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 ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление/специальность подготовки — 09.03.02 Информационные системы и технологии

Специализация/профиль/программа подготовки — Информационная безопасность

Уровень высшего образования — Бакалавриат

Форма обучения — Очная

Факультет — О Естественнонаучный

Выпускающая кафедра — О7 Информационные системы и программная инженерия

Кафедра-разработчик рабочей программы — О7 Информационные системы и программная инженерия

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
3	5	4	144	34	17	0	17	110	0	0	110	диф. зач.

Санкт-Петербург
2022 г.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.02 Информационные системы и технологии

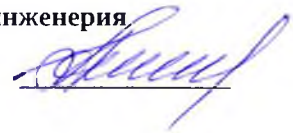
год набора группы: 2022

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

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

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
УК-2 — способность определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ПСК-2.14 — Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности
ПСК-2.17 — Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
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:

ОПК-3

знания:

знать основы организационной и правовой защиты информации, ее современные проблемы и терминологию;

умения:

умение использовать специализированную терминологию;

навыки:

навык использования нормативных документов в профессиональной деятельности.

УК-2

знания:

изучить руководящие документы по обеспечению режима секретности и конфиденциальности на объекте;

умения:

использовать руководящие документы по обеспечению режима секретности и конфиденциальности на объекте;

навыки:

обеспечения режима секретности и конфиденциальности на объекте.

ПСК-2.14

знания:

изучить руководящие документы по обеспечению режима секретности и конфиденциальности на объекте;

умения:

оценивать состояние организационной защиты информации на объекте;

навыки:

обеспечения режима секретности и конфиденциальности на объекте.

ПСК-2.17

знания:

получить базовые представления о типовой структуре службы безопасности, ее основные задачи и функции должностных лиц;

умения:

определять рациональные меры по обеспечению организационной и правовой защиты на объекте;

навыки:

иметь навыки выявления угроз информационной безопасности объекта.

ПСК-2.18

знания:

знать основные документы, регламентирующую организационную безопасность на объекте;

умения:

оценивать состояние организационной защиты информации на объекте;

навыки:

иметь навыки выявления угроз информационной безопасности объекта.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ПРАВОВЕДЕНИЕ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**.

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

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- 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-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- УК-10 — Способен формировать нетерпимое отношение к коррупционному поведению
- УК-2 — Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

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		ОПК-3	УК-2	ПСК-2.14	ПСК-2.17	ПСК-2.18
3	5	**Раздел 1. Правовые основы защиты информации.** 1.1 Органы законодательства, регламентирующие деятельность по информационной безопасности. 1.2 Структура органов власти по защите информации в Российской Федерации. 1.3 Совет Безопасности Российской Федерации. 1.4 Межведомственные и государственные комиссии. 1.5 Федеральная служба безопасности Российской Федерации (ФСБ). 1.6 Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). 1.7 Комитет по вопросам информационной безопасности. 1.8 Понятия и виды защищаемой информации по российскому законодательству. 1.9 Организация службы безопасности на предприятии.	18	3	3	0	15	10	10	10	10	10
3	5	**Раздел 2. Режим защиты государственной тайны.** 2.1 Степени секретности сведений и грифы секретности носителей этих сведений. 2.2 Органы защиты государственной тайны. 2.3 Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. 2.4 Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. 2.5 Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.	17	2	2	0	15	10	10	10	10	10
3	5	**Раздел 3. Защита персональных данных.** 3.1 Регуляторы в области защиты ПДн. 3.2 Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных. 3.3 Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. 3.4 Требования к защите персональных данных. 3.5 Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных. 3.6 Базовая модель угроз безопасности персональных данных. 3.7 Методика определения актуальных угроз безопасности персональных данных. 3.8 Обеспечение с помощью криптосредств безопасности персональных данных.	21	6	3	3	15	20	20	20	20	20
3	5	**Раздел 4. Защита критической информационной инфраструктуры.** 4.1 Основные направления госполитики в области обеспечения безопасности. 4.2 Обеспечение безопасности КИИ РФ. 4.3 Категорирование объектов КИИ РФ и перечня показателей критериев значимости объектов КИИ РФ и их значений. 4.4 Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. 4.5 Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования.	21	6	2	4	15	15	15	15	15	15
3	5	**Раздел 5. Режим защиты государственных информационных систем.** 5.1 Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем. 5.2 Создание и функционирование системы защиты информации. 5.3 Стадии и этапы создания системы защиты государственных информационных систем. 5.4 Внедрение системы защиты информации. 5.5 Аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие. 5.6 Сопровождение системы защиты информации в ходе эксплуатации объекта информатизации. 5.7 Разработка эксплуатационной документации на систему защиты информации.	18	3	3	0	15	20	20	20	20	20
3	5	**Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации.** 6.1 Лицензирование и система сертификации средств защиты информации 6.2 Организационно-	22	7	2	5	15	15	15	15	15	15

		правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. 6.3 Организационная структура системы аттестации объектов информатизации. 6.4 Цели и виды аттестации объектов информатизации. Участники аттестации и их полномочия. Задачи, функции права и обязанности органов по аттестации. 6.5 Организационно-правовые основы лицензирования деятельности по защите информации. 6.6 Лицензирование деятельности технической и криптографической защите информации. 6.7 Порядок и методы проведения сертификационных испытаний. 6.8 Особенности сертификации средств защиты информации от утечки по техническим каналам. 6.9 Особенности сертификации средств защиты информации от НСД.										
3	5	**Раздел 7. Ответственность за правонарушения в области информационной безопасности.** 7.1 Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. 7.2 Меры дисциплинарной ответственности. 7.3 Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. 7.4 Уголовная ответственность за правонарушения в области конфиденциальной информации.	27	7	2	5	20	10	10	10	10	10
Всего за 5 семестр			144	34	17	17	110	100	100	100	100	100
Всего по дисциплине			144	34	17	17	110	100	100	100	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 3. Защита персональных данных.	Практическая работа №1	3
2	Раздел 4. Защита критической информационной инфраструктуры.	Практическая работа №2	4
3	Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации.	Практическая работа №3	5
4	Раздел 7. Ответственность за правонарушения в области информационной безопасности.	Практическая работа №4	5
Всего за 5 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Правовые основы защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	15
2	Раздел 2. Режим защиты государственной тайны.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	15
3	Раздел 3. Защита персональных данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	11
4		Подготовка к практической работе №1 и оформление отчета.	4
5	Раздел 4. Защита критической информационной инфраструктуры.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	11
6		Подготовка к практической работе №2 и оформление отчета.	4
7	Раздел 5. Режим защиты государственных информационных систем.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	15
8	Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	11

9		Подготовка к практической работе №3 и оформление отчета	4
10	Раздел 7. Ответственность за правонарушения в области информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	14
11		Подготовка к практической работе №4 и оформление отчета	6
Всего за 5 семестр			110

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	**НЕДЕЛИ СЕМЕСТРА**																
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
5						ДР		Отч. по ПЗ		ДР		Отч. по ПЗ				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. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности. М.: Изд-во МГТУ им. Н. Э. Баумана, 2018, 30 экз.
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. А. К. Жарова. . Защита интеллектуальной собственности. Москва: Юрайт, 2021, эл. рес.
4. В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2003, 70 экз.
5. Н. П. Попова, А. П. Дмитриева. . Защита интеллектуальной собственности. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 39 экз.
6. Н. П. Попова, А. П. Дмитриева. . Защита интеллектуальной собственности. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
7. Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности. Москва: Юрайт, 2020, эл. рес.
8. Я. М. Радкевич, А. Г. Схиртладзе. Метрология, стандартизация и сертификация. Ч. 3 Сертификация. Москва: Юрайт, 2022, эл. рес.

5.2. Дополнительная литература по дисциплине:

1. В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации. М.: Форум, 2009, 2 экз.

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. http://library.voenmeh.ru — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
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»; 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 **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О* Естественнонаучный БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:
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;
УК-2 способность определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений;
ПСК-2.14 Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности;
ПСК-2.17 Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
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 правовыми аспектами информационной безопасности, нормативными актами и положениями Российской Федерации в отношении информационной безопасности, обеспечением режимов секретности в организациях.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

Промежуточная аттестация проводится в формах:
- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **4** з.е., **144** ч. Программой дисциплины предусмотрены лекционные занятия **(17 ч.)**, практические занятия **(17 ч.)**, самостоятельная работа студента **(110 ч)**.

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 34 ч. аудиторных занятий, и 110 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. Правовые основы защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. К. Жарова. . Защита интеллектуальной собственности: Москва: Юрайт, 2021 (1) Н. П. Попова, А. П. Дмитриева. . Защита интеллектуальной собственности: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (1) Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (1)	15
Итого по разделу 1		15
Раздел 2. Режим защиты государственной тайны.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Н. П. Попова, А. П. Дмитриева. . Защита интеллектуальной собственности: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1-2) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (4) Н. П. Попова, А. П. Дмитриева. . Защита интеллектуальной собственности: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1-2) Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (2) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (2) П. Н. Девянин, О. О. Михальский, Д. И. Правиков. . Теоретические основы компьютерной безопасности: М.: Радио и связь, 2000 (2)	15
Итого по разделу 2		15
Раздел 3. Защита персональных данных.		
Изучение предусмотренных программой дидактических	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020	11

единиц по рекомендуемой литературе	(3) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (3) В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий: СПб.: БХВ-Петербург, 2003 (1-3) П. Н. Девянин, О. О. Михальский, Д. И. Правиков. . Теоретические основы компьютерной безопасности: М.: Радио и связь, 2000 (3)	
Подготовка к практической работе №1 и оформление отчета.		4
Итого по разделу 3		15
Раздел 4. Защита критической информационной инфраструктуры.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (4) В. Зима, А. Молдовян, Н. Молдовян. . Безопасность глобальных сетевых технологий: СПб.: БХВ-Петербург, 2003 (4) П. Н. Девянин, О. О. Михальский, Д. И. Правиков. . Теоретические основы компьютерной безопасности: М.: Радио и связь, 2000 (4) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (4)	11
Подготовка к практической работе №2 и оформление отчета.		4
Итого по разделу 4		15
Раздел 5. Режим защиты государственных информационных систем.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (3) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (4-5) Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (4-5)	15
Итого по разделу 5		15
Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Я. М. Радкевич, А. Г. Схиртладзе. Метрология, стандартизация и сертификация. Ч. 3 Сертификация: Москва: Юрайт, 2022 (1-3) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (2-4) В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (3)	11
Подготовка к практической работе №3 и оформление отчета	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова. . Организационное и правовое обеспечение информационной безопасности: Москва: Юрайт, 2020 (2-4) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (5)	4
Итого по разделу 6		15
Раздел 7. Ответственность за правонарушения в области информационной безопасности.		
Изучение предусмотренных	А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. .	14

программой дидактических единиц по рекомендуемой литературе	Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (5-6)	
Подготовка к практической работе №4 и оформление отчета	Я. М. Радкевич, А. Г. Схиртладзе. Метрология, стандартизация и сертификация. Ч. 3 Сертификация: Москва: Юрайт, 2022 (5) А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев. . Организационно-правовое обеспечение информационной безопасности: М.: Изд-во МГТУ им. Н. Э. Баумана, 2018 (5-6) В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (5) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (3-5)	6
Итого по разделу 7		20

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

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

ПР считается выполненным и защищенным успешно при условии:
- наличие корректно решенной задачи;
- наличия отчета;
- защиты ПР по комплекту тестовых вопросов для защиты ПР, размещенного в УМК дисциплины.

Критерии оценивания:
- соответствие решения указанным требованиям, его 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 – 3 балла.

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

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

Вопросы к дифференцированному зачету

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

Дифференцированный зачет

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.

На 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 зачета 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		ОПК-3	УК-2	ПСК-2.14	ПСК-2.17	ПСК-2.18	
3	5	**Раздел 1. Правовые основы защиты информации.**	18	3	3	0	15	10	10	10	10	10	Отчет по практическому заданию
3	5	**Раздел 2. Режим защиты государственной тайны.**	17	2	2	0	15	10	10	10	10	10	Отчет по практическому заданию
3	5	**Раздел 3. Защита персональных данных.**	21	6	3	3	15	20	20	20	20	20	Отчет по практическому заданию
3	5	**Раздел 4. Защита критической информационной инфраструктуры.**	21	6	2	4	15	15	15	15	15	15	Отчет по практическому заданию
3	5	**Раздел 5. Режим защиты государственных информационных систем.**	18	3	3	0	15	20	20	20	20	20	Отчет по практическому заданию
3	5	**Раздел 6. Аттестация объектов информатизации по требованиям безопасности информации.**	22	7	2	5	15	15	15	15	15	15	Отчет по практическому заданию
3	5	**Раздел 7. Ответственность за правонарушения в области информационной безопасности.**	27	7	2	5	20	10	10	10	10	10	Отчет по практическому заданию, Вопросы к дифференцированному зачету
Всего за 5 семестр			144	34	17	17	110	100	100	100	100	100	
Всего по дисциплине			144	34	17	17	110	100	100	100	100	100	