Аннотация к рабочей программе дисциплины «Основы управления информационной безопасностью»

Цель преподавания дисциплины

Дисциплина «Основы управления информационной безопасностью» является получение студентами знаний о основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

– рассмотреть основы управления информационной безопасностью;

– рассмотреть угрозы информационной безопасности в информационных системах;

– рассмотреть оценочные стандарты в информационной безопасности;

– рассмотреть стандарты управления информационной безопасностью;

– рассмотреть создание системы управления информационной безопасности на предприятии;

– рассмотреть методики и технологии управления рисками;

– рассмотреть разработку корпоративной методики анализа рисков;

– рассмотреть современные методы и средства анализа и управление рисками информационных систем компаний;

– рассмотреть правовые меры обеспечения информационной безопасности;

– рассмотрение организационных меры обеспечения безопасности компьютерных информационных систем;

– рассмотреть программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом.

Компетенции, формируемые в результате освоения дисциплины

Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7);

Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13).

Разделы дисциплины

Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах. Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью. Создание СУИБ на предприятии. Методики и технологии управления рисками. Разработка корпоративной методики анализа рисков. Современные методы и средства анализа и управление рисками информационных систем компаний. Правовые меры обеспечения информационной безопасности.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
информатики
(наименование факультета полностью)
_____Т.А. Ширабакина
(подпись, инициалы, фамилия)
«_1_» _февраля_ 2017г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

(наименование дисциплины)

направления подготовки (специальность) 10.03.01

(шифрсогласно ФГОС

«Информационная безопасность»

и наименование направления подготовки (специальности)

«Безопасность автоматизированных систем»

наименование профиля, специализации или магистерской программы

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность , одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «1» 02 2017г.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы Демченко О.А.

Согласовано:

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 25.08.2017, №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 29.06.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019, №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина «Основы управления информационной безопасностью» является получение студентами знаний о основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

−рассмотреть основы управления информационной безопасностью;

−рассмотреть угрозы информационной безопасности в информационных системах;

−рассмотреть оценочные стандарты в информационной безопасности;

−рассмотреть стандарты управления информационной безопасностью;

– рассмотреть создание системы управления информационной безопасности на предприятии;

– рассмотреть методики и технологии управления рисками;

– рассмотреть разработку корпоративной методики анализа рисков;

– рассмотреть современные методы и средства анализа и управление рисками информационных систем компаний;

– рассмотреть правовые меры обеспечения информационной безопасности;

– рассмотрение организационных меры обеспечения безопасности компьютерных информационных систем;

– рассмотреть программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом;

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

– современные подходы к управлению информационной безопасности;

– основные стандарты, регламентирующие управление информационной безопасности;

– принципы построения системы управления информационной безопасности;

уметь:

– анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;

– определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;

– используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность/

владеть:

– навыками управления информационной безопасностью простых объектов;

– терминологией и процессным подходом построения систем управления ИБ;

Процесс изучения дисциплины направлен на формирование следующих компетенций*:*

– способен использовать нормативные правовые документы в своей профессиональной деятельности;

– способен формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

– способен организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

– способен организовывать и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;

– способен администрировать подсистемы информационной безопасности объекта;

– способен выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.

У обучающихся формируются следующие компетенции:

ОПК-7 – способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-4 – способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПК-13 – способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам базовой части профессионального цикла (Б1.Б.23). Изучается на 2 курсе в 4 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 2 зачётных единиц, 72 часов

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36,1
лекции	18
лабораторные занятия	0
практические занятия	18
экзамен	не предусмотрен
зачет	0,1
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	35,9
Контроль/экз (подготовка к экзамену)	0

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Основные понятия информационной безопасности.	Понятие информационной системы, основные составляющие информационной безопасности, управление информационной безопасностью, важность и сложность проблемы информационной безопасности.
2.	Угрозы информационной безопасности в информационных системах.	Основные определения и критерии классификации угроз, основные угрозы доступности, основные угрозы целостности, основные угрозы конфиденциальности, вредительские программы.
3.	Оценочные стандарты в информационной безопасности	Роль стандартов ИБ, «Оранжевая книга» как оценочный стандарт, Международный стандарт ISO/IEC 15408, критерии оценки безопасности информационных систем.
4.	Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения, международный стандарт ISO/IEC 27001:2005, сертификация СУИБ на соответствие ISO 27001.
5.	Создание СУИБ на предприятии	Этапы разработки и внедрения системы управления ИБ, содержание этапов разработки и внедрения системы управления ИБ.
6.	Методики и технологии управления рисками	Качественные методики управления рисками, количественные методики управления рисками, метод CRAMM.
7.	Разработка корпоративной методики анализа рисков	Методы оценивания информационных рисков, табличные методы оценки рисков, методика анализа рисков Microsoft
8.	Современные методы и средства анализа и управление рисками информационных систем компаний	Обоснование необходимости инвестиций в информационную безопасность компании, методика FRAP (фреп), методика OCTAVE (октэйв), методика Risk Watch (риск вэтч).
9.	Правовые меры обеспечения информационной безопасности	Основные направления обеспечения информационной безопасности, законодательно-правовая база обеспечения информационной безопасности на предприятии, нормативные акты предприятия по информационной

		безопасности, формы правовой защиты информации на предприятии.

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лб.	№ пр.			
1	2	3	4	5	6	7	8
1.	Основные понятия информационной безопасности.	2		1	У-1	С,Т	ОПК-7, ПК-4, ПК-13
2.	Угрозы информационной безопасности в информационных системах.	2			У-1-3, 6	С	ОПК-7, ПК-4, ПК-13
3.	Оценочные стандарты в информационной безопасности	2		2	У-1,4-6	С	ОПК-7, ПК-4, ПК-13
4.	Стандарты управления информационной безопасностью	2		3	У-2,8	С	ОПК-7, ПК-4, ПК-13
5.	Создание СУИБ на предприятии	2			У-1,9-12	С	ОПК-7, ПК-4, ПК-13
6.	Методики и технологии управления рисками	2			У-1,4-6	С	ОПК-7, ПК-4, ПК-13
7.	Разработка корпоративной методики анализа рисков	2			У-1,8-10	С	ОПК-7, ПК-4, ПК-13
8.	Современные методы и средства анализа и управление рисками информационных систем компаний	2			У-1,4-6	С	ОПК-7, ПК-4, ПК-13
9.	Правовые меры обеспечения информационной безопасности	2		4	У-1,4-6	С	ОПК-7, ПК-4, ПК-13

С – собеседование, Т – тест

4.2. Практические занятия

4.2.1. Практические занятия

Таблица 4.4 – Практические занятия

№	Наименование практической работы	Объем, час.
1.	Определение класса государственной информационной системы	4

	(ГИС)	
2.	Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации	6
3.	Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности	4
4.	Анализ заданного нормативно-правового акта Российской Федерации	4
Итого		18

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Основные понятия информационной безопасности.	1-3 недели	4
2.	Угрозы информационной безопасности в информационных системах.	3-5 недели	4
3.	Оценочные стандарты в информационной безопасности	5-7 недели	6
4.	Стандарты управления информационной безопасностью	7-8 недели	4
5.	Создание СУИБ на предприятии	8-10 недели	4
6.	Методики и технологии управления рисками	11-13 недели	3
7.	Разработка корпоративной методики анализа рисков	13-15 недели	3
8.	Современные методы и средства анализа и управление рисками информационных систем компаний	15-16 недели	4
9.	Правовые меры обеспечения информационной безопасности	17-18 недели	3,9
Итого			35,9

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

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к зачету, методических указаний к выполнению практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 по направлению подготовки 10.03.01 «Информационная безопасность» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами в области информационной безопасности. Удельный вес занятий, проводимых в интерактивных формах, составляет 24,8 процентов от аудиторных занятий согласно УП.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической №1 «Определение класса государственной информационной системы (ГИС)»	Исследование основных принципов разработки организационно-правовых аспектов деятельности службы защиты информации.	4
2.	Выполнение практической №2 «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»	Выполнение студентом интерактивных заданий по изучению системного подхода при создании структуры ГОСТ и ИСО.	6
3.	Выполнение практической работы №3 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности »	Выполнение студентом интерактивных заданий по анализу сертифицированных продуктов в заданной области информационной безопасности	4
4.	Выполнение практической работы №4 «Анализ заданного нормативно-правового акта Российской Федерации »	Выполнение студентом интерактивных заданий по знакомству с нормативно-правовыми актами и законодательством Российской Федерации, регулирующим вопросы защиты информации.	4

	Итого		38

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способность определение класса государственной информационной системы (ОПК-7)	Патентоведение	Введение в криптографию; Криптографические методы защиты информации; Экология; Технологическая практика; Проектно-технологическая практика	Инженерно-техническая защита информации; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность разрабатывать структуру государственных стандартов Российской Федерации в области информационной безопасности и защиты информации (ПК-4)	Введение в направление подготовки и планирование профессиональной карьеры	Основы управления информационной безопасностью	Защита информационных процессов в компьютерных системах; Защита и обработка конфиденциальных документов; Сети и системы передачи информации (специальные разделы); Беспроводные сети связи;

			Эксплуатационная практика; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способностью анализа нормативно-правовых актов в области информационной безопасности Российской Федерации (ПК-13)	История информационного противоборства	Основы управления информационной безопасностью	Экономика защиты информации; Оценка рисков и угроз; Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2. Описание показателей и критериев оценивания компетенций на раз- личных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

Наименование компетенции	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
способность определение класса государственной информационной системы (ОПК-7)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания,	**Знать**: организационно-правового обеспечение защиты информации **Уметь**: определять факторы, влияющие на формирование организационно-правового обеспечения защиты информации **Владеть навыками**:	**Знать**: технико-математические аспекты организационно-правового обеспечения **Уметь**: Определять подразделения и лиц, ответственных за организацию защиты информации **Владеть навыками**: реализация организационно-	**Знать**: юридические аспекты организационно-правового обеспечения защиты **Уметь**: налаживать порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации **Владеть навыками**: - реализация

	умения, навыки в типовых и нестандартных ситуациях	определение формы конфиденциальных отношений	правовых мероприятий защиты	технических мероприятий по защите информации
Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации (ПСК-4.1)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: используемые в работе с ОС программные средства **Уметь**: использовать в работе с ОС программные средства разработки ПО и администрирования **Владеть навыками**: навыками работы с информационно-техническими средствами	**Знать**: инструментальные средства проведения проверок информационных систем **Уметь**: анализ кода программных СЗИ **Владеть навыками**: методы проектирования информационных систем с учетом требований информационной безопасности	**Знать**: основные угрозы работоспособности прогаммным компонентам СЗИ **Уметь**: выявлять недекларируемые возможности программных систем **Владеть навыками**: использования особенностей реализации ПО для обеспечения ИБ
способность анализа нормативно-правовых актов в области информационной безопасности Российской Федерации (ПК-13)	1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД 2.Качество освоенных обучающимся знаний, умений, навыков 3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях	**Знать**: нормативно-правовые акты и законодательства Российской Федерации, регулирующие вопросы защиты информации **Уметь**: Определять сферу действия документа **Владеть навыками**: Составление иерархической системы	**Знать**: основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации **Уметь**: определять какая цель в разборе документа **Владеть навыками**: Составление интеллектуальной карты	**Знать**: ответственность за нарушения в сфере информационной безопасности **Уметь**: определять статус документа по отношению к задаче **Владеть навыками**: квалифицировать нарушения в сфере информационной безопасности.

7.3. 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 7.3 – Паспорт комплекта оценочных средств для текущего контроля

п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1.	Основные понятия информационной безопасности.	ПК-4	Лекция, СРС, практическая работа	собеседование	1-5	Согласно табл.7.2
				контрольные вопросы к ПР №1		
2.	Угрозы информационной безопасности в информационных системах.	ПК-4	Лекция, СРС	Собеседование	1-15	Согласно табл.7.2
3.	Оценочные стандарты в информационной безопасности Стандарты управления информационн	ПК-4, ПК-13	Лекция, СРС, практическая работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№2		
4.	Методики и технологии управления рисками Разработка корпоративной методики анализа	ПК-4, ПСК-13	Лекция, СРС, практическая работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№3		
5.	Современные методы и средства	ПК-4, ПСК-13,	Лекция, СРС, практическая работа	собеседование		Согласно табл.7.2

	анализа и управление рисками информационн			контрольные вопросы к ПР№3	1-5	
6.	Основные понятия информационн	ПК-4, ПК-4.13		собеседование		Согласно табл.7.2
7.	Оценочные стандарты в информационной безопасности	ПК-4, ПК-13		собеседование		Согласно табл.7.2
8.	Стандарты управления информационной безопасностью	ПК-4		собеседование		Согласно табл.7.2
9.	Создание СУИБ на предприятии	ОПК-7, ПК-13	Лекция, СРС, практическая работа	собеседование		Согласно табл.7.2
				контрольные вопросы к ПР№4		

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 1. «Основные понятия информационной безопасности»:

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Важность и сложность проблемы информационной безопасности

Контрольные вопросы к практической работе №1 «Определение класса государственной информационной системы (ГИС)»:

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какова специфика организации и выполнения охранных функций?
4. Каковы суть и содержание нормативной основы организации ЗСИ?
5. Какие факторы влияют на формирование организационно-правового обеспечения защиты информации?
6. Какова структура организационно-правовой основы защиты информации?
7. Опишите организационно-правовые мероприятия по защите конфиденциальной информации.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Выполнение практической работы №1 «Определение класса государственной информационной системы (ГИС)»	5	Выполнил, но «не защитил»	9	Выполнил и «защитил»
Выполнение практической работы №2 «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»	5	Выполнил, но «не защитил»	9	Выполнил и «защитил»
Выполнение практической работы №3 «Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности»	5	Выполнил, но «не защитил»	9	Выполнил и «защитил»
Выполнение практической работы №4 «Анализ заданного нормативно-правового акта Российской Федерации»	5	Выполнил, но «не защитил»	9	Выполнил и «защитил»
СРС	4		12	
ИТОГО	24		48	
Посещаемость	0		16	
Зачет	0		36	
ИТОГО	24		100	

При итоговом контроле (зачёте) в форме компьютерного теста студенту предлагается 20 вопросов по различным темам курса. Полученную итоговое количество правильных ответов (максимум 15) переводят в баллы на зачёте (максимум 36) путём умножения на 2,4 и округления до целого значения..

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная литература

1) Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 // Режим доступа - http://biblioclub.ru/

2) Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. : ил., табл., схем. - ISBN 978-5-4332-0020-3 // Режим доступа - http://biblioclub.ru/

3) Мельников, В. В. Безопасность информации в автоматизированных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 2003. - 368 с. -

8.2. Дополнительная литература

4) Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с. : ил. - Б. ц.

5) Артемов, А.В Информационная безопасность : курс лекций [Электронный ресурс] / А.В. Артемов - Орел : МАБИВ, 2014. - 257 с. // Режим доступа - http://biblioclub.ru/

6) Галатенко, В. А. Основы информационной безопасности. Курс лекций [Текст] : учебное пособие для студентов вузов / Под ред. В. Б. Бетелина. - 2-е изд., испр. - М. : ИНТУИТ. РУ Интернет-университет Информационных Технологий, 2004. - 264 с. - (Основы информационных технологий). - ISBN 5-9556-0015-9 : 184.00 р.

8.3. Перечень методических указаний

1) Определение класса государственной информационной системы (ГИС) [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (295 КБ). - Курск : ЮЗГУ, 2017. - 12 с. : ил., табл. - Библиогр.: с. 12. - Б. ц.

2) Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (398 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

3) Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (324 КБ). - Курск : ЮЗГУ, 2017. - 7 с. : ил., табл. - Библиогр.: с. 7. - Б. ц.

4) Анализ заданного нормативно-правового акта Российской Федерации [Электронный ресурс] : методические указания по выполнению практической работы : [для студентов укрупненной группы специальностей 10.00.00 дневной формы обучения] / Юго-Зап. гос. ун-т ; сост.: Е. С. Волокитина, М. О. Таныгин. - Электрон. текстовые дан. (251 КБ). - Курск : ЮЗГУ, 2017. - 7 с. - Библиогр.: с. 7. - Б. ц.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru
5) Справочно-поисковая система «Гарант» [официальный сайт]. Режим доступа: http://www.garant.ru
6) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Основы управления информационной безопасностью» являются лекции и практические. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются

рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; за крепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Основы управления информационной безопасностью»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Основы управления информационной безопасностью» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Основы управления информационной безопасностью» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»,

Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

Windows 7, договор IT000012385

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/l 7"TFT E700 (6 шт)