

УТВЕРЖДАЮ
Декан факультета

_____ Страхов С.Ю.

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление/специальность подготовки	09.03.01 Информатика и вычислительная техника
Специализация/профиль/программа подготовки	Автоматизированные системы обработки информации и управления
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	И Информационных и управляющих систем
Выпускающая кафедра	И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра-разработчик рабочей программы	И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
4	7	4	144	51	34	0	17	93	0	0	93	ЭКЗ.

ЛИСТ СОГЛАСОВАНИЯ

**РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)**

09.03.01 Информатика и вычислительная техника

год набора группы: 2025

Программу составил:

Кафедра И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ
ТЕХНОЛОГИЙ _____

Яковенко Николай Григорьевич, к.т.н., доцент, доцент

Программа рассмотрена

на заседании кафедры-разработчика

рабочей программы **И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

Заведующий кафедрой Сырцев А.Н., д.воен.н., снс _____

Программа рассмотрена

на заседании выпускающей кафедры

И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Заведующий кафедрой Сырцев А.Н., д.воен.н., снс _____

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

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

Формированию компетенций служит достижение следующих результатов образования:

ОПК-3

знания:

Опасности утечки значимой информации и способов предотвращения таких утечек. Опасности атак на компьютер и обрабатываемую информацию и способы уменьшения опасности от таких атак;

умения:

Пользоваться антивирусными программами, программно-аппаратными средствами защиты информации;

навыки:

Соблюдения цифровой гигиены. Резервирования и сохранения информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*.

Содержание дисциплины является логическим продолжением дисциплин: **ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ, КОМПЬЮТЕРНЫЙ ПРАКТИКУМ**.

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-2 — Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
- ОПК-8 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения
- ОПК-9 — Способен осваивать методики использования программных средств для решения практических задач
- ПК-1.1 — Способен разрабатывать требования и проектировать программное обеспечение
- ПК-93 — Способен генерировать новые идеи для решения задач цифровой экономики, абстрагироваться от стандартных моделей, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов
- ПК-94 — Способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ОПК-3
4	7	Раздел 1. Общая проблема информационной безопасности информационных систем. Стоймость и важность информации в современном обществе Угрозы информации, их источники и классификация Законодательные, организационные, технические и программные средства и способы защиты информации.	15	5	4	1	10	15
4	7	Раздел 2. Программа информационной безопасности России и пути ее реализации. Действующее законодательство в области информационной безопасности Стандарты и другие акты в области информационной безопасности.	14	4	2	2	10	15
4	7	Раздел 3. Защита информации при реализации информационных процессов. Программные средства нападения на ЭВМ, сети и устройства хранения информации при реализации информационных процессов и средства защиты от них Аппаратные средства снятия информации при вводе, выводе, передаче и обработке и защита от них. Вирусы, трояны и черви как средства нападения и защита от них Резервирование информации как средство защиты.	17	6	4	2	11	15
4	7	Раздел 4. Организационное обеспечение информационной безопасности. Разделение доступа к информации Контроль доступа Введение системы сменных паролей Настройка программ с целью уменьшения фоновой записи информации Удаление промежуточных итогов, очистка временных каталогов, очистка корзины, очистка файла свопинга.	18	8	6	2	10	15
4	7	Раздел 5. Защита информации от несанкционированного доступа. Защита помещений и защита компьютера Защита носителей информации Антивирусные программы Программы удаленного администрирования и наблюдения активности Пароли и защита файлов.	18	8	6	2	10	15
4	7	Раздел 6. Математические и методические средства защиты. Понятие о криптографии и шифровании данных. Стойкость шифров. Симметричные шифры Шифрование с открытым ключом Стеганография Гражданские шифры.	18	8	6	2	10	15
4	7	Раздел 7. Компьютерные средства реализации защиты в информационных системах. Электронная подпись Аутентификация доступа Пароли Раздельный доступ Биометрические методы Аппаратно-программные замки Скрытие данных на диске Контейнеры и защищенные диски Файрволлы и межсетевые экраны.	44	12	6	6	32	10
Всего за 7 семестр			144	51	34	17	93	100
Всего по дисциплине			144	51	34	17	93	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Общая проблема информационной безопасности информационных систем.	Законодательные, организационные, технические и программные средства и способы защиты информации.	1
2	Раздел 2. Программа информационной безопасности России и пути ее реализации.	Стандарты и другие акты в области информационной безопасности	2
3	Раздел 3. Защита информации при реализации информационных процессов.	Средства снятия информации при вводе, выводе, передаче и обработке и защита от них. Защита от троянов, вирусов и червей, исследование антивирусного пакета DRWEB.	2
4	Раздел 4. Организационное обеспечение информационной безопасности.	Организация раздельного доступа к информации. Настройка офисных программ, исследование защиты информации в Microsoft Office.	2
5	Раздел 5. Защита информации от несанкционированного доступа.	Пароли и защита конкретных файлов, защита дисков и каталогов. Установка и использование антивирусных программ как средство защиты от сбора информации.	2

6	Раздел 6. Математические и методические средства защиты.	Шифрование с открытым ключом. Настройка почтовых программ на шифрование с открытым ключом. Получение сертификата на сертификационном центре. Получение личных криптоключей.	2
7	Раздел 7. . Компьютерные средства реализации защиты в информационных системах.	Организация защищенных контейнеров и защищенных дисков на компьютере. Настройка фаерволлов и межсетевых экранов. Скрытие данных на дисках. Фаерволлы и межсетевые экраны	6
Всего за 7 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Общая проблема информационной безопасности информационных систем.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	10
2	Раздел 2. Программа информационной безопасности России и пути ее реализации.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	10
3	Раздел 3. Защита информации при реализации информационных процессов.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	11
4	Раздел 4. Организационное обеспечение информационной безопасности.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	10
5	Раздел 5. Защита информации от несанкционированного доступа.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	10
6	Раздел 6. Математические и методические средства защиты.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	10
7	Раздел 7. . Компьютерные средства реализации защиты в информационных системах.	Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	32
Всего за 7 семестр			93

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
7						ДР		ВРЗД		ДР		ВРЗД				ДР	

Условные обозначения:

- ДР – диагностическая работа;
- ВРЗД – вопросы по разделу.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- вопросы по разделу.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004, эл. рес.
2. Б. А. Фороузан. . Криптография и безопасность сетей. М.: Интернет-Ун-т Информ. Технол., 2010, 12 экз.
3. В. А. Галатенко. . Основы информационной безопасности. М.: Интернет-Университет Информационных Технологий, 2012, 14 экз.
4. В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах. М.: Форум, 2010, 5 экз.
5. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

не требуются.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <https://repository.library.voenmeh.ru/jspui/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. <https://e.lanbook.com/> — ЭБС Лань;
3. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;
4. <https://ibooks.ru/> — ЭБС Айбукс.ру - это большой выбор актуальной литературы для вашей библиотеки в электронном виде;
5. <http://www.tnt-ebook.ru/> — TNT-EBOOK - Электронно-библиотечная система.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
3. <http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. OpenOffice.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. OpenOffice.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*. Дисциплина реализуется на факультете *И Информационных и управляющих систем* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой *И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ*.

Дисциплина нацелена на формирование *компетенций*:

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.

Содержание дисциплины охватывает круг вопросов, связанных с защитой информации на компьютере и при передаче по каналам связи, цифровой гигиеной при работе с информацией, защитой от вирусов и спама.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- вопросы по разделу.

Промежуточная аттестация проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **4 з.е., 144 ч.** Программой дисциплины предусмотрены лекционные занятия (**34 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**93 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 51 ч. аудиторных занятий, и 93 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Общая проблема информационной безопасности информационных систем.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1) С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1) В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (1)	10
Итого по разделу 1		10
Раздел 2. Программа информационной безопасности России и пути ее реализации.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	В. А. Галатенко. . Основы информационной безопасности: М.: Интернет-Университет Информационных Технологий, 2012 (1) В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (2)	10
Итого по разделу 2		10
Раздел 3. Защита информации при реализации информационных процессов.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	Б. А. Фороузан. . Криптография и безопасность сетей: М.: Интернет-Ун-т Информ. Технол., 2010 (3) В. А. Галатенко. . Основы информационной безопасности: М.: Интернет-Университет Информационных Технологий, 2012 (3) А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004 (1-3)	11
Итого по разделу 3		11
Раздел 4. Организационное обеспечение информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	В. А. Галатенко. . Основы информационной безопасности: М.: Интернет-Университет Информационных Технологий, 2012 (3) А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004 (1-3) Б. А. Фороузан. . Криптография и безопасность сетей: М.: Интернет-Ун-т Информ. Технол., 2010 (3)	10

Итого по разделу 4		10
Раздел 5. Защита информации от несанкционированного доступа.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	Б. А. Фороузан. . Криптография и безопасность сетей: М.: Интернет-Ун-т Информ. Технол., 2010 (3-5) А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004 (1-3)	10
Итого по разделу 5		10
Раздел 6. Математические и методические средства защиты.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004 (1-3) В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (4-5)	10
Итого по разделу 6		10
Раздел 7. . Компьютерные средства реализации защиты в информационных системах.		
Изучение предусмотренных программой дидактических единиц по лекциям и рекомендуемой литературе. Подготовка к выполнению аудиторных заданий.	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (4-5) А. А. Васильев, Н. Н. Смирнова, А. В. Яшин. . Программное обеспечение современных компьютерных сетей: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2004 (1-3)	32
Итого по разделу 7		32

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- вопросы по разделу;
- экзамен.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Вопросы по разделу

Приведены в УМК дисциплины. Студенту предлагается 5 вопросов, из которых он должен правильно ответить не менее, чем на три вопроса.

Экзамен

Экзамен оформляется при сдаче всех контрольных мероприятий семестра, при этом обязательным является посещение не менее 90% лекционных и практических занятий.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-3	
4	7	Раздел 1. Общая проблема информационной безопасности информационных систем.	15	5	4	1	10	15	Вопросы по разделу
4	7	Раздел 2. Программа информационной безопасности России и пути ее реализации.	14	4	2	2	10	15	Вопросы по разделу
4	7	Раздел 3. Защита информации при реализации информационных процессов.	17	6	4	2	11	15	Вопросы по разделу
4	7	Раздел 4. Организационное обеспечение информационной безопасности.	18	8	6	2	10	15	Вопросы по разделу
4	7	Раздел 5. Защита информации от несанкционированного доступа.	18	8	6	2	10	15	Вопросы по разделу
4	7	Раздел 6. Математические и методические средства защиты.	18	8	6	2	10	15	Вопросы по разделу
4	7	Раздел 7. . Компьютерные средства реализации защиты в информационных системах.	44	12	6	6	32	10	Вопросы по разделу
Всего за 7 семестр			144	51	34	17	93	100	
Всего по дисциплине			144	51	34	17	93	100	

Оценочные материалы по дисциплине ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

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

- № 1 Прочитайте текст и запишите развернутый обоснованный ответ
Из применяемых биометрических методов идентификации наименее стойким является метод по ...
- № 2 Прочитайте текст и запишите развернутый обоснованный ответ
Компьютерный вирус это ...
- № 3 Прочитайте текст и запишите развернутый обоснованный ответ
Полиморфизм вируса это ...
- № 4 Прочитайте текст и запишите развернутый обоснованный ответ
Антивирус это ...
- № 5 Прочитайте текст и запишите развернутый обоснованный ответ
Симметричный шифр отличается от шифра с открытым ключом тем, что ...
- № 6 Прочитайте текст и установите соответствие
Способы закрытия информации
- 1.Симметричное шифрование
 - 2.Асимметричное шифрование
 - 3.Шифрование с открытым ключом
 - 4.Стеганография
- А. Использует один ключ для зашифровывания и расшифровывания
- Б. Использует открытый ключ для зашифровывания и закрытый ключ для расшифровывания
- В. Скрывает сам факт наличия информации
- № 7 Прочитайте текст и установите соответствие
Вход в информационную систему
- 1.Регистрация
 - 2.Авторизация
 - 3.Идентификация
 - 4.Аутентификация
 - 5.Двухфакторная аутентификация
- А. Предоставление определенных прав
- Б. Процесс распознавания пользователя по его идентификатору.
- В. Доказательство того, что пользователь является именно тем, за кого себя выдает
- № 8 Прочитайте текст и запишите развернутый обоснованный ответ
Угроза информационной безопасности это ...
- № 9 Прочитайте текст и запишите развернутый обоснованный ответ
«Окно опасности» это...
- № 10 Прочитайте текст и запишите развернутый обоснованный ответ
Угроза инфобезопасности чаще всего является следствием ...
- № 11 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор

ответов

Как классифицируется стратегическая информация на уровне государства

1. Государственная
2. Военно – политическая
3. Военная
4. Экономическая

№ 12 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Основными недостатками облачных сервисов является:

- 1 Многочисленные сбои при большой нагрузке и возможность кражи данных
- 2 Неконтролируемость хранения данных со стороны пользователя
- 3 Необходимость наличия высокоскоростного устойчивого интернета
- 4 Непонимание работы облачных сервисов со стороны пользователя

№ 13 Прочитайте текст и установите последовательность

Наиболее безопасный порядок действий при резервном копировании информации

1. Подключить носитель для резервного копирования
2. Скопировать информацию
3. Проверить антивирусом
4. Отключить носитель для резервного копирования
5. Отключить компьютер от локальной или глобальной сети

№ 14 Прочитайте текст и установите последовательность

Документы, определяющие ИБ и ЗИ в РФ в порядке убывания важности документов

1. Указы Президента
2. ГОСТы по информационной безопасности
3. Конституция Российской Федерации
4. Федеральные законы
5. Ведомственные и межведомственные инструкции

№ 15 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что определяет стоимость и важность информации в современном обществе

1. Роль и влияние информации на современное общество и промышленность
2. Возрастание доли информации в валовом внутреннем продукте государств
3. Рост количества средств обработки и передачи информации в современном обществе
4. Рост затрат на производство, передачу и хранение информации

№ 16 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что принципиально отличает информацию от материальных объектов?

1. Всеобщность информации в нашем информационном обществе

2. Важность информации для общества и управления государством и экономикой на всех уровнях

3. При краже информация остается и у того, у кого она украдена, и появляется у того, кто ее украл

4. Необходимость специальных мер по защите информации

№ 17 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что определяет стоимость экономической информации

1. Время, которое необходимо для того, чтобы придумать и произвести что-то новое, оригинальное, что заинтересует рынок

2. Сумма, которую готовы заплатить конкуренты за экономическую информацию

3. Сумма, потраченная на разработку и производство товара

4. Текущая конъюнктура рынка в рассматриваемой области экономической деятельности

№ 18 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какие законодательные документы предусматривают наказание за нарушение безопасности и сохранности информации

1. Конституция РФ

2. Указы Президента РФ

3. Закон о гостайне № 5485-1 от 21.07.1993 г

4. Уголовный Кодекс РФ и Административный Кодекс РФ

№ 19 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Как классифицируется информация с целью управления ее сохранностью и защитой

1. Государственная Корпоративная Частная

2. Стратегическая Оперативная Тактическая

3. Важная и не важная для конкретного государства, компании, организации и человека

4. Долгосрочная, среднесрочная и краткосрочная