

УТВЕРЖДАЮ
 Декан факультета

_____ Матвеев П.В.

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
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	
3	5	3	108	34	17	0	17	74	0	0	74	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.02 Информационные системы и технологии

год набора группы: 2025

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Шимкун Вячеслав Владиславович, старший преподаватель

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 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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:

ПК-2.1 — Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-2.2 — Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Формированию компетенций служит достижение следующих результатов образования:

ПК-2.1

знания:

анализ структуры защиты промышленного предприятия;

технологии реализации защиты информации на промышленном предприятии;

умения:

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

навыки:

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

ПК-2.2

знания:

различия защиты физической, организационной, математической и программной модели и методы построения защищенных систем обработки информации;

методы организации защищенных каналов передачи информации через компьютерные сети общего пользования;

умения:

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

навыки:

реализация механизмов разграничения доступа пользователей к ресурсам распределенной системы обработки информации или компьютерной сети;

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

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 применения в области информационных систем и технологий
- 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		ПК-2.1	ПК-2.2
3	5	Раздел 1. Понятие о защите информации, виды защищаемой информации. Информационная безопасность в системе национальной безопасности Российской Федерации.	10	2	2	0	8	15	15
3	5	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.	10	2	2	0	8	15	15
3	5	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации. Способы контактного и бесконтактного съема информации.	12	4	2	2	8	15	15
3	5	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.	14	6	2	4	8	15	15
3	5	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.	10	2	2	0	8	10	10
3	5	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.	14	6	2	4	8	10	10
3	5	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.	14	6	2	4	8	10	10
3	5	Раздел 8. Безопасность Интернета. 8.1. Разрушительные программы: вирусы, черви, троянские кони, мобильные программы. 8.2. Безопасность электронной почты.	13	5	2	3	8	5	5
3	5	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.	11	1	1	0	10	5	5
Всего за 5 семестр			108	34	17	17	74	100	100
Всего по дисциплине			108	34	17	17	74	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 – «Установка и настройка сервера управления Кибер Бэкап»	4
3	Раздел 6. Основные угрозы безопасности сетей.	Практическая работа №3 – «Подключение хранилища и установка агентов Кибер Бэкап»	4
4	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Практическая работа №4 – «Настройка планов резервного копирования и репликации Кибер Бэкап»	4
5	Раздел 8. Безопасность Интернета.	Практическая работа №5 – «Восстановление информации в Кибер Бэкап. Мониторинг и отчёты»	3
Всего за 5 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	8
2	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	8
3	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
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	4
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	4
8		Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», оформление отчета.	4
9	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», посылка отчета по электронной почте преподавателю.	4
10		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
11	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета.	4
12		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
13	Раздел 8. Безопасность Интернета.	Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.	4
14		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
15	Раздел 9. Криптографические методы защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
Всего за 5 семестр			74

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
5				Отч. по ПЗ		ДР		Отч. по ПЗ		ДР		Отч. по ПЗ				ДР	Вопр.Диф.Зач, диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр.Диф.Зач – вопросы к дифференцированному зачету;

- диф. зач. – дифференцированный зачет.

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к дифференцированному зачету.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

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 | Информация;
2. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
3. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;
4. <http://e.lanbook.com/> — ЭБС Лань;;
5. <http://library.voennmeh.ru/jirbis2/> — Р“Р”Р°РІРSP°СЦ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
6. <http://library.voennmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
7. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;
8. <http://library.voennmeh.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.voenmeh.ru/jrbis2/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 **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПК-2.1 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-2.2 Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

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 дифференцированному зачету.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены лекционные занятия (**17 ч.**), практические занятия (**17 ч.**), самостоятельная работа студента (**74 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 34 ч. аудиторных занятий, и 74 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)	8
Итого по разделу 1		8
Раздел 2. Структуры и основные задачи службы безопасности предприятия.		
Изучение предусмотренных программой дидактических единиц 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)	8
Итого по разделу 2		8
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) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1)	4
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)	4
Итого по разделу 3		8

Раздел 4. Защита информации в современных информационных системах.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . КRYPTOграфические 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)	4
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, 2011 (1-3) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	4
Итого по разделу 4		8
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) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	4
Подготовка к практической работе №3 – «Реализация механизмов разграничения доступа пользователей к объектам ПЭВМ. Защита рабочих станций, работающих под Windows», оформление отчета.	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (8) А. В. Бабаш, Е. К. Баранова. . КRYPTOграфические методы защиты информации: М.: КноРус, 2018 (8) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9)	4
Итого по разделу 5		8
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», посылка отчета по электронной почте преподавателю.	А. В. Бабаш, Е. К. Баранова. . КRYPTOграфические методы защиты информации: М.: КноРус, 2018 (8) А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (8)	4
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) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	4

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

	защиты информации: М.: КноРус, 2018 (8)	
Итого по разделу 9		10

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- отчет по практическому заданию;
- вопросы к дифференцированному зачету;
- дифференцированный зачет.

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

К каждой ПР 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 каждой ПР.

ПР считается выполненным и защищенным успешно при условии:

- наличия программного приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПР по комплекту тестовых вопросов для защиты ПР, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие программного приложения 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 программного приложения 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 ПР 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 ПР была сдана, требуется набрать 12 баллов.

Вопросы к дифференцированному зачету

Перечень теоретических вопросов к дифф. зачету предоставляется преподавателем. Перечень вопросов лежит в УМК дисциплины. При подготовке ответов на теоретические вопросы рекомендуется помимо конспектов лекций использовать источники основной и дополнительной литературы.

Дифференцированный зачет

График контрольных мероприятий предусматривает выполнение студентом пяти заданий, каждое из которых может быть оценено максимально на 20 баллов.

Дифференцированный зачет выставляется по сумме результатов контрольных мероприятий, проводимых в течение семестра. Максимальная сумма баллов за семестр – 100 баллов. Набранная итоговая сумма баллов пересчитывается в оценку по следующей схеме: - 86 – 100 баллов – отлично; - 61 – 85 балла - хорошо; - 45 – 60 баллов – удовлетворительно.

В случае несогласия студента с оценкой согласно набранным баллам, при условии выполнения всех работ, может быть проведён устный зачёт, вопросы к которому располагаются в УМК дисциплины. В этом случае дифференцированный зачёт проходит в форме ответов на два вопроса из перечня При

успешном ответе на оба вопроса выставляется оценка «зачтено-отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «зачтено-хорошо». При отсутствии успешных ответов зачет может быть оформлен с оценкой «зачтено-удовлетворительно» на основании успешных ответов на дополнительные вопросы. 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		ПК-2.1	ПК-2.2	
3	5	Раздел 1. Понятие о защите информации, виды защищаемой информации.	10	2	2	0	8	15	15	Отчет по практическому заданию
3	5	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	10	2	2	0	8	15	15	Отчет по практическому заданию
3	5	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	12	4	2	2	8	15	15	Отчет по практическому заданию
3	5	Раздел 4. Защита информации в современных информационных системах.	14	6	2	4	8	15	15	Отчет по практическому заданию
3	5	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	10	2	2	0	8	10	10	Отчет по практическому заданию
3	5	Раздел 6. Основные угрозы безопасности сетей.	14	6	2	4	8	10	10	Отчет по практическому заданию
3	5	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	14	6	2	4	8	10	10	Отчет по практическому заданию
3	5	Раздел 8. Безопасность Интернета.	13	5	2	3	8	5	5	Отчет по практическому заданию
3	5	Раздел 9. Криптографические методы защиты информации.	11	1	1	0	10	5	5	Отчет по практическому заданию, Вопросы к дифференцированному зачету
Всего за 5 семестр			108	34	17	17	74	100	100	
Всего по дисциплине			108	34	17	17	74	100	100	

Оценочные материалы по дисциплине ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПК-2.1 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

№ 1 Прочитайте текст и установите последовательность

Распределите нарушителей по уровню возможностей от самого низкого к высокому:

1. Определяет возможность управления функционированием системы, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
2. Определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
3. Определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.
4. Определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

На чём основан формальный подход при рассмотрении вопросов информационной безопасности?

№ 3 Прочитайте текст и запишите развернутый обоснованный ответ

Расшифруйте аббревиатуру "ФСТЭК".

№ 4 Прочитайте текст и установите соответствие

- | | | |
|---|---|---|
| 1 | Активная сущность, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов - | А объект доступа |
| 2 | Пассивная сущность, процессы над которой могут в определенных случаях быть источником порождения новых субъектов - | Б монитор безопасности
В субъект доступа |

№ 5 Прочитайте текст и установите соответствие

- | | | |
|---|---|--|
| 1 | Состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам) - | А безопасность информации |
| 2 | Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования - | Б информационная безопасность
В защита информации |

№ 6 Прочитайте текст и установите последовательность

Расставьте уровни представления информации по порядку от уровня носителей к

семантическому уровню:

1. Логический уровень
2. Синтаксический уровень
3. Уровень средств взаимодействия с носителем

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

Характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа:

1. Сложность
2. Стойкость
3. Криптостойкость
4. Криповость

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

Формальное выражение политики безопасности называют:

1. Стратегией безопасности.
2. Корпоративной политикой безопасности.
3. Моделью безопасности.
4. Регламентом безопасности.

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

Какой подход при рассмотрении вопросов информационной безопасности основан на понятии политики безопасности и определении способов гарантирования выполнения её положений?

1. Неформальный
2. Описательный
3. Формальный
4. Последовательный

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

Виды моделей разграничения доступа:

1. Дискреционные
2. Защищённые
3. Тематические
4. Парольные
5. Физико-математические
6. Теоретико-информационные
7. Мандатные
8. Ролевые

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

Задачи модели безопасности:

1. прохождение сертификации ФСТЭК
2. защита от НСД
3. составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных систем
4. подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности
5. выбор и обоснование базовых принципов архитектуры защищенных систем, определяющих механизмы реализации средств и методов защиты информации

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

Применение модели безопасности:

1. при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности
2. в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели
3. при составлении формальной спецификации политики безопасности разрабатываемой системы
4. при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты
5. при защите информации от утечки по техническим каналам

ПК-2.2 - Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

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

Какой из вариантов наиболее точно описывает правила модели мандатного доступа?

1. Нет чтения вниз
2. Нет чтения вниз, нет записи вверх
3. Нет записи вниз
4. Нет чтения вверх, нет записи вниз

№ 2 Прочитайте текст и установите соответствие

1 Информационная безопасность – это

2 Уровень защищенности – это

одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным уровнем защищенности.
А
Б процесс, который должен выполняться непрерывно на всем протяжении

		жизненного цикла информационной системы. состояние защищенности В информации и поддерживающей инфраструктуры.
3	Защита информации – это	
№ 3 Прочитайте текст и установите соответствие		
1	Формальные средства защиты	А выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.
2	Неформальные средства защиты	Б регламентируют деятельность человека. выполняют защитные В функции без заранее предусмотренной процедуры.
№ 4 Прочитайте текст и запишите развернутый обоснованный ответ		
Расшифруйте аббревиатуру «СЗИ».		
№ 5 Прочитайте текст и запишите развернутый обоснованный ответ		
Как называется комбинация IP-адреса и номера порта?		
№ 6 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов		
Виды скрытых каналов утечки информации:		
1. скрытые каналы по памяти		
2. скрытые статистические каналы		
3. скрытые каналы по времени		
4. скрытые каналы по вводу-выводу		
5. скрытые семантические каналы		
№ 7 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов		
Категории методов защиты от НСД:		
1. финансовые		
2. военные		
3. организационные		
4. технологические		
5. научные		

- 6. конфиденциальные
- 7. морально-этические
- 8. правовые

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

По каким признакам классифицируют государственные информационные системы (ГИС)?

- 1. По признаку отраслевой принадлежности.
- 2. По масштабу ГИС.
- 3. По значимости обрабатываемой в ГИС информации.
- 4. По географическому признаку.

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

Скрытым каналом утечки информации называется...

- 1. механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход аутентификации.
- 2. механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа.
- 3. механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход монитора безопасности.
- 4. механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями скрытый от пользователя.

№ 10 Прочитайте текст и установите последовательность

Распределите по порядку этапы жизненного цикла информации от "Оценки" до "Использования":

- 1. Оценка
- 2. Выборка
- 3. Подготовка к хранению
- 4. Обработка
- 5. Хранение
- 6. Использование

№ 11 Прочитайте текст и установите последовательность

Распределите нарушителей по уровню возможностей от первого до четвертого:

- 1. Определяет возможность управления функционированием системы, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.
- 2. Определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
- 3. Определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.
- 4. Определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

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

Под целостностью данных подразумевается...

1. отсутствие фрагментации.
2. отсутствие ненадлежащих изменений.
3. совпадение контрольных сумм.
4. наличие данных в полном объёме.