Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Основы информационной безопасности

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2021 года

Квалификация
Бакалавр

КАФЕДРА **Информационные технологии и программирование**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		**2 (1.2)**		Итого	
Недель	16		16			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	32	32	32	32	64	64
Лабораторные	48	48	48	48	96	96
Итого ауд.	80	80	80	80	160	160
Контактная работа	80	80	80	80	160	160
Сам. работа	28	28	28	28	56	56
Часы на контроль			36	36	36	36
Итого	108	108	144	144	252	252

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): д.э.н., проф., Тищенко Е.Н.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры, профессиональной культуры, формирование научного мировоззрения и развитие системного мышления.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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-13: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

В результате освоения дисциплины обучающийся должен:

Знать:

основы профессиональной деятельности в области информационной безопасности и методов защиты личности, общества и государства (соотнесено и индикатором ОПК-1.1);
основные методы реализации политики информационной безопасности и принципы применения комплексного подхода к обеспечению информационной безопасности объекта защиты (соотнесено и индикатором ОПК-13.1).

Уметь:

применять основы знаний в области информационной безопасности и методов защиты личности, общества и государства (соотнесено и индикатором ОПК-1.2);
применять основные методы реализации политики информационной безопасности и комплексный подход к обеспечению информационной безопасности объекта защиты (соотнесено и индикатором ОПК-13.2).

Владеть:

методами анализа области применения средств и методов обеспечения информационной безопасности и методов защиты личности, общества и государства (соотнесено и индикатором ОПК-1.2);
навыками использования основных методов реализации политики информационной безопасности и принципами комплексного подхода к защите (соотнесено и индикатором ОПК-13.2).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Понятие национальной безопасности: виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная,информационная, военная, пограничная, экологическая и другие / Лек /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.2	Понятие национальной безопасности: изучение структуры и основных руководящих документов Федеральной службы по техническому и эспортному контролю на официальном интернет-русурсе с составлением отчета. Использование системы Consultant Plus. / Лаб /	1	6	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.3	Понятие национальной безопасности: анализ нормативных докуиентов зарубежных стран в сравнении с руководящими документами Федеральной службы по техническому и эспортному контролю. Использование системы Consultant Plus. / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.4	Виды защищаемой информации: основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства / Лек /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.5	Виды защищаемой информации: классификация и структурный анализ информации в сети интернет с выделением защищаемых данных, обоснование полученных результатов, составление отчета / Лаб /	1	6	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
1.6	Виды защищаемой информации: выявление перспективных видов защищаемой информации на основе анализа современных тенденций цифровизации общества развития цифровых технологий / Ср /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

1.7	Выполнение заданий с использованием LibreOffice. / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5
Раздел 2. Информационная война, методы и средства ее ведения					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
2.1	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: интересы личности в информационной сфере, интересы общества в информационной сфере, интересы государства в информационной сфере; основные составляющие национальных интересов Российской Федерации в информационной сфере; угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России; внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности / Лек /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.2	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение:выявление актуальных угроз информационной безопасности страны исходя из текущей международной обстановки / Лаб /	1	6	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.3	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: выделение перспективных методов обеспечения информационной безопасности на основе анализа актуальных угроз / Ср /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.4	Содержание информационного противоборства на межгосударственном уровне: информационная безопасность и информационное противоборство; субъекты информационного противоборства; цели информационного противоборства; составные части и методы информационного противоборства; информационное оружие, его классификация и возможности / Лек /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.5	Содержание информационного противоборства на межгосударственном уровне: классификация субъектов информационного противоборства на международном уровне с выделением особо опасных направвлений атаки на государственные информационные ресурсы / Лаб /	1	8	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.6	Содержание информационного противоборства на межгосударственном уровне: анализ современного цифрового оружия, применяемого за последние три года против информационных ресурсов страны / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.7	Содержание информационного противоборства на военном уровне: методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации; основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны / Лек /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.8	Содержание информационного противоборства на военном уровне: основные методы и инструментальные средства обеспечения информационной безопасности в военной сфере /	1	8	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

	Лаб /				
2.9	Содержание информационного противоборства на военном уровне: анализ методов и средств обеспечения информационной безопасности в военной сфере, применяемых зарубежными странами / Ср /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.10	Компьютерная система как объект информационного воздействия: методы воздействия, субъекты и объекты воздействия. Основные угрозы, возникающие в компьютерной информационной среде / Лек /	1	6	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.11	Компьютерная система, как объект информационного воздействия: классификация угроз компьютерной информационной среде на предприятиях любых форм собственности и сфер деятельности / Лаб /	1	8	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.12	Компьютерная система как объект информационного воздействия: формирование информационной структуры предприятия по выбору студента и разработка комплексной системы обеспечения информационной безопасности в виде описательной модели / Ср /	1	4	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
2.13	Выполнение заданий с использованием LibreOffice. / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5

Раздел 3. Критерии защищенности компьютерных систем

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Методы и средства обеспечения информационной безопасности компьютерных систем: компьютерная система как объект информационной безопасности; общая характеристика методов и средств защиты информации; организационно-правовые, технические и криптографические методы обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности. Методы оценки защищенности компьютерных систем от НСД. / Лек /	1	8	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
3.2	Методы и средства обеспечения информационной безопасности компьютерных систем: классификация методов и средств обеспечения информационной безопасность для криптографической и программно-аппаратной защиты. Методы оценки защищенности компьютерных систем от НСД. / Лаб /	1	6	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
3.3	Методы и средства обеспечения информационной безопасности компьютерных систем: классификация методов и средств обеспечения информационной безопасность для организационно-правовой и технической защиты информации / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
3.4	Методы оценки защищенности компьютерных систем от НСД. Выполнение заданий с использованием LibreOffice. / Ср /	1	2	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5
3.5	/ Зачёт /	1	0	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

Раздел 4. Защита информации, обрабатываемой в автоматизированных системах, от технических разведок

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Классификация и возможности технических разведок: компьютерная разведка, технические каналы утечки информации при эксплуатации автоматизированных системю. Анализ основных характеристик технических каналов утечки информации. / Лек /	2	8	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
4.2	Классификация и возможности технических разведок: использование аппаратно-программных средств выявления технических каналов утечки информации с использованием нелинейного локатора и комплексного поискового прибора / Лаб /	2	12	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6
4.3	Классификация и возможности технических разведок: анализ зарубежных аппаратно-программных средств выявления технических каналов утечки информации на примере	2	6	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5, Л2.6

	использования нелинейного локатора и комплексного поискового прибора / Ср /				
4.4	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: классификация методов, алгоритмы оценки качества систем защиты. Особенности использования систем защиты от несанкционированного доступа и систем доверенной загрузки / Лек /	2	8	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
4.5	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: защита информационных ресурсов от несанкционированного доступа с использованием системы DallasLock и межсетевого экрана PFSense / Лаб /	2	12	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
4.6	Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: построение коомпьютерных информационных систем с использованием средств доверенной загрузки на примере системы DallasLock и межсетевого экрана PFSense / Ср /	2	6	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5, Л2.6

Раздел 5. Защита АС и СВТ от внешнего электромагнитного воздействия

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
5.1	Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на автоматизированные системы ии ситемы вычислительной техники / Лек /	2	8	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5, Л2.6
5.2	Генераторы электромагнитных импульсов: типы генераторов электромагнитных импульсов. Использование генератора электромагнитных импульсов Гром в различных конфигурациях объекта защиты и защищаемой зоны / Лаб /	2	12	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5, Л2.6
5.3	Генераторы электромагнитных импульсов: анализ и классификация возможных генераторов электромагнитных импульсов, функционирующих в стандартной городской среде / Ср /	2	4	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.4	Методы защиты автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала / Лек /	2	8	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5, Л2.6
5.5	Методы защиты автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия: методы кодирования сигнала, возможные подходы к экранированию с использованием современных материалов / Лаб /	2	12	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.6	Методы защиты АС и СВТ от внешнего электромагнитного воздействия: особенности работы генераторов белого шума и методы их аппаратной реализации. Параметры аппаратных генераторов белого шума / Ср /	2	10	ОПК-1, ОПК-13	Л1.1, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.7	Выполнение заданий с использованием LibreOffice. / Ср /	2	2	ОПК-1, ОПК-13	Л1.1, Л1.4, Л1.5, Л2.1, Л2.2, Л2.4, Л2.5
5.8	/ Экзамен /	2	36	ОПК-1, ОПК-13	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5, Л2.6

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Сычев Ю. Н.	Основы информационной безопасности: учебно -практическое пособие: учебное пособие	Москва: Евразийский открытый институт, 2010	https://biblioclub.ru/index.php?page=book&id=90790 неограниченный доступ для зарегистрированных пользователей
Л1.2		Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/52209.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Платунова, С. М.	Применение межсетевых экранов фирмы ZyXEL в корпоративных сетях: учебное пособие по дисциплинам «сети эвм и телекоммуникации», «защита информации в сетях»	Санкт-Петербург: Университет ИТМО, 2015	http://www.iprbookshop.ru/67579.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Голиков, А. М.	Кодирование в телекоммуникационных системах: учебное пособие для специалитета: 090302.65 информационная безопасность телекоммуникационных систем. курс лекций, компьютерный практикум, задание на самостоятельную работу	Томск: Томский государственный университет систем управления и радиоэлектроники, 2016	https://www.iprbookshop.ru/72111.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Сафонова, Л. А.	Экономические аспекты информационной безопасности: учебное пособие	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2019	https://www.iprbookshop.ru/90606.html неограниченный доступ для зарегистрированных пользователей
5.2. Дополнительная литература				
	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	https://biblioclub.ru/index.php?page=book&id=210607 неограниченный доступ для зарегистрированных пользователей
Л2.2	Загинайлов Ю. Н.	Основы информационной безопасности: курс визуальных лекций: учебное пособие	Москва, Берлин: Директ-Медиа, 2015	https://biblioclub.ru/index.php?page=book&id=362895 неограниченный доступ для зарегистрированных пользователей
Л2.3	Теплов, Э. П., Гатчин, Ю. А., Нырков, А. П., Коробейников, А. Г., Сухостат, В. В.	Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции	Санкт-Петербург: Университет ИТМО, 2016	http://www.iprbookshop.ru/66435.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Гуляев, В. П.	Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплект	Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2014	https://www.iprbookshop.ru/68221.html неограниченный доступ для зарегистрированных пользователей
Л2.5		Вестник Института законодательства и правовой информации им. М.М. Сперанского	, 2009	https://www.iprbookshop.ru/6394.html неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.6	Бахаров, Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография): практикум	Москва: Издательский Дом МИСиС, 2019	http://www.iprbookshop.ru/98171.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ИСС "КонсультантПлюс"
ИСС "Гарант"http://www.internet.garant.ru/
База данных Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
Libreoffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; 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.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и свободно распространяемыми программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства			
З: основы профессиональной деятельности в области информационной безопасности и методов защиты личности, общества и государства	поиск и сбор информации в рамках профессиональной деятельности и методов ее осуществления	полнота собранной информации и соответствие ее области профессиональной деятельности	О – опрос (1-22), З – вопросы к зачету (1-60), Э – вопросы к экзамену (1-28).
У: применять основы знаний в области информационной безопасности и методов защиты личности, общества и государства	классификация информации в области информационной безопасности и методов ее обеспечения	корректность применяемых методов и подходов к классификации	О – опрос (23-44), З – вопросы к зачету (61-70), Э – вопросы к экзамену (29-39). ПОЗЗ – практико-ориентированные задания к зачету (1-9) ПОЗЭ - практико-ориентированные задания к экзамену (1-9)
В: методами анализа области применения средств и методов обеспечения информационной безопасности и методов защиты личности, общества и государства	сравнительный анализ методов и средств обеспечения информационной безопасности	соответствие результатов анализа реальным функциональным характеристикам методов и средств обеспечения информационной безопасности	О – опрос (23-44), З – вопросы к зачету (61-70), Э – вопросы к экзамену (29-39). ПОЗЗ – практико-ориентированные задания к зачету (1-9) ПОЗЭ - практико-ориентированные задания к экзамену (1-9)
ОПК-13: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма			
З: основные методы реализации политики информационной безопасности и принципы применения комплексного подхода к обеспечению информационной безопасности объекта защиты	поиск и сбор информации по методам реализации политики информационной безопасности в зависимости от типа объекта защиты	полнота собранной информации и соответствие ее типу объекта защиты	ЛР – лабораторное задание (1-14), З – вопросы к зачету (1-60), Э – вопросы к экзамену (1-28).
У: применять основные методы реализации политики информационной безопасности и комплексный подход к обеспечению информационной безопасности объекта защиты	анализ текущего состояния политики безопасности и выявление ее уязвимых мест	соответствие результатов анализа текущему состоянию политики безопасности	ЛР – лабораторное задание (15-24) , З – вопросы к зачету (61-70), Э – вопросы к экзамену (29-39). ПОЗЗ – практико-ориентированные задания к зачету (1-9) ПОЗЭ - практико-ориентированные задания к экзамену (1-9)
В: навыками использования основных методов реализации политики информационной безопасности и принципами комплексного подхода к защите	конфигурирование политики безопасности объекта защиты с учетом комплексного подхода	отсутствие выявленных при первоначальном анализе уязвимостей политики безопасности	ЛР – лабораторное задание (15-24), З – вопросы к зачету (61-70), Э – вопросы к экзамену (29-39). ПОЗЗ – практико-ориентированные задания к зачету (1-9) ПОЗЭ - практико-ориентированные задания к экзамену (1-9)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляются в рамках накопительной больно-рейтинговой системы в 100-балльной шкале.

1 семестр:
50-100 баллов (зачет);
0-49 баллов (незачет).

2 семестр:
84-100 баллов (оценка «отлично»);
67-83 баллов (оценка «хорошо»);
50-66 баллов (оценка «удовлетворительно»);
0-49 баллов (оценка «неудовлетворительно»).

2 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

Вопросы к зачету
по дисциплине «Основы информационной безопасности»

1. Состав элементов внешнего периметра информационной системы
2. Состав элементов внутреннего периметра информационной системы
3. Состав угроз информационной безопасности
4. Состав каналов утечки информации
5. Какая группа каналов утечки информации используется при DDoS-атаке
6. Функции криптографии
7. Определение понятия «криптостойкость»
8. Определение понятия «криптоалгоритм» («криптосистема»)
9. Определение понятия «криптограф»
10. Определение понятия «криптоаналитик»
11. Определение понятия «криптоанализ»
12. Определение понятия «ключ криптосистемы»
13. Длина ключа в «идеальной» криптосистеме
14. Метод формирования ключа «идеальной» криптосистемы
15. Срок действия ключа в «идеальной» криптосистеме
16. Критический параметр криптосистемы
17. Смысл и ассемблерное выражение операции «замена»
18. Смысл и ассемблерное выражение операции «перестановка»
19. Смысл и ассемблерное выражение операции Шеннона
20. Соотношение операции «замена» и тактовой частоты процессора
21. Соотношение операции «перестановка» и тактовой частоты процессора
22. Алгоритм работа криптопреобразования «шифр Цезаря»
23. Основные отличия блочного и поточного шифров
24. Недостатки простого блочного алгоритма
25. Смысл и определение блочных алгоритмов с обратной связью
26. Определение операции «гаммирование»
27. Определение понятия «имитоприставка»
28. Определение понятия «однонаправленная математическая функция»
29. Достоинства и недостатки классических криптоалгоритмов
30. Достоинства и недостатки криптоалгоритмов с открытым ключем
31. Определение понятия «симметричный криптоалгоритм»
32. Определение понятия «асимметричный криптоалгоритм»
33. Количество ключей в алгоритмах классической криптографии с N абонентами
34. Количество ключей в алгоритмах open key с N абонентами
35. Определение понятия «хэш-функция»
36. Тип алгоритма и длина ключа в ГОСТ 28147-89
37. Режимы функционирования ГОСТ 28147-89
38. Сущность и назначение таблиц замен в ГОСТ 28147-89

39. Количество циклов ГОСТ 28147-89 при выработке имитоприставки
40. Количество и размер подблоков разбиения основного блока в ГОСТ 28147-89
41. Тип алгоритма и длина ключа в DES
42. Режимы функционирования DES
43. Сущность и назначение начальной и конечной перестановок в DES
44. Сущность и назначение функции расширения в DES
45. Сущность и назначение таблицы преобразований в DES
46. Типы однонаправленных функций в RSA
47. Количество ключей в RSA
48. Тип зависимости ключей в RSA
49. Исходная информация для атаки на RSA
50. Решаемая задача криптоаналитиком при атаке на RSA
51. Типы однонаправленных функций в ГОСТ Р 34.10-2001
52. Количество ключей в ГОСТ Р 34.10-2001
53. Исходная информация для атаки на ГОСТ Р 34.10-2001
54. Решаемая задача криптоаналитиком при атаке на ГОСТ Р 34.10-2001
55. Определение понятия «электронная подпись»
56. Структура электронной подписи
57. Количество ключей в алгоритмах электронной подписи
58. Используемые алгоритмы при формировании электронной подписи
59. Определение понятия «удостоверяющий центр»
60. Юридическая значимость электронной подписи
61. Изучение структуры и основных руководящих документов Федеральной службы по техническому и экспортному контролю на официальном интернет-ресурсе. Использование системы Consultant Plus
62. Виды защищаемой информации: классификация и структурный анализ информации в сети интернет с выделением защищаемых данных, обоснование полученных результатов
63. Выявление актуальных угроз информационной безопасности страны исходя из текущей международной обстановки
64. Основные методы и инструментальные средства обеспечения информационной безопасности в военной сфере
65. Классификация угроз компьютерной информационной среде на предприятиях любых форм собственности и сфер деятельности
66. Классификация методов и средств обеспечения информационной безопасность для криптографической и программно-аппаратной защиты
67. Выделение перспективных методов обеспечения информационной безопасности на основе анализа актуальных угроз
68. Анализ современного цифрового оружия, применяемого за последние три года против информационных ресурсов страны
69. Формирование информационной структуры предприятия по выбору студента и разработка комплексной системы обеспечения информационной безопасности в виде описательной модели
70. Классификация методов и средств обеспечения информационной безопасность для организационно-правовой и технической защиты информации

Практико-ориентированные задания к зачету

1. Применение симметричных алгоритмов для шифрования блока информации.
2. Применение асимметричных алгоритмов для шифрования блока информации.
3. Криптоанализ зашифрованного блока информации с помощью метода «встреча в середине атаки».
4. Обработка первичной информации об объекте исследования.
5. Разработка модели угроз нарушения информационной безопасности системы электронного документооборота
6. Разработка модели нарушителя информационной безопасности системы электронного документооборота

7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
8. Подбор и обоснование выбора средств защиты информации и их компонентов на основании модели угроз
9. Проведение аудита защищенности системы электронного документооборота по требованиям контролирующих органов

Зачетное задание включает 2 теоретических вопроса (раздел «Вопросы к зачету») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к зачету»).

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
– 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
– 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
– 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
– 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
– 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
– 11-24 балла выставляется, если задание решено частично.
– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
– 50-100 баллов (зачтено);
– 0-49 баллов (не зачтено).

Вопросы к экзамену
по дисциплине «Основы информационной безопасности»

1.Понятие национальной безопасности.
2.Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.
3.Виды защищаемой информации»: основные понятия и общеметодологические принципы теории информационной безопасности.
4.Роль информационной безопасности в обеспечении национальной безопасности государства.
5. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение»: интересы личности в информационной сфере, интересы общест-

ва в информационной сфере, интересы государства в информационной сфере.
6. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России, угрозы информационному обеспечению государственной политики Российской Федерации, угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов, угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.
8. Внешние источники угроз, внутренние источники угроз; направления обеспечения информационной безопасности государства; проблемы региональной информационной безопасности.
9. Содержание информационного противоборства на межгосударственном уровне»: информационная безопасность и информационное противоборство.
10. Субъекты информационного противоборства; цели информационного противоборства; сотставные части и методы информационного противоборства.
11. Информационное оружие, его классификация и возможности.
12. Содержание информационного противоборства на военном уровне»: методы нарушения конфиденциальности, целостности и доступности информации.
13. Причины, виды, каналы утечки и искажения информации.
14. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
15. Компьютерная система как объект информационного воздействия»: методы воздействия, субъекты и объекты воздействия.
16. Методы и средства обеспечения информационной безопасности компьютерных систем»: компьютерная система как объект информационной безопасности.
17. Ообщая характеристика методов и средств защиты информации.
18. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.
19. Программно-аппаратные средства обеспечения информационной безопасности.
20. Методы оценки защищенности компьютерных систем от НСД»: модели, стратегии и системы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
22. Классификация и возможности технических разведок»: компьютерная разведка, технические каналы утечки информации при эксплуатации АС.
23. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок»: классификация методов, алгоритмы оценки качества систем защиты.
24. Анализ наиболее актуальных источников угроз со стороны технических разведок.
25. Генераторы электромагнитных импульсов: эффекты, возникающие от внешнего электромагнитного воздействия на АС и СВТ.
26. Методы защиты АС и СВТ от внешнего электромагнитного воздействия: экранирование, создание преднамеренных помех, кодировка сигнала.
27. Методы измерения и обнаружения электромагнитных импульсов.
28. Методы адаптивного экранирования электромагнитных импульсов.
29. Методы создания адаптивных преднамеренных помех.
30. Использование анализатора уязвимостей для определения уязвимостей компьютерной системы с неопределенной архитектурой и сетевой топологией
31. Методы оценки защищенности компьютерных систем от НСД: использование анализатора уязвимостей для определения уязвимостей компьютерной системы с неопределенной архитектурой и сетевой топологией
32. Использование аппаратно-программных средств выявления технических каналов утечки информации с использованием нелинейного локатора и комплексного поискового прибора

33. Анализ зарубежных аппаратно-программных средств выявления технических каналов утечки информации на примере использования нелинейного локатора и комплексного поискового прибора
34. Защита информационных ресурсов от несанкционированного доступа с использованием системы доверенной загрузки и межсетевого экрана.
35. Построение компьютерных информационных систем с использованием средств доверенной загрузки на примере системы имеющейся системы и межсетевого экрана
36. Типы генераторов электромагнитных импульсов. Использование генератора электромагнитных импульсов Гром в различных конфигурациях объекта защиты и защищаемой зоны
37. Анализ и классификация возможных генераторов электромагнитных импульсов, функционирующих в стандартной городской среде
38. Методы кодирования сигнала, возможные подходы к экранированию с использованием современных материалов
39. Особенности работы генераторов белого шума и методы их аппаратной реализации. Параметры аппаратных генераторов белого шума.

Практико-ориентированные задания к экзамену

1. Разработка алгоритма аудита информационной системы.
2. Формирование схемы подключения межсетевых экранов.
3. Разработка плана аттестации выделенного помещения.
4. Разработка плана подготовки выделенного помещения для конфиденциальных разговоров.
5. Разработка плана настройки системы обнаружения вторжений
6. Развертывание топологии частных виртуальных сетей на предприятии.
7. Разработка комплекта типовых эксплуатационных документов системы электронного документооборота
8. Подбор и обоснование выбора средств защиты информации и их компонентов на основании модели угроз
9. Настройка DLP-системы предприятия.

Экзаменационное задание включает 2 теоретических вопроса (раздел «Вопросы к экзамену») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к экзамену»).

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
– 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
– 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
– 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:

– 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
– 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
– 11-24 балла выставляется, если задание решено частично.
– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
84-100 баллов (оценка «отлично»);
67-83 баллов (оценка «хорошо»);
50-66 баллов (оценка «удовлетворительно»);
0-49 баллов (оценка «неудовлетворительно»).

Опрос:

1. Состав элементов внешнего периметра информационной системы
2. Состав элементов внутреннего периметра информационной системы
3. Состав угроз информационной безопасности
4. Состав каналов утечки информации
5. Какая группа каналов утечки информации используется при DDoS-атаке
6. Функции криптографии
7. Определение понятия «криптостойкость»
8. Определение понятия «криптоалгоритм» («криптосистема»)
9. Определение понятия «криптограф»
10. Определение понятия «криптоаналитик»
11. Определение понятия «криптоанализ»
12. Определение понятия «ключ криптосистемы»
13. Длина ключа в «идеальной» криптосистеме
14. Метод формирования ключа «идеальной» криптосистемы
15. Срок действия ключа в «идеальной» криптосистеме
16. Критический параметр криптосистемы
17. Смысл и ассемблерное выражение операции «замена»
18. Смысл и ассемблерное выражение операции «перестановка»
19. Смысл и ассемблерное выражение операции Шеннона
20. Соотношение операции «замена» и тактовой частоты процессора
21. Соотношение операции «перестановка» и тактовой частоты процессора
22. Алгоритм работа криптопреобразования «шифр Цезаря»
23. Основные отличия блочного и поточного шифров
24. Недостатки простого блочного алгоритма
25. Смысл и определение блочных алгоритмов с обратной связью
26. Определение операции «гаммирование»
27. Определение понятия «имитоприставка»
28. Определение понятия «однонаправленная математическая функция»
29. Достоинства и недостатки классических криптоалгоритмов
30. Достоинства и недостатки криптоалгоритмов с открытым ключем
31. Определение понятия «симметричный криптоалгоритм»
32. Определение понятия «асимметричный криптоалгоритм»
33. Количество ключей в алгоритмах классической криптографии с N абонентами
34. Количество ключей в алгоритмах open key с N абонентами
35. Определение понятия «хэш-функция»
36. Тип алгоритма и длина ключа в ГОСТ 28147-89
37. Режимы функционирования ГОСТ 28147-89
38. Сущность и назначение таблиц замен в ГОСТ 28147-89
39. Количество циклов ГОСТ 28147-89 при выработке имитоприставки

40. Количество и размер подблоков разбиения основного блока в ГОСТ 28147-89
41. Тип алгоритма и длина ключа в DES
42. Режимы функционирования DES
43. Сущность и назначение начальной и конечной перестановок в DES
44. Сущность и назначение функции расширения в DES

Критерии оценивания:
Правильный ответ на 1 вопрос – 1 балл;
Неправильный ответ на 1 вопрос – 0 баллов.

Лабораторные задания

1 семестр:
1. Понятие национальной безопасности: изучение структуры и основных руководящих документов Федеральной службы по техническому и экспортному контролю на официальном Интернет-ресурсе с составлением отчета. Использование системы Consultant Plus.
2. Понятие национальной безопасности: анализ нормативных документов зарубежных стран в сравнении с руководящими документами Федеральной службы по техническому и экспортному контролю. Использование системы Consultant Plus.
3. Виды защищаемой информации: классификация и структурный анализ информации в сети интернет с выделением защищаемых данных, обоснование полученных результатов, составление отчета.
4. Виды защищаемой информации: выявление перспективных видов защищаемой информации на основе анализа современных тенденций цифровизации общества развития цифровых технологий.
5. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: выявление актуальных угроз информационной безопасности страны исходя из текущей международной обстановки.
6. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение: выделение перспективных методов обеспечения информационной безопасности на основе анализа актуальных угроз.
7. Содержание информационного противоборства на межгосударственном уровне: классификация субъектов информационного противоборства на международном уровне с выделением особо опасных направлений атаки на государственные информационные ресурсы.
8. Содержание информационного противоборства на межгосударственном уровне: анализ современного цифрового оружия, применяемого за последние три года против информационных ресурсов страны.
9. Содержание информационного противоборства на военном уровне: основные методы и инструментальные средства обеспечения информационной безопасности в военной сфере.
10. Содержание информационного противоборства на военном уровне: анализ методов и средств обеспечения информационной безопасности в военной сфере, применяемых зарубежными странами.
11. Компьютерная система, как объект информационного воздействия: классификация угроз компьютерной информационной среде на предприятиях любых форм собственности и сфер деятельности.
12. Компьютерная система как объект информационного воздействия: формирование информационной структуры предприятия по выбору студента и разработка комплексной системы обеспечения информационной безопасности в виде описательной модели.
13. Методы и средства обеспечения информационной безопасности компьютерных систем: классификация методов и средств обеспечения информационной безопасность для криптографической и программно-аппаратной защиты.
14. Методы и средства обеспечения информационной безопасности компьютерных систем: классификация методов и средств обеспечения информационной безопасность для организационно-правовой и технической защиты информации.

Критерии оценивания:

Правильное решение 1 лабораторного задания – 4 балла;
При выполнении 1 лабораторного задания были допущены неточности, не влияющие на результат – 3 балла;
При выполнении 1 лабораторного задания были допущены ошибки – 2 балла;
При выполнении 1 лабораторного задания были допущены существенные ошибки – 1 балл;
Неправильное решение 1 лабораторного задания – 0 баллов.

2 семестр:

15. Методы оценки защищенности компьютерных систем от НСД: использование анализатора уязвимостей для определения уязвимостей компьютерной системы с неопределенной архитектурой и сетевой топологией.
16. Методы оценки защищенности компьютерных систем от НСД: использование анализатора уязвимостей для определения уязвимостей компьютерной системы с неопределенной архитектурой и сетевой топологией.
17. Классификация и возможности технических разведок: использование аппаратно-программных средств выявления технических каналов утечки информации с использованием нелинейного локатора и комплексного поискового прибора.
18. Классификация и возможности технических разведок: анализ зарубежных аппаратно-программных средств выявления технических каналов утечки информации на примере использования нелинейного локатора и комплексного поискового прибора.
19. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: защита информационных ресурсов от несанкционированного доступа с использованием системы доверенной загрузки и межсетевого экрана.
20. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок: построение компьютерных информационных систем с использованием средств доверенной загрузки и межсетевого экрана.
21. Генераторы электромагнитных импульсов: типы генераторов электромагнитных импульсов. Использование генератора электромагнитных импульсов Гром в различных конфигурациях объекта защиты и защищаемой зоны.
22. Генераторы электромагнитных импульсов: анализ и классификация возможных генераторов электромагнитных импульсов, функционирующих в стандартной городской среде.
23. Методы защиты автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия: методы кодирования сигнала, возможные подходы к экранированию с использованием современных материалов.
24. Методы защиты АС и СВТ от внешнего электромагнитного воздействия: особенности работы генераторов белого шума и методы их аппаратной реализации. Параметры аппаратных генераторов белого шума.

Критерии оценивания:
Правильное решение 1 лабораторного задания – 10 баллов;
При выполнении 1 лабораторного задания были допущены неточности, не влияющие на результат – 7-9 баллов;
При выполнении 1 лабораторного задания были допущены ошибки – 4-6 баллов;
При выполнении 1 лабораторного задания были допущены существенные ошибки – 1-3 балла;
Неправильное решение 1 лабораторного задания – 0 баллов.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.
Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета и экзамена.

Зачет проводится по расписанию промежуточной аттестации в письменном виде. Количество вопросов в зачетном задании – 3. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику промежуточной аттестации, должны ликвидировать задолженность в установленном порядке.

Экзамен проводится по расписанию промежуточной аттестации в письменном виде. Количество вопросов в экзаменационном задании – 3. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику промежуточной аттестации, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия, формулируются методы, определяются средства обеспечения информационной безопасности, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач дисциплины.

При подготовке к лабораторным занятиям каждый студент должен:
- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы, помещённые в конце описания лабораторной работы.

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.