МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **39.03.03 Организация работы с молодежью**
Направленность (профиль): **Организация работы с молодежью**
Форма обучения: **очная**
Факультет: **ГФ, Гуманитарный факультет**
Кафедра: **ФиС, Кафедра Философии и социологии**
Курс: **3**
Семестр: **5**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	10	10	часов
2	Практические занятия	18	18	часов
3	Всего аудиторных занятий	28	28	часов
4	Из них в интерактивной форме	10	10	часов
5	Самостоятельная работа	44	44	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е

Зачет: 5 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 1 от «30» 1 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований Федерального Государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 39.03.03 Организация работы с молодежью , утвержденного 2015-10-20 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

ассистент каф. КИБЭВС _____ Новохрестов А. К.

Заведующий обеспечивающей каф. КИБЭВС _____ Шелупанов А. А.

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ГФ _____ Суслова Т. И.

Заведующий выпускающей каф. ФиС _____ Суслова Т. И.

Эксперты:

директор Центр системного проектирования _____ Конев А. А.

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Информационная безопасность» является заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, рассмотреть основные методологические принципы теории информационной безопасности, изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации

1.2. Задачи дисциплины

- ознакомление студентов с терминологией информационной безопасности
- развитие мышления студентов
- изучение методов и средств обеспечения информационной безопасности
- обучение определению причин, видов, каналов утечки и искажения информации

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» (Б1.В.ОД.6) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информатика, Математика.

Последующими дисциплинами являются: .

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-1 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

В результате изучения дисциплины студент должен:

- **знать** основные понятия информационной безопасности; основные угрозы информационной безопасности; способы атак на информацию; методы защиты корпоративных сетей и программные продукты реализующие системы защиты.
- **уметь** работать с программными продуктами, обеспечивающими защиту информации; работать с программно-аппаратными средствами аутентификации; определять источники и оценивать риски атак на информацию.
- **владеть** навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		5 семестр
Аудиторные занятия (всего)	28	28
Лекции	10	10
Практические занятия	18	18
Из них в интерактивной форме	10	10
Самостоятельная работа (всего)	44	44
Подготовка к контрольным работам	8	8
Проработка лекционного материала	8	8
Подготовка к практическим занятиям, семинарам	18	18

Всего (без экзамена)	72	72
Общая трудоемкость час	72	72
Зачетные Единицы Трудоемкости	2.0	2.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

№	Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
1	Базовые понятия в сфере обеспечения информационной безопасности	2	0	2	4	ОПК-1
2	Комплексный подход к обеспечению информационной безопасности	2	8	14	24	ОПК-1
3	Основные принципы, направления и требования обеспечения информационной безопасности организации	2	6	6	14	ОПК-1
4	Методы оценки рисков и угроз информационной безопасности	2	4	10	16	ОПК-1
5	Концепция и политика информационной безопасности. Менеджмент информационной безопасности	2	0	12	14	ОПК-1
	Итого	10	18	34	62	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Базовые понятия в сфере обеспечения информационной безопасности	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	2	ОПК-1
	Итого	2	
2 Комплексный подход к обеспечению информационной безопасности	Методы защиты информации: правовые, организационные, технические, физические и	2	ОПК-1

	криптографические.		
	Итого	2	
3 Основные принципы, направления и требования обеспечения информационной безопасности организации	Стандартизация. Сертификация. Управление доступом. Разграничение уровней доступа.	2	ОПК-1
	Итого	2	
4 Методы оценки рисков и угроз информационной безопасности	Информационные измерения. Идентификация и анализ рисков. Определение соответствующих защитных мер.	2	ОПК-1
	Итого	2	
5 Концепция и политика информационной безопасности. Менеджмент информационной безопасности	Политика безопасности. Контроль выполнения и функционирования защитных мер, которые являются необходимыми для обеспечения эффективной защиты информации и услуг в пределах организации. Обнаружение инцидентов и реагирование на них	2	ОПК-1
	Итого	2	
Итого за семестр		10	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представ-лены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

№	Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин				
		1	2	3	4	5
Предшествующие дисциплины						
1	Информатика	+	+			
2	Математика				+	

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5. 4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

	Виды занятий	Формы контроля

Компетенции	Лекции	Практические занятия	Самостоятельная работа	
ОПК-1	+	+	+	Контрольная работа, Защита отчета, Опрос на занятиях, Зачет, Выступление (доклад) на занятии

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
5 семестр			
Презентации с использованием слайдов с обсуждением		4	4
IT-методы	6		6
Итого за семестр:	6	4	10
Итого	6	4	10

7. Лабораторный практикум

Не предусмотрено РУП

8. Практические занятия

Содержание практических работ приведено в таблице 8.1.

Таблица 8. 1 – Содержание практических работ

Названия разделов	Содержание практических занятий	Трудоемкость, ч	Формируемые компетенции
5 семестр			
2 Комплексный подход к обеспечению информационной безопасности	Программные средства защиты. Защита от атак в локальных и глобальных сетях	8	ОПК-1
	Итого	8	
3 Основные принципы, направления и требования обеспечения информационной безопасности организации	Защита персональных данных	2	ОПК-1
	Защита государственной тайны	2	
	Защита коммерческой тайны	2	
	Итого	6	
4 Методы оценки рисков и угроз информационной безопасности	Оценка рисков информационной безопасности	4	ОПК-1

	Итого	4	
Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость ч	Формируемые компетенции	Формы контроля
5 семестр				
1 Базовые понятия в сфере обеспечения информационной безопасности	Проработка лекционного материала	2	ОПК-1	Опрос на занятиях
	Итого	2		
2 Комплексный подход к обеспечению информационной безопасности	Подготовка к практическим занятиям, семинарам	8	ОПК-1	Выступление (доклад) на занятии, Защита отчета, Контрольная работа, Опрос на занятиях
	Проработка лекционного материала	2		
	Подготовка к контрольным работам	4		
	Итого	14		
3 Основные принципы, направления и требования обеспечения информационной безопасности организации	Подготовка к практическим занятиям, семинарам	6	ОПК-1	Выступление (доклад) на занятии, Защита отчета, Опрос на занятиях
	Проработка лекционного материала	0		
	Итого	6		
4 Методы оценки рисков и угроз информационной безопасности	Подготовка к практическим занятиям, семинарам	4	ОПК-1	Выступление (доклад) на занятии, Защита отчета, Контрольная работа, Опрос на занятиях
	Проработка лекционного материала	2		
	Подготовка к контрольным работам	4		
	Итого	10		
5 Концепция и политика информационной безопасности. Менеджмент информационной безопасности	Проработка лекционного материала	2	ОПК-1	Зачет, Опрос на занятиях
	Подготовка к экзамену / зачету	10		
	Итого	12		
Итого за семестр		34		
Итого		44		

10. Курсовая работа

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
5 семестр				
Выступление (доклад) на занятии	4	4	3	11
Зачет			30	30
Защита отчета	10	10	10	30
Контрольная работа	10	10		20
Опрос на занятиях	3	3	3	9
Итого максимум за период	27	27	46	100
Нарастающим итогом	27	54	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Основы защиты информации. Учебное пособие / Шелупанов А.А., Сопов М.А. и др.. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

12.2. Дополнительная литература

1. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А,. и др В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. «Методические указания к лабораторным работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf
2. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А. , 2012г. – 2 с. [Электронный ресурс] [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://www.edu.tusur.ru – образовательный портал университета
2. http://www.lib.tusur.ru – веб-сайт библиотеки университета
3. http://www.elibrary.ru – научная электронная библиотека
4. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 3 этаж, ауд. 310. Состав оборудования: Учебная мебель; Экран раздвижной - 1 шт.; Доска магнитно-маркерная - 1 шт.; Мультимедийный проектор ViewSonic PJD5151 – 1 шт.; Компьютер лекционный acer travelmate 2300; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP SP2, Microsoft

Powerpoint Viewer; Имеется помещение для хранения и профилактического обслуживания учебного оборудования.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебно-исследовательская вычислительная лаборатория, расположенная по адресу 634045, Томская область, г. Томск, Красноармейская улица, д. 146, 8 этаж, ауд. 804. Состав оборудования: Учебная мебель;– 1 шт.; Доска магнитно-маркерная - 1 шт.; Компьютеры класса не ниже CPU AMD A4-6300/DDR-III DIMM 4Gb x2/ HDD 250 Gb SATA-II 300 Seagate Pipeline HD.2 . с широкополосным доступом в Internet, – 10 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows 8.1 Professional; Visual Studio 2012; Oracle VM VirtualBox; VMware Player. Имеется помещение для хранения и профилактического обслуживания учебного оборудования. Экран раздвижной - 1 шт.; Мультимедийный проектор ViewSonic PJD5151

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Красноармейская, 146, 2 этаж, ауд. 204. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Ce1егоп D336 2.8ГГц. - 7 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка

С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Информационная безопасность

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **39.03.03 Организация работы с молодежью**
Направленность (профиль): **Организация работы с молодежью**
Форма обучения: **очная**
Факультет: **ГФ, Гуманитарный факультет**
Кафедра: **ФиС, Кафедра Философии и социологии**
Курс: **3**
Семестр: **5**

Учебный план набора 2013 года

Разработчики:

- ассистент каф. КИБЭВС Новохрестов А. К.

Зачет: 5 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Должен знать основные понятия информационной безопасности; основные угрозы информационной безопасности; способы атак на информацию; методы защиты корпоративных сетей и программные продукты реализующие системы защиты. ; Должен уметь работать с программными продуктами, обеспечивающими защиту информации; работать с программно-аппаратными средствами аутентификации; определять источники и оценивать риски атак на информацию. ; Должен владеть навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ОПК-1

ОПК-1: способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	основные понятия информационной безопасности; основные угрозы информационной безопасности; способы атак на информацию; методы защиты корпоративных сетей и программные продукты реализующие системы защиты.	работать с программными продуктами, обеспечивающими защиту информации; работать с программно-аппаратными средствами аутентификации; определять источники и оценивать риски атак на информацию.	навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Контрольная работа; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем;	• Контролирует работу, проводит оценку, совершенствует действия работы;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой	• Обладает диапазоном практических умений, требуемых для решения определенных проблем	• Берет ответственность за завершение задач в исследовании,

	области ;	в области исследования;	приспосабливает свое поведение к обстоятельствам в решении проблем;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями;	• Обладает основными умениями, требуе¬мыми для выполнения простых задач;	• Работает при прямом наблюдении;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются 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, в следующем составе.

3.1 Зачёт

– 1. Основные регуляторы 2. Основные нормативно-правовые акты 3. Определения: информация, безопасность информации, защита информации, информационная безопасность, информационный процесс, документ, носитель 4. Свойства информации 5. Виды информации и их определения 6. Государственная тайна 7. Определения: угрозы, несанкционированный доступ. 8. Формы представления информации 9. Классификация угроз 10. Способы реализации угроз 11. Определения: защищаемая информация, доступ, допуск, уязвимость, сзи... 12. Виды защиты информации 13. Конституционные основы в информационной сфере 14. Доктрина ИБ РФ (составляющие национальных интересов РФ) 15. ФЗ «Об информации, информационных технологиях и о защите информации» 16. Преступления в информационной сфере (УК) 17. Задачи организационного обеспечения ЗИ 18. Управление ИБ 19. Модель угроз и модель нарушителя 20. Сложности в работе с персоналом 21. Классификация инсайдерских угроз 22. Социальная инженерия 23. Определения (программно-аппаратная ЗИ): СВТ, доступ, допуск, идентификация, аутентификация 24. Дискреционное и мандатное управление доступом 25. Сертификация 26. Группы классов защищенности АС от НСД 27. Межсетевой экран, антивирус, СОВ

3.2 Темы опросов на занятиях

– Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.

– Методы защиты информации: правовые, организационные, технические, физические и криптографические.

– Стандартизация. Сертификация. Управление доступом. Разграничение уровней доступа.

– Информационные измерения. Идентификация и анализ рисков. Определение соответствующих защитных мер.

– Политика безопасности. Контроль выполнения и функционирования защитных мер, которые являются необходимыми для обеспечения эффективной защиты информации и услуг в пределах организации. Обнаружение инцидентов и реагирование на них

3.3 Темы докладов

– Организация защиты персональных данных. Организация защиты государственной тайны. Организация защиты коммерческой тайны. Сравнение антивирусов/межсетевых экранов/систем обнаружения вторжений. Методы оценки рисков.

3.4 Темы контрольных работ

– Основные понятия информационной безопасности. Организационно-правовое обеспечение информационной безопасности.

– Оценка рисков. Программно-аппаратные средства защиты информации.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие

материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Основы защиты информации. Учебное пособие / Шелупанов А.А., Сопов М.А. и др.. Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf

4.2. Дополнительная литература

1. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А,. и др В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf

4.3. Обязательные учебно-методические пособия

1. «Методические указания к лабораторным работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс] [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf
2. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А. , 2012г. – 2 с. [Электронный ресурс] [Электронный ресурс]. - http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. http://www.edu.tusur.ru – образовательный портал университета
2. http://www.lib.tusur.ru – веб-сайт библиотеки университета
3. http://www.elibrary.ru – научная электронная библиотека
4. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов