисциплины. Компетенции, полученные в результате освоения дисциплины, необходимы обучающемуся при изучении следующих дисциплин: Б1.Б.14 «Экономическая безопасность» и других, а также при выполнении научно-исследовательской работы, прохождении производственной и преддипломной практик, подготовке к государственной итоговой аттестации.

3 ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины составляет 4 зачетных единицы (ЗЕ), или 144 часа.

Вид учебной работы	**Всего часов**	Курс 2
Всего часов	144	144
Контактная работа обучающихся с преподавателем (всего)	8	8
В том числе:		
Лекции	4	4
лабораторные работы (ЛР)	4	4
практические занятия (ПЗ)	-	-
Самостоятельная работа студентов (всего)	136	136
В том числе:		
контроль	9	9
контрольная работа	10	10
Иные виды самостоятельной работы	117	117
Форма контроля		экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

4.1 Содержание дисциплины, структурированное по темам

Раздел дисциплины	Содержание
1. Защита информации, ее составляющие и виды	Защита информации как деятельность. Виды защиты информации. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг
2. Цели и направления защиты информации	Цели защиты информации. Направления защиты информации. Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия.
3. Объекты защиты информации	Определение понятия объект защиты информации. Информация как объект защиты. Сущность и определение понятия информация как объекта защиты. Свойства информации как объективного явления. Информация как объект правовых отношений. Носитель информации как объект защиты. Определение понятия носитель информации и классификация носителей информации. Документированная информация и информационные ресурсы. Информационный процесс как объект защиты. Информационный процесс и информационная технология. Информационная система как средство реализации информационного процесса и комплексный объект защиты информации. Автоматизированная система как комплексный объект защиты информации. Определение понятия автоматизированная система. Классификация автоматизированных систем.
4. Государственная система информационной безопасности.	Законодательный уровень информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

5. Методы обеспечения информационной безопасности	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от несанкционированного доступа. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
6. Основные положения теории информационной безопасности информационных систем.	Модели безопасности и их применение. Понятие угрозы. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
7. Организационно-распорядительные документы в сфере информационной безопасности.	Политика информационной безопасности Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.
8. Комплексная защита информационной инфраструктуры и ресурсов.	Оценка эффективности системы защиты информации. Архитектура защищенных экономических систем. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем. Защита информационной инфраструктуры от атак. Антивирусные средства защиты.

4.2 Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

Заочная форма обучения

Тема	**Общая трудоемкость, всего часов**	**Контактная работа обучающихся с преподавателем**				**Самостоятельная работа обучающихся**
		Всего	**Лекции**	**Практические занятия,**	**Лабораторные работы**	
1. Защита информации, ее составляющие и виды	19	2	2	-	-	17
2. Цели и направления защиты информации	17	-	-	-	-	17
3. Объекты защиты информации	21	4	2	-	2	17
4. Государственная система информационной безопасности	17	-	-	-	-	17
5. Методы обеспечения информационной безопасности	17	-	-	-	-	17
6. Основные положения теории информационной безопасности информационных систем	19	2	-	-	2	17
7. Организационно-распорядительные документы в сфере информационной	17	-	-	-	-	17

безопасности						
8. Комплексная защита информационной инфраструктуры и ресурсов	17	-	-	-	-	17
Всего:	**144**	**8**	**4**	**-**	**4**	**136**

Виды практических лабораторных и самостоятельных работ

Тема	Вид работы	Наименование и содержание работы	Трудоемкость, часов
Тема 1. Защита информации, ее составляющие и виды	Самостоятельная работа	Изучение конспекта лекций Изучение литературы Подготовка к экзамену Выполнение заданий контрольной работы	6 8 1 2
Тема 2. Цели и направления защиты информации	Самостоятельная работа	Изучение литературы Подготовка к экзамену Выполнение заданий контрольной работы	14 1 2
Тема 3. Объекты защиты информации	Лабораторные работы	Настройка локальной политики безопасности Windows 7	2
	Самостоятельная работа	Изучение конспекта лекций Изучение литературы. Подготовка к выполнению и защите лабораторной работы Подготовка к экзамену Выполнение заданий контрольной работы	4 3 7 1 2
Тема 4. Государственная система информационной безопасности	Самостоятельная работа	Изучение литературы Подготовка к экзамену Выполнение заданий контрольной работы	13 2 2
Тема 5. Методы обеспечения информационной безопасности	Самостоятельная работа	Изучение литературы Подготовка к экзамену Выполнение заданий контрольной работы	14 1 2
Тема 6. Основные положения теории информационной безопасности информационных систем	Лабораторные работы	Создание и управление учетными записями пользователей	2
	Самостоятельная работа	Изучение литературы Подготовка к выполнению и защите лабораторной работы Подготовка к экзамену	9 7 1
Тема 7. Организационно-распорядительные документы в сфере информационной безопасности	Самостоятельная работа	Изучение литературы Подготовка к экзамену	16 1
Тема 8. Комплексная защита информационной инфраструктуры и ресурсов	Самостоятельная работа	Изучение литературы Подготовка к экзамену	16 1

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Бабаев С.И. Сети ЭВМ и телекоммуникаций: Учеб. пособие / РГРТУ. - Рязань 2014 - 80с.
2. Колесенков А.Н., Конкин Ю.В. Основы сетевых технологий: учеб. пособие / РГРТУ. - Рязань 2015 - 65 с.
3. Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И Компьютерные сети: метод. указ к лаб. работам / РГРТУ. - Рязань, 2015. – 80с.

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств приведен в Приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Защита информации на режимных объектах»).

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная учебная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. – Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с. – Режим доступа : http://www.iprbookshop.ru/29257.
2. Ветров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.
3. Соколов, М. С.Информация как объект информационной безопасности [Электронный ресурс] / М.С. Соколов // Закон и право. – 2013. – № 12. – С. 27-33. – Режим доступа : http://elibrary.ru/item.asp?id=20780302
4. Бабаев С.И. Сети ЭВМ и телекоммуникаций: Учеб. пособие / РГРТУ. - Рязань 2014 - 80с.
5. Колесенков А.Н., Конкин Ю.В. Основы сетевых технологий: учеб. пособие / РГРТУ. - Рязань 2015 - 65 с.
6. Пржегорлинский В.Н., Бабаев С.И., Калинкина Т.И Компьютерные сети: метод. указ к лаб. работам / РГРТУ. - Рязань, 2015. – 80с.

Дополнительная учебная литература

1. Кияев В., Граничин О. Безопасность информационных систем: курс.- Национальный Открытый Университет «ИНТУИТ», 2016 г. - 192 с.
2. Кузнецов И. Н. Бизнес-безопасность. - Издательско-торговая корпорация «Дашков и К°», 2016 г. - 416 с.
3. Балдин К. В., Уткин В. Б. Информационные системы в экономике: учебник. - Издательско-торговая корпорация «Дашков и К°», 2017 г. - 395 с.
4. Загинайлов Ю. Н. Основы информационной безопасности : учебное пособие. - Директ-Медиа, 2015 г. - 105 с.
5. Лапина М. А., Ревин А. Г., Лапин В. И. Информационное право: учебное пособие.- Юнити-Дана, 2015 г. - 336 с.
6. Хаулет Т. Инструменты безопасности с открытым исходным кодом. - Национальный Открытый Университет «ИНТУИТ», 2016 г. – 566 с.
7. Лапонина О. Р. Криптографические основы безопасности. - Национальный Открытый Университет «ИНТУИТ», 2016 г. - 244 с.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Обучающимся предоставлена возможность индивидуального доступа к следующим электронно-библиотечным системам:

Электронно-библиотечная система «IPRbooks», режим доступа – с любого компьютера РГРТУ без пароля, из сети интернет по паролю. – URL: https://iprbookshop.ru/.

9. Методические указания для обучающихся по освоению дисциплины

Рекомендации по планированию и организации времени, необходимого для изучения дисциплины

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Изучение конспекта лекции в тот же день, после лекции (10 – 15 минут).

Изучение конспекта лекции за день перед следующей лекцией (10 – 15 минут).

Изучение теоретического материала по учебнику и конспекту (1 час в неделю).

Описание последовательности действий студента («сценарий изучения дисциплины»)

При изучении дисциплины рекомендуется самостоятельно изучать материал, который еще не прочитан на лекции и не применялся на лабораторном занятии. Тогда лекция будет гораздо понятнее. Но легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий.

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10 – 15 минут).

2. При подготовке к лекции следующего дня нужно просмотреть текст предыдущей лекции, подумать о том, какой может быть тема следующей лекции (10 – 15 минут).

В течение недели выбрать время (1 час) для работы с литературой.

Рекомендации по работе с литературой

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта изучаются и книги по теории принятия решений. Литературу по дисциплине необходимо читать только в бумажном (не в электронном) виде. Полезно использовать несколько учебников и пособий по дисциплине. Рекомендуется после изучения очередного параграфа ответить на несколько вопросов по данной теме. Кроме того, полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): «о чем этот параграф?», «какие новые понятия введены, каков их смысл?».

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При проведении занятий по дисциплине используются следующие информационные технологии:

– удаленные информационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством информационной образовательной среды ФГБОУ ВО «РГРТУ», позволяющие осуществлять оперативный контроль графика выполнения и содержания образовательного процесса, решение организационных вопросов, консультирование;

– доступ к современным профессиональным базам данных (в том числе международным реферативным базам данных научных изданий) и информационным справочным системам.

Перечень лицензионного программного обеспечения:

Название ПО	№ лицензии	Количество мест
Операционная система Windows	номер подписки 700102019	бессрочно
Kaspersky Endpoint Security	№2922-190228-101204-557-1191	На 1000
Mozilla Firefox	свободно распространяемая	без ограничений
Adobe Acrobat Reader	свободно распространяемая	без ограничений
LibreOffice	свободно распространяемая	без ограничений
OpenOffice	свободно распространяемая	без ограничений
7Zip-Manager	свободно распространяемая	без ограничений

Перечень информационных справочных систем:

1. Справочная правовая система КонсультантПлюс [Электронный ресурс]. – URL: http://www.consultant.ru/online/. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный, Договор № 1342/455-10, без ограничений.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

№ п/п	Наименование специальных помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного обеспечения и информационных справочных систем
1	Ауд. № 337 (здание учебно-административного корпуса) Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	компьютерная техника (1ПК) Компьютер Intel, мультимедийное оборудование: Проектор Epson EB-X12 специализированная мебель: 100 стульев, 50 столов компьютерная техника (1ПК)	1.Операционная система семейства Windows (Microsoft Imagint, номер подписки 700102019 (бессрочно). 2. Лицензия на право использования Kaspersky Endpoint Security для бизнеса на 1000 рабочих посадочных мест (Коммерческая лицензия на 1000 компьютеров №2922-190228-101204-557-1191 с 28.02.2019 по 07.03.2021). 3. 7Zip-manager – свободное ПО, 4. LibreOffice - свободное ПО
2	№ 270 (здание учебно-административного корпуса) Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, лабораторных работ, практических и самостоятельных занятий	Ноутбук Acer Aspire ИБП 1025 VA Принтер HP LaserJet P2015n Манипулятор МЦ0000010244 Система активной защиты. Генератор шума SEL SP-21 «Баррикада» Виброакустический электромагнитный излучатель SEL SP-55/V Проектор Epson EN-TW420 Интерактивная доска Hitachi FX Шкаф металлический КБ-010 Доска вращающаяся 44 места	1.Операционная система семейства Windows (Microsoft Imagint, номер подписки 700102019 (бессрочно). 2. Kaspersky Endpoint Security (Коммерческая лицензия на 1000 компьютеров №2922-190228-101204-557-1191 с 28.02.2019 по 07.03.2021). 3. 7Zip-manager – свободное ПО, 4. OpenOffice - свободное ПО, 5. LibreOffice - свободное ПО
3	№ 266 (здание учебно-административного корпуса) Учебная лаборатория, оснащенная лабораторным оборудованием, для проведения лабораторных работ, практических и самостоятельных занятий,	Анализатор спектра GSP-827 Анализатор спектра ANRITSU Комплекс средств для пров. измерений Rohde Генератор сигналов НМ8135 Приемник сканирующий IC-PCR2500 для ПК Прибор нелинейной радиолокации «Люкс» Изделие «Шиповник-2» Штатив диэлектрический ШД-1 Антенна дополнительная для УЗ «Соната-Р2» ПЭВМ System Biock ПЭВМ System Biock ИБП IMP-625AP Устройство защиты «Соната-	1.Операционная система семейства Windows (Microsoft Imagint, номер подписки 700102019 (бессрочно). 2. Kaspersky Endpoint Security (Коммерческая лицензия на 1000 компьютеров №2922-190228-101204-557-1191 с 28.02.2019 по 07.03.2021). 3. 7Zip-manager – свободное ПО, 4. OpenOffice - свободное ПО, 5. LibreOffice - свободное ПО

		Р2» Шкаф металлический КБ-010 Стол компьютерный 70х70 Столы - 12 шт. Доска магнитно-маркерная 120х250 см 16 мест	
4	№ 501 к.2 (здание лабораторного корпуса) Аудитория для самостоятельной работы	25 компьютеров (компьютерный класс) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду РГРТУ, Компьютеры Intel, специализированная мебель: 25 стульев, 13 столов	1.Операционная система семейства Windows (Microsoft Imagint, номер подписки 700102019 (бессрочно). 2. Kaspersky Endpoint Security (Коммерческая лицензия на 1000 компьютеров №2922-190228-101204-557-1191 с 28.02.2019 по 07.03.2021). 3. Справочно-правовая система «Консультант Плюс» - договор об информационной поддержке № 1342/455-100 от 28.10.2011г. 4. 7Zip-manager – свободное ПО, 5. OpenOffice - свободное ПО, 6. LibreOffice - свободное ПО

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 38.05.01 Экономическая безопасность (квалификация выпускника – специалист, форма обучения – очная, срок обучения – 5 лет).

Разработчики

доцент кафедры ИБ _____ Ю.В. Конкин

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Экономическая безопасность, анализ и учет»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.ДВ.04.01 «ЗАЩИТА ИНФОРМАЦИИ НА РЕЖИМНЫХ ОБЪЕКТАХ»

Специальность
38.05.01 Экономическая безопасность

Специализация № 2
Экономика и организация производства на режимных объектах

Уровень подготовки
специалитет

Квалификация выпускника – экономист

Формы обучения – заочная

Рязань 2019 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (практических заданий, описаний форм и процедур проверки), предназначенных для оценки качества освоения обучающимися данной дисциплины как части ОПОП.

Цель – оценить соответствие знаний, умений и владений, приобретенных обучающимся в процессе изучения дисциплины, целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций.

Контроль знаний обучающихся проводится в форме промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена. Форма проведения экзамена - тестирование, письменный опрос по теоретическим вопросам и выполнение практических заданий.

2 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

3) эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Уровень освоения компетенций, формируемых дисциплиной:

Описание критериев и шкалы оценивания тестирования:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100%
2 балла (продвинутый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84%
1 балл (пороговый уровень)	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69%
0 баллов	уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49%

Описание критериев и шкалы оценивания теоретического вопроса:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя
2 балла (продвинутый уровень)	выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов
1 балл (пороговый уровень)	выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя
0 баллов	выставляется студенту, который не смог ответить на вопрос

Описание критериев и шкалы оценивания практического задания:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

Описание критериев оценки контрольной работы

Домашняя контрольная работа по заочной форме обучения, признанная рецензентом удовлетворительной, оценивается словом «зачтено». В зачтенной работе допускаются следующие недочеты:

- незначительные ошибки, описки;
- неправильное оформление титульного листа, списка используемой литературы,

Домашняя контрольная работа признается рецензентом неудовлетворительной и оценивается словом «незачтено». Основания для незачета контрольной работы:

- неправильные, неточные и неконкретные ответы на поставленные вопросы;
- несамостоятельный характер выполнения контрольной работы;
- описательный характер ответа на сравнительно-аналитические вопросы, отсутствие необходимых объяснений и ответов;
- фактические ошибки, допущенные при ответе на вопросы;
- неправильное, небрежное оформление работы, наличие значительного количества грамматических ошибок.

На промежуточную аттестацию (экзамен, зачет) выносится тест, два теоретических вопроса и 2 задачи. Максимально студент может набрать 15 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется студенту, который набрал в сумме 15 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «хорошо» выставляется студенту, который набрал в сумме от 10 до 14 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме от 5 до 9 баллов при условии выполнения всех заданий на уровне не ниже порогового. Обязательным условием является выполнение всех предусмотренных в течение семестра практических заданий.

Оценка «неудовлетворительно» выставляется студенту, который набрал в сумме менее 5 баллов или не выполнил всех предусмотренных в течение семестра практических заданий.

3 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1. Защита информации, ее составляющие и виды	ПСК-1	Экзамен

2. Цели и направления защиты информации	ПСК-1	Экзамен
3. Объекты защиты информации	ПСК-1	Экзамен
4. Государственная система информационной безопасности	ПСК-1	Экзамен
5. Методы обеспечения информационной безопасности	ПСК-1	Экзамен
6. Основные положения теории информационной безопасности информационных систем	ПСК-1	Экзамен
7. Организационно-распорядительные документы в сфере информационной безопасности	ПСК-1	Экзамен
8. Комплексная защита информационной инфраструктуры и ресурсов	ПСК-1	Экзамен

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация в форме экзамена

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ПСК-1	способность применять в профессиональной деятельности в сфере экономики и организации производства на режимных объектах знание технологий промышленного производства, а также технологий обеспечения информационной безопасности, защиты информации и секретности

Типовые тестовые вопросы:

1. Что относится к физическим средствам защиты информации?
   - средства, которые реализуются в виде автономных устройств и систем;
   - устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
   - программы, предназначенные для выполнения функций, связанных с защитой информации;
   - средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

2. Что относится к техническим средствам защиты информации?
   - средства, которые реализуются в виде автономных устройств и систем;
   - устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;
   - это программы, предназначенные для выполнения функций, связанных с защитой информации;
   - средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

3. Что такое несанкционированный доступ?
   - доступ субъекта к объекту в нарушение установленных в системе правил разгра-

ничения доступа;
- создание резервных копий в организации;
- правила и положения, выработанные в организации для обхода парольной защиты;
- вход в систему без согласования с руководителем организации;
- удаление не нужной информации.

4. Что такое целостность информации?
- свойство информации, заключающееся в возможности ее изменения любым субъектом;
- свойство информации, заключающееся в возможности изменения только единственным пользователем;
- свойство информации, заключающееся в ее существовании в виде единого набора файлов;
- свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

5. Под информационной безопасностью понимают;
- защиту от несанкционированного доступа;
- защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера;
- защиту информации от компьютерных вирусов.

6. Что такое аутентификация?
- проверка количества переданной и принятой информации;
- нахождение файлов, которые изменены в информационной системе несанкционированно;
- проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа);
- определение файлов, из которых удалена служебная информация;
- определение файлов, из которых удалена служебная информация.

7. Верификация это:
- это проверка принадлежности субъекту доступа предъявленного им идентификатора;
- проверка целостности и подлинности информации, программы, документа;
- это присвоение имени субъекту или объекту.

8. Утечка информации это:
- несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;
- ознакомление постороннего лица с содержанием секретной информации;

– потеря, хищение, разрушение или неполучение переданных данных.

9. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется:

– кодируемой;
– шифруемой;
– достоверной;
– защищаемой.

10. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие – это:

– текст;
– данные;
– информация;
– пароль.

11. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется:

– угрозой;
– опасностью;
– намерением;
– предостережением.

12. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

– операционной системы, сетевого программного обеспечения;
– операционной системы, сетевого программного обеспечения и системы управления базами данных;
– операционной системы, системы управления базами данных;
– сетевого программного обеспечения и системы управления базами данных.

13. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:

– системой угроз;
– системой защиты;
– системой безопасности;
– системой уничтожения.

14. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется:

- политикой информации;
- защитой информации;
- политикой безопасности;
- организацией безопасности.

15. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

- информационная;
- техническая;
- системная;
- сетевая.

16. Что такое компьютерный вирус?

- разновидность программ, которые способны к размножению;
- разновидность программ, которые самоуничтожаются;
- разновидность программ, которые не работают;
- разновидность программ, которые плохо работают.

17. Как подразделяются вирусы в зависимости от деструктивных возможностей?

- сетевые, файловые, загрузочные, комбинированные;
- безвредные, неопасные, опасные, очень опасные;
- резидентные, нерезидентные;
- полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы.

18. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

- физического;
- организационного;
- системного;
- технического.

19. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы:

- идентификации;
- аутентификации;
- защиты данных;
- защиты от копирования.

20. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется:

- каналом несанкционированного доступа;
- каналом утечки информации;
- каналом искажения информации;
- каналом дешифрования информации.

Типовые практические задания:

Задание 1

Настройка параметров политики учетных записей операционной системы Windows7

С помощью средств ОС Windows 7 необходимо задать следующие параметры политики учетных записей:

- пользователь должен сменить минимум пять паролей, прежде чем повторно применить старый;

- после обновления пароля пользователь может его снова сменить не ранее, чем через 24 часа;

- пользователь должен менять пароль каждые три недели.

Критерии выполнения задания 1

Задание считается выполненным, если обучающийся успешно использовал для задания указанных параметров оснастку «Политика паролей» ОС Windows 7.

Задание 2

Настройка параметров политики блокировки учетных записей операционной системы Windows 7

С помощью средств ОС Windows 7 необходимо настроить параметры политики учетных записей так, чтобы:

- учетная запись пользователя блокировалась после четырех неудачных попыток войти в систему;

- продолжительность блокировки учетной записи равнялась 30 минутам;

- разблокировать учетную запись мог только администратор.

Критерии выполнения задания 2

Задание считается выполненным, если обучающийся под учетной записью «Администратор» открыл консоль «Локальная политика безопасности» и далее использовал группу «Политика учетных записей» и оснастку «Политика блокировки учетных записей» для задания указанных параметров.

Задание 3

Настройка и проверка параметров безопасности операционной системы Windows7

С помощью средств ОС Windows 7 необходимо настроить параметры политики безопасности на компьютере так, чтобы пользователи:

- при входе в систему имели возможность выключить компьютер;

- должны были нажимать <Ctrl-Alt-Delete> для входа в систему;

- не смогли увидеть в окне Windows Security имя последнего пользователя.

Критерии выполнения задания 3

Задание считается выполненным, если обучающийся под учетной записью «Администратор» открыл консоль «Локальная политика безопасности» и далее выполнил настройку указанных выше пареметров.

Задание 4

Настройка минимальной длины пароля в операционной системе Windows7

С помощью средств ОС Windows 7 необходимо для пользователя с именем user задать минимальную длину пароля не менее 6 символов.

Критерии выполнения задания 4

Задание считается выполненным, если обучающийся под учетной записью «Администратор» открыл консоль «Локальная политика безопасности», далее группе «Политика учетных записей» открыл оснастку «Политика паролей» и правой панели выделил параметр «Минимальная длина пароля» и установил для него значение 6.

Типовые теоретические вопросы:

1. Понятие защиты информации.
2. Виды защиты информации.
3. Цели защиты информации.
4. Направления защиты информации.
5. Защита информации от утечки.
6. Защита информации от несанкционированных воздействий.
7. Защита информации от непреднамеренных воздействий.
8. Понятие объект защиты информации.
9. Понятие информации как объекта защиты.
10. Информационная система как комплексный объект защиты информации.
11. Категории персональных данных.
12. Автоматизированная система как объект защиты информации.
13. Классификация автоматизированных систем.
14. Объект информатизации с точки зрения защиты информации.
15. Вредоносные воздействия на объекты.
16. Способы несанкционированное воздействие на защищаемую информацию без использования специальных средств.
17. Настройка разграничения доступа к файлу.
18. Уровни конфиденциальности и их настройка.
19. Признаки классификация информационных систем в соответствии с законодательством РФ.
20. Разделение информационных систем в зависимости от круга лиц, являющихся участниками информационного взаимодействия.

4.2. Темы контрольной работы для заочных форм обучения

1. Признаки классификации информационных систем в соответствии с законодательством РФ.
2. Разделение на классы федеральных информационных систем общего пользования.
3. Понятие корпоративной информационной системы.
4. Понятие информационной системы общего пользования.
5. Понятие информационной системы персональных данных.
6. Информационная система как комплексный объект защиты информации.
7. Понятие автоматизированной системы в защищенном исполнении.

8. Виды обеспечений комплекса средств автоматизации автоматизированной системы.

9. Требования по защите информации к автоматизированным системам, обрабатывающим персональные данные.

10. Объект информатизации с точки зрения защиты информации.

Критерии выполнения контрольной работы

Задания контрольной работы считаются выполненными, если обучающийся рассмотрел заданную тему с четом нормативно-справочные документов и стандартов.

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Экономическая безопасность, анализ и учет»

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Б1.В.ДВ.04 «ЗАЩИТА ИНФОРМАЦИИ НА РЕЖИМНЫХ ОБЪЕКТАХ»

Специальность
38.05.01 Экономическая безопасность

Специализация № 2
Экономика и организация производства на режимных объектах

Уровень подготовки
специалитет

Квалификация выпускника – экономист

Формы обучения – заочная

Рязань 2019 г

1 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Рекомендации по планированию и организации времени, необходимого для изучения дисциплины

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.

Изучение конспекта лекции за день перед следующей лекцией – не менее 10-15 минут.

Изучение теоретического материала по учебнику и конспекту – 1 час в неделю в ходе подготовки к практическому занятию.

Кроме чтения учебной литературы из обязательного списка рекомендуется активно использовать информационные ресурсы сети Интернет по изучаемой теме.

Самостоятельное изучение тем учебной дисциплины способствует:

- закреплению знаний, умений и навыков, полученных в ходе аудиторных занятий;
- углублению и расширению знаний по отдельным вопросам и темам дисциплины;
- освоению умений выявлять экономические проблемы в области современных экономических отношений;
- получению навыков прикладного и практического использования полученных знаний при оценке эффективности результатов деятельности.

Самостоятельная работа как вид учебной работы может использоваться на лекциях и практических занятиях, а также иметь самостоятельное значение – внеаудиторная самостоятельная работа обучающихся – при подготовке к лекциям, практическим занятиям, а также к экзамену.

Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение отдельных вопросов и тем дисциплины "Экономическая теория";
- подготовка к тестированию;

Описание последовательности действий студента («сценарий изучения дисциплины»)

1. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины;
2. Подготовка к практическим занятиям: необходимо изучить рекомендованные преподавателем источники (основную и дополнительную литературу, интернет-ресурсы) и выполнить подготовительные задания;
3. При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции, не применялся на практическом занятии. Тогда лекция будет гораздо понятнее. Однако легче при изучении курса следовать изложению материала на лекции.

Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к следующей лекции, нужно просмотреть текст предыдущей лекции (45-50 минут),
3. В течение периода времени между занятиями выбрать время (минимум 1 час) для самостоятельной работы, проверить термины, понятия с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на

практическом занятии.

4. Подготовка к экзамену: необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

Рекомендации по работе с литературой

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучается и дополнительная рекомендованная литература (законодательство, научные и публицистические статьи и др.). Литературу по курсу рекомендуется изучать в библиотеке или с помощь сети Интернет (источники, которые могут быть скачены без нарушения авторских прав).

Перечень основной и дополнительной литературы представлен в рабочей программе дисциплины.

Работа студента на лекции

Только слушать лекцию и записывать за лектором все, что он говорит, недостаточно. В процессе лекционного занятия студент должен выделять важные моменты, выводы, анализировать основные положения. Прослушанный материал лекции студент должен проработать. От того, насколько эффективно он это сделает, зависит и прочность усвоения знаний, и, соответственно, качество восприятия предстоящей лекции, так как он более целенаправленно будет ее слушать. Необходим систематический труд в течение всего семестра.

При написании конспекта лекций следует придерживаться следующих правил и рекомендаций:

- конспект лекций нужно записывать «своими словами» лишь после того, как излагаемый лектором тезис будет вами дослушан до конца и понят;
- при конспектировании лекции следует отмечать непонятные вопросы, записывать те пояснения лектора, которые показались особенно важными;
- при ведении конспекта лекций рекомендуется вести нумерацию тем, разделов, что позволит при подготовке к сдаче экзамена не запутаться в структуре лекционного материала;
- рекомендуется в каждом пункте выразить свое мнение, комментарий, вывод.

При изучении лекционного материала у студента могут возникнуть вопросы. С ними следует обратиться к преподавателю после лекции, на консультации, практическом занятии.

Конспект лекций каждый студент записывает лично для себя. Поэтому конспект надо писать так, чтобы им было удобно пользоваться.

Подготовка к лабораторным работам

Практические занятия существенно дополняют лекции по дисциплине. В процессе анализа и решения задач, тестов, обсуждения теоретических и практических вопросов студенты расширяют и углубляют знания, полученные из лекционного курса, учебных пособий и учебников, дистанционного учебного курса. В процессе решения задач вырабатываются навыки вычислений, работы литературой.

В часы самостоятельной работы студенты должны решать задачи, тесты, которые они не успели решить во время аудиторных занятий, а также те задачи, тесты, которые не получились дома. Отсутствие спешки на таких занятиях должно дать положительный эффект.

Подготовка к сдаче экзамена

Экзамен – форма промежуточной проверки знаний, умений, владений, степени освоения дисциплины.

Главная задача экзамена состоит в том, чтобы у студента из отдельных сведений и деталей составилось представление об общем содержании соответствующей дисциплины. Готовясь к экзамену, студент приводит в систему знания, полученные на лекциях, на практических занятиях, разбирается в том, что осталось непонятным, и тогда изучаемая им дисциплина может быть воспринята в полном объеме с присущей ей строгостью и логичностью, ее практической направленностью.

Экзамен дает возможность также выявить, умеют ли студенты использовать теоретические знания при решении задач.

На экзамене оцениваются:

- понимание и степень усвоения теории;
- методическая подготовка;
- знание фактического материала;
- знакомство с основной и дополнительно литературой, а также с современными публикациями по данному курсу;
- умение приложить теорию к практике, решать задачи, тесты, правильно проводить расчеты и т. д.;
- логика, структура и стиль ответа, умение защищать выдвигаемые положения.

Но значение экзамена не ограничивается проверкой знаний. Являясь естественным завершением работы студента, он способствует обобщению и закреплению знаний и умений, приведению их в строгую систему, а также устранению возникших в процессе занятий пробелов.

Студенту важно понять, что самостоятельность предполагает напряженную умственную работу. Невозможно предложить алгоритм, с помощью которого преподаватель сможет научить любого студента успешно осваивать дисциплину. Нужно, чтобы студент ставил перед собой вопросы по поводу изучаемого материала, которые можно разбить на две группы:

- вопросы, необходимые для осмысления материала в целом;
- текущие вопросы, которые возникают при детальном разборе материала.

Студент должен их ставить перед собой при подготовке к экзамену, и тогда на подобные вопросы со стороны преподавателя ему несложно будет ответить.

Подготовка к экзамену не должна ограничиваться беглым чтением конспекта лекций, даже, если они выполнены подробно и аккуратно. Механического заучивания также следует избегать. Более надежный и целесообразный путь – это тщательная систематизация материала при вдумчивом повторении, запоминании формулировок, увязке различных тем и разделов, закреплении путем решения задач, тестов.

Перед экзаменом назначается консультация, цель которой – дать ответы на вопросы, возникшие в ходе самостоятельной подготовки. Здесь студент имеет полную возможность получить ответ на все неясные ему вопросы. А для этого он должен проработать до консультации весь курс. Кроме того, преподаватель будет отвечать на вопросы других студентов, что будет повторением и закреплением знаний для всех студентов. Лектор на консультации, как правило, обращает внимание на те разделы, по которым на предыдущих экзаменах ответы были неудовлетворительными, а также фиксирует внимание на наиболее трудных разделах курса.

На непосредственную подготовку к экзамену обычно дается три - пять дней. Этого времени достаточно только для углубления, расширения и систематизации знаний, на устранение пробелов в знании отдельных вопросов, для определения объема ответов на каждый из вопросов программы.

Планируйте подготовку с точностью до часа, учитывая сразу несколько факторов:

- *неоднородность материала и этапов его проработки (например, на первоначальное изучение уходит больше времени, чем на повторение),*
- *свои индивидуальные способности,*
- *ритмы деятельности;*
- *привычки организма.*

Чрезмерная физическая нагрузка наряду с общим утомлением приведет к снижению интеллектуальной деятельности. Рекомендуется делать перерывы в занятиях через каждые 50-60 минут на 10 минут. После 3-4 часов умственного труда следует сделать часовой перерыв. Для сокращения времени на включение в работу целесообразно рабочие периоды делать более длительными, разделяя весь день примерно на три части – с утра до обеда, с обеда до ужина и с ужина до сна.

Подготовку к экзамену следует начинать с общего планирования своей деятельности в сессию, с определения объема материала, подлежащего проработке. Необходимо внимательно сверить свои конспекты лекций с программой, чтобы убедиться в том, все ли разделы отражены в лекциях. Отсутствующие темы законспектировать по учебнику и учебному пособию. Более подробное планирование на ближайшие дни будет первым этапом подготовки к очередному экзамену. Второй этап предусматривает системное изучение материала по данному предмету с обязательной записью всех выкладок, выводов, терминов. На третьем этапе - этапе закрепления – полезно чередовать углубленное повторение особенно сложных вопросов с беглым повторением всего материала.

2. ПРИМЕРНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2.1 ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Понятие защиты информации.
2. Виды защиты информации.
3. Цели защиты информации.
4. Направления защиты информации.
5. Защита информации от утечки.
6. Защита информации от несанкционированных воздействий.
7. Защита информации от непреднамеренных воздействий.
8. Понятие объект защиты информации.
9. Понятие информации как объекта защиты.
10. Информационная система как комплексный объект защиты информации.
11. Категории персональных данных.
12. Автоматизированная система как объект защиты информации.
13. Классификация автоматизированных систем.
14. Объект информатизации с точки зрения защиты информации.

15. Вредоносные воздействия на объекты.

16. Способы несанкционированное воздействие на защищаемую информацию без использования специальных средств.

17. Настройка разграничения доступа к файлу.

18. Уровни конфиденциальности и их настройка.

11. Признаки классификация информационных систем в соответствии с законодательством РФ.

20. Разделение информационных систем в зависимости от круга лиц, являющихся участниками информационного взаимодействия.

21 Разделение на классы федеральных информационных систем общего пользования.

22. Понятие корпоративной информационной системы.

23. Понятие информационной системы общего пользования.

24. Понятие информационной системы персональных данных.

25. Информационная система как комплексный объект защиты информации.

26. Понятие автоматизированной системы в защищенном исполнении.

27. Виды обеспечений комплекса средств автоматизации автоматизированной системы.

28. Требования по защите информации к автоматизированным системам, обрабатывающим персональные данные.