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

УТВЕРЖДАЮ
Декан факультета

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление/специальность подготовки — **45.05.01 Перевод и переводоведение**

Специализация/профиль/программа подготовки — **Специальный перевод**

Уровень высшего образования — **Специалитет**

Форма обучения — **Очная**

Факультет — **Р Международного промышленного менеджмента и коммуникации**

Выпускающая кафедра — **Р7 ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ ЛИНГВИСТИКА**

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	
5	9	3	108	51	34	0	17	57	0	0	57	диф. зач.

Санкт-Петербург
2022г.

ЛИСТ СОГЛАСОВАНИЯ

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

45.05.01 Перевод и переводоведение

год набора группы: 2022

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Бармина Анастасия Александровна, 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

Р7 ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ ЛИНГВИСТИКА

Заведующий кафедрой Невзорова Г.Д., к.ф.н., доц.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-2 — умение использовать в практической деятельности современные высокотехнологичные программные продукты
ОПК-4 — способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий
ОПК-5 — способность понимать принципы работы современных информационных технологий и использовать их при решении задач профессиональной деятельности

Формированию компетенций служит достижение следующих результатов образования:

ПСК-2

знания:

программных и аппаратных средства для защиты информации;;

умения:

использовать специализированное программное обеспечение для защиты информации;;

навыки:

навыками поиска информации;.

ОПК-4

знания:

понятие и сущность информации, формы ее представления;;

умения:

работать со специализированным программным обеспечением;;

навыки:

ориентироваться в современной системе источников информации;.

ОПК-5

знания:

основные методы и средства хранения, поиска, систематизации, обработки и передачи компьютерной информации;;

умения:

использовать современные информационные технологии;;

навыки:

навыками поиска информации в глобальной информационной сети Интернет и работы с базами данных и Интернет-ресурсами;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *45.05.01 Перевод и переводоведение*.

Содержание дисциплины является логическим продолжением дисциплин: **ОСНОВЫ СИСТЕМНОГО АНАЛИЗА, ПРАВОВЕДЕНИЕ**.

Содержание дисциплины является основой для освоения дисциплин: **ПОДГОТОВКА К ПРОЦЕДУРЕ ЗАЩИТЫ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ, НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- УК-1 — Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
- УК-11 — Способен формировать нетерпимое отношение к коррупционному поведению
- УК-6 — Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни

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		ПСК-2	ОПК-4	ОПК-5
5	9	**Раздел 1. Информация как объект защиты.** Понятие информации. Свойства информации. Информационные процессы. Информационные технологии. ИТ в лингвистике. Информационные системы. Информатизация общества. Информационная культура. Понятие информационной безопасности (ИБ). Основные составляющие ИБ. Важность и сложность проблемы ИБ. Актуальность защиты информации. Собственник, владелец и пользователь информации.	9	2	2	0	7	5	5	5
5	9	**Раздел 2. Основные понятия информационной безопасности.** Определение ИБ. Защита информации. Объект защиты. Цель защиты информации. Компьютерная безопасность. Доктрина ИБ РФ. Основные составляющие ИБ: доступность, целостность, конфиденциальность.	10	3	3	0	7	10	10	10
5	9	**Раздел 3. Угрозы ИБ и их классификация.** Угроза. Атака. Источники угроз. Целевая характеристика угроз ИБ. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности. Каналы утечки информации.	10	4	2	2	6	15	15	15
5	9	**Раздел 4. Способы и средства защиты информации.** Способы защиты информации. Средства защиты информации: технические (физические, аппаратные), программные, организационные, законодательные.	14	8	4	4	6	10	10	10
5	9	**Раздел 5. Законодательный уровень ИБ.** Обзор российского законодательства в области ИБ. Правовые акты общего назначения, затрагивающие вопросы ИБ. Закон об информации, информатизации и защите информации. Текущее состояние российского законодательства в области ИБ.	11	5	5	0	6	15	15	15
5	9	**Раздел 6. Вредоносные программы.** Классификация вредоносных программ. Самостоятельная диагностика заражения вредоносными программами.	16	10	6	4	6	15	15	15
5	9	**Раздел 7. Основы функционирования антивирусного программного обеспечения.** Основы функционирования антивирусного программного обеспечения. Задачи антивируса. Технологии, применяемые в антивирусах. Классификация антивирусного программного обеспечения.	19	10	6	4	9	20	20	20
5	9	**Раздел 8. Содержание и основные понятия криптологии и криптографии.** Криптология и криптография. Содержание и основные понятия криптологии и криптографии. Методы криптологии и криптографии.	19	9	6	3	10	10	10	10
Всего за 9 семестр			108	51	34	17	57	100	100	100
Всего по дисциплине			108	51	34	17	57	100	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 3. Угрозы ИБ и их классификация.	Выполнение практической работы №1	2
2	Раздел 4. Способы и средства защиты информации.	Выполнение практической работы №2	4
3	Раздел 6. Вредоносные программы.	Выполнение практической работы №3	4
4	Раздел 7. Основы функционирования антивирусного программного обеспечения.	Основы функционирования антивирусного программного обеспечения.	4
5	Раздел 8. Содержание и основные понятия криптологии и криптографии.	Обсуждение методов криптологии и применении их на практике	3
Всего за 9 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Информация как объект	Изучение предусмотренных программой	7

	защиты.	дидактических единиц по рекомендуемой литературе	
2	Раздел 2. Основные понятия информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	7
3	Раздел 3. Угрозы ИБ и их классификация.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	2
4		Подготовка к практической работе №1, оформление отчета.	4
5	Раздел 4. Способы и средства защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	2
6		Подготовка к практической работе №2, оформление отчета.	4
7	Раздел 5. Законодательный уровень ИБ.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
8	Раздел 6. Вредоносные программы.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	2
9		Подготовка к практической работе №3, оформление отчета.	4
10	Раздел 7. Основы функционирования антивирусного программного обеспечения.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	9
11	Раздел 8. Содержание и основные понятия криптологии и криптографии.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
Всего за 9 семестр			57

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**
9						ДР				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. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
5. Д. А. Мельников. . Информационная безопасность открытых систем. Москва: Флинта, 2014, эл. рес.
6. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.

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://library.voenmeh.ru — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. http://urait.ru — Образовательная платформа «Юрайт». Для вузов и ссузов.;
3. http://www.intuit.ru/department/security/secst — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
4. http://www.intuit.ru/department/security/secbasics — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
5. http://e.lanbook.com/ — ЭБС Лань;;
6. http://urait.ru/ — Образовательная платформа «Юрайт». Для вузов и ссузов.;
7. 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 *45.05.01 Перевод и переводоведение*. Дисциплина реализуется на факультете *О* Естественнонаучный БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:
ПСК-2 умение использовать в практической деятельности современные высокотехнологичные программные продукты;
ОПК-4 способен работать с электронными словарями, различными источниками информации, осуществлять поиск, хранение, обработку и анализ информации, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий;
ОПК-5 способность понимать принципы работы современных информационных технологий и использовать их при решении задач профессиональной деятельности.

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 **(34 ч.)**, практические занятия **(17 ч.)**, самостоятельная работа студента **(57 ч)**.

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 51 ч. аудиторных занятий, и 57 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. Информация как объект защиты.		
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)	7
Итого по разделу 1		7
Раздел 2. Основные понятия информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1-3)	7
Итого по разделу 2		7
Раздел 3. Угрозы ИБ и их классификация.		
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 (4) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (1)	2
Подготовка к практической работе №1, оформление отчета.		4
Итого по разделу 3		6
Раздел 4. Способы и средства защиты 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 (8-9) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (2)	2
Подготовка к практической работе №2, оформление отчета.		4
Итого по разделу 4		6
Раздел 5. Законодательный уровень ИБ.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (1)	6
Итого по разделу 5		6

Раздел 6. Вредоносные программы.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Д. А. Мельников. . Информационная безопасность открытых систем: Москва: Флинта, 2014 (3)	2
Подготовка к практической работе №3, оформление отчета.		4
Итого по разделу 6		6
Раздел 7. Основы функционирования антивирусного программного обеспечения.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (9) А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (8)	9
Итого по разделу 7		9
Раздел 8. Содержание и основные понятия криптологии и криптографии.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (8) 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)	10
Итого по разделу 8		10

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

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

Темы практических заданий указаны в УМК дисциплины.

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

К каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.
ПЗ считается выполненным и защищенным успешно при условии:
- наличия корректного решения поставленной задачи;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

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

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

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

Вопросы к дифференцированному зачету

Вопросы к диф.зачету содержатся в УМК дисциплины.

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

Дифференцированный зачет

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

Перечень теоретических вопросов к диф.зачету, представленный в УМК дисциплины, предоставляется преподавателем. Задачи соответствуют программе практических занятий. При подготовке ответов на

теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы. Особое внимание следует уделить подготовке практических примеров к теоретическим вопросам.

На диф.зачете студенту предлагается два теоретических вопроса. При успешном ответе на оба вопроса выставляется оценка «отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «хорошо» при успешном выполнении всех практических заданий. При отсутствии успешных ответов зачет может быть оформлен с оценкой «удовлетворительно» на основании успешного выполнения предусмотренных рабочей программой практических заданий. При несвоевременном или неполном выполнении практических заданий и при неуспешной сдачи 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	ОПК-4	ОПК-5	
5	9	**Раздел 1. Информация как объект защиты.**	9	2	2	0	7	5	5	5	Вопросы к дифференцированному зачету, Отчет по практическому заданию
5	9	**Раздел 2. Основные понятия информационной безопасности.**	10	3	3	0	7	10	10	10	Вопросы к дифференцированному зачету
5	9	**Раздел 3. Угрозы ИБ и их классификация.**	10	4	2	2	6	15	15	15	Отчет по практическому заданию
5	9	**Раздел 4. Способы и средства защиты информации.**	14	8	4	4	6	10	10	10	Отчет по практическому заданию
5	9	**Раздел 5. Законодательный уровень ИБ.**	11	5	5	0	6	15	15	15	Вопросы к дифференцированному зачету
5	9	**Раздел 6. Вредоносные программы.**	16	10	6	4	6	15	15	15	Вопросы к дифференцированному зачету
5	9	**Раздел 7. Основы функционирования антивирусного программного обеспечения.**	19	10	6	4	9	20	20	20	Вопросы к дифференцированному зачету
5	9	**Раздел 8. Содержание и основные понятия криптологии и криптографии.**	19	9	6	3	10	10	10	10	Вопросы к дифференцированному зачету
Всего за 9 семестр			108	51	34	17	57	100	100	100	
Всего по дисциплине			108	51	34	17	57	100	100	100	