

УТВЕРЖДАЮ
 Декан факультета

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

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	6	5	180	85	34	0	51	95	0	0	95	ЭКЗ.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.02 Информационные системы и технологии

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

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

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-2.18 — Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Формированию компетенций служит достижение следующих результатов образования:

ПСК-2.18

знания:

- о задачах, структуре и возможностях технической разведки, основных этапах и процессах добывания ею информации;
- о физических процессах в технических средствах и системах, способствующих утечке защищаемой информации;
- о характеристиках используемых и перспективных технических средств добывания и защиты информации;
- о видах, источниках и носителях защищаемой информации;
- об основных угрозах безопасности информации;
- о концепции инженерно-технической защиты информации;
- о государственной системе защиты информации и ее основных документах;

умения:

- применять наиболее эффективные методы и средства инженерно-технической защиты информации;
- выявлять угрозы и технические каналы утечки информации;
- описывать (моделировать) объекты защиты и угрозы безопасности информации;

навыки:

- работы с нормативными правовыми актами;
- работы с методами и средствами выявления угроз безопасности автоматизированным системам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

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

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ, АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**.

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
- 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

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 з.е., 180 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-2.18
3	6	Раздел 1. Концепции инженерно-технической защиты информации. 1.1 Основные понятия и определения 1.2 Классификация и структура технических каналов утечки информации 1.3 Характеристики каналов утечки информации.	59	28	11	17	31	20
3	6	Раздел 2. Теоретические основы инженерно-технической защиты информации. 2.1. Оптические каналы утечки информации 2.2. Радиоэлектронные каналы утечки информации.	60	28	11	17	32	20
3	6	Раздел 3. Физические основы защиты информации. 3.1 Акустические каналы утечки информации 3.2 Материально-вещественные каналы утечки информации 3.3 Системный подход к инженерно-технической защите информации 3.4 Основные этапы проектирования системы защиты информации техническими средствами 3.5 Инструментальные методы контроля эффективности технической защиты информации. 3.6 Оборудование для контроля эффективности технической защиты информации.	61	29	12	17	32	60
Всего за 6 семестр			180	85	34	51	95	100
Всего по дисциплине			180	85	34	51	95	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Концепции инженерно-технической защиты информации.	Практическая работа №1	17
2	Раздел 2. Теоретические основы инженерно-технической защиты информации.	Практическая работа №2	17
3	Раздел 3. Физические основы защиты информации.	Практическая работа №3	8
4		Практическая работа №4	9
Всего за 6 семестр			51

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Концепции инженерно-технической защиты информации.	Подготовка к практической работе №1 и оформление отчета.	4
2		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	27
3	Раздел 2. Теоретические основы инженерно-технической защиты информации.	Подготовка к практической работе №2 и оформление отчета.	4
4		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	28
5	Раздел 3. Физические основы защиты информации.	Подготовка к практической работе №3 и оформление отчета.	4
6		Подготовка к практической работе №4 и оформление отчета.	4
7		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	24
Всего за 6 семестр			95

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
6						ДР				ДР			Отч. по ПЗ			ДР	Вопр. Экз

Условные обозначения:

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

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

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

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. Средства перехвата информации в линиях связи. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007, эл. рес.
2. Средства технической разведки. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007, эл. рес.
3. А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах. Москва: Форум, 2020, эл. рес.
4. А. Голдсмит. . Беспроводные коммуникации. М.: Техносфера, 2011, 5 экз.
5. В. В. Платонов. . Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. М.: Академия, 2006, 17 экз.
6. В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2003, 70 экз.
7. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
8. Д. А. Мельников. . Информационная безопасность открытых систем. Москва: Флинта, 2014, эл. рес.
9. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
10. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
11. Л. Б. Кочин. . Средства радиоэлектронной защиты. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008, эл. рес.
12. Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации. Старый Оскол: ТНТ, 2010, 22 экз.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

не требуются.

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

1. <https://urait.ru/> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
2. <https://e.lanbook.com/> — ЭБС Лань;
3. <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»;
3. <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;
3. Notepad++.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. LibreOffice;
3. Linux;
4. Notepad++.

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 **ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ** 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*:

ПСК-2.18 Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

Содержание дисциплины охватывает круг вопросов, связанных с концепциями инженерно-технической защиты информации, с теоретическими основами инженерно-технической защиты информации, с физическими основами инженерно-технической защиты информации, с техническими средствами добывания, с организационными основами инженерно-технической защиты информации, с методическим обеспечением инженерно-технической защиты информации.

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 **5 з.е., 180 ч.** Программой дисциплины предусмотрены лекционные занятия (**34 ч.**), практические занятия (**51 ч.**), самостоятельная работа студента (**95 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 180 ч., из них 85 ч. аудиторных занятий, и 95 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. Концепции инженерно-технической защиты информации.		
Подготовка к практической работе №1 и оформление отчета.	Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2-4) А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (1-3)	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2-4) А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах: Москва: Форум, 2020 (4-6) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (1-4) В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий: СПб.: БХВ-Петербург, 2003 (3) В. В. Платонов. . Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: М.: Академия, 2006 (5) Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (5)	27
Итого по разделу 1		31
Раздел 2. Теоретические основы инженерно-технической защиты информации.		
Подготовка к практической работе №2 и оформление отчета.	А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (4)	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (4-5) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (1-4) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (4-5) А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах: Москва: Форум, 2020 (4-6) В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий: СПб.: БХВ-Петербург, 2003 (4) . Средства перехвата информации в линиях связи:	28

	СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1) Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (4-5) . Средства технической разведки: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1) В. В. Платонов. . Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: М.: Академия, 2006 (4)	
Итого по разделу 2		32
Раздел 3. Физические основы защиты информации.		
Подготовка к практической работе №3 и оформление отчета.	Д. А. Мельников. . Информационная безопасность открытых систем: Москва: Флинта, 2014 (1-3) В. В. Платонов. . Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: М.: Академия, 2006 (4-6)	4
Подготовка к практической работе №4 и оформление отчета.	А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах: Москва: Форум, 2020 (4-6) . Средства технической разведки: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1-2)	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	. Средства перехвата информации в линиях связи: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2007 (1-2) Л. Б. Кочин. . Средства радиоэлектронной защиты: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2008 (1-2)	24
Итого по разделу 3		32

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

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

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Отчет по практическому заданию

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

ПЗ считается выполненным и защищенным успешно при условии:

- наличия программного приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, 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 ПЗ и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20.

Вопросы к экзамену

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

Экзамен

Итоговый контроль по дисциплине проходит в форме экзамена.

Экзаменационный билет для экзамена включает в себя два теоретических вопроса. Оценка «удовлетворительно» – один неполный ответ; оценка «хорошо» – один полный или два неполных ответа; оценка «отлично» – два полных ответа.

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-2.18	
3	6	Раздел 1. Концепции инженерно-технической защиты информации.	59	28	11	17	31	20	Отчет по практическому заданию
3	6	Раздел 2. Теоретические основы инженерно-технической защиты информации.	60	28	11	17	32	20	Отчет по практическому заданию
3	6	Раздел 3. Физические основы защиты информации.	61	29	12	17	32	60	Отчет по практическому заданию, Вопросы к экзамену
Всего за 6 семестр			180	85	34	51	95	100	
Всего по дисциплине			180	85	34	51	95	100	

Критерии оценивания

ПСК-2.18

- Вопросы открытого типа:*
- № 1 Доступность информации – это
 - № 2 Государственная тайна это:
 - № 3 Что можно отнести к правовым мерам ИБ?
 - № 4 Что можно отнести к организационным мерам ИБ?
 - № 5 Что можно отнести к техническим мерам ИБ?
 - № 6 Что такое компьютерный вирус?
 - № 7 Основные типы компьютерных вирусов:
 - № 8 Ответьте на вопрос «Что называется вирусной атакой?»
 - № 9 Программные средства защиты можно разделить на:
 - № 10 Наибольшую угрозу для безопасности сети представляют:
- Вопросы закрытого типа:*
- № 1 Расставьте соответствующие понятия
 - 1) Каналом утечки называется
 - 2) Техническим каналом утечки называется
 - А) физический путь переноса информации от ее источника к несанкционированному получателю
 - Б) если запись информации на носитель канала утечки и съем ее с носителя производится с помощью технических средств
 - В) попадание информации к заинтересованному в ней несанкционированному получателю
 - № 2 Поставьте в соответствие наименования типов сетевых атак их описаниям
 - 1) Непосредственный доступ к пакетам, передаваемым по сети
 - 2) Сбор информации о сети с помощью общедоступных данных и приложений
 - 3) Недоступность сети из-за превышения допустимых пределов функционирования
 - 4) Хакер выдает себя за санкционированного пользователя
 - 5) Подбор пароля легального пользователя сети
 - А) Man-in-the-Middle
 - Б) Сетевая разведка
 - В) DDoS
 - Г) IP-спуфинг
 - Д) Парольная атака
 - № 3 Поставьте в соответствие типу защиты информации необходимую для этого типа технологию
 - 1) Традиционное шифрование
 - 2) Шифрование с открытым ключом
 - 3) Защита с помощью электронного ключа
 - А) Используется 1 ключ

	Б)Используются 2 ключа
№ 4	<p>В)Электронное устройство подключается к порту компьютера</p> <p>Разместите средства защиты по группам:</p> <ol style="list-style-type: none"> 1. Формальные средства защиты: 2. Неформальные средства защиты: <ol style="list-style-type: none"> 1. Физические средства 2. Аппаратные средства 3. Программные средства <ol style="list-style-type: none"> 1. Законодательные средства 2. Организационные средства 3. Морально-этические средства 3. Антивирусные средства
№ 5	<p>3. Религиозные средства</p> <p>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:</p> <p>С –</p> <p>I –</p> <p>A –</p> <p>Целостность</p> <p>Авторизованность</p> <p>Интегральность</p> <p>Безопасность</p> <p>Безнаказанность</p> <p>Конфиденциальность</p> <p>Санкционированность</p> <p>Доступность</p>
№ 6	<p>Защищённость</p> <p>Характер происхождения угроз:</p> <ol style="list-style-type: none"> 1. Умышленные факторы. 2. ... факторы. <p>Неумышленные</p>

	Естественные
	Фантастические
	Противоестественные
	Потусторонние
	Сверхестественные
№ 7	<p>Целостность можно подразделить на _____ (понимаемую как неизменность информационных объектов) и _____ (относящуюся к корректному выполнению сложных действий (транзакций)).</p> <p>холодную</p> <p>неизменную</p> <p>горячую</p> <p>ликвидную</p> <p>корректную</p> <p>динамическую</p> <p>статическую</p> <p>транзакционную</p>
№ 8	<p>изменяемую</p> <p>Виды угроз. Основные нарушения:</p> <ol style="list-style-type: none"> 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). <p>Логической</p> <p>Двоичной</p> <p>Программной</p> <p>Криптографической</p> <p>Шестнадцатеричной</p>
№ 9	<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>

- [3] защищать?

[1] – что / зачем / на какие деньги

[2] – чего (кого) / чего / кого

[3] – как / кем / с чем

№ 10

Ущерб может быть [1] или [2].

[1] – приемлемым, моральным, финансовым, репутационным

[2] - моральным, финансовым, репутационным, неприемлемым