МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Информационная безопасность»

«СОГЛАСОВАНО»
Декан ИЭФ
_____ Е.Н. Евдокимова
«26» 06 2018 г.
Руководитель ОПОП
_____ С.Г. Чеглакова
«26» 06 2018 г.

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ К.В. Бухенский
«26» 06 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.3.В.06а «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Специальность
38.05.01 Экономическая безопасность

ОПОП «Экономико-правовое обеспечение экономической безопасности»

Квалификация (степень) выпускника – экономист

Форма обучения – заочная
Срок обучения – 5,5 лет

Рязань 2018

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

Рабочая программа дисциплины «Информационная безопасность» является составной частью основной профессиональной образовательной программы (далее – ОПОП) «Экономико-правовое обеспечение экономической безопасности», 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 ОПОП «Экономико-правовое обеспечение экономической безопасности», реализуемой по специальности 38.05.01 Экономическая безопасность (уровень специалитета).

Целью освоения дисциплины «Информационная безопасность» является изучение современных принципов обеспечения информационной безопасности в компьютерных системах и приобретение компетенций, необходимых выпускнику специальности 38.05.01 «Экономическая безопасность» специализации «Экономико-правовое обеспечение экономической безопасности» для его профессиональной деятельности и (или) обучения в аспирантуре.

Для решения поставленной цели определены следующие задачи:

- получение знаний по обеспечению информационной безопасности государства;
- изучение методологий создания систем защиты информации;
- изучение процессов сбора, передачи и накопления информации;
- получение знаний, необходимых для проведения оценки защищенности и обеспечения информационной безопасности компьютерных систем.

Перечень планируемых результатов обучения по дисциплине

Коды компе-тенций	Результаты освоения ОПОП Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ПК-28	Способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Знать: основные методы, способы и средства хранения, систематизации, обработки, передачи информации; методы, средства обеспечения и стандарты информационной безопасности. Уметь: проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач, обеспечивать информационную безопасность компьютерных сетей. Владеть: навыками работы с различными источниками информации, информационными ресурсами и технологиями, навыками обеспечения защиты информации в компьютерных сетях.
ПСК-3	Способность применять в профессиональной деятельности законодательство об информатизации и защите информации в целях обеспечения информационной безопасности хозяйствующих субъектов	Знать: законодательство Российской Федерации в области защиты информации. Уметь: применять действующую законодательную базу в области информационной безопасности. Владеть: навыками работы с нормативными правовыми актами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» реализуется в рамках блока № 1 дисциплин

вариативной части ОПОП «Экономико-правовое обеспечение экономической безопасности» специальности 38.05.01 Экономическая безопасность ФГБОУ ВО «РГРТУ».

Дисциплина изучается по заочной форме обучения на 2-м курсе в 4-м семестре.

Студент до начала изучения дисциплины «Информационная безопасноть» должен иметь представление о том, на каких участках своей будущей профессиональной деятельности он сможет использовать полученные им знания в рамках компетенций, обусловленных спецификой его предстоящей работы.

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 «Информационная безопасность» логически взаимосвязана с другими дисциплинами, такими как: Б1.2.Б.02 «Информационные системы в экономике», Б1.2.В.02 «Пакеты прикладных программ» и другими.

Программа курса 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: Б1.3.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 И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость (объем) дисциплины составляет 4 зачетные единицы (ЗЕ), 144 часа.

Вид учебной работы	Всего часов
	Заочная форма обучения
Общая трудоемкость дисциплины	144
1. Контактная работа обучающихся с преподавателем (всего), в том числе:	10
лекции	4
практические занятия	6
лабораторные работы	-
2. Самостоятельная работа обучающихся (всего), в том числе:	134
курсовой проект (работа)	-
подготовка к экзамену и консультации	13
контрольные работы	10
иные виды самостоятельной работы	111
Вид промежуточной аттестации обучающихся	экзамен – 4-й семестр

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 разделам (темам)

В структурном отношении содержание дисциплины представлено следующими темами:
Тема 1. Основные понятия и определения информационной безопасности.
Тема 2. Государственная система информационной безопасности.
Тема 3. Теоретические основы угроз информационной безопасности.
Тема 4. Организационно-распорядительные документы в сфере информационной безопасности.
Тема 5. Методы обеспечения информационной безопасности.
Тема 6. Управление информационными рисками.
Тема 7. Криптографические методы защиты информации.
Тема 8. Комплексная защита информационной инфраструктуры и ресурсов.

Раздел дисциплины	Содержание
Тема 1. Основные понятия и определения информационной безопасности.	Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
Тема 2. 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.
Тема 3. Теоретические основы угроз информационной безопасности.	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Понятие угрозы. Виды противников или "нарушителей". Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
Тема 4. Организационно-распорядительные документы в сфере информационной безопасности.	Политика информационной безопасности Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.
Тема 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.

Тема 6. Управление информационными рисками.	Основные понятия и определения управления информационными рисками. Технологии (методики) управления информационными рисками. Управление информационными рисками, стандарты, нормативные документы, рекомендации. Программные средства, используемые для анализа и управления рисками. Аудит безопасности и анализ информационных рисков.
Тема 7. Криптографические методы защиты информации.	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Методы криптографии. Обеспечиваемая шифром степень защиты.
Тема 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)

4.2.1. Заочная форма обучения

Тема	Общая трудо-емкость, всего часов	Контактная работа обучающихся с преподавателем			Самосто-ятельная работа обучаю-щихся
		всего	лекции	практические занятия	
Тема 1. Основные понятия и определения информационной безопасности.	15	1	0,5	0,5	14
Тема 2. Государственная система информационной безопасности.	15	1	0,5	0,5	14
Тема 3. Теоретические основы угроз информационной безопасности.	15	1	0,5	0,5	14
Тема 4. Организационно-распорядительные документы в сфере информационной безопасности.	15	1	0,5	0,5	14
Тема 5. Методы обеспечения информационной безопасности.	15,5	1,5	0,5	1	14
Тема 6. Управление информационными рисками.	15,5	1,5	0,5	1	14
Тема 7. Криптографические методы защиты информации.	15,5	1,5	0,5	1	14
Тема 8. Комплексная защита информационной инфраструктуры и ресурсов.	14,5	1,5	0,5	1	13
Всего:	**144**	**10**	**4**	**6**	**111**

Виды практических и самостоятельных работ

Тема	Вид работы*	Наименование и содержание работы	Трудо-емкость, часов
Тема 1. Основные понятия и определения информационной безопасности.	ПР	Устный опрос, решение типовых задач, тестирование	0,5
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 2. Государственная система информационной безопасности.	ПР	Устный опрос, решение типовых задач, тестирование	0,5
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 3. Теоретические основы угроз информационной безопасности.	ПР	Устный опрос, решение типовых задач, тестирование	0,5
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 4. Организационно-распорядительные документы в сфере информационной безопасности.	ПР	Устный опрос, решение типовых задач, тестирование	0,5
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 5. Методы обеспечения информационной безопасности.	ПР	Устный опрос, решение типовых задач, тестирование	1
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 6. Управление информационными рисками.	ПР	Устный опрос, решение типовых задач, тестирование	1
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14

Тема	Вид работы*	Наименование и содержание работы	Трудо-емкость, часов
Тема 7. Криптографические методы защиты информации.	ПР	Устный опрос, решение типовых задач, тестирование	1
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	14
Тема 8. Комплексная защита информационной инфраструктуры и ресурсов.	ПР	Устный опрос, решение типовых задач, тестирование	1
	СР	Изучение конспекта лекций, основной и дополнительной литературы, материалов дистанционного учебного курса, подготовка к текущему тестированию. Подготовка к лабораторным работам и практическим занятиям. Подготовка к экзамену и консультации	13

* СР – самостоятельная работа, ПР – практические занятия

Перечень тем контрольных работ

В качестве контрольной работы студентам предлагается написать реферат на одну из следующих тем:

1. Основные нормативные акты РФ, связанные с правовой защитой информации.
2. Угрозы безопасности компьютера.
3. Виды защищаемой информации.
4. Защита интеллектуальной собственности средствами патентного и авторского права.
5. Международное законодательство в области защиты информации.
6. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
7. Криптографические методы защиты информации
8. Организационные методы обеспечения информационной безопасности.
9. Экономическая разведка и промышленный шпионаж.
10. Технические средства защиты информации.
11. Инженерная защита и охрана объектов.
12. Экономическая безопасность государства.
13. Служба безопасности организации.

Студенты также могут определить тему контрольной самостоятельно в рамках предметной области дисциплины.

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.

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Оценочные материалы приведены в приложении к рабочей программе дисциплины (см. документ “Оценочные материалы по дисциплине «Информационная безопасность»).

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

а) 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. (дата обращения: 15.01.2018)
2. Бабаев С.И. Сети ЭВМ и телекоммуникаций: Учеб. пособие / РГРТУ. - Рязань 2014 - 80с.
3. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность: учеб. пособие. - М.: Форум, 2010. – 528 с.

б) дополнительная учебная литература

1. 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 (дата обращения: 15.01.2018)
2. Пржегорлинский В.Н. Объекты защиты информации : учеб. пособие. Ч.1: Элементарные объекты защиты информации / В. Н. Пржегорлинский; РГРТУ. - Рязань, 2012. - 131с.
3. Пржегорлинский В.Н. Защита информации : учеб. пособие. Ч.2 : Комплексные объекты защиты информации. Условия защиты информации / В. Н. Пржегорлинский; РГРТУ. - Рязань, 2013. - 87с.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Информационно-правовой портал ГАРАНТ.РУ [Электронный ресурс]. – URL: http://www.garant.ru.

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/.

– Электронная библиотека РГРТУ [Электронный ресурс]. – Режим доступа: из корпоративной сети РГРТУ – по паролю. – URL: http://elib.rsreu.ru/.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1. 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 – не менее 10-15 минут.

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

Изучение теоретического материала по учебнику и конспекту – не менее 1 часа в неделю.

Работа в дистанционном учебном курсе – не менее 1 часа в неделю.

9.2. Описание последовательности действий студента («сценарий изучения дисциплины»)

Рекомендуется следующим образом организовать работу, необходимую для изучения дисциплины:

1) написание конспекта лекций: основные положения, выводы, формулировки, обобщения фиксировать кратко, схематично и последовательно, а также помечать важные мысли, выделять ключевые слова, термины;

2) подготовка к практическим занятиям и лабораторным работам: 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 понятнее). Однако легче при изучении дисциплины следовать изложению материала на лекции.

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

- после лекции и окончания учебных занятий, при подготовке к занятиям следующего дня нужно сначала просмотреть и обдумать текст прослушанной лекции;
- при подготовке к следующей лекции нужно просмотреть текст предыдущей лекции;
- в течение периода времени между занятиями выбрать время для самостоятельной работы в библиотеке, проверить термины, понятия с помощью рекомендованной основной и дополнительной литературы, выписать толкования в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендованной основной и дополнительной литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии;

9.3. Рекомендации по работе с литературой

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта изучается и дополнительная рекомендованная литература. Полезно использовать несколько источников по дисциплине. Рекомендуется после изучения очередного параграфа ответить на несколько простых вопросов по данной теме. Кроме того, очень полезно мысленно задать себе вопросы по изученной теме, попробовать ответить на них. Литературу по дисциплине рекомендуется изучать в библиотеке или с помощью сети Интернет.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

В рамках реализации образовательной программы при проведении занятий по дисциплине используются следующие информационные технологии:

- удаленные информационные коммуникации между студентами и преподавателем, ведущим лекционные и практические занятия, посредством электронной почты, позволяющие осуществлять оперативный контроль графика выполнения и содержания контрольных заданий, решение организационных вопросов, удаленное консультирование;
- поиск актуальной информации для выполнения самостоятельной работы и контрольных заданий;
- доступ к информационным справочным системам;

Перечень лицензионного программного обеспечения:

- операционная система Windows;
- LibreOffice, лицензия LGPLv3.
-

Перечень профессиональных баз данных и информационных справочных систем:

- Справочная правовая система «Консультант Плюс» [Электронный ресурс]. – Режим доступа: доступ из корпоративной сети РГРТУ – свободный.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ

ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Для освоения дисциплины необходимы следующие материально-технические ресурсы:

1) аудитория РГРТУ для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная маркерной (меловой) доской;

2) аудитория РГРТУ для самостоятельной работы студентов, оснащенная компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ;

3) аудитории должны иметь достаточное количество посадочных мест, соответствовать необходимым противопожарным нормам и санитарно-гигиеническим требованиям.

Программу составил:

старший преподаватель каф. ИБ _____ /И.С. Дудко/

Программа обсуждена и одобрена на заседании кафедры ИБ, протокол № 12 от «26» 06 2018 г.

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

ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Экономическая безопасность, анализ и учет»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.3.В.06а «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Специальность
38.05.01 Экономическая безопасность

ОПОП «Экономико-правовое обеспечение экономической безопасности»

Квалификация выпускника – экономист
Форма обучения – очная

Рязань 2018

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных 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.

Промежуточная аттестация проводится в форме зачета. Форма проведения экзамена – тестирование, выполнение практического задания, ответ на теоретический вопрос.

2. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Контролируемые разделы (темы) дисциплины	***Код контролируемой компетенции (или ее части)***	**Вид, метод, форма оценочного мероприятия**
Тема 1. Основные понятия и определения информационной безопасности.	ПК-28 ПСК-3	Экзамен
Тема 2. Государственная система информационной безопасности.	ПК-28 ПСК-3	Экзамен
Тема 3. Теоретические основы угроз информационной безопасности.	ПК-28 ПСК-3	Экзамен
Тема 4. Организационно-распорядительные документы в сфере информационной безопасности.	ПК-28 ПСК-3	Экзамен
Тема 5. Методы обеспечения информационной безопасности.	ПК-28 ПСК-3	Экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции 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.

Описание критериев и шкалы оценивания:

а) 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%

б) 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

в) описание критериев и шкалы оценивания практического задания:

На экзамен выносится одно практическое задание. Максимально обучающийся может набрать 25 баллов.

Шкала оценивания	**Критерий**
3 балла (эталонный уровень)	практическое задание выполнено правильно
2 балла (продвинутый уровень)	практическое задание выполнено правильно, но имеются технические неточности в расчетах (описаниях)
1 балл (пороговый уровень)	практическое задание выполнено правильно, но с дополнительными наводящими вопросами преподавателя
0 баллов	практическое задание не выполнено или выполнено не правильно

На промежуточную аттестацию (экзамен) 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».

Шкала оценивания	**Итоговый суммарный балл**
отлично	14 баллов (эталонный уровень)
хорошо	10 – 14 баллов (продвинутый уровень)
удовлетворительно	6 – 9 баллов (пороговый уровень)
неудовлетворительно	5 баллов и ниже

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1 Промежуточная аттестация (экзамен)

Коды	**Результаты освоения ОПОП**

компетенций	Содержание компетенций
ПК-28	Способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач

а) типовые тестовые вопросы:

Требуется выбрать правильные варианты ответов.

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

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

3. Что такое несанкционированный доступ?
а) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;
б) создание резервных копий в организации;
в) правила и положения, выработанные в организации для обхода парольной защиты;
г) вход в систему без согласования с руководителем организации;
д) удаление не нужной информации.

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

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

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

7. Верификация это:
а) один из 3 вариантов ответа:
б) это проверка принадлежности субъекту доступа предъявленного им идентификатора;
в) проверка целостности и подлинности информации, программы, документа;
г) это присвоение имени субъекту или объекту.

8. Утечка информации это:

а) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;
б) ознакомление постороннего лица с содержанием секретной информации;
в) 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:
а) кодируемой;
б) шифруемой;
в) достоверной;
г) защищаемой.

10. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие – это:
а) текст;
б) данные;
в) информация;
г) пароль.

<u>б) типовые практические задания:</u>

Задание 1

Настройка параметров политики учетных записей операционной системы Windows 7

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.

<u>в) типовые теоретические вопросы:</u>

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.

Коды компетенций	Результаты освоения ОПОП Содержание компетенций
ПСК-3	Способность применять в профессиональной деятельности законодательство об информатизации и защите информации в целях обеспечения информационной безопасности хозяйствующих субъектов

а) типовые тестовые вопросы:

Требуется выбрать правильные варианты ответов.
1. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется:
а) угрозой;
б) опасностью;
в) намерением;
г) предостережением.

2. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:
а) системой угроз;
б) системой защиты;
в) системой безопасности;
г) системой уничтожения.

3. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется:
а) политикой информации;
б) защитой информации;
в) политикой безопасности;
г) организацией безопасности.

4. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?
а) информационная;
б) техническая;
в) системная;
г) сетевая.

5. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?
а) физического;
б) организационного;
в) системного;
г) технического.

6. Какие законы существуют в России в области компьютерного права?
а) о государственной тайне;
б) об авторском праве и смежных правах;

в) о гражданском долге;
г) о правовой охране программ для ЭВМ и БД;
д) о правовой ответственности;
е) об информации, информатизации, защищенности информации.

7. Какие существуют основные уровни обеспечения защиты информации?
а) законодательный;
б) административный;
в) программно-технический;
г) физический;
д) вероятностный;
е) процедурный;
ж) распределительный.

8. К видам защиты информации относятся:
а) правовые и законодательные:
б) морально-этические;
в) юридические;
г) административно-организационные.

9. Организационные угрозы подразделяются на:
а) угрозы воздействия на персонал;
б) физические угрозы;
в) действия персонала;
г) несанкционированный доступ.

10. Разновидности угроз безопасности:
а) техническая разведка;
б) программные;
в) программно-математичекие;
г) организационные;
д) технические.

<u>б) типовые практические задания:</u>
Типовые практические задания:
Задание 1
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 1
Задание считается выполненным, если обучающийся под учетной записью «Администратор» открыл консоль «Локальная политика безопасности» и далее выполнил настройку указанных выше пареметров.

Задание 2
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 2
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.

<u>в) типовые теоретические вопросы:</u>

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.