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

Шматко А. Д.
(подпись) ФИО
«31» 05 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление/специальность подготовки — **38.03.05 Бизнес-информатика**

Специализация/профиль/программа подготовки — **Управление технологиями искусственного интеллекта**

Уровень высшего образования — **Бакалавриат**

Форма обучения — **Очно-заочная**

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

Выпускающая кафедра — **Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ**

Кафедра-разработчик рабочей программы — **Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ**

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	4	144	51	17	0	34	93	0	0	93	экз.

Санкт-Петербург
2022г.

13237

ЛИСТ СОГЛАСОВАНИЯ

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

38.03.05 Бизнес-информатика

год набора группы: 2022

Программу составил:

Кафедра Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ
Глинкин Андрей Сергеевич, старший преподаватель

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ**

Заведующий кафедрой Шматко А.Д., д.э.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ

Заведующий кафедрой Шматко А.Д., д.э.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-6 — способность управлять информационной безопасностью ресурсов информационных технологий
УК-11 — способность формировать нетерпимое отношение к коррупционному поведению

Формированию компетенций служит достижение следующих результатов образования:

ПСК-6

знания:

Знать свойства и признаки информации, особенности информационно аналитических систем; основные информационные процессы, источники и каналы утечки информации на защищаемых объектах; основы построения систем обработки и передачи информации, их современное состояние развития;

умения:

Уметь анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа; воспроизводить и корректно использовать основные понятия, связанные с обработкой информации, в том числе и с помощью персонального компьютера;

навыки:

Владеть навыками использования информационных технологий для обработки и поиска информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации; осуществления поиска наиболее эффективных путей обработки информации и (или) ее управления; практического восприятия информации.

УК-11

знания:

Знать структуру современного общества; основные социокультурные закономерности и особенности межкультурных взаимодействий;

умения:

Уметь выстраивать социальные взаимодействия с учетом этнокультурных и конфессиональных различий; последовательно и грамотно формулировать и высказывать свои мысли;

навыки:

Владеть основами культуры современного общества, историческим методом и применять его к анализу социокультурных явлений; нормами взаимодействия и сотрудничества, социальной мобильностью.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** является дисциплиной **части, формируемой участниками образовательных отношений блока 1,** программы подготовки по направлению *38.03.05 Бизнес-информатика*.

Содержание дисциплины является логическим продолжением дисциплин: **ВВЕДЕНИЕ В ПРОФЕССИОНАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ**.

Содержание дисциплины является основой для освоения дисциплин: **ПОДГОТОВКА К ПРОЦЕДУРЕ ЗАЩИТЫ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- УК-6 — Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни
- УК-9 — Способен использовать базовые дефектологические знания в социальной и профессиональной сферах

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-6	УК-11
5	9	**Раздел 1. Информационная безопасность в системе национальной безопасности.** Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности.	24	9	4	5	15	20	20
5	9	**Раздел 2. Информационные уязвимости объектов.** Антропогенные информационные уязвимости. Техно-генные информационные уязвимости. Организационно-правовые и комбинированные информационные уязвимости.	30	13	4	9	17	20	20
5	9	**Раздел 3. Угрозы информационной безопасности и их источники.** Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности.	31	11	3	8	20	20	20
5	9	**Раздел 4. Средства обеспечения информационной безопасности.** Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стегано-графические средства обеспечения информационной безопасности. Пассивные и активные средства противодействия техническим разведкам. Защита информации от утечки по техническим каналам.	32	11	3	8	21	20	20
5	9	**Раздел 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации.** Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.	27	7	3	4	20	20	20
Всего за 9 семестр			144	51	17	34	93	100	100
Всего по дисциплине			144	51	17	34	93	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Информационная безопасность в системе национальной безопасности.	Практическое занятие №1: Виды национальной безопасности и их краткая характеристика	5
2	Раздел 2. Информационные уязвимости объектов.	Практическое занятие №2: Антропогенные информационные уязвимости. Практическое занятие №3: Техногенные информационные уязвимости. Практическое занятие №4: Организационно-правовые и комбинированные информационные уязвимости	9
3	Раздел 3. Угрозы информационной безопасности и их источники.	Практическое занятие №5: Угрозы конфиденциальности, целостности и доступности информации. Практическое занятие №6: Информационная война как высшая форма угрозы информационной безопасности.	8
4	Раздел 4. Средства обеспечения информационной безопасности.	Практическое занятие №7: Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Практическое занятие №8: Защита информации от утечки по техническим каналам.	8
5	Раздел 5. Риски информационной безопасности и проблема	Практическое занятие №9: Оценка рисков и организация управления процессом защиты информации	4

	построения комплексной системы защиты информации.		
Всего за 9 семестр			34

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Информационная безопасность в системе национальной безопасности.	Изучение основной и дополнительной литературы по вопросам раздела 1 Подготовка к самостоятельной работе Выбор темы реферата и подбор литературы по теме реферата, сбор статистических данных по теме реферата	15
2	Раздел 2. Информационные уязвимости объектов.	Изучение основной и дополнительной литературы по вопросам раздела 2. Подготовка к самостоятельной работе Обработка и анализ статистических данных по теме реферата. Написание и оформление реферата. Подготовка презентации по проведенному исследованию	17
3	Раздел 3. Угрозы информационной безопасности и их источники.	Изучение основной и дополнительной литературы по вопросам раздела 3. Подготовка к самостоятельной работе Обработка и анализ статистических данных по теме реферата. Написание и оформление реферата. Подготовка презентации по проведенному исследованию. Защита реферата.	20
4	Раздел 4. Средства обеспечения информационной безопасности.	Изучение основной и дополнительной литературы по вопросам раздела 4. Подготовка к самостоятельной работе Подготовка к экзамену.	21
5	Раздел 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации.	Изучение основной и дополнительной литературы по вопросам раздела 5. Подготовка к самостоятельной работе Подготовка к экзамену. Сдача экзамена	20
Всего за 9 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
9						ДР		Реф		ДР						ДР	Вопр. Экз

Условные обозначения:
- ДР – диагностическая работа;
- Реф – реферат;
- Вопр. Экз – вопросы к экзамену.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:
- диагностическая работа;
- реферат;
- вопросы к экзамену.

Промежуточная аттестация проводится в формах:
- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. . Информационные системы и технологии в экономике и управлении. Москва: Юрайт, 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, эл. рес.
3. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.
4. Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности. Москва: Юрайт, 2020, 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:

не требуется.

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:

не требуется.

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.

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** является дисциплиной **части, формируемой участниками образовательных отношений блока 1,** программы подготовки по направлению *38.03.05 Бизнес-информатика*. Дисциплина реализуется на факультете *Р* Международного промышленного менеджмента и коммуникации БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой Р1 МЕНЕДЖМЕНТ ОРГАНИЗАЦИИ.

Дисциплина нацелена на формирование *компетенций*:
ПСК-6 способность управлять информационной безопасностью ресурсов информационных технологий;
УК-11 способность формировать нетерпимое отношение к коррупционному поведению.

Содержание дисциплины охватывает круг вопросов, связанных с местом и ролью информационной безопасности в системе национальной безопасности Российской Федерации; основными нормативными правовыми актами в области информационной безопасности и защиты информации; техническими каналами утечки информации; принципами и методами противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:
- диагностическая работа;
- реферат;
- вопросы к экзамену.

Промежуточная аттестация проводится в формах:
- экзамен.

Общая трудоемкость освоения дисциплины составляет **4** з.е., **144** ч. Программой дисциплины предусмотрены лекционные занятия **(17 ч.)**, практические занятия **(34 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. Информационная безопасность в системе национальной безопасности.		
Изучение основной и дополнительной литературы по вопросам раздела 1 Подготовка к самостоятельной работе Выбор темы реферата и подбор литературы по теме реферата, сбор статистических данных по теме реферата	. Информационные системы и технологии в экономике и управлении: Москва: Юрайт, 2018 (1-7)	15
Итого по разделу 1		15
Раздел 2. Информационные уязвимости объектов.		
Изучение основной и дополнительной литературы по вопросам раздела 2. Подготовка к самостоятельной работе Обработка и анализ статистических данных по теме реферата. Написание и оформление реферата. Подготовка презентации по проведенному исследованию	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (1-5)	17
Итого по разделу 2		17
Раздел 3. Угрозы информационной безопасности и их источники.		
Изучение основной и дополнительной литературы по вопросам раздела 3. Подготовка к самостоятельной работе Обработка и анализ статистических данных по теме реферата. Написание и оформление реферата. Подготовка презентации по проведенному исследованию. Защита реферата.	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (5-10)	20
Итого по разделу 3		20
Раздел 4. Средства обеспечения информационной безопасности.		
Изучение основной и дополнительной литературы по вопросам раздела 4. Подготовка к самостоятельной работе Подготовка к экзамену.	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (7-10)	21
Итого по разделу 4		21
Раздел 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации.		
Изучение основной и дополнительной литературы по вопросам раздела 5. Подготовка к самостоятельной работе Подготовка к экзамену. Сдача экзамена	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (10-13)	20
Итого по разделу 5		20

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- вопросы к экзамену;
- реферат;
- 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.

Вопросы к экзамену

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информа-ции.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информа-ции.
18. Программно-аппаратные средства обеспечения информацион-ной безопасности в ин-формационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Реферат

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сиг-налов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов,

соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих струк-тур, имеющих доступ к интересующей информации.
18. Способы наблюдения с использованием технических средств.
19. Каналы утечки информации. Технические каналы утечки
20. Классификация технических каналов утечки по физической природе носителя.
21. Классификация технических каналов утечки по информативности.
22. Классификация технических каналов утечки по времени функционирования.
23. Классификация технических каналов утечки по структуре.
24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
25. Перехват электромагнитных излучений.
26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
27. Понятия скрытия информации, виды скрытий. Информационный портрет.
28. Противодействие наблюдению. Способы маскировки.
29. Способы и средства противодействия подслушиванию.
30. Нейтрализация закладных устройств.
31. Состав инженерной защиты и технической охраны объектов.
32. Инженерные конструкции и сооружения для защиты информации. Их классификация.
33. Средства идентификации личности.
34. Классификация датчиков охранной сигнализации.
35. Классификация извещателей.
36. Телевизионные системы наблюдения.
37. Основные средства системы видеоконтроля.
38. Защита личности как носителя информации.
39. Системный подход к защите информации.
40. Параметры системы защиты информации.
41. этапы проектирования системы защиты информации.
42. Потенциальные каналы утечки информации.
43. Этапы разработки мер по предотвращению угроз утечки информации.

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.
оценка ОТЛИЧНО – студент свободно, достаточно подробно излагает материал, демонстрирует понимание процессов по всем вопросам, пользуется специальной профессио-нальной терминологией;
оценка ХОРОШО – студент, в целом, владеет материалом, но недостаточно полно и уверенно демонстрирует понимание процессов по вопросам, редко пользуется профессио-нальными терминами;
оценка УДОВЛЕТВОРИТЕЛЬНО – студент слабо владеет материалом, с трудом понимает процессы по вопросам, специальной профессиональной терминологией практически не пользуется.
оценка НЕУДОВЛЕТВОРИТЕЛЬНО – студент не в состоянии изложить материал и выразить понимание процессов по вопросам.

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-6	УК-11	
5	9	**Раздел 1. Информационная безопасность в системе национальной безопасности.**	24	9	4	5	15	20	20	Вопросы к экзамену
5	9	**Раздел 2. Информационные уязвимости объектов.**	30	13	4	9	17	20	20	Вопросы к экзамену
5	9	**Раздел 3. Угрозы информационной безопасности и их источники.**	31	11	3	8	20	20	20	Реферат
5	9	**Раздел 4. Средства обеспечения информационной безопасности.**	32	11	3	8	21	20	20	Вопросы к экзамену
5	9	**Раздел 5. Риски информационной безопасности и проблема построения комплексной системы защиты информации.**	27	7	3	4	20	20	20	Вопросы к экзамену
Всего за 9 семестр			144	51	17	34	93	100	100	
Всего по дисциплине			144	51	17	34	93	100	100	