МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Первый проректор – проректор
по учебной работе

_____
(подпись, ФИО)
«____»_____20__ г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Основы информационной безопасности

УГСН	10.00.00 Информационная безопасность
Направление подготовки (специальность)	10.03.01 Информационная безопасность
Квалификация	*Бакалавр*
Форма обучения	*Очная*
Год начала подготовки	*2025*
Объем дисциплины, ч. / з.е. / недели	*144/4/3*
Образовательные технологии	*Смешанные*
Форма контроля (промежуточная аттестация)	*Семестр 1: Экзамен*
Подразделение – разработчик	*Кафедра "Электронные системы и информационная безопасность"*

Самара 2025

Основы информационной безопасности

Разработчик

Разработчик РПМ
Андреева Наталья Викторовна
Руководитель подразделения
Карпова Надежда Евгеньевна

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы 3

2. Место модуля в структуре образовательной программы 3

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 4

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5

4.1. Содержание лекционных занятий 6

4.2. Содержание лабораторных занятия 7

4.3. Содержание практических занятий 8

4.4. Содержание самостоятельной работы 9

5. Перечень учебной литературы и учебно-методического обеспечения по модулю 9

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю 10

ПРИЛОЖЕНИЕ 11

Фонд оценочных средств 11

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть)
Общепрофессиональные компетенции			
Коммуникация	ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства
		ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	Умеет классифицировать угрозы информационной безопасности
		ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	Владеет навыками оценивания угроз информационной безопасности
Информационная и библиографическая культура	ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 Знает принципы и порядок работы информационно-справочных систем	Знает принципы и порядок работы информационно-справочных систем
		ОПК-8.2 Умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	Умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации
		ОПК-8.3 Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов

2. Место модуля в структуре образовательной программы

Модуль входит в Обязательную часть.

Входные требования:

Предшествующие осваиваемые модули: Теория и методология информационной безопасности; *Последующие осваиваемые модули:* Выполнение и защита выпускной квалификационной работы, Основы кибербезопасности, Защита информации от утечки по техническим каналам, Теоретические основы обработки сигналов, Учебная практика: ознакомительная практика, Конфиденциальный документооборот, Организационно-правовое обеспечение информационной безопасности.

3. Объем модуля в зачетных единицах с указанием количества академических часов,

выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 3

Вид учебной работы	Всего часов	В том числе часов в электронной форме	В том числе часов в форме практической подготовки	Семестр 1 часов/часов в электронной форме/в форме практической подготовки
Аудиторная контактная работа (всего), в том числе:	**56**	**0**	**0**	**56**
лекционные занятия (ЛЗ)	24	0	0	24
лабораторные работы (ЛР)	0	0	0	0
практические занятия (ПЗ)	32	0	0	32
Внеаудиторная контактная работа, КСР	**4**	**0**	**0**	**4**
Самостоятельная работа (всего), в том числе:	**84**	**0**	**0**	**84**
Выполнение задач, заданий, упражнений (в том числе разноуровневых)	*32*	*0*	*0*	*32*
Подготовка к лекциям	*12*	*0*	*0*	*12*
Подготовка к практическим занятиям	*16*	*0*	*0*	*16*
Составление конспектов	*16*	*0*	*0*	*16*
Подготовка к экзамену	*8*	*0*	*0*	*8*
ИТОГО: час.	**144**	**0**	**0**	**144**
ИТОГО: з.е.	**4.0**	**0.0**	**0.0**	**4.0**

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

Таблица 4

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	4	0	4	19	27
2.	Понятие информационной войны, методы и средства ее ведения	8	0	12	19	39
3.	Методология защиты информации на объектах информатизации	8	0	12	19	39
4.	Компьютерные преступления и компьютерная безопасность	4	0	4	27	35
	КСР					*4*
	Итого:	*24*	*0*	*32*	*84*	*144*

4.1. Содержание лекционных занятий

Таблица 4.1

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
Семестр 1					
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности.	.1. Роль информационной безопасности в обеспечении национальной безопасности. Основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.	2	0
2.	Информационная безопасность в системе национальной безопасности Российской Федерации	Основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.	Основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.	2	0
3.	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.1. Информационная безопасность и информационное противоборство.	2	0
4.	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	Составные элементы информационного противоборства.	2	0
5.	Понятие информационной войны, методы и средства ее ведения	Модель информационного противоборства	2.2. Информационное противоборство на военном уровне. Понятие и сущность информационной войны. Методы ее проведения.	2	0
6.	Понятие информационной войны, методы и средства ее ведения	Модель информационного противоборства	Информационное оружие как средство ведения информационной войны. Понятие информационного оружия. Виды информационного оружия. Характерные особенности информационного оружия	2	0
7.	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	Угрозы и методология оценки уязвимости информации. Классификация и содержание угроз информации.	2	0
8.	Методология защиты информации на объектах информатиз	Основные положения теории защиты информации.	Внешние и внутренние источники угроз.	2	0

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
	ации				
9.	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	Методологический базис теории защиты информации. Основные положения теории нечетких множеств.	2	0
10.	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	Основные положения нестрогой математики. Стратегии защиты информации	2	0
11.	Компьютерные преступления и компьютерная безопасность	Компьютерная безопасность.	4.1.Методы и средства обеспечения информационной безопасности компьютерных систем.	2	0
12.	Компьютерные преступления и компьютерная безопасность	Компьютерные преступления	Компьютерные преступления	2	0
			Итого за семестр:	*24*	*0*
			Итого:	**24**	**0**

4.2. Содержание практических занятий

Таблица 4.3

№ ПЗ	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количествочасов в электронной форме	Количество часов в форме практической подготовки
Семестр 1						
1.	Информационная безопасность в системе национальной безопасности Российской Федерации	Информационная безопасность как средство обеспечения национальной безопасности.	Национальные интересы РФ в информационной сфере. Интересы личности, общества, государства.	4	0	*0*
2.	Понятие информационной войны, методы и средства	Информационное противоборство.	Понятие информационного противоборства. Цели информационного противоборства.	4	0	*0*

№ ПЗ	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количествочасов в электронной форме	Количество часов в форме практической подготовки
	ее ведения					
3.	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	Информационная война, уровни и методы ее ведения.	4	0	*0*
4.	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	Понятие информационного оружия. Классификация и возможности информационного оружия.	4	0	*0*
5.	Методология защиты информации на объектах информатизации	Основы защиты информации.	Общая характеристика методов и средств защиты информации. Каналы утечки информации.	4	0	*0*
6.	Методология защиты информации на объектах информатизации	Основы защиты информации.	Направления защиты информации и обеспечения информационной безопасности. Организационно-правовое обеспечение информационной безопасности. Программно-аппаратное обеспечение ЗИ. Криптографическое обеспечение ЗИ.	4	0	*0*
7.	Методология защиты информации на объектах информатизации	Основы защиты информации.	Системы защиты информации. Общая модель защиты информации. Управление защитой информации.	4	0	*0*
8.	Компьютерные преступления и компьютерная безопасность	Компьютерная безопасность.	Компьютерные преступления. Угрозы информации в персональных ЭВМ.	4	0	*0*
			Итого за семестр:	*32*	*0*	*0*
			Итого:	**32**	**0**	***0***

4.3. Содержание самостоятельной работы

Таблица 4.4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 1			

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Информационная безопасность в системе национальной безопасности Российской Федерации	Подготовка к лекциям	Национальные интересы РФ в информационной сфере.	3
Информационная безопасность в системе национальной безопасности Российской Федерации	Подготовка к практическим занятиям	Национальные интересы РФ в информационной сфере.	4
Информационная безопасность в системе национальной безопасности Российской Федерации	Составление конспектов	Национальные интересы РФ в информационной сфере.	4
Информационная безопасность в системе национальной безопасности Российской Федерации	Выполнение задач, заданий, упражнений (в том числе разноуровневых)	Национальные интересы РФ в информационной сфере.	8
Понятие информационной войны, методы и средства ее ведения	Подготовка к лекциям	Понятие информационного противоборства. Цели информационного противоборства.	3
Понятие информационной войны, методы и средства ее ведения	Подготовка к практическим занятиям	Понятие информационного противоборства. Цели информационного противоборства.	4
Понятие информационной войны, методы и средства ее ведения	Составление конспектов	Информационная война, уровни и методы ее ведения.	4
Понятие информационной войны, методы и средства ее ведения	Выполнение задач, заданий, упражнений (в том числе разноуровневых)	Понятие информационного оружия. Классификация и возможности информационного оружия.	8
Методология защиты информации на объектах информатизации	Подготовка к лекциям	Общая характеристика методов и средств защиты информации. Каналы утечки информации.	3
Методология защиты информации на объектах информатизации	Подготовка к практическим занятиям	Общая характеристика методов и средств защиты информации. Каналы утечки информации.	4
Методология защиты информации на объектах информатизации	Выполнение задач, заданий, упражнений (в том числе разноуровневых)	Программно-аппаратное обеспечение ЗИ. Криптографическое обеспечение ЗИ.	8
Методология защиты информации на объектах информатизации	Составление конспектов	Общая модель защиты информации. Управление защитой информации.	4
Компьютерные преступления и компьютерная безопасность	Подготовка к лекциям	Компьютерные преступления.	3
Компьютерные преступления и компьютерная безопасность	Подготовка к практическим занятиям	Угрозы информации в персональных ЭВМ.	4
Компьютерные преступления и компьютерная безопасность	Выполнение задач, заданий, упражнений (в том числе разноуровневых)	Угрозы информации в персональных ЭВМ.	8
Компьютерные преступления и компьютерная	Составление конспектов	Угрозы информации в персональных ЭВМ.	4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
безопасность			
Компьютерные преступления и компьютерная безопасность	Подготовка к экзамену	Управление защитой информации.	8
		Итого за семестр:	*84*
		Итого:	**84**

5. Перечень учебной литературы и учебно-методического обеспечения по модулю

Таблица 5

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ	Ссылка на ресурс
1.	Галатенко, В.А. Основы информационной безопасности : Курс лекций / Под.ред.В.Б.Бетелина.- М., Интернет-Ун-т Информ.Технологий, 2003.- 277 с.	Книжный фонд СамГТУ	http://platform.samgtu.ru/getinfo?uid=els_samgtu-catalog-61728
2.	Белов, Е.Б. Основы информационной безопасности : Учеб.пособие / Е.Б.Белов,В.П.Лось,Р.В.Мещеряков,А.А.Шелупанов.- М., Горячая линия-Телеком, 2006.- 544 с.	Книжный фонд СамГТУ	http://platform.samgtu.ru/getinfo?uid=els_samgtu-catalog-96926
3.	Малюк, А.А. Информационная безопасность : концепт. и методол. основы защиты информ. : учеб. пособие / А. А. Малюк.- М., Горячая линия-Телеком, 2004.- 280 с.	Книжный фонд СамГТУ	http://platform.samgtu.ru/getinfo?uid=els_samgtu-catalog-64243
4.	Основы информационной безопасности при работе на компьютере; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	ЭБС IPR Books	http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-89453
5.	Основы информационной безопасности; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	ЭБС IPR Books	http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-97562
6.	Основы информационной безопасности; ЮНИТИ-ДАНА, 2017	ЭБС IPR Books	http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-72444
7.	Основы информационной безопасности; Евразийский открытый институт, 2010	ЭБС IPR Books	http://platform.samgtu.ru/getinfo?uid=els_samgtu-iprbooks-10746
8.	Рощупкин, В. Г. Информационно-психологическое противоборство и обеспечение информационной безопасности : [учеб. пособие] [Электронный ресурс] / В. Г. Рощупкин; М-во науки и высш. образования Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т).- Самара, Изд-во Самар. ун-та, 2018.- on-line с	Электронная библиотека Самарского Университета	http://platform.samgtu.ru/getinfo?uid=els_samgtu-ssau-9177
9.	Носаль, И. А. Особенности обеспечения информационной безопасности социально важных объектов / И. А. Носаль.- Издательство Самарского научного центра РАН, 2014	Электронная библиотека Самарского Университета	http://platform.samgtu.ru/getinfo?uid=els_samgtu-ssau-11126

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 6

№ п/п	Наименование	Ссылка на веб-страницу ресурса	Режим доступа
1.	*Scopus: база данных рефератов и цитирования [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.scopus.com*	*Ресурсы ограниченного доступа*
2.	*eLIBRARY.RU (НЭБ - Научная электронная библиотека "Российский*	*http://www.elibrary.ru/*	*Ресурсы открытого доступа*

№ п/п	Наименование	Ссылка на веб-страницу ресурса	Режим доступа
	индекс научного цитирования") [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет		
3.	*УИС РОССИЯ - Университетская информационная система РОССИЯ [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.cir.ru/*	*Ресурсы открытого доступа*
4.	*Кодекс - Информационно-правовой консорциум [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://kodeks.samgtu.local/*	*Ресурсы открытого доступа*
5.	*Единое окно доступа к образовательным ресурсам [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://window.edu.ru/*	*Ресурсы открытого доступа*

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю

Лекционные занятия проводятся в:
Учебная аудитория
Учебная аудитория.

Практические занятия проводятся в:
Учебная аудитория
Учебная аудитория.

Самостоятельная работа проводятся в:
Корпус № 8/111 - Учебная аудитория (Аудитория на 24 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные, доска аудиторная. Мультимедийное оборудование: проектор Acer Projector P1283; экран. Специализированное оборудование: стенд К-32 - 7шт., осциллограф С1-48Б - 5 шт., осциллограф С-93 - 2шт., осциллограф GRS-6052 - 1шт.)
Корпус № 8/200 - Читальный зал (Аудитория на 70 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные.).

Лабораторные занятия не предусмотрены.

ПРИЛОЖЕНИЕ

Фонд оценочных средств

Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации обучающихся по модулю

Настоящий Фонд оценочных средств (ФОС) по модулю Основы информационной безопасности является неотъемлемым приложением к рабочей программе модуля. На данный ФОС распространяются все реквизиты утверждения, представленные в рабочей программе модуля.

1. Перечень оценочных средств

Таблица 1

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Количество	Представление оценочного средства в ФОС
1	Устный опрос	Диалог преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.	4	Перечень вопросов для обсуждения
2	Отчёт по практическому занятию	Оценка способности студента применить полученные ранее знания для выполнения расчетов.	8	Требования к содержанию и оформлению отчета
3	Тесты	Инструмент, с помощью которого преподаватель оценивает степень достижения студентом требуемых знаний, умений, навыков в формате текущего контроля по итогам изучения разделов. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.	2	Спецификация тестов и примеры вариантов тестовых заданий

Раздел 2. Этапы формирования компетенций, соотнесенные с видами оценочных средств

Таблица 2

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
Информационная безопасность в системе национальной безопасности Российской Федерации	ОПК-1.1 Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Устный опрос	1
Информационная	ОПК-8.1 Знает	Знает принципы и	Отчёт по практическому	1

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
безопасность в системе национальной безопасности Российской Федерации	принципы и порядок работы информационно-справочных систем	порядок работы информационно-справочных систем	занятию	
Понятие информационной войны, методы и средства ее ведения	ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	Умеет классифицировать угрозы информационной безопасности	Устный опрос	2
Понятие информационной войны, методы и средства ее ведения	ОПК-8.2 Умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	Умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	Отчёт по практическому занятию	2-4
Методология защиты информации на объектах информатизации	ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	Владеет навыками оценивания угроз информационной безопасности	Устный опрос	3
Методология защиты информации на объектах информатизации	ОПК-8.3 Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	Отчёт по практическому занятию	5-7
Методология защиты информации на объектах информатизации	ОПК-1.1 Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Знает понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Тесты	1
Компьютерные преступления и компьютерная безопасность	ОПК-8.1 Знает принципы и порядок работы информационно-справочных систем	Знает принципы и порядок работы информационно-справочных систем	Устный опрос	4
Компьютерные преступления и компьютерная безопасность	ОПК-8.3 Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	Владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	Отчёт по практическому занятию	8
Компьютерные преступления и компьютерная	ОПК-1.3 Владеет навыками оценивания угроз	Владеет навыками оценивания угроз информационной	Тесты	2

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
безопасность	информационной безопасности	безопасности		

3. Содержание оценочных средств текущего контроля

Оценочное средство 1:
1. Основные понятия и принципы теории информационной безопасности. 2. Понятие информационной безопасности. 3. Интересы личности в информационной сфере. 4. Интересы общества в информационной сфере.
Оценочное средство 2:
Методические указания к практическим занятиям по дисциплине «Основы информационной безопасности» Занятие 1. Информационная безопасность как средство обеспечения национальной безопасности. Интересы личности, общества, государства.
Оценочное средство 3:
1. Под … понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ. Варианты ответа: a) национальной безопасностью РФ; b) информационной безопасностью РФ; c) национальными интересами РФ; d) государственной безопасностью РФ.

4. Содержание оценочных средств промежуточной аттестации

Семестр 1:

Вид аттестационного испытания 1: Устное собеседование.
Форма проведения промежуточной аттестации: Экзамен.
Типовые задания: Пример экзаменационного билета приведен в приложении.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Модуль состоит из набора разделов. Объем учебного раздела раскрывает отдельную (ые) тему(ы) модуля / этап прохождения практики. Модуль разбивается, как правило, на 2-4 раздела в семестр.

Раздел состоит из учебных элементов (дидактических единиц), сгруппированных по темам в рамках раздела. Объем учебного материала учебного элемента раскрывает отдельный вопрос темы. Путем набора соответствующих тем и учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

По каждому разделу устанавливается перечень обязательных видов работы студента, включающий: ответы на теоретические вопросы на семинаре; решение практических задач и выполнение заданий на практических занятиях; выполнение лабораторных работ; выполнение контрольных работ; написание рефератов; участие в коллоквиумах; тестирование по теме (группе тем); другие виды работ, определяемые преподавателем (в соответствии с установленными требованиями балльно-рейтинговой технологии).

Каждый раздел включает определенные формы контроля для оценки уровня усвоения учебного материала и определения рейтинговой оценки качества усвоения учебного материала.

Рейтинговая оценка знаний студентов определяется по 100-балльной шкале в каждом семестре и включает текущий, рубежный и итоговый контроль.

Накопленный рейтинг (фиксированная величина по окончании семестра) — это фактический рейтинг по всем освоенным к данному моменту разделам дисциплины, включая их текущий, рубежный и итоговый контроль, составляет N баллов (N – индивидуальная величина, зависящая от проделанной работы студента по дисциплине).

Проходной рейтинг (включает текущий контроль, рубежный контроль в семестре и промежуточную аттестацию) — это минимум баллов, набрав который студент будет считаться аттестованным по дисциплине, составляет 60 баллов в семестр по одной дисциплине.

Пороговый рейтинг (включает текущий контроль и рубежный контроль в семестре) — это минимальный фактический рейтинг семестрового контроля, набрав который, студент проходит на итоговый контроль, составляет 50% от суммы баллов, которые студент может набрать за текущий контроль и рубежный контроль в течение семестра.

Текущий контроль служит для получения первичной информации о ходе усвоения отдельных элементов содержания учебной дисциплины. Основное его назначение состоит в осуществлении контроля за всеми видами аудиторной и самостоятельной внеаудиторной деятельности студентов, результаты которого оцениваются в баллах.

Рубежный контроль (контрольные точки текущего контроля) проводится после изучения завершенной в смысловом и логическом плане части учебного материала (раздела, модуля). Этот вид контроля позволяет получить информацию о ходе усвоения некоторой совокупности содержательных элементов учебной дисциплины (раздела, модуля) и оценивается в баллах.

Промежуточный итоговый контроль (контрольные точки промежуточной аттестации) – курсовой проект, курсовая работа и экзамен, зачет, зачет с оценкой. Итоговый контроль по дисциплине в семестре предназначен для аттестации студента по учебной дисциплине: процедура установления соответствия уровня и качества подготовки студентов системе требований, зафиксированной в ФГОС ВО.

Распределение баллов рейтинговой оценки между видами контроля

Таблица 3

Номер семестра	Распределение баллов					Проходной рейтинг
	Текущий и рубежный контроль			Промежуточный итоговый контроль		
	Текущий контроль	Рубежный контроль	Пороговый рейтинг	Курсовая работа/курсовой проект	Зачет/зачет с оценкой/экзамен	
1	92	0	46	0	8	60

Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации

Таблица 4

100-балльная шкала	85-100	75-84	60-74	0-59
5-балльная шкала	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Бинарная шкала	Зачтено			Не зачтено

Распределение рейтинговых баллов по разделам модуля с указанием применяемых для их начисления оценочных средств представлено в Технологической карте БРТ.

Технологическая карта БРТ

Семестр 1

Раздел учебного модуля	Оценочные средства				Итого
	Устный опрос	**Тесты**	**Отчёт по практическому занятию**	**Экзамен**	
Раздел 1					
ЛЗ 1.1	4				4
ЛЗ 1.2	4				4
ПЗ 1.1			4		4
Итого по разделу 1	8		4		12
Раздел 2					
ЛЗ 2.3	4				4
ЛЗ 2.4	4				4
ЛЗ 2.5	4				4
ЛЗ 2.6	4				4
ПЗ 2.2			4		4
ПЗ 2.3			4		4
ПЗ 2.4			4		4
Итого по разделу 2	16		12		28
Раздел 3					
ЛЗ 3.7	4	0			4
ЛЗ 3.8	4	0			4
ЛЗ 3.9	4	0			4
ЛЗ 3.10	4	6			10
ПЗ 3.5			4		4
ПЗ 3.6			4		4
ПЗ 3.7			4		4
Итого по разделу 3	16	6	12		34
Раздел 4					
ЛЗ 4.11	4	0			4
ЛЗ 4.12	4	6			10
ПЗ 4.8			4		4
Итого по разделу 4	8	6	4		18
Промежуточная аттестация				8	8
Итого	48	12	32	8	100