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

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ / О.В. Юсупова
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.03.03 «Основы информационной безопасности»

Код и направление подготовки (специальность)	10.03.01 Информационная безопасность
Направленность (профиль)	Техническая защита информации
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	108 / 3
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2022

Б1.О.03.03 «Основы информационной безопасности»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **10.03.01 Информационная безопасность**, утвержденного приказом Министерства образования и науки РФ от № 1427 от 17.11.2020 и соответствующего учебного плана.

Разработчик РПД:

Старший преподаватель	Н.В Андреева
(должность, степень, ученое звание)	(ФИО)
Заведующий кафедрой	Н.Е. Карпова, кандидат технических наук
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	Я.Г Стельмах, кандидат педагогических наук
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	Н.Е. Карпова, кандидат технических наук
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Место дисциплины (модуля) в структуре образовательной программы 4
3. Объем дисциплины (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 дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5
4.1 Содержание лекционных занятий 5
4.2 Содержание лабораторных занятий 7
4.3 Содержание практических занятий 7
4.4. Содержание самостоятельной работы 9
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) 10
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения 11
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 11
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) 11
9. Методические материалы 12
10. Фонд оценочных средств по дисциплине (модулю) 13

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

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	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	Знать 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	Уметь классифицировать угрозы информационной безопасности
		ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	Владеть навыками оценивания угроз информационной безопасности

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **базовая часть**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ОПК-1	Учебная практика: ознакомительная практика	Теория информации	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

3. Объем дисциплины (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

Вид учебной работы	Всего часов / часов в электронной форме	3 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	64	64

Лекции	32	32
Практические занятия	32	32
Внеаудиторная контактная работа, КСР	3	3
Самостоятельная работа (всего), в том числе:	14	14
подготовка к лекциям	5	5
подготовка к практическим занятиям	5	5
подготовка к экзамену	4	4
Контроль	27	27
Итого: час	108	108
Итого: з.е.	3	3

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

№ 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	3	11
2	Понятие информационной войны, методы и средства ее ведения	12	0	12	3	27
3	Методология защиты информации на объектах информатизации	12	0	12	3	27
4	Компьютерные преступления и компьютерная безопасность	4	0	4	5	13
	КСР	0	0	0	0	3
	Контроль	0	0	0	0	27
	Итого	32	0	32	14	108

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
3 семестр				

1	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности.	1.1. Роль информационной безопасности в обеспечении национальной безопасности. Основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.	2
2	Информационная безопасность в системе национальной безопасности Российской Федерации	Понятие национальной безопасности.	1.1. Роль информационной безопасности в обеспечении национальной безопасности. Основные составляющие национальных интересов и угроз Российской Федерации в информационной сфере.	2
3	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.1. Информационная безопасность и информационное противоборство. Составные элементы информационного противоборства. Модель информационного противоборства (для самостоятельного изучения).	2
4	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.1. Информационная безопасность и информационное противоборство. Составные элементы информационного противоборства. Модель информационного противоборства (для самостоятельного изучения).	2
5	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.2. Информационное противоборство на военном уровне. Понятие и сущность информационной войны. Методы ее проведения.	2
6	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.2. Информационное противоборство на военном уровне. Понятие и сущность информационной войны. Методы ее проведения.	2
7	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.3. Информационное оружие как средство ведения информационной войны. Понятие информационного оружия. Виды информационного оружия. Характерные особенности информационного оружия	2
8	Понятие информационной войны, методы и средства ее ведения	Информационное противоборство.	2.3. Информационное оружие как средство ведения информационной войны. Понятие информационного оружия. Виды информационного оружия. Характерные особенности информационного оружия	2
9	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	3.1. Угрозы и методология оценки уязвимости информации. Классификация и содержание угроз информации. Внешние и внутренние источники угроз.	2
10	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	3.1. Угрозы и методология оценки уязвимости информации. Классификация и содержание угроз информации. Внешние и внутренние источники угроз.	2

11	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	3.2. Методологический базис теории защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Стратегии защиты информации (для самостоятельного изучения).	2
12	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	3.2. Методологический базис теории защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Стратегии защиты информации (для самостоятельного изучения).	2
13	Методология защиты информации на объектах информатизации	Основные положения теории защиты информации.	3.3. Модели систем и процессов защиты информации. Общая модель защиты. Обобщенная модель защиты. Управление защитой информации.	2
14	Методология защиты информации на объектах информатизации	сновные положения теории защиты информации.	3.3. Модели систем и процессов защиты информации. Общая модель защиты. Обобщенная модель защиты. Управление защитой информации.	2
15	Компьютерные преступления и компьютерная безопасность	Компьютерная безопасность.	4.1.Методы и средства обеспечения информационной безопасности компьютерных систем. Компьютерные преступления.	2
16	Компьютерные преступления и компьютерная безопасность	Компьютерная безопасность.	4.1.Методы и средства обеспечения информационной безопасности компьютерных систем. Компьютерные преступления.	2
			Итого за семестр:	**32**
			Итого:	**32**

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

№ занятия	**Наименование раздела**	**Тема практического занятия**	**Содержание практического занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**
3 семестр				
1	Информационная безопасность в системе национальной безопасности Российской Федерации	Тема 1. Информационная безопасность как средство обеспечения национальной безопасности.	1.1. Национальные интересы РФ в информационной сфере. Интересы личности, общества, государства.	2

2	Информационная безопасность в системе национальной безопасности Российской Федерации	Тема 1. Информационная безопасность как средство обеспечения национальной безопасности.	1.1. Национальные интересы РФ в информационной сфере. Интересы личности, общества, государства.	2
3	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.1. Понятие информационного противоборства. Цели информационного противоборства.	2
4	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.1. Понятие информационного противоборства. Цели информационного противоборства.	2
5	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.2. Информационная война, уровни и методы ее ведения.	2
6	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.2. Информационная война, уровни и методы ее ведения.	2
7	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.3. Понятие информационного оружия. Классификация и возможности информационного оружия.	2
8	Понятие информационной войны, методы и средства ее ведения	Тема 2. Информационное противоборство.	2.3. Понятие информационного оружия. Классификация и возможности информационного оружия.	2
9	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.1. Общая характеристика методов и средств защиты информации. Каналы утечки информации.	2
10	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.1. Общая характеристика методов и средств защиты информации. Каналы утечки информации.	2
11	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.2. Направления защиты информации и обеспечения информационной безопасности. Организационно-правовое обеспечение информационной безопасности. Программно-аппаратное обеспечение ЗИ. Криптографическое обеспечение ЗИ.	2

12	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.2. Направления защиты информации и обеспечения информационной безопасности. Организационно-правовое обеспечение информационной безопасности. Программно-аппаратное обеспечение ЗИ. Криптографическое обеспечение ЗИ.	2
13	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.3. Системы защиты информации. Общая модель защиты информации. Управление защитой информации.	2
14	Методология защиты информации на объектах информатизации	Тема 3. Основы защиты информации.	3.3. Системы защиты информации. Общая модель защиты информации. Управление защитой информации.	2
15	Компьютерные преступления и компьютерная безопасность	Тема 4. Компьютерная безопасность.	4.1. Компьютерные преступления. Угрозы информации в персональных ЭВМ.	2
16	Компьютерные преступления и компьютерная безопасность	Тема 4. Компьютерная безопасность.	4.1. Компьютерные преступления. Угрозы информации в персональных ЭВМ.	2
Итого за семестр:				**32**
Итого:				**32**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
3 семестр			
Информационная безопасность в системе национальной безопасности Российской Федерации	Написание реферата	Цель реферативной работы – закрепление полученных теоретических знаний и практических навыков в области информационной безопасности и защиты информации. Объем пояснительной записки должен составлять 10 м.п.с., графической части от 1 до 3 страниц, вшитых в пояснительную записку	3
Понятие информационной войны, методы и средства ее ведения	Написание реферата	Цель реферативной работы – закрепление полученных теоретических знаний и практических навыков в области информационной безопасности и защиты информации. Объем пояснительной записки должен составлять 10 м.п.с., графической части от 1 до 3 страниц, вшитых в пояснительную записку	1

Понятие информационной войны, методы и средства ее ведения	Вопросы для самостоятельного изучения	Модель информационного противоборства	2
Методология защиты информации на объектах информатизации	Написание реферата	Цель реферативной работы – закрепление полученных теоретических знаний и практических навыков в области информационной безопасности и защиты информации. Объем пояснительной записки должен составлять 10 м.п.с., графической части от 1 до 3 страниц, вшитых в пояснительную записку	2
Методология защиты информации на объектах информатизации	Вопросы для самостоятельного изучения	Стратегии защиты информации	1
Компьютерные преступления и компьютерная безопасность	Вопросы для самостоятельного изучения	Примеры вредоносных программ	2
Компьютерные преступления и компьютерная безопасность	Написание реферата	Цель реферативной работы – закрепление полученных теоретических знаний и практических навыков в области информационной безопасности и защиты информации. Объем пояснительной записки должен составлять 10 м.п.с., графической части от 1 до 3 страниц, вшитых в пояснительную записку	3
		Итого за семестр:	**14**
		Итого:	**14**

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

№ п/п	**Библиографическое описание**	**Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	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.	Электронный ресурс
Дополнительная литература		
2	Галатенко, В.А. Основы информационной безопасности : Курс лекций / Под.ред.В.Б.Бетелина.- М., Интернет-Ун-т Информ.Технологий, 2003.- 277 с.	Электронный ресурс
3	Шаньгин, В.Ф. Защита компьютерной информации : Эффектив.методы и средства:Учеб.пособие / В. Ф. Шаньгин.- М., ДМК Пресс, 2008.- 542 с.	Электронный ресурс

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 информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	операционная система	Microsoft Windows XP Professional (Зарубежный)	Лицензионное

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

№ п/п	Наименование	Краткое описание	Режим доступа
1	RSC	http://pubs.rsc.org/	Зарубежные базы данных ограниченного доступа
2	Кодекс	http://www.kodeks.ru/	Российские базы данных ограниченного доступа
3	КонсультантПлюс (правовые документы) - доступ с ПК в Медиацентре (ауд. 42)	http://www.consultant.ru/	Российские базы данных ограниченного доступа
4	РОСПАТЕНТ	http://www1.fips.ru/	Российские базы данных ограниченного доступа
5	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа
6	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Лекционные занятия:

Аудитория, оборудованная учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска.

Практические занятия

Практические занятия:

компьютерный класс на 10 посадочных мест (ауд. 109, 8 корпус), оснащенный пакетами ПО общего назначения.

Лабораторные занятия null

Самостоятельная работа

Прочее:

Для самостоятельной работы обучающихся предусмотрены рабочие места в читальных залах научно-технической библиотеки и компьютерных классах, ресурсы информационно-вычислительного центра ФГБОУ ВО «СамГТУ», оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной информационной среде.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.О.03.03 «Основы информационной безопасности»

Фонд оценочных средств
по дисциплине
Б1.О.03.03 «Основы информационной безопасности»

Код и направление подготовки (специальность)	10.03.01 Информационная безопасность
Направленность (профиль)	Техническая защита информации
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Электронные системы и информационная безопасность"
Кафедра-разработчик	кафедра "Электронные системы и информационная безопасность"
Объем дисциплины, ч. / з.е.	108 / 3
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
	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	Знать 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	Уметь классифицировать угрозы информационной безопасности
		ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	Владеть навыками оценивания угроз информационной безопасности

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
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	**Знать** понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	**Уметь** классифицировать угрозы информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да

ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	**Владеть** навыками оценивания угроз информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
Понятие информационной войны, методы и средства ее ведения				
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	**Знать** понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	**Уметь** классифицировать угрозы информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	**Владеть** навыками оценивания угроз информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
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	**Знать** понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	**Уметь** классифицировать угрозы информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	**Владеть** навыками оценивания угроз информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
Компьютерные преступления и компьютерная безопасность				

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	**Знать** понятия информации и информационной безопасности, источники и классификацию угроз информационной безопасности, основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.2 Умеет классифицировать угрозы информационной безопасности	**Уметь** классифицировать угрозы информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да
ОПК-1.3 Владеет навыками оценивания угроз информационной безопасности	**Владеть** навыками оценивания угроз информационной безопасности	Реферат	Да	Да
		Вопросы к экзамену	Нет	Да

Задания на выполнение реферативной работы по дисциплине

Цель реферативной работы – закрепление полученных теоретических знаний и практических навыков в области информационной безопасности и защиты информации. Объем пояснительной записки должен составлять 10 м.п.с., графической части от 1 до 3 страниц, вшитых в пояснительную записку Учебной программы, предусматривается время на его выполнение в объеме 20 часов.

Темы рефератов

1. Роль информационной безопасности и обеспечения национальной безопасности государства.
2. Понятие государственной, коммерческой, личной тайны.
3. Интересы государства в информационной сфере.
4. Виды угроз информационной безопасности.
5. Уязвимость компьютеров.
6. Меры и способы защиты компьютеров.
7. Информационное противоборство.
8. Информационное оружие, его классификация и возможности.
9. Компьютерные вирусы.
10. Методы нарушения конфиденциальности, целостности и доступности информации.
11. Вопросы защиты информации в компьютерных системах.
12. Общая характеристика методов и средств защиты.
13. Организационно-правовые методы обеспечения информационной безопасности.
14. Технические методы обеспечения информационной безопасности.
15. Криптографические методы обеспечения информационной безопасности.
16. Программно-аппаратные средства обеспечения информационной безопасности.
17. Компьютерная преступность.
18. Возможности сети Internet.
19. Защита информации в сети Internet.
20. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
21. Технические каналы утечки информации.
22. Методы защиты информации, обрабатываемой в автоматизированных системах.
23. Защита сотовых телефонов от прослушивания.
24. Методы защиты АС и СВТ от внешнего электромагнитного воздействия.
25. Понятие комплексной защиты информации

Список вопросов для промежуточного контроля (зачета с оценкой)

1. Основные понятия и принципы теории информационной безопасности.
2. Понятие информационной безопасности.
3. Интересы личности в информационной сфере.
4. Интересы общества в информационной сфере.
5. Интересы государства в информационной сфере.
6. Источники угроз: внешние и внутренние.
7. Направления обеспечения информационной безопасности государства.
8. Проблемы региональной информационной безопасности.
9. Субъекты и цели информационного противоборства.
10. Информационное оружие, его классификация и возможности.
11. Методы и средства обеспечения информационной безопасности компьютерных систем.
12. Компьютерная система как объект информационной безопасности.
13. Общая характеристика методов и средств защиты информации.
14. Методы оценки защищенности компьютерных систем от НСД.
15. Модели стратегии и системы обеспечения информационной безопасности.
16. Общие критерии и классы защищенности и средств вычислительной техники.
17. Классификация и возможности технических разведок.
18. Технические каналы утечки информации.
19. Методы защиты информации, обрабатываемой в технических системах, от технических разведок.
20. Методы защиты АС и СВТ от внешнего электромагнитного воздействия.
21. Признаки уязвимости компьютеров.
22. Меры и способы защиты компьютеров.
23. Компьютерная преступность.
24. Компьютерные вирусы.
25. Вопросы защиты информации в компьютерных системах.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций.Описание шкал оценивания

Учебная дисциплина формирует компетенции в соответствии с табл. 2, процедура оценивания представлена в табл. 3 и реализуетсяпоэтапно:

1-й этап процедуры оценивания:оценивание уровня достижения каждого из запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными картами компетенций ОПОП (Приложение 1 ОПОП). Экспертной оценке преподавателя подлежит сформированность отдельных

дескрипторов, для оценивания которых предназначена данная оценочная процедура текущего контроля и промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения (табл.2).

2-й этап процедуры оценивания:интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего контроля и промежуточнойаттестации.

Список вопросов для промежуточного контроля (зачета с оценкой)

1. Основные понятия и принципы теории информационной безопасности.
2. Понятие информационной безопасности.
3. Интересы личности в информационной сфере.
4. Интересы общества в информационной сфере.
5. Интересы государства в информационной сфере.
6. Источники угроз: внешние и внутренние.
7. Направления обеспечения информационной безопасности государства.
8. Проблемы региональной информационной безопасности.
9. Субъекты и цели информационного противоборства.
10. Информационное оружие, его классификация и возможности.
11. Методы и средства обеспечения информационной безопасности компьютерных систем.
12. Компьютерная система как объект информационной безопасности.
13. Общая характеристика методов и средств защиты информации.
14. Методы оценки защищенности компьютерных систем от НСД.
15. Модели стратегии и системы обеспечения информационной безопасности.
16. Общие критерии и классы защищенности и средств вычислительной техники.
17. Классификация и возможности технических разведок.
18. Технические каналы утечки информации.
19. Методы защиты информации, обрабатываемой в технических системах, от технических разведок.
20. Методы защиты АС и СВТ от внешнего электромагнитного воздействия.
21. Признаки уязвимости компьютеров.
22. Меры и способы защиты компьютеров.
23. Компьютерная преступность.
24. Компьютерные вирусы.
25. Вопросы защиты информации в компьютерных системах.