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

_____ Страхов С. Ю.
(подпись) ФИО
«31» 05 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление/специальность подготовки — 09.03.01 Информатика и вычислительная техника

Специализация/профиль/программа подготовки — Автоматизированные системы обработки информации и управления

Уровень высшего образования — Бакалавриат

Форма обучения — Очно-заочная

Факультет — И Информационных и управляющих систем

Выпускающая кафедра — И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра-разработчик рабочей программы — И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

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	
4	8	5	180	51	34	0	17	129	0	0	129	экз.

Санкт-Петербург
2022 г.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.01 Информатика и вычислительная техника

год набора группы: 2022

Программу составил:

Кафедра И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Емельянов Валентин Юрьевич, к.т.н., доцент

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

Заведующий кафедрой Матвеев С.А., к.т.н., доц.

Программа рассмотрена
на заседании выпускающей кафедры

И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Заведующий кафедрой Матвеев С.А., к.т.н., доц.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-2 — способность понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
ОПК-3 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Формированию компетенций служит достижение следующих результатов образования:

ОПК-2

знания:

технологий и программных средств защиты информации;

умения:

применять полученные знания в практике построения защищенных систем;

навыки:

применения, установки и настройки антивирусных систем и систем распознавания угроз и атак.

ОПК-3

знания:

основных принципов административно-правовой, программной и технической защиты информации;

умения:

быстро реагировать на различные угрозы информационной безопасности, применять современные технологии защиты информации;

навыки:

обнаружения компьютерных вирусов различными способами и применения методов борьбы с вирусами различной природы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*.

Содержание дисциплины является логическим продолжением дисциплин: **БАЗЫ ДАННЫХ, ИНФОРМАТИКА: ОСНОВЫ ПРОГРАММИРОВАНИЯ, ДИСКРЕТНАЯ МАТЕМАТИКА И МАТЕМАТИЧЕСКАЯ ЛОГИКА**.

Содержание дисциплины является основой для освоения дисциплин: **ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ, ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
- 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-8 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения
- ОПК-9 — Способен осваивать методики использования программных средств для решения практических задач
- 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-1.2 — Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности

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		ОПК-2	ОПК-3
4	8	**Раздел 1. Основные составляющие информационной безопасности.** 1.1. Основные понятия информационной безопасности. 1.2. Классификация угроз. 1.3. Классификация средств защиты информации. 1.4. Методы и средства организационно-правовой защиты информации. 1.5. Методы и средства инженерно-технической защиты. 1.6. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.	14	4	4	0	10	10	20
4	8	**Раздел 2. Правовое обеспечение информационной безопасности.** 2.1. Информация, информационные технологии и защита информации. 2.2. Безопасность персональных данных. 2.3. Результаты интеллектуальной деятельности. Авторское право. 2.4. Право промышленной собственности. Коммерческая тайна и правовой режим обеспечения ее безопасности. 2.5. Государственная тайна и ее правовая защита. 2.6. Электронная подпись и правовое обеспечение безопасности переписки. 2.7. Правовое обеспечение безопасности при использовании сетей связи. 2.8. Характеристика и последствия преступлений в сфере информационной безопасности.	22	6	6	0	16	0	20
4	8	**Раздел 3. Организационное обеспечение информационной безопасности.** 3.1. Государственная система обеспечения информационной безопасности. 3.2. Организация работ по защите конфиденциальной информации. Лицензирование.	10	2	2	0	8	0	5
4	8	**Раздел 4. Защита информации в современных информационных системах.** 4.1. Способы контактного и бесконтактного съема информации. 4.2. Возможности атаки на ОС, их классификация. 4.3. Парольная защита ПК. Взлом паролей Windows NT и UNIX. Защита от взлома. 4.4.Идентификация и аутентификация пользователей ОС. Windows, UNIX, Linux. 4.5. Формальные модели защищаемых систем и их применение в современных ОС. 4.6. Методы и средства ограничения доступа к ресурсам и компонентам ПК.	58	18	10	8	40	45	25
4	8	**Раздел 5. Защита информации в компьютерных сетях.** 5.1. Основные угрозы безопасности сетей. Модели угроз и модели противодействия. 5.2. Методы аутентификации пользователей в сети. 5.3. Разновидности вирусных программ. 5.4. Программные средства защиты: сканеры вирусов, сетевая защита, брандмауэры и др. 5.5. Системы обнаружения сетевого вторжения. 5.6. Безопасность глобальных сетей и электронной почты.	76	21	12	9	55	45	30
Всего за 8 семестр			180	51	34	17	129	100	100
Всего по дисциплине			180	51	34	17	129	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 4. Защита информации в современных информационных системах.	Разработка защищенных приложений. Программное управление учетной записью.	2
2		Управление правами пользователей.	3
3		Применение механизмов разграничения доступа пользователей.	3
4	Раздел 5. Защита информации в компьютерных сетях.	Моделирование атак в сети и способов их нейтрализации	6
5		Динамическая маршрутизация	3
Всего за 8 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Основные составляющие информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
2	Раздел 2. Правовое обеспечение информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	16

3	Раздел 3. Организационное обеспечение информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	8
4	Раздел 4. Защита информации в современных информационных системах.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	24
5		Подготовка к выполнению практических заданий и оформление отчетов	16
6	Раздел 5. Защита информации в компьютерных сетях.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	37
7		Подготовка к выполнению практических заданий и оформление отчетов	18
Всего за 8 семестр			129

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	**НЕДЕЛИ СЕМЕСТРА**												
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
8				Отч. по ПЗ		ДР		Отч. по ПЗ		ДР			Отч. по ПЗ

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Тест – тест.

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

- диагностическая работа;
- отчет по практическому заданию;
- тест.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, эл. рес.
2. А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, 30 экз.
3. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
4. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
5. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
6. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
7. М. В. Тумбинская, М. В. Петровский. . Комплексное обеспечение информационной безопасности на предприятии. СПб.: Лань, 2019, эл. рес.
8. С. А. Нестеров. . Основы информационной безопасности. СПб.: Лань, 2019, 22 экз.
9. С. А. Нестеров. . Основы информационной безопасности. СПб.: Лань, 2019, эл. рес.

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. http://library.voenmeh.ru/jirbis2 — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. https://urait.ru — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
3. http://e.lanbook.com — ЭБС Лань.

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. Microsoft SQL Server 2005 Express Edition;
2. Microsoft Windows.

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. Аудитория с числом посадочных мест не меньше количества обучающихся;
3. Microsoft SQL Server 2005 Express Edition;
4. Microsoft Windows.

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 **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.01 Информатика и вычислительная техника*. Дисциплина реализуется на факультете *И* Информационных и управляющих систем БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой И9 СИСТЕМ УПРАВЛЕНИЯ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ.

Дисциплина нацелена на формирование *компетенций*:
ОПК-2 способность понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;
ОПК-3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями и составляющими информационной безопасности, видами угроз и комплексом мер по их нейтрализации.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:
- диагностическая работа;
- отчет по практическому заданию;
- тест.

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 **(17 ч.)**, самостоятельная работа студента **(129 ч)**.

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 180 ч., из них 51 ч. аудиторных занятий, и 129 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. Основные составляющие информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (глава 1) С. А. Нестеров. . Основы информационной безопасности: СПб.: Лань, 2019 (парагр. 1.1-1.3) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (глава 1) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (раздел 1)	10
Итого по разделу 1		10
Раздел 2. Правовое обеспечение информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (главы 2-3) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (главы 2,4-15)	16
Итого по разделу 2		16
Раздел 3. Организационное обеспечение информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (главы 3,16-18) М. В. Тумбинская, М. В. Петровский. . Комплексное обеспечение информационной безопасности на предприятии: СПб.: Лань, 2019 (глава 1.1)	8
Итого по разделу 3		8
Раздел 4. Защита информации в современных информационных системах.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. А. Нестеров. . Основы информационной безопасности: СПб.: Лань, 2019 (парагр. 1.4-1.5) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (разделы 2-6) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (глава 9) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. .	24
Подготовка к выполнению практических заданий и оформление отчетов		16

	Информационная безопасность: М.: РУСАЙНС, 2017 (глава 4)	
Итого по разделу 4		40
Раздел 5. Защита информации в компьютерных сетях.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (глава 20) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (разделы 7-9,11) С. А. Нестеров. . Основы информационной безопасности: СПб.: Лань, 2019 (главы 4,5)	37
Подготовка к выполнению практических заданий и оформление отчетов		18
Итого по разделу 5		55

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- тест;
- отчет по практическому заданию;
- экзамен.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

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

Тест

Тест включает в себя 20 вопросов. Требуется выбирать один правильный ответ из предложенных. Время выполнения 40 минут.
Успешное прохождение теста регистрируется при условии получения не менее 12 правильных ответов.
Оценка "хорошо" - не менее 15 правильных ответов.
Оценка "отлично" - не менее 18 правильных ответов.
Комплект тестовых вопросов включен в состав УМК дисциплины.

Отчет по практическому заданию

Требования к выполнению практических заданий (ПЗ):
По всем ПЗ необходимо выполнить поставленную задачу согласно заданию, а также внимательно прочитать сопутствующую информацию о программном обеспечении, в котором осуществляется работа.
Отчет по ПЗ:
По каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При оформлении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.
Защита ПЗ:
Защита ПЗ предусматривает обсуждение порядка решения предусмотренных его тематикой задач, включая проверку усвоения студентом соответствующих сведений из теории.
Типовые практические задания включены в состав УМК дисциплины.

Экзамен

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.
Итоговый контроль по дисциплине проходит в форме экзамена. Допуск к экзамену оформляется при условии полного выполнения всех мероприятий, предусмотренных графиком контрольных мероприятий. Экзаменационный билет включает в себя два теоретических вопроса.
Комплект вопросов к экзамену размещен в УМК дисциплины
По желанию студент может сдавать экзамен в форме теста.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %		НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-2	ОПК-3	
4	8	**Раздел 1. Основные составляющие информационной безопасности.**	14	4	4	0	10	10	20	Тест
4	8	**Раздел 2. Правовое обеспечение информационной безопасности.**	22	6	6	0	16	0	20	Тест
4	8	**Раздел 3. Организационное обеспечение информационной безопасности.**	10	2	2	0	8	0	5	Тест
4	8	**Раздел 4. Защита информации в современных информационных системах.**	58	18	10	8	40	45	25	Отчет по практическому заданию, Тест
4	8	**Раздел 5. Защита информации в компьютерных сетях.**	76	21	12	9	55	45	30	Отчет по практическому заданию, Тест
Всего за 8 семестр			180	51	34	17	129	100	100	
Всего по дисциплине			180	51	34	17	129	100	100	