

УТВЕРЖДАЮ
 Декан факультета

 (подпись) Матвеев П.В.
 ФИО
 «___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление/специальность подготовки	09.03.04 Программная инженерия
Специализация/профиль/программа подготовки	Разработка программно-информационных систем
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	О7 Информационные системы и программная инженерия

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)

09.03.04 Программная инженерия

год набора группы: 2024

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Князьков Анатолий Викторович, д.ф.-м.н., профессор

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ 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 — способность 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:

методы аутентификации в современных операционных системах и специальные средства защиты информации;

умения:

применять полученные знания в практике построения защищенных систем обработки информации,

включая конфиденциальную информацию и обработку персональных данных;

навыки:

применять сетевые сканеры и анализаторы протоколов компьютерной сети.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.04 Программная инженерия*.

Содержание дисциплины является логическим продолжением дисциплин: **ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ**.

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-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
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов
- 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
- ПСК-1/23.4 — Способен использовать различные технологии разработки программного обеспечения

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. Понятие о защите информации, виды защищаемой информации. Информационная безопасность в системе национальной безопасности Российской Федерации.	15	2	2	0	13	5
4	7	Раздел 2. Структуры и основные задачи службы безопасности предприятия. 2.1. Этапы процесса организации системы защиты информации предприятия. 2.2. Защита информации в линиях связи. 2.3. Структура современных телефонных кабельных сетей.	13	3	3	0	10	10
4	7	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации. Способы контактного и бесконтактного съема информации.	14	4	2	2	10	15
4	7	Раздел 4. Защита информации в современных информационных системах. 4.1. Возможности атаки на ОС, их классификация. 4.2. Парольная защита ПК. Взлом паролей Windows NT и UNIX. Защита от взлома. 4.3. Идентификация и аутентификация пользователей ОС. Windows, UNIX, Linux. 4.4. Формальные модели защищаемых систем и их применение в современных ОС.	18	8	4	4	10	10
4	7	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК. 5.1. Защита программ. 5.2. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. 5.3. Технология хранения ключевой информации.	15	5	5	0	10	15
4	7	Раздел 6. Основные угрозы безопасности сетей. 6.1. Модели угроз. 6.2. Модели противодействия угрозам безопасности. 6.3. Основные требования к формированию и использованию имен пользователей и паролей в сети. 6.4. Методы аутентификации пользователей в сети.	18	8	4	4	10	15
4	7	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи. 7.1. Разновидности вирусных программ. 7.2. Сканеры вирусов. 7.3. Сетевая защита, брандмауэры, демилитаризованные зоны и частные виртуальные сети. 7.4. Системы обнаружения сетевого вторжения.	18	8	4	4	10	10
4	7	Раздел 8. Безопасность Интернета. 8.1. Разрушительные программы: вирусы, черви, троянские кони, мобильные программы. 8.2. Безопасность электронной почты.	15	5	2	3	10	10
4	7	Раздел 9. Криптографические методы защиты информации. 9.1. Неформальные понятия о шифрах. 9.2. Шифрование и дешифрование. 9.3. Математические основы криптографии. 9.4. Алгоритмы шифрования. 9.5. Понятие стойкости шифра. 9.6. Правило Кирхгофа. 9.7. Виды шифров. 9.8. Виды криптографических атак. 9.9. Шифрование и сетевая защита. 9.10. Электронная подпись. 9.11. Сертификаты. 9.12. Криптографические протоколы Интернета.	18	8	8	0	10	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 3. Методы нарушения конфиденциальности, целостности и доступности информации.	Практическая работа №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности.»	2
2	Раздел 4. Защита информации в современных информационных системах.	Практическая работа №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей.»	4
3	Раздел 6. Основные угрозы безопасности сетей.	Практическая работа №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows.»	4
4	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Практическая работа №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел.»	4
5	Раздел 8. Безопасность Интернета.	Практическая работа №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации.»	3
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. Понятие о защите информации, виды защищаемой информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	13
2	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
3	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
4		Подготовка к практической работе №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности», оформление отчета.	4
5	Раздел 4. Защита информации в современных информационных системах.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
6		Подготовка к практической работе №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей», оформление отчета.	4
7	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
8		Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows»	4
9		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
10	Раздел 6. Основные угрозы безопасности сетей.	Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», подготовка и отсылка отчета по электронной почте преподавателю.	4
11	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
12		Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета.	4
13		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
14	Раздел 8. Безопасность Интернета.	Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.	4
15	Раздел 9. Криптографические методы защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
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	ИПЗ, Отч. по ПЗ, ВПЗ		Отч. по ПЗ, ИПЗ, ВПЗ		ДР		Отч. по ПЗ, ИПЗ, ВПЗ		ДР		Отч. по ПЗ, ИПЗ, ВПЗ			ИПЗ, Отч. по ПЗ, ВПЗ		ДР	Вопр. Экз

Условные обозначения:

- ДР – диагностическая работа;

- Отч. по ПЗ – отчет по практическому заданию;
- ИПЗ – индивидуальное практическое задание;
- ВПЗ – вопросы/задания по темам ПЗ;
- Вопр. Экз – вопросы к экзамену.

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

- диагностическая работа;
- отчет по практическому заданию;
- индивидуальное практическое задание;
- вопросы/задания по темам ПЗ;
- вопросы к экзамену.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. А. Голдсмит. . Беспроводные коммуникации. М.: Техносфера, 2011, 5 экз.
3. А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации. М.: КноРус, 2017, 60 экз.
4. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
5. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
6. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
7. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
8. С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. . Операционные системы, сети и интернет-технологии. М.: Академия, 2014, 15 экз.

5.2. Дополнительная литература по дисциплине:

1. А. В. Бабаш, Г. П. Шанкин. Криптография. М.: СОЛОН-Пресс, 2007, 3 экз.
2. С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security. М.: БИНОМ, 2007, 3 экз.

5.3. Периодические издания:

не требуются.

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

1. <http://www.intuit.ru/department/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информатика;
2. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информатика;
3. <http://e.lanbook.com/> — ЭБС Лань;
4. <https://ura1t.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов;
5. <http://library.voenmeh.ru/jirbis2/> — Р«Р»Р°РІРSP°СЦІ1 — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
6. <https://ura1t.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;
7. <http://library.voenmeh.ru/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<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.voennemeh.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. LibreOffice;
2. Linux;

3. Microsoft Windows.

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. Проектор;
2. LibreOffice;
3. Linux;
4. Microsoft Windows.

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 **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.04 Программная инженерия*. Дисциплина реализуется на факультете О Естественнoнаучный БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:
ОПК-3 способность 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 основными понятиями и видами защищаемой информации, процессом организации системы защиты предприятия, утечками информации, методами защиты информации и алгоритмами шифрования. Рассматриваются основные способы проникновения вирусов в информационные системы и сети, виды вирусов и защита от них, формальные модели защищаемых систем и их применение. Сетевая защита и безопасность web и электронной почты.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

- диагностическая работа;
- отчет по практическому заданию;
- индивидуальное практическое задание;
- вопросы/задания по темам ПЗ;
- вопросы к экзамену.

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. Понятие о защите информации, виды защищаемой информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1)	13
Итого по разделу 1		13
Раздел 2. Структуры и основные задачи службы безопасности предприятия.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (4) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (1)	10
Итого по разделу 2		10
Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (2)	6
Подготовка к практической работе №1 – «Разработка защищенных приложений. Программное управление учетной записью. Политика безопасности», оформление отчета.	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы,	4

	сети и телекоммуникации: М.: КноРус, 2017 (8-9)	
Итого по разделу 3		10
Раздел 4. Защита информации в современных информационных системах.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (3) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)	6
Подготовка к практической работе №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей», оформление отчета.	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	4
Итого по разделу 4		10
Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3)	6
Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows»	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)	4
Итого по разделу 5		10
Раздел 6. Основные угрозы безопасности сетей.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8)	6
Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», подготовка и отсылка отчета по электронной почте преподавателю.	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3) А. Голдсмит. . Беспроводные коммуникации: М.:	4

	<p>Техносфера, 2011 (8) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)</p>	
Итого по разделу 6		10
Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	<p>В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (2-3) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (5)</p>	6
Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета.	<p>В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (2-3) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)</p>	4
Итого по разделу 7		10
Раздел 8. Безопасность Интернета.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	<p>А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (5) С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. .</p>	6
Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.	<p>Операционные системы, сети и интернет-технологии: М.: Академия, 2014 (8) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (20)</p>	4
Итого по разделу 8		10
Раздел 9. Криптографические методы защиты информации.		

Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	<p>А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8)</p> <p>А. В. Бабаш, Г. П. Шанкин. Криптография: М.: СОЛОН- Пресс, 2007 (4-6)</p> <p>С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security: М.: БИНОМ, 2007 (1-3)</p>	10
Итого по разделу 9		10

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- вопросы/задания по темам ПЗ;
- отчет по практическому заданию;
- индивидуальное практическое задание;
- вопросы к экзамену;
- 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/задания по темам ПЗ

Вопросы по темам ИПЗ приведены в комплекте типовых заданий по каждому разделу и в УМК дисциплины.

Отчет по практическому заданию

Оформление печатных отчетов по ПЗ предусмотрено в установленной форме (образцы оформления предоставляется студентам в ЭИОС и в основной литературе). При выполнении отчета следует руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

Индивидуальное практическое задание

Допуск к выполнению ПЗ не предусмотрен.

Требования к выполнению ПЗ: во всех ПЗ необходимо решить все задачи.

Предусмотрено оформление отчетов по ПЗ.

Защита ПЗ предусматривает проверку правильности решения задач, ответов на вопросы по заданию и ответов на контрольные вопросы, приведенные к комплекту типовых заданий по каждому разделу.

Вопросы к экзамену

Вопросы к экзамену размещены в курсе Moodle и в УМК дисциплины

Экзамен

Итоговый контроль по дисциплине проходит в форме экзамена. Экзаменационный билет включает в себя четыре теоретических вопроса.

Для получения положительной оценки по экзамену необходимо дать ответы на три теоретических вопроса.

Оценка удовлетворительно выставляется, если студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками; в процессе ответов допускаются ошибки по существу вопросов.

Хорошо - студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах); самостоятельно и отчасти при наводящих вопросах дает полноценные ответы на вопросы билета; не всегда выделяет наиболее существенное.

Отлично - студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину; самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы билета, подчеркивает при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи.

Также предусмотрено получение оценки согласно набранным во время семестра баллам, согласно размещённой в курсе в ЭОИС технологической карте.

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. Понятие о защите информации, виды защищаемой информации.	15	2	2	0	13	5	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ	
4	7	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	13	3	3	0	10	10	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ	
4	7	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	14	4	2	2	10	15	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ	
4	7	Раздел 4. Защита информации в современных информационных системах.	18	8	4	4	10	10	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ	
4	7	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	15	5	5	0	10	15	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ	

4	7	Раздел 6. Основные угрозы безопасности сетей.	18	8	4	4	10	15	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ
4	7	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	18	8	4	4	10	10	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ
4	7	Раздел 8. Безопасность Интернета.	15	5	2	3	10	10	Отчет по практическому заданию, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ
4	7	Раздел 9. Криптографические методы защиты информации.	18	8	8	0	10	10	Отчет по практическому заданию, Вопросы к экзамену, Индивидуальное практическое задание, Вопросы/ задания по темам ПЗ
Всего за 7 семестр			144	51	34	17	93	100	
Всего по дисциплине			144	51	34	17	93	100	

Критерии оценивания

ОПК-3

- Вопросы открытого типа:*
- № 1 **Государственная тайна это:**
- № 2 **Что можно отнести к правовым мерам ИБ?**
- № 3 **Что можно отнести к организационным мерам ИБ?**
- № 4 **Что можно отнести к техническим мерам ИБ?**
- № 5 **Что такое компьютерный вирус?**
- № 6 **Перечислите основные типы компьютерных вирусов**
- № 7 **Что может являться следствием вирусной атаки?**
- № 8 **Программные средства защиты можно разделить на:**
- № 9 **Наибольшую угрозу для безопасности сети представляют:**
- № 10 **Технические каналы утечки информации делятся на...**
- Вопросы закрытого типа:*
- № 1 **Как называется умышленно искажённая информация?**
1. - Дезинформация
 2. - Информативный поток
 3. - Достоверная информация
 4. - Перестает быть информацией
- № 2 **В зависимости от формы представления информация может быть разделена на?**
1. - Речевую, документированную и телекоммуникационную
 2. - Мысль, слово и речь
 3. - Цифровая, звуковая и тайная
 4. - Цифровая, звуковая
- № 3 **К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации?**
1. - Информационным процессам
 2. - Мыслительным процессам
 3. - Машинным процессам
 4. - Микропроцессам
- № 4 **Что называют защитой информации?**
1. - Называют деятельность по предотвращению утечки защищаемой информации
 2. - Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
 3. - Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
- № 5 **Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлён только тем лицам, которые на это имеют право**
1. - Управление доступом
 2. - Конфиденциальность
 3. - Аутентичность

4. - Целостность
5. - Доступность
- № 6 **Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе**
1. - Информационная безопасность
2. - Защитные технологии
3. - Заземление
4. - Конфиденциальность
- № 7 **Можно выделить следующие направления мер информационной безопасности**
1. - Правовые
2. - Организационные
3. - Все ответы верны
4. - Технические
- № 8 **Обеспечение достоверности и полноты информации и методов ее обработки.**
1. - Конфиденциальность
2. - Целостность
3. - Доступность
4. - Целесообразность
- № 9 **Целью информационной безопасности является?**
1. - Обезопасить ценности системы
2. - Защитить и гарантировать точность и целостность информации
3. - Минимизировать разрушения
- № 10 **К правовым мерам следует отнести?**
1. - Разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов
2. - Охрану вычислительного центра и аппаратуры связи
3. - Проектирование ЛВС и ГБС
4. - Средства идентификации и аутентификации пользователей