

УТВЕРЖДАЮ
 Декан факультета

 (подпись) Матвеев П.В.
 ФИО
 «___» _____ 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	4	144	51	34	0	17	93	0	0	93	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: 2024

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Шимкун Вячеслав Владиславович, 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:

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

ПСК-2.12 — Способность 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:

ПСК-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;.

ПСК-2.12

знания:

различия защиты физической, организационной, математической и программной;

модели и методы построения защищенных систем обработки информации;

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

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:

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-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	
				ВСЕГО	Лекции	Практические занятия		ПСК-2.1	ПСК-2.12
3	5	Раздел 1. Понятие о защите информации, виды защищаемой информации. Информационная безопасность в системе национальной безопасности Российской Федерации.	15	2	2	0	13	5	5
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.	13	3	3	0	10	10	10
3	5	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации. Способы контактного и бесконтактного съема информации.	14	4	2	2	10	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.	18	8	4	4	10	10	10
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.	15	5	5	0	10	15	15
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.	18	8	4	4	10	15	15
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.	18	8	4	4	10	10	10
3	5	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
3	5	Раздел 9. Криптографические методы защиты информации. 9.1. Неформальные понятия о шифрах. 9.2. Шифрование и дешифрование. 9.3. Математические основы криптографии. 9.4. Алгоритмы шифрования.	18	8	8	0	10	10	10
Всего за 5 семестр			144	51	34	17	93	100	100
Всего по дисциплине			144	51	34	17	93	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 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	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», оформление отчета.	4
9	Раздел 6. Основные угрозы безопасности сетей.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
10		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
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	Раздел 8. Безопасность Интернета.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
14		Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.	4
15	Раздел 9. Криптографические методы защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
Всего за 5 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
5						ДР		Отч. по ПЗ		ДР		Отч. по ПЗ		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, 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. <https://ura.it.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;
4. <http://e.lanbook.com/> — ЭБС Лань;;
5. <http://library.voenmeh.ru/jirbis2/> — Р^РР^РPIPSP^РСЦ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
6. <https://ura.it.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
7. <http://library.voenmeh.ru/jirbis2/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
8. <http://library.voenmeh.ru/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

Современные профессиональные базы данных:

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

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.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 **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 Естественнoнаучный БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

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

ПСК-2.12 Способность 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 **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	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)	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) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1)	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)	4
Итого по разделу 3		10

Раздел 4. Защита информации в современных информационных системах.		
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 (3)	6
Подготовка к практической работе №2 – «Управление правами. Анализ установок безопасности системы и привилегий пользователей», оформление отчета.	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3)	4
Итого по разделу 4		10
Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (1-3) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1-3)	6
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. . Криптографические 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		10
Раздел 6. Основные угрозы безопасности сетей.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .	6
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.	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) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .	4

	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)	
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. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (5) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9)	6
Подготовка к практической работе №4 – «Моделирование атак на host и действий по их отражению. Моделирование атак на web-узел», оформление отчета.	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) 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 (2-3)	4
Итого по разделу 7		10
Раздел 8. Безопасность Интернета.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (5) С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. .	6
Подготовка к практической работе №5 – «Настройка протокола динамической маршрутизации RIP. Разработка IP-адресации», оформление отчета.	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)	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) С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security: М.: БИНОМ, 2007 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы	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		ПСК-2.1	ПСК-2.12	
3	5	Раздел 1. Понятие о защите информации, виды защищаемой информации.	15	2	2	0	13	5	5	Отчет по практическому заданию
3	5	Раздел 2. Структуры и основные задачи службы безопасности предприятия.	13	3	3	0	10	10	10	Отчет по практическому заданию
3	5	Раздел 3. Методы нарушения конфиденциальности, целостности и доступности информации.	14	4	2	2	10	15	15	Отчет по практическому заданию
3	5	Раздел 4. Защита информации в современных информационных системах.	18	8	4	4	10	10	10	Отчет по практическому заданию
3	5	Раздел 5. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	15	5	5	0	10	15	15	Отчет по практическому заданию
3	5	Раздел 6. Основные угрозы безопасности сетей.	18	8	4	4	10	15	15	Отчет по практическому заданию
3	5	Раздел 7. Атаки изнутри системы. Виды, классификация и способы защиты. Атаки снаружи.	18	8	4	4	10	10	10	Отчет по практическому заданию
3	5	Раздел 8. Безопасность Интернета.	15	5	2	3	10	10	10	Отчет по практическому заданию
3	5	Раздел 9. Криптографические методы защиты информации.	18	8	8	0	10	10	10	Отчет по практическому заданию, Вопросы к дифференцированному зачету
Всего за 5 семестр			144	51	34	17	93	100	100	
Всего по дисциплине			144	51	34	17	93	100	100	

Критерии оценивания

ПСК-2.1

	<i>Вопросы открытого типа:</i>
№ 1	Интернет — браузеры предназначены:
№ 2	Веб — страницы передаются по этому протоколу:
№ 3	Описать функции современных вычислительных сетей и основные прикладные аспекты их использования
№ 4	Назовите определение IP-адреса
№ 5	Назовите определение маршрутизатора (коммутатора).
№ 6	Какие сетевые серверы бывают?
№ 7	Как называется комбинация IP-адреса и номера порта?
№ 8	Расшифруйте аббревиатуру «СЗИ».
№ 9	Что такое «аудит» в контексте информационной безопасности?
№ 10	Расшифруйте аббревиатуру «ИСПД».
	<i>Вопросы закрытого типа:</i>
№ 1	Разместите средства защиты по группам: 1. Формальные средства защиты: 2. Неформальные средства защиты: 1. Физические средства 2. Аппаратные средства 3. Программные средства 1. Законодательные средства 2. Организационные средства 3. Морально-этические средства 3. Антивирусные средства 3. Религиозные средства
№ 2	В 1975 году Джерри Зальцер и Майкл Шрёдер в статье «Защита информации в компьютерных системах» впервые предложили разделить нарушения безопасности на три основных категории. Позднее эти категории получили краткие наименования: С – I – А – Целостность Авторизованность Интегральность Безопасность Безнаказанность Конфиденциальность

	Санкционированность
	Доступность
№ 3	Защищённость
	Характер происхождения угроз:
	1. Умышленные факторы.
	2. ... факторы.
	Неумышленные
	Естественные
	Фантастические
	Противоестественные
	Потусторонние
№ 4	Сверхестественные
	Целостность можно подразделить на _____ (понимаемую как неизменность информационных объектов) и _____ (относящуюся к корректному выполнению сложных действий (транзакций)).
	холодную
	неизменную
	горячую
	ликвидную
	корректную
	динамическую
	статическую
	транзакционную
№ 5	изменяемую
	Виды угроз. Основные нарушения:
	1. Физической целостности (уничтожение, разрушение элементов).
	2. _____ целостности (разрушение логических связей).
	3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
	4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
	5. Прав собственности на информацию (несанкционированное копирование, использование).
	Логической

	Двоичной
	Программной
	Криптографической
	Шестнадцатеричной
№ 6	<p>Духовной</p> <p>Концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:</p> <p>- [1] защищать?</p> <p>- от [2] защищать?</p> <p>- [3] защищать?</p>
	<p>[1] – что / зачем / на какие деньги</p> <p>[2] – чего (кого) / чего / кого</p> <p>[3] – как / кем / с чем</p>
№ 7	<p>Ущерб может быть [1] или [2].</p> <p>[1] – приемлемым, моральным, финансовым, репутационным</p>
№ 8	<p>[2] - моральным, финансовым, репутационным, неприемлемым</p> <p>Чем отличаются информационная безопасность, защита информации и уровень защищенности?</p>
	<ol style="list-style-type: none"> 1. Информационная безопасность – это ... 2. Уровень защищенности – это ... 3. Защита информации – это ...
	<p>А - одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным уровнем защищенности.</p> <p>Б - процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.</p> <p>В - состояние защищенности информации и поддерживающей инфраструктуры.</p>
№ 9	<p>Правильно укажите соответствие средств защиты их определениям.</p> <ol style="list-style-type: none"> 1. Формальные средства защиты 2. Неформальные средства защиты <p>А – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.</p> <p>Б – регламентируют деятельность человека.</p>

В – выполняют защитные функции без заранее предусмотренной процедуры
Доступность информации – это

свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними.

свойство системы обеспечивать доступ субъектов к информации.

свойство информации быть понятной человеку с недостаточным уровнем образования и (или) интеллекта.

свойство системы осуществлять своевременный информационный обмен между субъектами информационной системы.

свойство системы сохранять стоимость доступа к информации на уровне или ниже прожиточного минимума.

ПСК-2.12

Вопросы открытого типа:

- № 1 Государственная тайна это:
- № 2 Что можно отнести к правовым мерам ИБ?
- № 3 Что можно отнести к организационным мерам ИБ?
- № 4 Что можно отнести к техническим мерам ИБ?
- № 5 Что такое компьютерный вирус?
- № 6 Основные типы компьютерных вирусов:
- № 7 Ответьте на вопрос «Что называется вирусной атакой?»
- № 8 Программные средства защиты можно разделить на:
- № 9 Наибольшую угрозу для безопасности сети представляют:
- № 10 Технические каналы утечки информации делятся на...

Вопросы закрытого типа:

- № 1 Защита информации это:

это одна из характеристик информационной системы.

комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности.

совокупность информационных технологий и технических средств.

состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

- № 2 Информационная угроза – это:

потенциальная возможность потери информации.

потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере информации.

потенциальная возможность неправомерного или случайного воздействия на объект защиты.

№ 3	потенциальная возможность неправомерного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.
	потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации. Конфиденциальность информации – это ...
	свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). свойство информации ограниченного доступа в силу личного характера. свойство информации быть известной только ее владельцу. свойство информации быть известной только субъектам информационной системы.
№ 4	степень ограниченности доступа. Угроза информации – это ...
№ 5	опасность нарушения физической целостности информационной системы (уничтожение, разрушение элементов). неблагожелательное намерение в адрес информации, высказанное в устной или письменной форме. опасность изменения содержания (изменение блоков информации, внешнее навязывание ложной информации). возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию. возможность нежелательного воздействия на информацию Целостность информации – это ...
№ 6	свойство информации, характеризующее ее состояние. свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. свойство информации не изменяться со временем. свойство информации, характеризующее ее неизменность. свойство информации, характеризующее ее исчерпывающий характер. Введите номер пункта с несуществующим грифом:
№ 7	1. С (Секретно) 2. ДСП (Служебная тайна) 3. КФД (Конфиденциальные данные) Верно ли, что информация с ограниченным доступом делится на государственную тайну, служебную тайну и конфиденциальную?

- Верно
- № 8 Неверно
Верно ли, что под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры?
- Верно
- № 9 Неверно
Основным назначением компьютерной сети является:
- № 10
1. Совместное удалённое использование ресурсов сети сетевыми пользователям
 2. Физическое соединение всех компьютеров сети
 3. Совместное решение распределённой задачи пользователями сети
- Маршрутизатор - устройство, соединяющее различные:
1. Компьютерные сети
 2. По архитектуре компьютеры
 3. Маршруты передачи адресов для e-mail