

УТВЕРЖДАЮ
 Декан факультета

« ____ » _____ 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	Заочная
Факультет	И Робототехника и инновационная инженерия
Выпускающая кафедра	Н2 Программная инженерия и интеллектуальные системы
Кафедра-разработчик рабочей программы	Н2 Программная инженерия и интеллектуальные системы

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	
5	10	3	108	6	4	0	2	102	0	0	102	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: 2026

Программу составил:

Кафедра Н2 Программная инженерия и интеллектуальные системы
Князьков Анатолий Викторович, д.ф.-м.н., профессор

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **Н2 Программная инженерия и интеллектуальные системы**

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

Программа рассмотрена
на заседании выпускающей кафедры

Н2 Программная инженерия и интеллектуальные системы

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 — 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:

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: **СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММИРОВАНИЕ**.

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-1.3 — Способен использовать различные технологии разработки программного обеспечения
- 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 3 з.е., 108 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
5	10	Раздел 1. Понятие о защите информации, виды защищаемой информации. Информационная безопасность в системе национальной безопасности Российской Федерации.	9	1	1	0	8	5
5	10	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.	4	0	0	0	4	10
5	10	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации. Способы контактного и бесконтактного съема информации.	8	0	0	0	8	15
5	10	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.	16.5	1.5	1	0.5	15	10
5	10	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.	12	0	0	0	12	15
5	10	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.	8	0	0	0	8	15
5	10	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.	17.5	1.5	1	0.5	16	10
5	10	Раздел 8. Безопасность Интернета. 8.1. Разрушительные программы: вирусы, черви, троянские кони, мобильные программы. 8.2. Безопасность электронной почты.	4	0	0	0	4	10
5	10	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.	29	2	1	1	27	10
Всего за 10 семестр			108	6	4	2	102	100
Всего по дисциплине			108	6	4	2	102	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 4. Защита информации в современных информационных системах.	Практическая работа №1 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей.»	0.5
2	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Практическая работа №2 – «Поиск уязвимостей системы и разрушительных программ»	0.5
3	Раздел 9. Криптографические методы защиты информации.	Практическая работа №3 – «Изучение алгоритма шифрования информации по ГОСТ 28147-89»	1
Всего за 10 семестр			2

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 основных понятий по рекомендуемой литературе	8
2	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	Изучение предусмотренных программой основных понятий по рекомендуемой	4

		литературе	
3	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	8
4		Подготовка к практической работе №1	2
5	Раздел 4. Защита информации в современных информационных системах.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	13
6	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	12
7	Раздел 6. Основные угрозы безопасности сетей.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	8
8		Подготовка к практической работе №2	3
9	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	13
10	Раздел 8. Безопасность Интернета.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	4
11		Подготовка к практической работе №3	3
12	Раздел 9. Криптографические методы защиты информации.	Изучение предусмотренных программой основных понятий по рекомендуемой литературе	24
Всего за 10 семестр			102

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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.

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, 2007, эл. рес.
6. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
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 | Информация;
2. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
3. <http://e.lanbook.com/> — ЭБС Лань;;
4. <http://library.voenmeh.ru/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
5. <http://ura.it.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов..

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.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. LibreOffice;
2. Linux.

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.

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 *Н Робототехника и инновационная инженерия* БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрами *Н2 Программная инженерия и интеллектуальные системы*.

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 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 3 з.е., **108 ч.** Программой дисциплины предусмотрены лекционные занятия (**4 ч.**), практические занятия (**2 ч.**), самостоятельная работа студента (**102 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 6 ч. аудиторных занятий, и 102 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 основных понятий 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)	8
Итого по разделу 1		8
Раздел 2. Структуры и основные задачи службы безопасности предприятия.		
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (1) 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)	4
Итого по разделу 2		4
Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.		
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	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, сети и телекоммуникации: М.: КноРус, 2017 (8-9) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (2)	8
Итого по разделу 3		8
Раздел 4. Защита информации в современных информационных системах.		
Подготовка к практической работе №1	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)	2
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	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:	13

	М.: РУСАЙНС, 2017 (9) 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)	
Итого по разделу 4		15
Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.		
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3) 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) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9)	12
Итого по разделу 5		12
Раздел 6. Основные угрозы безопасности сетей.		
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (8) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (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) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	8
Итого по разделу 6		8
Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.		
Подготовка к практической работе №2	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (2-3)	3
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (5) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (2-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) А. П. Пятибратов, Л. П. Гудыно, А. А.	13

	Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8)	
Итого по разделу 7		16
Раздел 8. Безопасность Интернета.		
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. . 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) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (5)	4
Итого по разделу 8		4
Раздел 9. Криптографические методы защиты информации.		
Подготовка к практической работе №3	А. В. Бабаш, Г. П. Шанкин. Криптография: М.: СОЛОН-Пресс, 2007 (4-6) С. Бернет, С. Пэйн. Криптография.	3
Изучение предусмотренных программой основных понятий по рекомендуемой литературе	Официальное руководство RSA Security: М.: БИНОМ, 2007 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8)	24
Итого по разделу 9		27

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

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

Вопросы к экзамену размещены в курсе Moodle 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.

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 размещенной в курсе в ЭИОС технологической карте.

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	
5	10	Раздел 1. Понятие о защите информации, виды защищаемой информации.	9	1	1	0	8	5	Вопросы к экзамену
5	10	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	4	0	0	0	4	10	Вопросы к экзамену
5	10	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	8	0	0	0	8	15	Вопросы к экзамену
5	10	Раздел 4. Защита информации в современных информационных системах.	16.5	1.5	1	0.5	15	10	Отчет по практическому заданию, Вопросы к экзамену
5	10	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	12	0	0	0	12	15	Вопросы к экзамену
5	10	Раздел 6. Основные угрозы безопасности сетей.	8	0	0	0	8	15	Вопросы к экзамену
5	10	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	17.5	1.5	1	0.5	16	10	Отчет по практическому заданию, Вопросы к экзамену
5	10	Раздел 8. Безопасность Интернета.	4	0	0	0	4	10	Вопросы к экзамену
5	10	Раздел 9. Криптографические методы защиты информации.	29	2	1	1	27	10	Вопросы к экзамену, Отчет по практическому заданию
Всего за 10 семестр			108	6	4	2	102	100	
Всего по дисциплине			108	6	4	2	102	100	

Оценочные материалы по дисциплине МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ 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 установите последовательность
Порядок действий при разработке системы защиты:
1. Выбор средств защиты;
 2. Разработка плана безопасности;
 3. Определение требований к безопасности;
 4. Анализ рисков;
 5. Мониторинг и оценка безопасности.
 6. Реализация плана безопасности.
- № 2 Прочитайте текст и запишите развернутый обоснованный ответ
Понятие криптографии. Симметричные и ассиметричные алгоритмы шифрования.
- № 3 Прочитайте текст и запишите развернутый обоснованный ответ
Определение электронной подписи, виды электронной подписи по ФЗ №63-ФЗ «Об электронной подписи».
- № 4 Прочитайте текст и установите соответствие
Сопоставьте понятия, связанные с информационной безопасностью.

К каждой позиции в левом столбце, подберите позицию из правого столбца.

1	Авторизация	Обеспечение А секретности информации.
2	Конфиденциальность	Защита данных Б от повреждений и изменений.
3	Управление доступом	Обеспечение доступности информации В для авторизованных пользователей.
4	Доступность	Проверка Г личности пользователя. Ограничение Д доступа к ресурсам на основе прав.

- № 5 Прочитайте текст, выберите правильный ответ и запишите аргументы,
обосновывающие выбор ответа
Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?
1. Аппаратным средствам защиты
 2. Программным средствам защиты

3. Техническим средствам защиты
4. Правовым средствам защиты
- № 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
- Технические меры защиты можно разделить на:
1. Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и т.д.
 2. Правовые, организационные, технические
 3. Правовые, аппаратные, программные
 4. Личные, организационные
- № 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
- Наиболее важной аппаратной защитой является:
1. Защита от сбоев в электропитании
 2. Защита от сбоев серверов, рабочих станций и локальных компьютеров
 3. Защита от сбоев устройств для хранения информации
 4. Защита от утечек информации электромагнитных излучений
- № 8 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
- Что называют защитой информации?
1. Деятельность по предотвращению утечки защищаемой информации
 2. Деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
 3. Деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию
 4. Деятельность по предотвращению кражи
- № 9 Прочитайте текст и установите соответствие
- Сопоставьте типы угроз с соответствующими методами защиты.**
- К каждой позиции в левом столбце, подберите позицию из правого столбца.

1	Потеря данных	А	Управление доступом, физическая защита.
2	Несанкционированный доступ к информации.	Б	Резервное копирование, защита от утечек.
3	Сетевые атаки.	В	Антивирусная защита, системы предотвращения вторжений.
		Г	Файервол, системы обнаружения вторжений.

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

Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

1. на основе произвольно выбранного шифротекста;
2. на основе произвольно выбранного открытого текста
3. на основе избранного открытого текста
4. на основе избранного открытого и шифротекста

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

Основные отличия протоколов L2TP и PPTP состоят в следующем:

1. Протокол L2TP обеспечивает не конфиденциальность, а только туннелирование.
2. Протокол PPTP используется только для туннелирования TCP/IP.
3. Протокол L2TP может использоваться со службами IPSec, а протокол PPTP используется самостоятельно
4. Протокол PPTP. Главным преимуществом этого протокола является безопасность передачи данных в Интернет.

№ 12 Прочитайте текст и установите последовательность

Порядок действий при разработке системы защиты:

1. Построение модели угроз
2. Анализ рисков
3. Определение активов и бизнес-процессов
4. Применение и использование технических средств защиты информации
5. Контроль и управление
6. Совершенствование разработанной системы
7. Создание ОРД (организационно-распорядительная документация)