МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

_____Василенко В.Н.
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки

09.03.03 Прикладная информатика

Направленность (профиль) подготовки

Цифровизация бизнес-процессов

Квалификация выпускника

бакалавр

Воронеж

1. Цели и задачи дисциплины

Целью освоения дисциплины (модуля) является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

- 06.033 Связь, информационные и коммуникационные технологии (в сфере исследования, разработки, внедрения и сопровождения информационных технологий и систем) и *Разработка систем защиты информации автоматизированных систем, формирование требований к защите информации в автоматизированных системах*.

Дисциплина направлена на решение задач профессиональной деятельности следующих типов:

- производственно-технологического типа:
  - *- ведение технической документации;*
  - *тестирование компонентов ИС по заданным сценариям;*
  - *- проведение работ по инсталляции программного обеспечения информационных систем и загрузке баз данных;*
  - *- осуществление технического сопровождения информационных систем в процессе ее эксплуатации;*
- организационно-управленческого типа*:*
  - *- участие в координации работ по созданию, адаптации и сопровождению информационной системы;*
- *проектного типа:*
  - *- сбор и анализ детальной информации для формализации предметной области проекта и требований пользователей заказчика, интервьюирование ключевых сотрудников заказчика.*

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.03.03 – Прикладная информатика.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции
1	2	3
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ИД1 ОПК-3* знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
		ИД2 ОПК-3 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
		ИД3 ОПК-3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*ИД1 ОПК-4* Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
		ИД2 ОПК-4 Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
		ИД3 ОПК-4 Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.

Код и наименование индикатора достижения компетенции	В результате изучения учебной дисциплины обучающийся должен:		
	знать	уметь	владеть
3	4	5	6
ИД1 ОПК-3 знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Применять принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ИД2 ОПК-3 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Применять методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ИД3 ОПК-3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Знать особенности подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ИД1 ОПК-4 Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Применять основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Навыками применения основных стандартов оформления технической документации на различных стадиях жизненного цикла ин-

			формационной системы.
ИД2 *ОПК-4* Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Методы открытия и закрытия общего доступа к локальной сети знать, как программировать простейшие методы шифрования и дешифрования в сети, а также задавание паролей в операционной системе, и использование антивирусных программ	Применять методы открытия и закрытия общего доступа к локальной сети программировать простейшие методы шифрования и дешифрования задавать пароли в операционной системе уметь пользоваться антивирусными программами.	Навыками методов открытия и закрытия общего доступа к локальной сети, программировать методы шифрования и дешифрования владеть знаниями работой с антивирусными программами, а также задавать пароли в операционной системе
ИД3 *ОПК-4* Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.	Методы задания разграничения прав доступа пользователей к информации управления их полномочиями, методы оценивания стойкости различных паролей и методов шифрования, методы формирования паролей и ключей шифрования с заданной стойкостью	Применять методы задания разграничения прав доступа пользователей к информации управления их полномочиями, уметь использовать методы оценивания стойкости различных паролей, а также шифрования и формировать пароли и ключи шифрования с заданной стойкостью	Навыками задания разграничения прав доступа пользователей к информации управления их навыками оценивания стойкости различных методов и паролей шифрования, владеть навыками формирования паролей и ключей шифрования с заданной стойкостью

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к обязательной части и ОП ВО. Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин: «Базы данных», «Исследование операций и методы оптимизации», «Вычислительные системы, сети и телекоммуникации», «Проектирование информационных систем».

Знания, полученные в ходе изучения дисциплины, используются при подготовке к ГИА.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины (модуля) составляет __2__ зачетные единицы.

Виды учебной работы	**Всего академических часов**	**Распределение трудоемкости по семестрам, ак. ч**
		Семестр 6
		Акад. ч
Общая трудоемкость дисциплины (модуля)	**72**	**72**
Контактная работа в т. ч. аудиторные занятия:	**37**	**37**
Лекции	18	18
в том числе в форме практической подготовки	-	-
Практические занятия	18	18
в том числе в форме практической подготовки	-	-
Консультации текущие	0,9	0,9
Вид аттестации: зачет	0,1	0,1

Самостоятельная работа:	**35**	**35**
Проработка материалов по лекциям, учебным пособиям	25	25
Подготовка к практическим и лабораторным занятиям	7	7
Домашнее задание, реферат,	3	3

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела (указывается в дидактических единицах)	Трудоемкость, час
1	Общие проблемы безопасности, роль и место информационной безопасности	Общие проблемы безопасности. Роль и место информационной безопасности	9
2	Общие сведения о защите информации	Характеристики информации, угрозы защищенности информации. Задачи, основные предметные направления, примеры способов и стандарты в области защиты информации	9
3	Защита информации в информационных системах	Предмет, элементы и объекты защиты информации в ИС, а также дестабилизирующие факторы, причины нарушения целостности информации, каналы несанкционированного получения информации и угрозы безопасности. Функции, задачи, методы и системы защиты информации в ИС	9
4	Криптографические методы защиты информации	Методы криптографического преобразования данных, электронная цифровая подпись. Проблемы реализации методов криптографической защиты в ЭИС, характеристики криптографических средств защиты	9
5	Особенности защиты информации в персональных компьютерах	Общие положения по применению системы «Кобра». Защита в среде MS-DOS, защита в средах Windows, классификация компьютерных вирусов	9
6	Антивирусные программы	Антивирусы-полифаги. Программы-ревизоры, антивирусные программы	9
7	Проблемы защиты информации в сетях	Цели, функции и задачи защиты информации в сетях, понятие сервисов безопасности, международные стандарты X.800 и X.509. Методы цифровой подписи данных, передаваемых в сети, пример системы защиты локальной вычислительной сети, межсетевые экраны – брандмауэры (FireWall), прокси (Proxy) серверы	9
8	Методы оценки эффективности защиты и комплексное обеспечение безопасности	Методы оценки эффективности защиты и комплексное обеспечение безопасности.	8

	Консультации текущие	0,9
	Зачет	0,1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Общие проблемы безопасности, роль и место информационной безопасности	2		2	4
2	Общие сведения о защите информации	2		2	4
3	Защита информации в информационных системах	2		2	4
4	Криптографические методы защиты информации	2		2	4
5	Особенности защиты информации в персональных компьютерах	2		2	4
6	Антивирусные программы	2		2	4
7	Проблемы защиты информации в сетях	3		3	6
8	Методы оценки эффективности защиты и комплексное обеспечение безопасности	3		3	5
	ИТОГО	18		18	35

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Общие проблемы безопасности, роль и место информационной безопасности	Общие проблемы безопасности. Роль и место информационной безопасности	2
2	Общие сведения о защите информации	Характеристики информации, угрозы защищенности информации. Задачи, основные предметные направления, примеры способов и стандарты в области защиты информации	2
3	Защита информации в информационных системах	Предмет, элементы и объекты защиты информации в ИС, а также дестабилизирующие факторы, причины нарушения целостности информации, каналы несанкционированного получения информации и угрозы безопасности. Функции, задачи, методы и системы защиты информации в ИС	2
4	Криптографические методы защиты информации	Методы криптографического преобразования данных, электронная цифровая подпись. Проблемы реализации методов криптографической защиты в ЭИС, характеристики криптографических средств защиты	2
5	Особенности защиты информации в персональных компьютерах	Общие положения по применению системы «Кобра». Защита в среде MS-DOS, защита в средах Windows, классификация компьютерных вирусов	2
6	Антивирусные программы	Антивирусы-полифаги. Программы-ревизоры, антивирусные программы	2
7	Проблемы защиты информации в сетях	Цели, функции и задачи защиты информации в сетях, понятие сервисов безопасности, международные стандарты X.800 и X.509. Методы цифровой подписи данных, передаваемых в сети, пример системы защиты локальной вычислительной сети, межсетевые экраны – брандмауэры (FireWall), прокси (Proxy) серверы	1
8	Методы оценки эффективности защиты и комплексное обеспечение безопасности	Методы оценки эффективности защиты и комплексное обеспечение безопасности.	1
	Итого		18

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Общие проблемы безопасности, роль и место информационной безопасности	Общие проблемы безопасности. Роль и место информационной безопасности	2
2	Общие сведения о защите информации	Характеристики информации, угрозы защищенности информации. Задачи, основные предметные направления, примеры способов и стандарты в области защиты информации	2
3	Защита информации в информационных системах	Предмет, элементы и объекты защиты информации в ИС, а также дестабилизирующие факторы, причины нарушения целостности информации, каналы несанкционированного получения информации и угрозы безопасности. Функции, задачи, методы и системы защиты информации в ИС	2
4	Криптографические методы защиты информации	Методы криптографического преобразования данных, электронная цифровая подпись. Проблемы реализации методов криптографической защиты в ЭИС, характеристики криптографических средств защиты	2
5	Особенности защиты информации в персональных компьютерах	Общие положения по применению системы «Кобра». Защита в среде MS-DOS, защита в средах Windows, классификация компьютерных вирусов	2
6	Антивирусные программы	Антивирусы-полифаги. Программы-ревизоры, антивирусные программы	2
7	Проблемы защиты информации в сетях	Цели, функции и задачи защиты информации в сетях, понятие сервисов безопасности, международные стандарты X.800 и X.509. Методы цифровой подписи данных, передаваемых в сети, пример системы защиты локальной вычислительной сети, межсетевые экраны – брандмауэры (FireWall), прокси (Proxy) серверы	1
8	Методы оценки эффективности защиты и комплексное обеспечение безопасности	Методы оценки эффективности защиты и комплексное обеспечение безопасности.	1
	Итого		18

5.2.3 Лабораторный практикум

Не предусмотрены

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Общие проблемы безопасности, роль и место информационной безопасности	Проработка конспекта лекций	1
		Проработка материалов учебников	1
		подготовка реферата по теме «Роль и место информационной безопасности»	2
2	Общие сведения о защите информации	Проработка конспекта лекций материалов учебников, подготовка реферата по теме «Примеры способов и стандарты в области защиты информации»	1
		Проработка материалов учебников	1
		подготовка реферата по теме «Примеры способов и стандарты в области защиты информации»	2
3	Защита информации в информационных системах	Проработка конспекта лекций, материалов учебников, подготовка реферата по теме «Предмет, элементы и объекты защиты информации в ИС»	1
		Проработка материалов учебников	1
		Подготовка реферата по теме «Предмет, элементы и объекты защиты информации в ИС»	2
4	Криптографические методы защиты информации	Реферат «Методы криптографического преобразования данных»	5
5	Особенности защиты информации в персональных компьютерах	Подготовка по конспекту лекций, учебнику к коллоквиуму по теме «Защита в среде MS-DOS, защита в средах Windows, классификация компьютерных вирусов»	5
6	Антивирусные программы	Подготовка по конспекту лекций, учебнику к коллоквиуму, тестированию по теме «Антивирусы-полифаги. Программы-ревизоры, антивирусные программы»	5
7	Проблемы защиты информации в сетях	Подготовка по конспекту лекций, учебнику к коллоквиуму, тестированию по теме «Методы цифровой подписи данных, передаваемых в сети, пример системы защиты локальной вычислительной сети, межсетевые экраны»	5
8	Методы оценки эффективности защиты и комплексное обеспечение безопасности	Подготовка по конспекту лекций, учебнику к коллоквиуму, тестированию по теме «Методы оценки эффективности защиты и комплексное обеспечение безопасности»	5
	Итого		72

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: 3http://biblioclub.ru/index.php?page= book&id=499170 (дата обращения: 14.01.2020). – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный.

2. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page= book&id=571485 (дата обращения: 14.01.2020). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – Текст : электронный.

3. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 14.01.2020). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

6.2. Дополнительная литература

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 14.01.2020). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

2. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 14.01.2020). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

6.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. *Сайт научной библиотеки ВГУИТ* <*http://cnit.vsuet.ru*>.
2. *Государственная публичная научно-техническая библиотека.* <*www.gpntb.ru/*>.
3. *Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов.* <*http://www.ict.edu.ru/*>.
4. *Национальная электронная библиотека.* <*www.nns.ru/*>.
5. *Электронная библиотечная система "Книгафонд"* <*http://www.knigafund.ru*>.
6. *Поисковая система «Рамблер».* <*www.rambler.ru/*>.
7. *Поисковая система «Яндекс».* <*www.yandex.ru/*>.
8. *Российская государственная библиотека.* <*www.rsl.ru/*>.
9. *Российская национальная библиотека.* <*www.nlr.ru/*>.
10. *Единый портал интернет-тестирования.* <*www.i-exam.ru*>.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Информационная безопасность и защита информации [Электронный ресурс] : методические указания для самостоятельной работы для студентов, обучающихся по направлению 09.03.02– «Информационные системы и технологии», очной формы обучения / А. В.Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. – Воронеж : ВГУИТ, 2016. - 20 с.

6.5 Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж : ВГУИТ, 2016. – Режим доступа : http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813. - Загл. с экрана

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Лекционные аудитории, оснащенные мультимедийной техникой	Аудио-визуальная система лекционных аудиторий (мультимедийный проектор, экран, усилитель мощности звука, акустические системы, микрофоны, устройство коммутации, сетевой коммутатор для подключения к компьютерной сети (Интернет))	MS Windows Vista Business UPG OLP AERussian договор 011 от 14.04.2007 MS Office 2007 Professional Plus Russian OLP AE договор Tr032591 от 12.09.2008
Аудитории для проведения занятий семинарского типа.	Комплекты мебели для учебного процесса – 30 шт.	
Читальные залы библиотеки.	Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами.	
Аудитории для проведения лабораторных и практических занятий	Комплекты мебели для учебного процесса. Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Core i5-4570), стенды – 5 шт., ауд.№ 420 комп класс каф. ИнфБ ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; ауд. №424 комп. класс каф. ИнфБ, количество ПЭВМ -12,(рабочая станция CPU Core 2Duo E6300 – 1.86), стенды – 3 шт.	Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Windows 2003 Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare PlayerБесплатное ПО; Антивирус “Зоркий глаз”Бесплатное ПО; Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop)Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free PascalБесплатное ПО; Программно-аппаратный комплекс средств защиты от несанкционированного доступа для ПЭВМ «Аккорд-АМДЗ» Сертификат ФСЭТЭК Д 567210 Сертификат ФСЭТЭК Д 567211 2 комплекса 26.12.2012 г.
Аудитории для СРС	Комплекты мебели для учебного процесса. Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Core i5-4570), стенды – 5 шт., ауд.№ 420 комп класс каф. ИнфБ ПЭВМ-12 (компьютер Core i5-4460), про-	Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Windows 2003 Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессио-

	ектор Acer projector X1383WH, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; ауд. №424 комп. класс каф. ИнфБ, количество ПЭВМ -12,(рабочая станция CPU Core 2Duo E6300 – 1.86), стенды – 3 шт.	нальная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare PlayerБесплатное ПО; Антивирус “Зоркий глаз”Бесплатное ПО; Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop)Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free PascalБесплатное ПО; Программно-аппаратный комплекс средств защиты от несанкционированного доступа для ПЭВМ «Аккорд-АМДЗ» Сертификат ФСЭТЭК Д 567210 Сертификат ФСЭТЭК Д 567211 2 комплекса 26.12.2012 г.
Помещения для хранения и профилактического обслуживания учебного оборудования	А.434. ПЭВМ-2 (компьютер Core i5-4570)	MS Windows XP, Windows 2003 Server, Windows 7 UPG OLP AERussian договор 011 от 14.04.2007 MS Office 2003, MS Office 2007 Professional Plus Russian OLP AE договор Tr032591 от 12.09.2008 FreePascal

7. Материально-техническое обеспечение дисциплины (модуля)

При чтении лекций используется мультимедийное оборудование (проектор) кафедры информационной безопасности (а. 420).

Для проведения практических работ, а также для проведения обучения и контроля знаний обучающихся на едином портале интернет-тестирования, для выполнения расчетных работ кафедра информационной безопасности обладает специализированными аудиториями (а. 332а, 420, 424), оснащенными в каждой аудитории 12 ПК Intel Core 2 Duo, сетью Интернет.

Документ составлен в соответствии с требованиями ФГОС 3++ ВО по направлению 09.03.03 – «Прикладная информатика».

ПРИЛОЖЕНИЕ
к рабочей программе

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Организационно-методические данные дисциплины для заочной формы обучения

1.1 Объемы различных форм учебной работы и виды контроля в соответствии с учебным планом

Виды учебной работы	Всего академических часов	Распределение трудоемкости по семестрам, ак. ч
		Семестр 6
		Акад. ч
Общая трудоемкость дисциплины (модуля)	**72**	**72**
Контактная работа в т. ч. аудиторные занятия:	**37**	**37**
Лекции	18	18
в том числе в форме практической подготовки	-	-
Практические занятия	18	18
в том числе в форме практической подготовки	-	-
Консультации текущие	0,9	0,9
Вид аттестации: зачет	0,1	0,1
Самостоятельная работа:	**35**	**35**
Проработка материалов по лекциям, учебным пособиям	25	25
Подготовка к практическим и лабораторным занятиям	7	7
Домашнее задание, реферат,	3	3

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Информационная безопасность

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ИД1 $_{ОПК-3}$* знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
			ИД2 $_{ОПК-3}$ Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
			ИД3 $_{ОПК-3}$. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
2	ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	*ИД1 $_{ОПК-4}$* Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
			ИД2 $_{ОПК-4}$ Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
			ИД3 $_{ОПК-4}$ Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 $_{ОПК-3}$ знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Умеет: применять принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Владеет: принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ИД2 $_{ОПК-3}$ Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает: методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Умеет: применять методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	Владеет: Методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной без-опасности.
ИД3 $_{ОПК-3}$. Иметь навыки: подготовки обзоров, аннотаций,	Знать: особенности подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской

составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	работе с учетом требований информационной безопасности.
	Уметь: проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ИД1 $_{ОПК-4}$ Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать: Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
	Применять основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
	Навыками применения основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.
ИД2 $_{ОПК-4}$ Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знать: Методы открытия и закрытия общего доступа к локальной сети знать, как программировать простейшие методы шифрования и дешифрования в сети, а также задавание паролей в операционной системе, и использование антивирусных программ
	Уметь: Применять методы открытия и закрытия общего доступа к локальной сети программировать простейшие методы шифрования и дешифрования задавать пароли в операционной системе уметь пользоваться антивирусными программами.
	Владеть: Навыками методов открытия и закрытия общего доступа к локальной сети, программировать методы шифрования и дешифрования владеть знаниями работой с антивирусными программами, а также задавать пароли в операционной системе
ИД3 $_{ОПК-4}$ Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.	Знать: Методы задания разграничения прав доступа пользователей к информации управления их полномочиями, методы оценивания стойкости различных паролей и методов шифрования, методы формирования паролей и ключей шифрования с заданной стойкостью
	Уметь: Применять методы задания разграничения прав доступа пользователей к информации управления их полномочиями, уметь использовать методы оценивания стойкости различных паро-лей, а также шифрования и формировать пароли и ключи шифрования с заданной стойкостью
	Владеть: Навыками задания разграничения прав доступа пользователей к информации управления их навыками оценивания стойкости раз-личных методов и па-ролей шифрования, владеть навыками формирования паролей и ключей шифрования с заданной стойкостью

Код и наименование индикатора достижения компетенции	В результате изучения учебной дисциплины обучающийся должен:		
	знать	уметь	владеть
3	4	5	6
ИД1 $_{ОПК-3}$ знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Применять принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ИД2 ОПК-3 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Применять методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ИД3 ОПК-3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Знать особенности подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ИД1 ОПК-4 Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Применять основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Навыками применения основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы.
ИД2 ОПК-4 Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Методы открытия и закрытия общего доступа к локальной сети знать как программировать простейшие методы шифрования и дешифрования в сети а также задавание паролей в операционной системе, и использование антивирусных программ	Применять методы открытия и закрытия общего доступа к локальной сети программировать простейшие методы шифрования и дешифрования задавать пароли в операционной системе уметь пользоваться антивирусными программами.	Навыками методов открытия и закрытия общего доступа к локальной сети, программировать методы шифрования и дешифрования владеть знаниями работой с антивирусными программами, а также задавать пароли в операционной системе
ИД3 ОПК-4 Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.	Методы задания разграничения прав доступа пользователей к информации управления их полномочиями, методы оценивания стойкости различных паролей и методов шифрования, методы формирования паролей и ключей шифрования с заданной стойкостью	Применять методы задания разграничения прав доступа пользователей к информации управления их полномочиями, уметь использовать методы оценивания стойкости различных паролей, а также шифрования и формировать пароли и ключи шифрования с заданной стойкостью	Навыками задания разграничения прав доступа пользователей к информации управления их навыками оценивания стойкости различных методов и паролей шифрования, владеть навыками формирования паролей и ключей шифрования с заданной стойкостью

2 Паспорт оценочных материалов по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Номера вопросов	Технология оценки (способ контроля)
1	Основы информационной безопасности. Основные понятия и определения. Политика государства в области информационной безопасности	ОПК-3, ОПК-4	Вопросы к зачету	1-8	Проверка преподавателем
			Тесты (тестовые задания)	65-79	Бланочное тестирование
			Вопросы к текущим опросам на лабораторных работах	223-230	Проверка преподавателем
2	Угрозы и нарушители безопасности информации. Модель угроз безопасности информации (Модель угроз ИБ)		Вопросы к зачету	9-17	Проверка преподавателем
			Тесты (тестовые задания)	80-94	Бланочное тестирование
			Вопросы к текущим опросам на лабораторных работах	231-238	Проверка преподавателем
3	Меры обеспечения защиты информации. Организационные меры защиты информации		Вопросы к зачету	18-26	Проверка преподавателем
			Тесты (тестовые задания)	55-109	Бланочное тестирование
			Вопросы к текущим опросам на лабораторных работах	239-246	Проверка преподавателем
4	Методы контроля и разграничения доступа		Тесты (тестовые задания)	110-124	Бланочное тестирование
			Вопросы к зачету	27-35	Проверка преподавателем
			Кейс-задания к практическим работам	167-222	Проверка преподавателем
			Вопросы к текущим опросам на лабораторных работах	247-254	Проверка преподавателем
5	Исторический обзор криптографических методов защиты информации		Вопросы к зачету	36-44	Проверка преподавателем
			Вопросы к текущим опросам на лабораторных работах	255-259	Проверка преподавателем
			Тесты (тестовые задания)	125-139	Бланочное тестирование
6	Криптографические методы защиты информации. Стеганографическая защита информации		Вопросы к зачету	45-53	Проверка преподавателем
			Темы рефератов	259-275	Проверка преподавателем
7	Техническая защита информации. Программно-технические меры защиты информации		Вопросы к зачету	54-62	Проверка преподавателем
			Тесты (тестовые задания)	140-154	Бланочное тестирование
8	Политика безопасности организации. Системы обнаружения и предотвращения компьютерных атак. Основные стандарты в области информационной безопасности		Темы рефератов	276-294	Проверка преподавателем
			Вопросы к зачету	63-64	Проверка преподавателем
			Тесты (тестовые задания)	155-166	Проверка преподавателем

3 Оценочные материалы для промежуточной аттестации.

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

Аттестация обучающегося по дисциплине проводится в форме собеседования (зачета).

Каждый вариант включает 3 контрольных заданий, из них:
- 1 контрольных заданий на проверку знаний;
- 2 контрольных заданий на проверку умений;
- 3 контрольных заданий на проверку навыков.

3.1 Вопросы к собеседованию на зачете

3.1.1 Шифр и наименование компетенции

ИД1 $_{ОПК-3}$ знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

№ задания	Формулировка вопроса
1.	Раскройте содержание основных принципов Доктрины ИБ РФ.
2.	Перечислите основные направления обеспечения ИБ в мировой практике
3.	Сформулируйте основные задачи обеспечения ИБ РФ
4.	Приведите основные функции государственной системы обеспечения ИБ РФ
5.	Каковы уровни доступа к информации с точки зрения законодательства?
6.	Что такое информация ограниченного распространения?
7.	Сформулируйте задачи обеспечения безопасности функционирования информации в КС
8.	Каковы виды доступа к информации?
9.	Каковы основные отечественные и зарубежные стандарты в области ИБ?

ИД2 $_{ОПК-3}$ Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

10.	В чем может заключаться ответственность за нарушение законодательства в информационной сфере?
11.	Приведите основную классификацию методов и средств нейтрализации угроз
12.	Какая система называется безопасной, а какая - надежной?
13.	Что такое политика безопасности?
14.	Каковы основные предметные направления защиты информации?

ИД3 $_{ОПК-3}$. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

15.	Что такое государственная тайна?
16.	Что такое коммерческая тайна?
17.	Что такое служебная тайна?
18.	Что такое профессиональная тайна?
19.	Что такое персональные данные?
20.	Что такое источники права на доступ к информации?

ИД1 $_{ОПК-4}$ Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

21.	Каковы основные эволюционные подходы к обеспечению ИБ деятельности общества?
22.	Дайте определение информационного оружия.
23.	Приведите формулу Д. Медоуза. Что она характеризует и каковы области ее применения?
24.	Сформулируйте основные проблемы ИБ.
25.	Перечислите основные объекты и субъекты защиты процессов переработки информации
26.	Сформулируйте три варианта доступа субъекта к объекту
27.	Перечислите основные признаки ИБ объектов и субъектов
28.	Перечислите основные принципы защиты процессов переработки информации в АИТ
29.	Приведите классификацию организационных и правовых методов и средств предотвращения угроз ИБ
30.	Приведите классификацию методов предотвращения угроз шпионажа и диверсий
31.	Приведите классификацию методов предотвращения угроз несанкционированного доступа в КС
32.	Приведите классификацию методов предотвращения случайных угроз
33.	Приведите классификацию криптографических методов предотвращения угроз
34.	Приведите классификацию основных методов и средств парирования угроз
35.	Перечислите четыре основные группы методов и средств защиты процессов переработки информации в защищенной КС.
36.	Какие цели преследует криптография?
37.	Перечислите основные алгоритмы криптографических преобразований
38.	Объясните понятия «целостности, подлинности и конфиденциальности» информации
39.	Роль и место информационной безопасности
40.	Характеристики информации, угрозы защищенности информации

ИД2 $_{ОПК-4}$ Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

41.	Примеры способов и стандарты в области защиты информации
42.	Предмет, элементы и объекты защиты информации в ИС
43.	Дестабилизирующие факторы ИС
44.	Причины нарушения целостности информации
45.	Каналы несанкционированного получения информации и угрозы безопасности
46.	Функции, задачи, методы и системы защиты информации в ИС
47.	Методы криптографического преобразования данных
48.	Электронная цифровая подпись
49.	Характеристики криптографических средств защиты
50.	Общие положения по применению системы «Кобра»
51.	Защита в среде MS-DOS

ИД3 $_{ОПК-4}$ Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.

52.	Защита в средах Windows
53.	Классификация компьютерных вирусов
54.	Антивирусы-полифаги
55.	Программы-ревизоры
56.	Антивирусные программы
57.	Цели, функции и задачи защиты информации в сетях
58.	Понятие сервисов безопасности, международные стандарты X.800 и X.509
59.	Методы цифровой подписи данных, передаваемых в сети
60.	Пример системы защиты локальной вычислительной сети
61.	Межсетевые экраны – брандмауэры (FireWall), прокси (Proxy) серверы
62.	Методы оценки эффективности защиты и комплексное обеспечение безопасности
63.	Концепция изолированной программной среды
64.	Эталонная модель защищенной автоматизированной системы

3.2 Тесты (тестовые задания)

3.2.1 *Шифр и наименование компетенции* ОПК-3,4 – Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

3.3 Тесты (тестовые задания)

3.1.1. Шифр и наименование компетенции

ИД1 ОПК-3 знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

№ задания	Тест (тестовое задание)
65.	Под информацией, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», понимается: а) Сведения, представленные в виде, пригодном для обработки средствами вычислительной техники; б) Совокупность сведений, хранимых, обрабатываемых и передаваемых в информационных системах; **в) Сведения независимо от формы их представления верно;** г) Совокупность сведений, подлежащих хранению, передаче, обработке и использованию
66.	В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», _____ информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Ответ: **обладатель**
67.	В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации», _____ _____ - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Ответ: информационная система
68.	_____ – свойство информации, заключающееся в отсутствии в ней любых изменений за исключением санкционированных.

	Ответ: **целостность**
69.	_____ – свойство информации, заключающееся в возможности легального пользователя получить к ней беспрепятственный доступ, возможно, при выполнении условий, установленных владельцем информации. Ответ: **доступность**
70.	Согласно федеральному закону «Об информации, информационных технологиях и о защите информации», _____ – сведения независимо от формы их представления. Ответ: **информация**
71.	Данными, согласно ГОСТ «Системы обработки информации. Термины и определения», называется информация, представленная в виде, пригодном для обработки: а) средствами вычислительной техники; б) автоматизированными системами; в) информационными системами под управлением человека; г**) автоматическими средствами при возможном участии человека.**
72.	Под электронным сообщением, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», понимается информация: а) представленная в электронном виде, пригодном для передачи при помощи средств вычислительной техники; б) оформленная в виде электронного документа, передаваемого или полученного по сетям связи; **в) переданная или полученная пользователем информационно-телекоммуникационной сети;** г) передаваемая по информационно-телекоммуникационной сети с использованеим средств вычислительной техники.
73.	Согласно федеральному закону «Об информации, информационных технологиях и о защите информации», лицо, не создавшее самостоятельно информацию, считается ее обладателем, если оно получило на основании закона или договора право: а) предоставлять информацию; **б) разрешать или ограничивать доступ к информации другим лицам;** в) разрешать доступ к информации другим лицам; г) использовать информацию.
74.	Укажите все компоненты, входящие, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», в понятие «Информационные технологии»: **а) процессы проведения операций над информацией;** **б) методы проведения операций над информацией**; в) программные реализации методов проведения операций над информацией; г) устройства, содержащие программные реализации методов проведения операций с информацией; д) технические средства, обеспечивающие работу устройств; **е) способы осуществления процессов и методов проведения операций над информацией;** ж) методы взаимодействия устройств и пользователей информации.
75.	Укажите все компоненты, входящие, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», в понятие «Информационная система»: а) аппаратное обеспечение; б) программное обеспечение; **в) технические средства;** **г) информация в базах данных;** д) информация на внутренних и внешних носителях; **е) информационные технологии;** ж) пользователь.
76.	Укажите все операции, для которых, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», пригоден вид представления информации, являющейся электронным документом: а) обработка при помощи электронно-вычислительных машин; **б) восприятие человеком с использованием электронно-вычислительных машин;** **в) обработка в информационных системах;** г) обработка в автоматизированных системах; **д) передача по информационно-телекоммуникационным сетям.**
77.	Автоматизированная система, согласно гост «информационная технология. комплекс стандартов на автоматизированные системы. автоматизированные системы. термины и определения», состо-

	ит из: а) установленных функций персонала и средств автоматизации их выполнения; б) информации и средств автоматизации ее обработки; в) информационной технологии и средств автоматизации ее осуществления; **г) персонала и комплекса средств автоматизации его деятельности.**
78.	Укажите все компоненты, входящие, согласно гост «защита информации. объект информатизации. факторы, воздействующие на информацию. общие положения», в понятие «объект информатизации»: **а) информационные ресурсы;** б) информационные технологии; в) носители информации; г) персонал; **д) помещения и объекты;** е) информационно-телекоммуникационная сеть; **ж) средства и системы обработки информации.**
79.	Укажите все возможные основания для защиты информации, предусмотренные понятием «Защищаемая информация», согласно ГОСТ «Защита информации. Основные термины и определения»: **а) требования собственника информации;** б) результат экспертной оценки; **в) требования правовых документов;** г) решение суда; д) соглашение между собственником и пользователем информации.
80.	Укажите все варианты того, что может являться объектом защиты информации, предусмотренные ГОСТ «Защита информации. Основные термины и определения»: **а) информация;** **б) носитель информации;** в) система обработки информации г) информационная технология **д) информационный процесс;**
81.	Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение, согласно ГОСТ «Защита информации. Основные термины и определения» называется _____ защищаемой информации. Ответ: **носитель**

ИД2 $_{ОПК-3}$ Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

82.	Целостность информации заключается в том, что: а) в информацию не было внесено никаких изменений с момента ее создания; б) информация является полностью и достоверно описывающей некоторое обстоятельство; **в) при предоставлении информации версии обладателя информации и лица, получившего к ней доступ, не отличаются;** г) информация находится на неповрежденном носителе.
83.	Доступность – свойство информации, заключающееся в возможности _____ пользователя получить к ней беспрепятственный доступ. Ответ: **легального**
84.	Укажите все действия с информацией, возможность которых, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», получает лицо, которому предоставлен доступ к информации: **а) получение;** б) ознакомление; в) распространение; **г) использование;** д) передача; е) предоставление.

85.	Предоставление информации отличается от распространения информации, согласно федеральному закону «Об информации, информационных технологиях и о защите информации»: **а) лицом или кругом лиц, осуществляющим получение информации верно;** б) количеством лиц, осуществляющих получение информации; в) лицом или кругом лиц, осуществляющим передачу информации; г) стороной, являющейся инициатором действий; д) конфиденциальностью передаваемой информации; ж) формой представления передаваемой информации.
86.	Укажите все компоненты, входящие, согласно ГОСТ «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», в понятие «Система обработки информации»: **а) программное обеспечение;** **б) технические средства;** **в) действия персонала;** **г) методы обработки информации;** д) методы хранения информации; е) методы передачи информации; ж) информационные технологии.
87.	Информация обладает свойством конфиденциальности в ситуации, когда: а) единственный носитель информации полностью уничтожен; **б) доступ к служебному документу имеет только несколько сотрудников верно;** в) единственный экземпляр неопубликованной рукописи хранится у ее автора; г) для получения доступа к ресурсам электронной библиотеки необходимо пройти регистрацию; д) документ присутствует только у ее автора, только что завершившего его создание.
88.	Укажите все ситуации, в которых указывается на нарушение конфиденциальности информации: **а) разглашение пользователем пароля от своей электронной почты по халатности верно;** б) уничтожение документа, содержащего секретные сведения, после прочтения; **в) утеря носителя информации верно;** г) уничтожение носителя информации.
89.	Укажите все ситуации, в которых указывается на нарушение целостности информации: а) внесение оперативных изменений в электронное расписание занятий ответственными за составление расписания сотрудниками; б) изменение службой вокзала расписания поездов, опубликованного на сайте, в связи с отменой части поездов; **в) внесение изменений в подписанный экземпляр договора верно;** **г) редактирование чужого сообщения на сайте верно;** д) ситуация, в которой сообщение пользователя на сайте скрыто модератором от других пользователей; е) физическое повреждение носителя информации.
90.	Систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере представляет документ под названием « _____ _____ _____ Российской Федерации». Ответ: **доктрина информационной безопасности**
91.	Информационная инфраструктура РФ, согласно Доктрине информационной безопасности Российской Федерации, - это совокупность объектов _____, информационных систем, сайтов в сети "Интернет" и сетей связи. Ответ: **информатизации**
92.	В соответствии с федеральным законом "Об информации, информационных технологиях и о защите информации", право разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, если иное не предусмотрено федеральными законами, принадлежит _____ информации. Ответ: **обладателю**
93.	В соответствии с федеральным законом "Об информации, информационных технологиях и о защите информации", обладатель информации обязан принимать меры по _____ _____. Ответ: **защите информации**
94.	В соответствии с Федеральным законом «О государственной тайне», отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с принципами законности, обоснованности и _____.

	Ответ: **своевременности**
95.	В соответствии с Федеральным законом «О государственной тайне», реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него, называются _____ _____. Ответ: **гриф секретности**
96.	В соответствии с Федеральным законом «О коммерческой тайне», коммерческая тайна - _____ конфиденциальности информации, позволяющий ее обладателю получить коммерческую выгоду. Ответ: **режим**
97.	В соответствии с Федеральным законом «О коммерческой тайне», не могут составлять коммерческую тайну сведения, содержащиеся в документах, дающих право на осуществление _____ деятельности. Ответ: **предпринимательской**
98.	В соответствии с Федеральным законом «О коммерческой тайне», лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны, называется _____ информации, составляющей коммерческую тайну. Ответ: **обладатель**

ИДЗ $_{ОПК-3}$. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

99.	В соответствии с Федеральным законом «О персональных данных», персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (_____ персональных данных). Ответ: **субъекту**
100.	В соответствии с Федеральным законом «О персональных данных», действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных, называются _____ персональных данных. Ответ: **уничтожением**
101.	Место информационной безопасности в национальной безопасности Российской Федерации как одной из ее составных частей определяется в **а) стратегии национальной безопасности;** б) законе «о безопасности»; в) доктрине информационной безопасности; г) стратегии информационной безопасности; д) доктрине национальной безопасности
102.	Информационная безопасность, согласно Стратегии национальной безопасности Российской Федерации, а) является самостоятельным видом безопасности наряду с национальной безопасностью; б) входит в понятие национальной безопасности вместе с другими видами безопасности; **в) входит в понятие национальной безопасности вместе с обороной страны и другими видами безопасности;** г) входит в понятие национальной безопасности вместе с внешней политикой и другими видами безопасности.
103.	Место информационной безопасности в национальной безопасности определено в документе под названием «_____ национальной безопасности Российской Федерации» Ответ: **стратегия**
104.	Укажите все компоненты, согласно Доктрине информационной безопасности Российской Федерации, входящие в понятие «Информационная инфраструктура РФ»: **А) объекты информатизации;**

	Б) информация в базах данных; **В) информационные системы;** Г) информационные технологии; **Д) сети связи.**
105.	В соответствии с Доктриной информационной безопасности Российской Федерации, совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере, называется _____ информационной безопасности РФ. Ответ: **угроза** или **угрозой**
106.	Согласно ГОСТ «Защита информации. Основные термины и определения», угроза (безопасности информации) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность _____ _____ информации. Ответ: **нарушения безопасности**
107.	Укажите все предусмотренные ГОСТ «Защита информации. Основные термины и определения» результаты явления, действия или процесса, при которых данное явление, действие или процесс является фактором, воздействующим на защищаемую информацию **А) утечка информации;** Б) блокирование работы информационной системы; В) вывод из строя информационной системы; Г) распространение информации; **Д) уничтожение информации.**
108.	Определение типа нарушителя, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., основывается на: а) возможности нарушителя легально попасть на территорию объекта информатизации; б) Месте нахождения нарушителя при реализации угрозы; **в) Наличии у нарушителя прав доступа к элементам АС;** г) Наличии у нарушителя конфиденциальной служебной информации, связанной с настройками и средствами защиты АС.
109.	Возможность осуществлять несанкционированный доступ к информации в АС, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., имеют нарушители с потенциалом: а) всех уровней; б) не ниже базового повышенного; **в) только высоким;** г) базовым повышенным или высоким.
110.	Модель нарушителя, составленная согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., «Внутренний, лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора; базовый; непреднамеренные, неосторожные или неквалифицированные действия; физическое воздействие на линии связи» соответствует **а) штатному электрику, при проведении регламентных работ случайно повреждающему кабель локальной вычислительной сети;** б) приглашенному электрику, при установке электрического счетчика случайно повреждающему кабель канал доступа к сети internet; в) уборщице, подкупленной конкурентами, во время проведения уборки повреждающей коммутатор локальной вычислительной сети; г) сотруднику компании, обеспечивающей электроснабжение объекта информатизации, повреждающему кабель локальной вычислительной сети во время производимой по собственной инициативе сверки показаний счетчика электроэнергии.
111.	Актуальность угрозы, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., означает, что: а) в информационной системе существует возможность реализации угрозы; б) существует актуальный для данной информационной системы нарушитель с достаточным потенциалом для реализации угрозы; **в) в информационной системе существует возможность реализации угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к нанесению ущерба;** г) реализация угрозы нанесет ущерб владельцу или оператору информации либо субъекту персональных данных д) в информационной системе существует достаточная (средняя или высокая) вероятность реализации угрозы, а ее последствия имеют средний или высокий уровень наносимого ущерба.
112.	При оценке вероятности реализации угрозы безопасности информации, согласно Методике опре-

	деления угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., характеристика «Зафиксированы случаи реализации данной угрозы» определяет _____ вероятность реализации угрозы. Ответ: **средняя**
113.	Для оценки возможности реализации угрозы безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., необходимо учитывать следующие параметры угрозы и информационной системы: а) уровень защищенности информационной системы, потенциал нарушителя; **б) уровень защищенности или проектной защищенности информационной системы, потенциал нарушителя;** в) уровень проектной защищенности информационной системы, потенциал нарушителя; г) уровень проектной защищённости информационной системы, потенциал нарушителя или уровень ущерба.
114.	По способам осуществления меры обеспечения защиты информации подразделяются на: **а) законодательные, морально-этические, административные, организационно-технические, программно-технические;** б) законодательные, морально-этические, административные, организационные, программно-технические; в) организационные, криптографические, меры технической зи, стеганографические; г) законодательные, морально-этические, административные, организационно-технические.
115.	Любые действующие на территории объекта информатизации правила, регламентирующие доступ к информации и порядок работы с ней, вместе с мерами обеспечения и контроля исполенния таких правил, составляют: а) административные меры ЗИ; б) координирующие меры ЗИ; **в) организационные меры ЗИ;** г) организационно-технические меры ЗИ.

ИД1 *ОПК-4* Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

116.	Укажите все документы, относящиеся к координирующим мерам ЗИ: Выберите все подходящие варианты а) кодекс об административных правонарушениях; **б) закон о коммерческой тайне;** в) уголовный кодекс; **г) руководящие документы ФСТЭК.**
117.	Разработка политики безопасности предусматривается в рамках а) организационно-технических мер ЗИ; б) программно-технических мер ЗИ; **в) административных мер ЗИ;** г) морально-этических мер ЗИ.
118.	Укажите все основные принципы разграничения доступа сотрудников к ресурсам ИС: а) ограничение доступа; **б) разделение обязанностей;** в) централизация управления; г) минимизация полномочий.
119.	Административные меры защиты информации включают: (выберите один вариант из перечисленных) а) контроль доступа на территорию объекта информатизации; б) защиту объекта информатизации от стихийных бедствий; **в) планирование действий в чрезвычайных ситуациях;** г) дублирование и резервирование информации.
120.	Согласно ГОСТ Р ИСО/МЭК 13335-1 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий», все, что имеет ценность для организации, обозначается термином (выберите все подходящие варианты) а) ценности; б) ресурсы;

	в) активы; г) собственность.
121.	Укажите все категории нарушителей, на противодействие которым направлены, главным образом, организационно-технические меры защиты информации: (выберите все подходящие варианты); а) внешние нарушители, реализующие атаки удаленно; **б) внутренние нарушители, действующие злоумышленно;** **в) внешние нарушители, стремящиеся проникнуть на территорию объекта информатизации верно;** г) внутренние нарушители, допускающие халатные или неквалифицированные действия.
122.	Совокупность людей, процедур и оборудования, защищающих объект информатизации в целом и его части от действий, нарушающих его безопасность составляет (выберите один вариант из перечисленных) а) систему безопасности; б) систему комплексной защиты; **в) систему физической защиты;** г) систему обеспечения безопасности.
123.	Комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и (или) обеспечивающих основу функционирования информационной системы называется (выберите один вариант из перечисленных) а) обслуживающей системой; б) функциональной инфраструктурой; **в) поддерживающей инфраструктурой;** г) вспомогательной системой.
124.	Процедура определения тождественности субъекта одному из зарегистрированных в ИС идентификаторов называется: (выберите один вариант из перечисленных) **а) идентификацией;** б) авторизацией; в) верификацией; г) аутентификацией.
125.	В процессе идентификации субъект представляет системе (выберите один вариант из перечисленных) **а) идентификатор пользователя;** б) пароль пользователя; в) учетную запись пользователя; г) индивидуальный ключ пользователя.
126.	Аутентификация – процедура: (выберите один вариант из перечисленных) **а) установления подлинности предъявляемого субъектом идентификатора;** б) установления подлинности предъявляемой субъектом учетной записи пользователя; в) сопоставления субъекта одному из зарегистрированных идентификаторов; г) подтверждения личности пользователем.
127.	Традиционно выделяются факторы аутентификации, условно обозначаемые как (выберите один вариант из перечисленных) а) «Я знаю», «Я имею» - 2 фактора; **б) «Я являюсь», «Я знаю», «Я имею» – 3 фактора;** в) «Я знаю», «Я имею», «Я умею» – 3 фактора; г) «Я знаю», «Я являюсь», «Я имею», «Я умею» – 4 фактора; д) «Я знаю», «Я являюсь» - 2 фактора.
128.	Примером трехфакторной аутентификации является следующее сочетание аутентификационных процедур: (выберите один вариант из перечисленных); **а) использование электронного ключа + снятие отпечатка пальца + ввод пароля;** б) снятие отпечатка пальца + ввод пароля + ввод подписи через сенсорный экран (тачскрин); в) сканирование радужки глаза + использование электронного ключа + ввод подписи через сенсорный экран (тачскрин); г) использование электронного ключа + ввод пароля + сканирование штрих-кода на пластиковой карте.
129.	Преобразование шифртекста в открытый текст на основе знания секретного ключа называется: (выберите один вариант из перечисленных) а) обратным преобразованием; б) дешифрованием; **в) расшифрованием;** г) криптоанализом.
130.	Условие $D_{k_1}\left(E_{k_1}(x)\right) = x, x \epsilon K$ означает (выберите один вариант из перечисленных)

	а) обратимость зашифрования; б) однозначность зашифрования; **в) однозначность расшифрования;** г) осмысленность расшифрования.
131.	Множество ключей представляет собой множество таблиц однозначного взаимного соответствия символов из X и Y в шифре (выберите один вариант из перечисленных) **а) простой замены;** б) простой перестановки; в) омофонной замены; г) маршрутной перестановки.
132.	Укажите все методы, применяемые для анализа шифров простой замены (выберите все подходящие варианты) а) тест Касиски; **б) протяжка вероятного слова;** г) дешифрование на основе индекса совпадения; **д) частотный анализ.**

ИД2 ОПК-4 Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

133.	Среди шифров перестановки отдельно выделяются шифры, в которых ключ задается как сочетание двух последовательностей обхода ячеек таблицы, называемы (выберите один вариант из перечисленных) **а) маршрутами;** б) направлениями; в) путями; г) цепочками.
134.	Блочный шифр в двоичном представлении отображает: (выберите один вариант из перечисленных) а) блок открытого текста длины n и ключ длины n в блок шифртекста длины n; б) блок открытого текста длины n и ключ длины m в блок шифртекста длины n; в) блок открытого текста длины n и ключ длины m в блок шифртекста длины m; г) блок открытого текста длины n и ключ длины n в блок шифртекста длины m.
135.	_____ шифр - шифр, обрабатывающий за каждое применение операции зашифрования группу символов открытого текста фиксированной длины. Ответ: **блочный**
136.	Одной из особенностей сети Фейстеля является разделение блока открытого текста, обрабатываемого за одно применение операции зашифрования, на два (левый и правый) или более _____. Ответ: **подблоков** или **подблока**
137.	В схемах электронной цифровой подписи владелец на основе секретного ключа может зашифровать (подписать) сообщение, а любой желающий может на основе открытого ключа владельца расшифровать сообщение, т. е. _____ корректность подписи. Ответ: **проверить**
138.	В шифре «Магма», основанном на сети Фейстеля, помимо операции «сложение по модулю 2» также используется операция сложения по модулю: (выберите один вариант из перечисленных) А) 2 в степени 128; Б) 2 в степени 64; **В) 2 в степени 32;** Г) 2 в степени 16.
139.	Применение невидимых чернил в сочетании с видимым текстом является примером маскирования секретного _____ в другом сообщении. Ответ: **сообщения**
140.	Информация, используемая для сокрытия секретного сообщения, называется стеганографическим _____. Ответ **контейнером**
141.	Укажите все перечисленные в списке классы исторических примеров стеганографической защиты а) использование контейнеров для сокрытия информации;

	б) использование необычного носителя информации; в) использование кодов для сокрытия информации; **г) маскирование сообщения в другом сообщении;** д) использование шифров для сокрытия информации; **е) сокрытие обычного носителя информации.**
142.	В истории стеганографической защиты информации термином «микроточки» обычно называют: (выберите один вариант из перечисленных) **а) изображения или иные документы, уменьшенные при помощи фотографической техники до размеров печатной точки;** б) способ кодирования символов открытого текста группами точек в маскирующем тексте; в) практически незаметные отметки на носителе, составляющие в совокупности или группами символы скрываемого текста; г) различимые только вооруженным глазом символы скрываемого текста.
143.	Меняя порядок слов в пересылаемой телеграмме, а также заменяя отдельные слова синонимами, нарушитель стремится реализовать угрозу: (выберите один вариант из перечисленных) а) искажения скрытого сообщения; **б) разрушения скрытого сообщения;** в) разрушения стеганографического контейнера; г) подмены стеганографического контейнера.
144.	Утечкой информации называется несанкционированный перенос информации от _____ информации к нарушителю. Ответ: **источника**
145.	Разговор, совещание, публичное выступление являются источниками информации в рамках _____ канала утечки информации. Ответ: **акустического**
146.	Паразитные электромагнитные связи и наводки является причиной возникновения: (выберите один вариант из перечисленных) а) содержащих информацию радиосигналов, распространяющихся в пространстве; б) содержащих информацию излучений вокруг звукоусилительной аппаратуры; **в) содержащих информацию сигналов в неинформационных линиях и цепях;** г) содержащих информацию излучений вокруг вычислительной техники.
147.	Укажите все объекты, являющиеся средой распространения для радиоэлектронного канала утечки информации является: (выберите все подходящие варианты) а) жидкости; **б) космос;** в) твердые тела; **г) воздух.**
148.	При перехвате информации по акустооптическому каналу злоумышленник облучает лазерными стетоскопами: (выберите один вариант из перечисленных) **а) оконные стекла;** б) воздуховоды и трубы системы отопления; в) камеры наружного наблюдения и датчики сигнализации; г) антенны.

ИД3 ОПК-4 Иметь навыки: составления технической документации на различных этапах жизненного цикла информационной системы.

149.	Сервис безопасности - набор функций, реализуемых _____ защиты информации для обеспечения защищенности системы. Ответ: **системой**
150.	Вредоносные программы, реализующие несанкционированные действия, направленные на нарушение безопасности информационной системы, без создания собственных копий, называются _____ _____ . Ответ: **троянскими конями** или **троянский конь**
151.	Укажите все виды вредоносных программ, относящихся к категории троянских программ: а) спуфер; **б) бэкдор;** в) флудер;

	г) руткит; **д) эксплоит.**
152.	Метод обнаружения вредоносных программ, суть которого заключается в поиске участков кода исполняемого объекта, отвечающих за конкретные вредоносные действия, называется **а) эвристическим анализом;** б) комплексным анализом; в) методом точного поиска; г) сигнатурным анализом; д) методом эмуляции кода.
153.	Запуск с ограниченными полномочиями заключается в: а) запуске исследуемой программы в среде эмуляции; **б) запуске в выделенной среде с ограничением, например, прав доступа;** в) перехвате запросов исследуемой программы на запись; г) перехвате и анализе всей активности программы.
154.	Совокупность правил, процедур или руководящих принципов в области безопасности для некоторой организации называется _____ _____ организации. Ответ: **политикой безопасности**
155.	Для обеспечения эффективности политики безопасности _____ организации должно установить четкое направление политики, демонстрировать ее соблюдение и поддержку. Ответ: **руководство**
156.	Для обеспечения безопасности, связанной с управлением персоналом, рекомендуется декларировать обязанности сотрудников, связанные с информационной безопасностью: **а) до непосредственного трудоустройства;** б) при инструктаже нового сотрудника перед допуском к исполнению обязанностей; в) в момент непосредственного трудоустройства; г) при обучении сотрудников на этапе внедрения политики безопасности организации.
157.	Одной из основных рекомендаций по вопросу управления доступом в политике безопасности организации является обеспечение управляемости доступа: а) к информации с учетом требований функций организации и задач обеспечения информационной безопасности; б) к информации с учетом задач обеспечения информационной безопасности; в) к средствам обработки информации с учетом требований функций организации и задач обеспечения информационной безопасности; **г) к информации и средствам обработки информации с учетом требований функций организации и задач обеспечения информационной безопасности.**
158.	Одной из основных рекомендаций по вопросам эксплуатации информационных систем является выявление и согласование требований безопасности: а) при проектировании ИС и ее компонентов; **б) до разработки или внедрения ИС или ее компонентов;** в) по результатам регулярного аудита безопасности при эксплуатации ИС; г) на этапе внедрения и апробации ИС.
159.	Основное назначение систем _____ и предотвращения атак - выявление действий нарушителей, не блокируемых другими средствами обеспечения защиты информации . Ответ: **обнаружения**
160.	Система обнаружения вторжений - средство защиты информации, предназначенное для выявления нарушений _____ _____ организации. Ответ: политики безопасности
161.	Укажите все уязвимости, присущие межсетевым экранам: **а) действуют на основе заранее определенных правил обработки сетевых пакетов верно;** б) не контролируют исходящие сетевые пакеты из локальной сети в глобальную; **в) не контролируют сетевую активность внутри сегментов сети верно;** **г) могут иметь правила-исключения для доверенных отправителей верно;** д) не препятствуют запуску пользователями программ, устанавливающих сетевые соединения; е) могут иметь разрешенные сетевые протоколы.
162.	Событием безопасности называется: **а) любое действие, направленное на любой объект системы;** б) любое действие, потенциально способное привести к нарушению политики безопасности орга-

	низации; в) любое событие, затрагивающее средства обеспечения безопасности информации в информационной системе; г) любое действие, нарушающее политику безопасности организации.
163.	Укажите все основные задачи систем обнаружения и предотвращения компьютерных атак: **а) контроль всех событий в системе;** б) ликвидация необходимости в наличии высококвалифицированного персонала; **в) упрощение обработки значительных объемов информации;** **г) контроль действий пользователей ИС;** д) автоматизация управления средствами защиты информации и их настройками.
164.	Оценочные стандарты в области защиты информации содержат _____ ИС и средств защиты информации. Ответ: **классификации**
165.	Функциональные требования безопасности определяют правила, по которым объект оценки управляет _____ к своим ресурсам. Ответ: **доступом**
166.	Руководство по оценке аудиторов системы менеджмента информационной безопасности предоставляется стандартом группы Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности: а) 27004 Менеджмент информационной безопасности. Измерения и аудит; б) 27002 Свод норм и правил по аудиту менеджмента информационной безопасности; в) 27006 Требования к органам, осуществляющим аудит и сертификацию систем менеджмента; информационной безопасности; **г) 27007 Руководство по аудиту систем менеджмента информационной безопасности.**

3.2. Кейс-задания к практическим работам

3.2.1 Шифр и наименование компетенции

ИД2 $_{ОПК-3}$ Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

167.	Разработка программного обеспечения (генератора паролей), которое может реализовывать следующие функции: индикация базового алфавита для исследования и генерации паролей. Индикация в отличие от генерации означает, что базовый алфавит жестко фиксирован и не может быть изменен. Параметры базового алфавита неизменны и отображаются в окне программы. Они определяются в индивидуальном задании как определяющие совокупность включаемых в него групп символов из числа следующих (всех присутствующих на русской раскладке клавиатуры): прописные латинские буквы, строчные латинские буквы, прописные русские буквы без «Ё», строчные русские буквы без «ё», буква «Ё», буква «ё», цифры, специальные символы стандартной клавиатуры компьютера. Базовый алфавит выводится в соответствующую таблицу с тремя столбцами. Первая строка таблицы является ее заголовком. Любая другая строка служит для вывода информации о взаимно-однозначно соответствующем ей символе базового алфавита. В первом столбце отображается номер очередного символа по порядку от одного до величины объема базового алфавита, во втором – код символа в кодировке ANSI, в третьем – сам символ. Предполагается, что пароль генерируется в виде случайной последовательности символов базового алфавита фиксированной длины. При этом скорость перебора паролей нужно задать равной 1000, а требуемую стой-

	кость пароля считать равной 10^i , где i – номер индивидуального задания (номер варианта задания).
168.	Исследование стойкости паролей по трем критериям в зависимости от длины (количества символов) пароля. Критерии стойкости пароля следующие: полное число P вариантов пароля для данного базового алфавита объема A и данной длины n пароля, определяемое по формуле: $P = A^n$. При этом скорость перебора паролей нужно задать равной 1000, а требуемую стойкость пароля считать равной 10^i , где i – номер индивидуального задания (номер варианта задания).
169.	Исследование стойкости паролей по трем критериям в зависимости от длины (количества символов) пароля. Критерии стойкости пароля следующие: Среднее число (математическое ожидание дискретной случайной величины числа) S вариантов пароля для данного базового алфавита объема A и данной длины n пароля, которое необходимо перебрать для вскрытия пароля, определяемое по формуле: $S = (P +1)/ 2 = (A^n +1)/ 2$. При этом скорость перебора паролей нужно задать равной 1000, а требуемую стойкость пароля считать равной 10^i , где i – номер индивидуального задания (номер варианта задания).
170.	Исследование стойкости паролей по трем критериям в зависимости от длины (количества символов) пароля. Критерии стойкости пароля следующие: Среднее время (математическое ожидание дискретной случайной величины времени) T, которое необходимо затратить на вскрытие пароля для данного базового алфавита объема A и данной длины n пароля при известной скорости V перебора паролей, определяемое по формуле: $T = S/V =(A^n +1)/(2V)$.
171.	Скорость перебора паролей в смысле количества вариантов пароля, перебираемых в единицу времени программой-взломщиком паролей под управлением злоумышленника, вводится в числе исходных данных в соответствующую строку редактирования окна выполняемой программы. Результаты проведенного исследования стойкости паролей выводятся в соответствующую таблицу с четырьмя столбцами. Первая строка таблицы является ее заголовком. Любая другая строка служит для вывода информации о взаимно-однозначно соответствующей ей длине пароля. В первом столбце отображается длина пароля, начиная с единичной и кончая известной максимальной для данного исследования. В остальных трех столбцах отображается величина стойкости пароля, измеренная по вышеуказанным трем критериям соответственно. Предполагается, что для ограничения вычислений и ввода-вывода информации максимальная длина пароля вводится в числе исходных данных в соответствующую строку редактирования окна выполняемой программы. При этом скорость перебора паролей нужно задать равной 1000, а требуемую стойкость пароля считать равной 10^i, где i – номер индивидуального задания (номер варианта задания).
172.	Определение и вывод в соответствующую строку редактирования минимальной длины пароля, достаточной для обеспечения требуемой стойкости по выбранному критерию из вышеуказанных трех. Предполагается, что величина требуемой стойкости вводится в числе исходных данных в соответствующую строку редактирования окна выполняемой программы после указания выбранного критерия. Минимально необходимое количество n выбираемых из базового алфавита объема A символов пароля, обеспечивающего требуемую стойкость K по первому критерию, определяется по формуле: $n = [\ln K/\ln A]+1$. Минимально необходимое количество n выбираемых из базового алфавита объема A символов пароля, обеспечивающего требуемую стойкость K по второму критерию, определяется по формуле: $n = [\ln K/\ln A]+1$. Минимально необходимое количество n выбираемых из базового алфавита объема A символов пароля, обеспечивающего требуемую стойкость K по третьему критерию, определяется по формуле: $n = [\ln K/\ln A]+1$. Квадратные скоб-

	ки везде обозначают целую часть числа.
173.	Генерация с выводом в соответствующую строку редактирования пароля минимальной длины, обеспечивающего требуемую стойкость по выбранному критерию из вышеуказанных трех. Предполагается, что длина генерируемого пароля выводится заранее. Вывод сгенерированного пароля в открытом виде. При этом скорость перебора паролей нужно задать равной 1000, а требуемую стойкость пароля считать равной 10^i , где i – номер индивидуального задания (номер варианта задания).
174.	Выбор метода закрытия пароля из двух произвольных методов из числа следующих: четыре метода замены (метод постоянного циклического сдвига алфавита, моноалфавитный метод замены, полиалфавитный метод замены и метод Вижинера), два метода перестановки (метод простой перестановки и метод чередующихся перестановок), два метода битовых манипуляций (метод битовой инверсии и метод XOR).
175.	Ввод задаваемой пользователем ключевой информации для закрытия пароля. Способ задания ключевой информации определяется выбранным методом закрытия пароля. В общем случае для задания ключа может использоваться ключевая строка редактирования и ключевая таблица.
176.	Генерация случайным образом ключевой информации для закрытия пароля. Ключ выбирается равновероятно среди всех возможных вариантов для данного метода закрытия пароля (и для данной длины ключа, если данный метод закрытия пароля предполагает, в частности, задание длины ключа). Сгенерированный ключ должен выводиться в те же визуальные компоненты окна выполняемой программы, в которые предусмотрен ввод задаваемой пользователем ключевой информации для закрытия пароля.
177.	Анализ стойкости закрытия пароля в виде расчета количества вариантов ключей для данного метода закрытия пароля. Количество вариантов ключей должно выводиться в соответствующую строку редактирования окна выполняемой программы. Для метода постоянного циклического сдвига алфавита количество вариантов ключей N при использовании базового алфавита объема A вычисляется по формуле: N = A-1. Для моноалфавитного метода замены количество вариантов ключей N при использовании базового алфавита объема A вычисляется по формуле: N = A!-1 . Для полиалфавитного метода замены количество вариантов ключей N при использовании базового алфавита объема A и m замещающих алфавитов вычисляется по формуле: $N = (A!-1)^m$. Для метода Вижинера количество вариантов ключей N длины n при использовании базового алфавита объема A вычисляется по формуле: $N = A^n -1$. Для метода простой перестановки количество вариантов ключей N длины n вычисляется по формуле: N = n!-1. Для метода чередующихся перестановок количество вариантов ключей N при использовании m перестановок одинаковой длины n вычисляется по формуле: $N = (n!-1)^m$. Метод битовой инверсии вообще не предполагает использования ключа. Для метода XOR количество вариантов ключей N длины n при использовании базового алфавита объема A вычисляется по формуле: $N = A^n$.
178.	Вывод в соответствующую строку редактирования окна выполняемой программы сгенерированного пароля в закрытом первым методом виде. Вывод в соответствующую строку редактирования окна выполняемой программы сгенерированного пароля в закрытом вторым методом виде.
179.	История и современные направления защиты информации.
180.	Правовая основа защиты информации за рубежом.
181.	Правовая основа защиты информации в России.
182.	Засекречивание информации. Политический и социальный аспекты засекречивания информации.

183.	Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию.
184.	Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены.
185.	Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа.
186.	Защита информации, составляющей профессиональную тайну.
187.	Защита информации, составляющей банковскую тайну.
188.	Защита сведений, составляющих личную тайну.
189.	Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности.
190.	Система защиты информации, ее структурная и функциональная части.
191.	Уголовная ответственность за государственную измену, шпионаж, разглашение государственной тайны и утрату секретных документов, объективная и субъективная сторона этих преступлений.
192.	Защита интеллектуальной собственности в системе правового регулирования информационной безопасности.
193.	Основы авторского права.
194.	Основные положения патентного права.
195.	Организационно-правовая система обеспечения защиты объектов промышленной собственности на основе патентов.
196.	Правовая основа обеспечения защиты коммерческой тайны.
197.	Основные положения по защите коммерческой тайны.
198.	Особенности правовой охраны программ для ЭВМ и баз данных.
199.	Особенности правовой охраны топологий интегральных микросхем.
200.	Понятие и классификация видов компьютерных правонарушений.
201.	Особенности проведения экспертизы в области компьютерной информации.
202.	Понятие юридической ответственности за нарушение правовых норм в области информационной безопасности.
203.	Виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
204.	Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.
205.	Административная ответственность за нарушения правовых норм в сфере информационной безопасности.
206.	Особенности юридической ответственности за нарушения норм информационной безопасности в области трудовых и гражданско-правовых отношений.
207.	Способы совершения компьютерных преступлений: понятие, структура. Механизм совершения преступления.
208.	Классификация способов совершения компьютерных преступлений.
209.	Понятие комплексной защиты информации на объекте.
210.	Понятие и основные задачи комплексных специальных проверок.
211.	Правовая база организации комплексных специальных проверок.
212.	Основные принципы организации и проведения комплексных специальных проверок.
213.	Содержание этапов комплексного контроля состояния защиты информации на объекте.

	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: заказ. Параметры шифрования p, q: 7, 16
214.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: казак. Параметры шифрования p, q: 5, 6
215.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: жаба. Параметры шифрования p, q: 3, 11
216.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: забава. Параметры шифрования p, q: 9, 11
217.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: гадалка. Параметры шифрования p, q: 14, 17
218.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: загадка. Параметры шифрования p, q: 3, 7
219.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: багаж. Параметры шифрования p, q: 5, 12
220.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: бивак. Параметры _____шифрования p, q: 8, 13.
221.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: кабак. Параметры шифрования p, q: 11, 17
222.	Задание включает в себя алгоритм асимметричного шифрования - дешифрования. В соответствии с заданием необходимо зашифровать информацию по методу RSA для последующей передачи по вариантам. Шифруемое слово: визига. Параметры шифрования p, q: 5, 15

3.3 Контрольные вопросы к текущим опросам на лабораторных работах

Шифр и наименование компетенции

ИД1 $_{ОПК-3}$ знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Номер задания	Формулировка вопроса
223.	Какие цели преследует криптография?
224.	Перечислите основные алгоритмы криптографических преобразований
225.	Поясните понятие «целостности, подлинности и конфиденциальности» информации
226.	Перечислите основные методы криптографической защиты информации в компьютерных сетях и системах
227.	Как классифицируются средства криптографической защиты информации?
228.	Перечислите основные схемы идентификации пользователя
229.	Назовите основные способы управления ключевой информацией
230.	Назовите два общих принципа, используемых в симметричных криптосистемах
231.	Основные достоинства и недостатки алгоритма шифрования данных с помощью DES
232.	Перечислите основные режимы работы алгоритма DES
233.	Перечислите основные комбинации, используемые при шифровании алгоритма DES
234.	Преимущества и недостатки ассиметричных криптосистем
235.	С какой целью в ассиметричных криптосистемах используются два ключа?
236.	Как обеспечивается криптостойкость ассиметричных криптосистем?
237.	Какова длина ключей для симметричных и ассиметричных криптосистем при одинаковой их криптостойкости?
238.	Каково основное назначение хэш-функций?
239.	Каковы основные принципы формирования хеш-функции?
240.	Какими свойствами должны обладать хэш-функция_@@ЩП__, используемая в процессе аутентификации?
241.	В чем отличительные особенности отечественного стандарта хеш-функции (ГОСТ Р 34.11-94) от алгоритмов хэширования MD5 и SHA?
242.	Где и с какой целью используется электронная цифровая подпись?
243.	Перечислите основные этапы формирования электронной цифровой подписи
244.	Какими свойствами должна обладать электронная цифровая подпись?
245.	Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия
246.	Укажите особенности слепой и неоспоримой цифровой подписи
247.	Как осуществляется взаимная проверка подлинности пользователей?
248.	Приведите основные схемы идентификации аутентификации пользователя
249.	В чем суть параллельной схемы идентификации с нулевой передачей знаний?
250.	Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными
251.	Особенности генерации и хранения ключей
252.	Укажите основные методы генерации сеансовых ключей
253.	Перечислите основные методы генерации сеансовых ключей
254.	Перечислите основные носители ключевой информации
255.	Перечислите функции и компоненты сети VPN
256.	Классифицируйте VPN по способу технической реализации и архитектуре технического решения
257.	Каковы способы защиты информации при межсетевом взаимодействии?
258.	Какие криптографические протоколы используются для защиты технологии кли-

	ент-сервер?

3.4 Темы рефератов

Шифр и наименование компетенции

ИДЗ $_{ОПК-3}$. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

№	Формулировка вопроса
259.	История и современные направления защиты информации
260.	Правовая основа защиты информации за рубежом
261.	Правовая основа защиты информации в России
262.	Источники угроз защищаемой информации
263.	Утечка, разглашение, раскрытие и распространение защищаемой информации. Объективные и субъективные условия утечки информации
264.	Легальные, агентурные и технические каналы утечки информации
265.	Засекречивание информации. Политический и социальный аспекты засекречивания информации
266.	Принципы засекречивания информации: законность, обоснованность, своевременность
267.	Организационно-правовые формы засекречивания информации: перечневая форма и система первоначального засекречивания
268.	Рассекречивание информации. Виды сведений, подлежащих и не подлежащих рассекречиванию
269.	Классификация защищаемой информации по принадлежности, содержанию и степени секретности
270.	Носители секретной информации: документы, изделия (предметы), электромагнитные излучения
271.	Понятие государственной тайны. Сведения, которые подлежат засекречиванию и которые не могут быть засекречены
272.	Определение грифа секретности сведений, составляющих государственную тайну
273.	Порядок допуска к государственной тайне. Основания для отказа в допуске. Прекращение допуска
274.	Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленного шпионажа
275.	Правовые основы защиты коммерческой тайны за рубежом и в России
276.	Ответственность за нарушение законодательства о коммерческой тайне.
277.	Цели незаконного получения сведений, составляющих коммерческую тайну
278.	Субъекты незаконного собирания сведений, составляющих коммерческую тайну
279.	Способы незаконного получения сведений, составляющих коммерческую тайну
280.	Закрытие свободного доступа к сведениям, составляющим коммерческую тайну
281.	Политический, экономический и моральный ущерб от утечки сведений, составляющих государственную тайну
282.	Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами, составляющими коммерческую тайну
283.	Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствами вычислительной техники
284.	Организация защиты конфиденциальной информации от утечки по техническим

	каналам
285.	Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охрана коммерческой тайны
286.	Защита информации, составляющей профессиональную тайну
287.	Защита информации, составляющей банковскую тайну
288.	Защита сведений, составляющих личную тайну
289.	Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режима конфиденциальности
290.	Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические
291.	Система защиты информации, ее структурная и функциональная части
292.	Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально- нравственные методы, учет, кодирование, шифрование
293.	Средства защиты информации, требования к ним и решаемые с их помощью задачи
294.	Уголовная ответственность за государственную измену, шпионаж, разглашение государственной тайны и утрату секретных документов, объективная и субъективная сторона этих преступлений

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03-2017 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02-2017 Положение о рейтинговой оценке текущей успеваемости, а также методическими указаниями.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине/практике

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
***Шифр и наименование компетенции* ОПК-3 –** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ин-формационно-коммуникационных технологий и с учетом основных требований информационной безопасности					
ЗНАТЬ: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Методы решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Знать особенности подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: Применять принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Применять методы реше-	Доклад	Умение применять полученные знания	выставляется студенту при наличии доклада, преобразовании информации в единую	Зачтено	Освоена (повышенный)
			форму, т.е. презентации по выбранной теме	Не зачено	Не освоена (недостаточный)

ния стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. проводить подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.					
ВЛАДЕТЬ: принципами, методами и средствами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Методами решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной	Домашняя работа	Методика и правильность решения задачи	обучающийся выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе	Удовлетворительно	Освоена (базовый)

безопасности.			обучающийся выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)
***Шифр и наименование компетенции* ОПК-4 –** Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью					
ЗНАТЬ: Основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. Методы открытия и закрытия общего доступа к локальной сети знать, как программировать простейшие методы шифрования и дешифрования в сети, а также задавание паролей в операционной системе, и использование антивирусных программ Методы задания разграничения прав доступа пользователей к информации управления их полномочиями, методы оценивания стойкости различных паролей и методов шифрования, методы формирования паролей и ключей шифрования с заданной стойкостью	Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: Применять основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Доклад	Умение применять полученные знания	выставляется студенту при наличии доклада, преобразовании информации в единую	Зачтено	Освоена (повышенный)

Применять методы открытия и закрытия общего доступа к локальной сети программировать простейшие методы шифрования и дешифрования задавать пароли в операционной системе уметь пользоваться антивирусными программами. Применять методы задания разграничения прав доступа пользователей к информации управления их полномочиями, уметь использовать методы оценивания стойкости различных паролей, а также шифрования и формировать пароли и ключи шифрования с заданной стойкостью			форму, т.е. презентации по выбранной теме	Не зачено	Не освоена (недостаточный)
ВЛАДЕТЬ: Навыками применения основных стандартов оформления технической документации на различных стадиях жизненного цикла информационной системы. Навыками методов открытия и закрытия общего доступа к локальной сети, программировать методы шифрования и дешифрования владеть знаниями работой с антивирусными программами, а также задавать пароли в операционной системе Навыками задания разграничения прав доступа пользователей к информации управления их навыками оценивания стойкости различных методов и паролей шифрования, владеть навыками формирования паролей и ключей шифрования с заданной стойкостью	Домашняя работа	Методика и правильность решения задачи	обучающийся выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (продвинутый)
			обучающийся выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе	Удовлетворительно	Освоена (базовый)

			обучающийся выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)