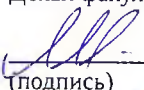


МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДАЮ
Декан факультета

 Матвеев П.В.
(подпись) ФИО
« 31 » 05 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии 09.03.04 Программная инженерия
Специализация/профиль/программа подготовки	Технологии разработки информационных систем ✓ Разработка программно-информационных систем
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	07 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	07 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

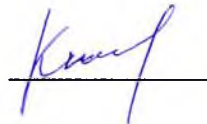
РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

09.03.02 Информационные системы и технологии
09.03.04 Программная инженерия

год набора группы: 2022

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:

09.03.04 (О7)	ПСК-1.05 — Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества
09.03.02 (О7)	ПСК-1.9 — Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности
09.03.02 (О7)	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
09.03.04 (О7)	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
09.03.04 (О7)	ОПК-4 — способность участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

Формированию компетенций служит достижение следующих результатов образования:

ПСК-1.05 (09.03.04, О7)

знания:

анализ структуры защиты промышленного предприятия;;

умения:

технологии реализации защиты информации на промышленном предприятии;;

навыки:

моделировать атаки в защищенной системе как изнутри, так и снаружи для подтверждения и ликвидации их последствий;.

ПСК-1.9 (09.03.02, О7)

знания:

современные методы кодирования и шифрования;;

умения:

программные механизмы и методы реализации систем защиты информации;;

навыки:

применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;.

ОПК-3 (09.03.02, О7)

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;.

ОПК-3 (09.03.04, О7)

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;.

ОПК-4 (09.03.04, О7)

знания:

модели и методы построения защищенных систем обработки информации;;

умения:

применять полученные знания в практике построения защищенных систем обработки информации, включая конфиденциальную информацию и обработку персональных данных;.

навыки:

обнаруживать компьютерные вирусы различными способами и применять методы борьбы с вирусами различной природы;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлениям: 09.03.02 Информационные системы и технологии, 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-5 — Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- 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-1.4 — Владение навыками использования различных технологий разработки программного обеспечения
- ПСК-1.5 — Способность оценивать качество программного обеспечения, в том числе проведение тестирования и исследование результатов
- ПСК-1.8 — Способность выполнять интеграцию программных модулей и компонент

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		ПСК-1.05 (09.03.04)	ПСК-1.9 (09.03.02)	ОПК-3 (09.03.02)	ОПК-3 (09.03.04)	ОПК-4 (09.03.04)
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	5	5	5	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	10	10	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	15	15	15	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	10	10	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	15	15	15	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	15	15	15	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	10	10	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	10	10	10	10
4	7	Раздел 9. Криптографические методы защиты информации. 9.1. Неформальные понятия о шифрах 9.2. Шифрования 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	10	10	10	10
Всего за 7 семестр			144	51	34	17	93	100	100	100	100	100
Всего по дисциплине			144	51	34	17	93	100	100	100	100	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	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10

методы защиты информации.	
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		Отч. по ПЗ		ДР		Отч. по ПЗ		Отч. по ПЗ		ДР	Вопр. Экз

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр. Экз – вопросы к экзамену.

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

Промежуточная аттестация проводится в формах:

- экзамен.

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.

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 направлениям: 09.03.02 Информационные системы и технологии, 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*:

ПСК-1.05 (09.03.04) Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества;

ПСК-1.9 (09.03.02) Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности;

ОПК-3 (09.03.02) способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3 (09.03.04) способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-4 (09.03.04) способность участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью.

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;
- 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. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8-9) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1)	4
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. Бабащ, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (3) 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) 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.		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, 2011 (1-3) А. В. Бабащ, 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»	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3) 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. Бабащ, 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. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (8) 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	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.		4

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

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- отчет по практическому заданию;
- 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.

Отчет по практическому заданию

При подготовке к выполнению практических заданий рекомендуется повторить теоретические сведения по теме данной работы в соответствии с указаниями в таблице Приложения 3 к настоящей рабочей программе. При подготовке к защите рекомендуется подготовить ответы на контрольные вопросы по теме данной работы. В случаях затруднений обращаться к преподавателю на очередном практическом занятии или на консультации.

К каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

ПЗ считается выполненным и защищенным успешно при условии:

- наличия корректного решения поставленной задачи;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие решения указанным требованиям, его работоспособность и эффективность – 7 баллов;
- отчет оформлен полностью в соответствии с ГОСТ 7.32-2017 – 3 балла;
- правильность ответов на вопросы – 7 баллов;
- своевременность выполнения и защиты индивидуального задания – 3 балла.

Основанием для снижения количества баллов являются:

- несоответствие решения указанным требованиям, его неэффективность или некорректная работа;
- оформление отчета не соответствует ГОСТ 7.32-2017 в 3 и более пунктах;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

В случае, если ПЗ и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20. Для того, чтобы ПЗ было сдано, требуется набрать 12 баллов.

Вопросы к экзамену

Вопросы к экзамену содержатся в УМК дисциплины.

При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы.

Экзамен

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4.

Перечень теоретических вопросов к экзамену, представленный в УМК дисциплины, предоставляется преподавателем. Задачи соответствуют программе практических занятий. При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы. Особое внимание следует уделить подготовке практических примеров к

теоретическим экзаменационным вопросам.

На экзамене студенту предлагается два теоретических вопроса. При успешном ответе на оба вопроса выставляется оценка «отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «хорошо» при успешном выполнении всех практических заданий. При отсутствии успешных ответов зачет может быть оформлен с оценкой «удовлетворительно» на основании успешного выполнения предусмотренных рабочей программой практических заданий. При несвоевременном или неполном выполнении практических заданий и при неуспешной сдаче экзамена выставляется оценка «не зачтено».

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		ПСК-1.05 (09.03.04)	ПСК-1.9 (09.03.02)	ОПК-3 (09.03.02)	ОПК-3 (09.03.04)	ОПК-4 (09.03.04)	
4	7	Раздел 1. Понятие о защите информации, виды защищаемой информации.	15	2	2	0	13	5	5	5	5	5	Отчет по практическому заданию
4	7	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	13	3	3	0	10	10	10	10	10	10	Вопросы к экзамену, Отчет по практическому заданию
4	7	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	14	4	2	2	10	15	15	15	15	15	Отчет по практическому заданию
4	7	Раздел 4. Защита информации в современных информационных системах.	18	8	4	4	10	10	10	10	10	10	Отчет по практическому заданию
4	7	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	15	5	5	0	10	15	15	15	15	15	Отчет по практическому заданию
4	7	Раздел 6. Основные угрозы безопасности сетей.	18	8	4	4	10	15	15	15	15	15	Отчет по практическому заданию
4	7	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	18	8	4	4	10	10	10	10	10	10	Отчет по практическому заданию
4	7	Раздел 8. Безопасность Интернета.	15	5	2	3	10	10	10	10	10	10	Отчет по практическому заданию, Вопросы к экзамену
4	7	Раздел 9. Криптографические методы защиты информации.	18	8	8	0	10	10	10	10	10	10	Отчет по практическому заданию, Вопросы к экзамену
Всего за 7 семестр			144	51	34	17	93	100	100	100	100	100	
Всего по дисциплине			144	51	34	17	93	100	100	100	100	100	

