МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Организационное и правовое обеспечение информационной безопасности»

Направление подготовки – 10.03.01 «Информационная безопасность»
Направленность (профиль) – «Техническая защита информации»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих подкомпетенций:

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5. ОиПОИБ. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	**Знания:** нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности. **Умения:** применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации при разработка организационно-распорядительных по защите информации в организации. **Опыт практической деятельности:** по разработке проектов документов для получения лицензий в области технической защиты информации.
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6. ОиПОИБ Способен использовать нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при организации защиты информации ограниченного доступа	**Знания:** нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы защите информации ограниченного доступа. **Умения:** применять нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при разработке органи-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		зационно-распорядительных документов по защите информации ограниченного доступа. **Опыт практической деятельности:** по разработке проектов документов для получения лицензий в области технической защиты информации.

В результате изучения дисциплины студент должен:

Знать:

- иерархию, сущность и содержание основных нормативных правовых актов в области информационной безопасности (защиты информации);
- понятия (термины) и определения в области обеспечения информационной безопасности (защиты информации) в Российской Федерации и модель правовой защиты информации;
- государственную систему защиты информации в Российской Федерации, направления, полномочия, задачи, функции обязанности и права федеральных органов исполнительной власти в области защиты информации;
- правовые основы обеспечения информационной безопасности (защиты информации), том числе правовые основы защиты государственной тайны и конфиденциальной информации.
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;
- государственную систему лицензирования и сертификации в области защиты информации. Правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- организационные основы обеспечения информационной безопасности (защиты информации) в государственных и коммерческих организациях, принципы и методы организационной защиты информации;
- основы организации и обеспечения режима конфиденциальности (секретности) информации;
- ответственность за нарушение законодательства в области обеспечения информационной безопасности (защиты информации).

- основы государственного контроля (надзора) и аудита в области обеспечения информационной безопасности (защиты информации).

Уметь:

- применять нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при разработке организационных документов по защите информации ограниченного доступа.

Иметь опыт практической деятельности:

- по разработке проектов документов для получения лицензий в области технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и читается на 2 курсе в 4-м семестре.

Изучение дисциплины базируется на дисциплинах основной образовательной подготовки бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Техническая защита информации»: «Правоведение» и «Основы информационной безопасности».

Знания и практические навыки, полученные в результате изучения дисциплины, используются в дисциплинах «Основы управления информационной безопасностью», а также при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
2	4	5	180	80	32	-	32	16	64	Экз. (36), КР

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. Правовое обеспечение информационной безопасности	20	-	16	8	38	Компьютерный тест КТ- 1. Сдача КР
2. Организационное обеспечение информационной безопасности	12	-	16	8	26	Зачет по ПЗ (ГУ) № 5 – 7. Компьютерный тест КТ-2.

4.1. Лекционные занятия

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
1	1	2	**Информация – как объект защиты.** Определение информации. Виды информации. Носители информации. Классификация защищаемой информации. Общедоступная информация. Понятие «тайна информации». Информация ограниченного доступа (гос. тайна, конфиденциальная информация). Информация как объект права собственности.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	2	2	**Содержание правового обеспечения информационной безопасности** Сущность основных понятий в области обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ). Предмет, субъект, методы информационного права, информационные отношения. Функции и принципы правового регулирования в информационной области.
	3	2	**Система нормативных правовых актов Российской Федерации по обеспечению информационной безопасности** Иерархия нормативных правовых актов в области ИБ. Федеральные законы и Указы Президента Российской Федерации в области ИБ и ЗИ. Постановления Правительства Российской Федерации в области ИБ и ЗИ. Приказы и НМД ФСБ России, ФСТЭК России и Роскомнадзора в области ИБ и ЗИ.
	4	2	**Государственная система обеспечения ИБ и ЗИ в Российской Федерации.** Структура органов государственного управления в области обеспечения ИБ и ЗИ Полномочия, права и обязанности Президента Российской Федерации и Совета безопасности. Направления, полномочия, задачи, функции обязанности и права ФСБ России. Задачи, полномочия, обязанности и права ФСТЭК России. Задачи, полномочия, обязанности и права Федеральной службы по надзору в сфере связи, массовых коммуникаций и информационных технологий.
	5	2	**Правовые основы защиты государственной тайны.** Сущность основных понятий в области зашиты государственной тайны. Уровни секретностей сведений. Перечень сведений, составляющих гос. тайну. Государственная система защиты государственной тайны в Российской Федерации. Порядок допуска должностных лиц и граждан к государственной тайне. Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну и их носителей.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	6	2	**Правовые основы защиты коммерческой тайны.** Сущность и содержание коммерческой тайны. Подходы к определению уровней конфиденциальности сведений, составляющих коммерческую тайну, на основе потенциального ущерба. Порядок отнесения сведений к коммерческой тайне. Права и обязанности работника и работодателя по защите коммерческой тайне.
	7	2	**Правовые основы защиты персональных данных.** Сущность и содержание обработки и защиты персональных данных в России. Государственная система защиты персональных данных Российской Федерации. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
	8	2	**Правовые основы лицензирования и сертификации в области защиты информации в Российской Федерации.** Полномочия и права лицензирующих органов в области ЗИ. Порядок лицензирования деятельности в области ТЗИ (гос. тайна, конфиденциальная информация). Порядок лицензирования деятельности при использовании криптографических средств (гос. тайна, конфиденциальная информация). Порядок лицензирования деятельности при использовании СТС (гос. тайна, конфиденциальная информация). Порядок сертификации средств защиты информации.
	9	2	**Виды ответственности за нарушение законодательства в области защиты информации.** Уголовная ответственность. Административная ответственность. Гражданско-правовая ответственность. Дисциплинарная ответственность. Порядок назначения и приведение в исполнение наказаний.
	10	2	**Основы государственного контроля (надзора) в области обеспечения информационной безопасности (защиты информации).** Правовые основы государственного контроля (надзора) в области защиты информации. Виды проверок, их содержание. Ответственность за нарушения законодательства в области государственного контроля (надзора).

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
2	11	2	**Организационные основы обеспечения ИБ и ЗИ. Сущность и содержание организационных основ защиты информации.** Принципы и методы организационной защиты информации. Классификация организационных мероприятий по обеспечению ИБ и ЗИ. Понятие режима конфиденциальности информации.
	12	2	**Организация режима коммерческой тайны в организации (на предприятии).** Определения перечня сведений относящихся к коммерческой тайне. Регулирование отношений между работником и работодателем при использовании сведений, отнесенных к коммерческой тайне. Обязанности должностных лиц по защите коммерческой тайны. Порядок допуска лиц к коммерческой тайне. Порядок обработки информации, составляющую коммерческую тайну.
	13	2	**Организация защиты персональных данных в организации (на предприятии).** Модель угроз безопасности ПДн. Классификация ИСПДн. Положение об обработке и защите ПДн в организации (на предприятии).
	14	2	**Организация конфиденциального делопроизводства и документооборота в организации (на предприятии).** Организация конфиденциального делопроизводства. Организация электронного конфиденциального документооборота.
	15	2	**Физическая защита объектов и организация пропускного режима в организации.** Физическая защита объектов организации (предприятия). Пропускной режим в организации.
	16	2	**Аудит информационной безопасности организации (предприятия)** Внутренний аудит (самооценка) ИБ. Внешний аудит ИБ.

4.2 Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1.	1.	4	**Практическое занятие (семинар). Нормативные правовые акты Российской Федерации в области обеспечения информационной безопасности (ИБ) и защиты информации (ЗИ).** Федеральные законы и Указы Президента Российской Федерации в области ИБ и ЗИ. Постановления Правительства Российской Федерации в области ИБ и ЗИ. Приказы ФСБ России и ФСТЭК России в области ИБ и ЗИ.
	2.	4	**Практическое занятие (семинар). Правовые основы защиты государственной тайны.** Уровни секретностей сведений. Перечень сведений, составляющих гос. тайну. Государственная система защиты государственной тайны в Российской Федерации. Порядок допуска должностных лиц и граждан к государственной тайне. Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну и их носителей. Ответственности за нарушение законодательства в области защиты информации, отнесенной к государственной тайне.
	3.	4	**Практическое занятие (семинар). Правовые основы защиты информации ограниченного доступа.** Подходы к определению уровней конфиденциальности сведений, составляющих коммерческую тайну, на основе потенциального ущерба. Порядок отнесения сведений к коммерческой тайне. Права и обязанности работника и работодателя по защите коммерческой тайне. Сущность и содержание обработки и защиты персональных данных в России. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные. Служебная тайна. Порядок отнесения сведений к служебной тайне. Порядок обработке сведений, отнесенных к служебной тайне. Ответственности за нарушение законодательства в области защиты конфиденциальной информации.
	4.	4	**Практическое занятие (семинар). Порядок подготовки документов для получения лицензии на деятельность по технической защите конфиденциальной информации (ТЗИ).** Лицензионные требования, предъявляемые к соискателю лицензии на осуществление деятельности по ТЗИ. Перечень документов, предоставляемых для получения лицензии. Порядок подготовки сведений, подтверждающие квалификацию специалистов по защите информации (с указанием реквизитов дипломов, удостоверений, свидетельств). Порядок подготовки сведений, подтверждающих наличие аттестован-

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
			ных по требованиям безопасности информации защищаемых помещений. Порядок подготовки сведений, подтверждающие наличие аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации. Порядок подготовки сведений, подтверждающих наличие контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности. Порядок подготовки сведений об имеющихся технической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг. Порядок подготовки сведений, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами
2	5.	4	**Практическое занятие (групповое упражнение).** Разработка проекта перечня сведений, относящихся к сведениям, конфиденциального характера. Порядок разработки перечня сведений, относящихся к сведениям, конфиденциального характера. Оценка потенциального ущерба разглашения сведений конфиденциального характера. Категорирование сведений конфиденциального характера. Классификация сведений конфиденциального характера.
	6.	4	**Практическое занятие (групповое упражнение). Разработка организационно-распорядительных по созданию режима коммерческой тайны в организации.**
	7.	4	**Практическое занятие (групповое упражнение). Разработка организационно-распорядительных по защите персональных данных в организации.**
	8.	4	**Практическое занятие (семинар).** Организация защиты конфиденциальной информации в организации.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к практическому занятию (семинару) № 1.** Изучение материалов лекции № 1 - 4 и рекомендованной литературы. Изучение плана проведения семинара № 1. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 2.** Изучение материалов лекции № 5 и рекомендованной литературы. Изучение плана проведения семинара № 2. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 3.** Изучение материалов лекции № 6 и 7 и рекомендованной литературы. Изучение плана проведения семинара № 3. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 4.** Изучение материалов лекции № 8 и рекомендованной литературы. Изучение плана проведения семинара № 4. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к компьютерному тесту КТ-1.** Изучение материалов лекции №№ 1 - 10 и рекомендованной литературы.
2	6	**Подготовка к практическому занятию (групповому упражнению) № 5.** Изучение материалов лекции № 11 - 16 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 1.
	6	**Подготовка к практическому занятию (групповому упражнению) № 6.** Изучение материалов лекции № 11 - 16 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 2.
	6	**Подготовка к практическому занятию (групповому упражнению) № 7.** Изучение материалов лекции № 11 - 16 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 3.
	4	**Подготовка к практическому занятию (семинару) № 8.** Изучение материалов лекции № 11-16 и рекомендованной литературы. Изучение плана проведения семинара № 4. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к компьютерному тесту КТ-2.** Изучение материалов лекции № 11 - 16 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	18	**Подготовка курсовой работы**

4.5. Примерная тематика курсовых работ

Подготовка комплекта документов для получения лицензии:

1. В соответствии с Постановлением Правительства РФ от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» на:

1) разработку средств технических средств защиты информации;
2) разработку средств защищенных технических средств обработки информации;
3) разработку средств технических средств контроля эффективности мер защиты информации;
4) разработку средств программных (программно-технических) средств защиты информации;
5) разработку средств, защищенных программных (программно-технических) средств обработки информации;
6) разработку средств программных (программно-технических) средств контроля защищенности информации;
7) производство технических средств защиты информации;
8) производство защищенных технических средств обработки информации;
9) работы и услуги по проектированию в защищенном исполнении защищаемых помещений;
10) производство технических средств контроля эффективности мер защиты информации;
11) производство программных (программно-технических) средств защиты информации;
12) производство защищенных программных (программно-технических) средств обработки информации;
13) производство программных (программно-технических) средств контроля защищенности информации.

2. В соответствии с Постановлением Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» на:

14) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;
15) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
16) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в помещениях со средствами (системами), подлежащими защите;

17) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);
18) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
19) услуги по мониторингу информационной безопасности средств и систем информатизации;
20) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации средств и систем информатизации;
21) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации помещений со средствами (системами) информатизации, подлежащими защите;
22) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации защищаемых помещений;
23) работы и услуги по проектированию в защищенном исполнении средств и систем информатизации;
24) работы и услуги по проектированию в защищенном исполнении помещений со средствами (системами) информатизации, подлежащими защите;
25) работы и услуги по проектированию в защищенном исполнении защищаемых помещений;
26) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных.
27) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;
28) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1. Правовое обеспечение информационной безопасности:

Тексты лекций № 1 – 10. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения практических (семинарских) занятий) № 1-4. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Организационное обеспечение информационной безопасности

Тексты лекций № 11 – 16. ОРИОКС// URL: http://orioks.miet.ru/

Методические рекомендации студентам по подготовке и проведению практических занятий (групповых упражнений) № 5 – 7. ОРИОКС// URL: http://orioks.miet.ru/

План проведения практического (семинарского) занятия № 5. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Воеводин, В.А. Аудит информационной безопасности автоматизированных систем: учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 : - Текст : непосредственный.

2. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учеб. пособие / Ю.И. Коваленко. - М. : Горячая линия-Телеком, 2012. - 140 с. - URL: https://e.lanbook.com/book/5163 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0261-9. - Текст : непосредственный.

3. Мельников, Д. А. Информационная безопасность открытых систем: учебник / Д. А. Мельников. - Москва: Флинта : Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 15.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7. - Текст : электронный.

4. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 15.03.2021). - ISBN 978-5-534-03600-8. - Текст : электронный.

5. Новиков В.К.Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 1 :Правовое обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 184 с. - Имеется электронная версия издания. - ISBN 978-5-7256-0733-8.

6. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х ч.: Учеб. пособие. Ч. 2 Организационное обеспечение информационной безопасности/ В.К. Новиков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2013. - 172 с. - ISBN 978-5-7256-0738-3.

7. Галатенко В.А. Основы информационной безопасности : Учеб. пособие / В.А. Галатенко. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: https://e.lanbook.com/book/100295 (дата обращения: 16.03.2021). - ISBN 978-5-94774-821-5 .

8. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021. - 180 с. - ISBN 978-5-7256-0961-5 .

9. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1 .

10. Зайцев А.П.Технические средства и методы защиты информации : Учебник / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2018. - 444 с. - URL: https://e.lanbook.com/book/111057 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.

11. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8 .

12. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

13. Хорев П.Б. Программно-аппаратная защита информации : Учеб. пособие / П.Б. Хорев. - М. : Форум, 2013. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8 .

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : [сайт]. – URL: https://docs.cntd.ru/document/901990051 - (дата обращения 15.03.2021) .

2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ: (ред. от 02.07.2021) «О персональных данных»; Текст: электронный // Техэксперт : [сайт]. https://docs.cntd.ru/document/573249803?marker=64U0IK - (дата обращения 15.03.2021).

3. Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 30.11.2020) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации".

4. Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (ред. от 30.11.2020).

5. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

6. Методический документ. Методика оценки угроз безопасности информации. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2021 г. (утверждена ФСТЭК России 5 февраля 2021 г.)

7. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.

8. Методика определения актуальных угроз безопасности персональных данных

при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.

9. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

11. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

12. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

13. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

14. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования; Computers technique. Information protection against unauthorised access to information. General technical requirements: Национальный стандарт РФ: Введ. 01.01.1996: М.: Издательство стандартов, 1995 Стандартинформ, 2006.- URL: https://docs.cntd.ru/document/9039120 (дата обращения 16.03.2021).- Текст: электронный.

15. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Protection of information. Basic terms and definitions: Национальный стандарт РФ: Введ. 01.02.2008:М.: Стандартинформ, 2008, -URL: https://docs.cntd.ru/document/1200058320 -Текст: электронный.

16. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021) -Текст: электронный.

17. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Information protection. Sequence of protected operational system formation. General provisions; Национальный стандарт РФ: Введ. 01.09.2014.- М.: Стандартинформ, (Переиздание) октябрь 2018. -URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 10.03.2021)- Текст: электронный.

18. Рекомендации по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.

19. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.

Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный : непосредственный.

2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online). - Текст : электронный.

3. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

4. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL: https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения: 15.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021). - Текст: электронный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe).

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) – 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal (Из реестра МИЭТ п.78) – 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе:	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-5. ОиПОИБ. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ФОС по подкомпетенции ОПК-6. ОиПОИБ Способен использовать нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при организации защиты информации ограниченного доступа

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В целях практической подготовки в дисциплине предусмотрены практические занятия (групповые упражнения) и выполнение курсовой работы.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучаемых,

вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обучаемых. Главная задача преподавателя при проведении такого семинарского занятия состоит в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучаемых коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

11.2. Методические указания студентам по подготовке к групповым упражнениям

Ведущей дидактической целью групповых упражнений является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория), порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на групповых упражнения: индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения групповому упражнению преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждому групповому упражнению, предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению группового упражнения (ГУ) включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ГУ;
- наименование темы ГУ;
- цель ГУ (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению ГУ (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;

- список рекомендуемой литературы;
- приложения.

При подготовке к ГУ студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ГУ;
- ознакомиться с методическими рекомендации по выполнению ГУ;
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к ГУ;
- подготовить отчеты для заполнения.

На ГУ студент должен выполнить задание в соответствии с методическими указаниями.

Отчет по ГУ должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета по ГУ убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и выполнить ГУ, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на ГУ обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

Каждое практическое занятие – групповое упражнение направлено на формирование отдельных умений, необходимых для формирования компетенций и подкомпетенций.

11.3. Методические указания студентам по подготовке курсовой работы

Тема курсовой работы «Подготовка комплекта документов для получения лицензии».

Студенты готовят проекты документов для получения лицензии по выбору:

1. В соответствии с Постановлением Правительства РФ от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» на разработку или производство одного одно из средств:

а) разработка средств защиты конфиденциальной информации, в том числе:

технических средств защиты информации;

защищенных технических средств обработки информации;

технических средств контроля эффективности мер защиты информации;

программных (программно-технических) средств защиты информации;

защищенных программных (программно-технических) средств обработки информации;

программных (программно-технических) средств контроля защищенности информации;

б) производство средств защиты конфиденциальной информации, в том числе:

технических средств защиты информации;

защищенных технических средств обработки информации;

технических средств контроля эффективности мер защиты информации;

программных (программно-технических) средств защиты информации;

защищенных программных (программно-технических) средств обработки информации;

программных (программно-технических) средств контроля защищенности информации.

Перечень проектов документов, которые должны быть разработаны:

Заявление о предоставлении лицензии на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации юридическому лицу.

Сведения о квалификации специалистов по защите информации.

Сведения о наличии аттестованных по требованиям безопасности информации защищаемых помещений.

Сведения о наличии аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, а также автоматизированных систем, предназначенных для разработки средств защиты конфиденциальной информации.

Описание технологического процесса обработки конфиденциальной информации в автоматизированных системах.

Перечень защищаемых в автоматизированной системе ресурсов.

Сведения об оборудовании, необходимом для выполнения заявленных видов работ, в соответствии с перечнем, предусмотренным подпунктом "г" пункта 4 Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171.

Сведения о технической документации, национальных стандартах и методических документах, необходимых для выполнения заявленных видов работ по разработке и производству средств защиты конфиденциальной информации.

Опись прилагаемых документов.

2. В соответствии с» Постановлением Правительства РФ от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» на оказание одного из видов услуг:

а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:

в средствах и системах информатизации;

в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;

в помещениях со средствами (системами), подлежащими защите;

в помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации:

средств и систем информатизации;

помещений со средствами (системами) информатизации, подлежащими защите;

защищаемых помещений;

д) работы и услуги по проектированию в защищенном исполнении:

средств и систем информатизации;

помещений со средствами (системами) информатизации, подлежащими защите;

защищаемых помещений;

е) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Перечень проектов документов, которые должны быть разработаны:

Заявление о предоставлении лицензии на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации юридическому лицу.

Сведения о квалификации специалистов по защите информации.

Сведения о наличии аттестованных по требованиям безопасности информации защищаемых помещений.

Сведения о наличии аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, а также автоматизированных систем, предназначенных для разработки средств защиты конфиденциальной информации.

Описание технологического процесса обработки конфиденциальной информации в автоматизированных системах.

Перечень защищаемых в автоматизированной системе ресурсов.

Сведения об оборудовании, необходимом для выполнения заявленных работ и (или) оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации, в соответствии с перечнем, предусмотренным подпунктом "в" пункта 5 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79.

Сведения о технической документации, национальных стандартах и методических документах, необходимых для выполнения заявленных видов работ по разработке и производству средств защиты конфиденциальной информации.

Опись прилагаемых документов.

Структура курсовой работы должна отвечать традиционным требованиям, предъявляемым к научным работам и включать следующие части (структурные элементы):

Титульный лист.

Задание на КР.

Реферат.

Содержание.

Перечень условных обозначений и сокращений.

Введение.

Основная часть (основные разделы работы, предусмотренные заданием).

Заключение.

Список использованных источников.

Приложения.

Объем пояснительно записки составляет 50 – 70 страниц машинописного текста с приложениями, выполненных на стандартных листах формата А4.

Титульный лист является первым листом в пояснительной записке.

Реферат – это сокращенное изложение содержания и существа КР с основными сведениями о выполненных разработках и полученных результатах.

Реферат имеет следующую структуру:

− перечень количественных сведений о КР;

− перечень ключевых слов;

− текст реферата.

Перечень количественных сведений о КР должен включать количество: ___ с., ___ рис., ___ табл., __ источник, ___ прил.)..

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста КР, которые в наибольшей мере характеризуют содержание и обеспечивают возможность информационного поиска. Ключевые слова приводятся в именительном падеже и печатаются строчными буквами в строку через запятые.

Текст реферата в общем случае должен отражать сведения:

− об организации, получающей лицензию;

− виде деятельности, на который получается лицензия;

− перечне разработанных проектах документов.

Объем реферата определяется содержанием КР, количеством сведений и их научной и практической ценностью. Средний объем реферата составляет 1500 − 2000 знаков.

Перечень условных обозначений и сокращений. Принятые в работе малораспространенные условные обозначения, сокращения, символы, единицы и специфические термины необходимо представлять в виде отдельного списка. Если сокращения, условные обозначения, символы, единицы и термины повторяются в работе менее трех раз, отдельный список не составляют, а расшифровку дают непосредственно в тексте при первом упоминании.

Содержание пояснительной записки включает введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования), заключение, список использованных источников и наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки.

Введение должно содержать сведения:

− об организации, получающей лицензию;

− виде деятельности, на который получается лицензия;

− требования, предъявляемым к лицензиату.

Объем введения 3 − 5 страниц.

Основная часть. Основная часть должна включать проекты следующих документов:

Заявление о предоставлении лицензии на осуществление деятельности по разработке и производству средств защиты конфиденциальной информации юридическому лицу.

Сведения о квалификации специалистов по защите информации.

Сведения о наличии аттестованных по требованиям безопасности информации защищаемых помещений.

Сведения о наличии аттестованных по требованиям безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации, а также автоматизированных систем, предназначенных для разработки средств защиты конфиденциальной информации.

Описание технологического процесса обработки конфиденциальной информации в автоматизированных системах.

Перечень защищаемых в автоматизированной системе ресурсов.

Сведения об оборудовании, необходимом для выполнения заявленных работ и (или) оказания услуг при осуществлении деятельности по технической защите конфиденциальной информации.

Сведения о технической документации, национальных стандартах и методических документах, необходимых для выполнения заявленных видов работ по разработке и производству средств защиты конфиденциальной информации.

Опись прилагаемых документов.

Заключение должно содержать:

− краткие выводы по результатам выполнений работы;

− оценку полноты решений поставленных задач.

Типовой объем заключения составляет 1-2 страницы.

Список использованных источников должен содержать сведения обо всех источниках, использованных при написании КР. В список следует включать только те наименования, с которыми автор КР ознакомился лично. На все источники, приведенные в списке, должны быть ссылки в тексте. На источники, содержащие общие сведения по теме ВКР, ссылки делаются обычно во введении.

Источники в списке нумеруются в порядке появления ссылок в тексте.

При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ 7.1–2003.

Курсовая работа должна быть написана студентом самостоятельно, грамотно, по логически построенному плану. Прямое переписывание в работе текста из учебной и научной литературы не допускается.

11.4. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно- бальная система.

Под накопительно-бальной системой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего $R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, выступление на семинарах, защита отчетов по практическим заданиям, защита курсовой работы), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерная структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица 11.1

Структура и график контрольных мероприятий дисциплины

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
6	Практическое занятие (семинар) № 1	6	3
7	Практическое занятие (семинар) № 2	6	3
8	Практическое занятие (семинар) № 3	6	3
9	Практическое занятие (семинар) № 4	6	3
9	Компьютерный тест (КТ-1)	6	3
13	Практическое занятие (групповое упражнение) № 5	6	3
14	Практическое занятие (групповое упражнение) № 6	6	3
15	Практическое занятие (групповое упражнение) № 7	6	3
16	Практическое занятие (семинар) № 8	6	3
16	Компьютерный тест (КТ-2)	6	3
16	Посещаемость, активность	6	3
	Итого за текущий контроль	***66***	***33***
	Итоговый контроль	***34***	***17***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Примерная структура и график контрольных мероприятий при выполнении курсовой работы приведены в таблице 11.2.

Таблица 11.2

Структура и график контрольных мероприятий курсовой работы

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
10	Контроль № 1	10	5
12	Контроль № 2	10	5
14	Контроль № 3	10	5
16	Итоговый просмотр (оценка качества курсового проекта)	40	20
	Итого за текущий контроль	***70***	***35***
17	***Итоговый контроль*** *(защита курсового проекта)*	***30***	***15***
	Накопленный рейтинг	**100**	**50**

За курсовую работу в зачетную ведомость и зачетную книжку вносится ***итоговая 5-балльная оценка***, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в зачетную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в зачетную ведомость.

РАЗРАБОТЧИК
Доцент кафедры «Информационная безопасность»
Кандидат технических наук _____ Воеводин В.А.

Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Лист согласования
Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____/ Т.П.Филиппова /