

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

**ПЛАНИРОВАНИЕ И ФИНАНСИРОВАНИЕ РАБОТ ПО КОМПЛЕКСНОЙ
ЗАЩИТЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность

Код и наименование направления подготовки

Организация и технологии защиты государственной тайны

Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Планирование и финансирование работ по комплексной защите информации,
составляющей государственную тайну
Рабочая программа дисциплины

Составитель:

К.т.н., доцент, доцент, Н.В.Гришина

Ответственный редактор

К.и.н., доцент, зав. кафедрой, Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры
информационной безопасности
№ 10 от 30.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка.....	Ошибка! Закладка не определена.
1.1. Цель и задачи дисциплины	Ошибка! Закладка не определена.
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций	Ошибка! Закладка не определена.
1.3. Место дисциплины в структуре образовательной программы.....	Ошибка! Закладка не определена.
2. Структура дисциплины.....	Ошибка! Закладка не определена.
3. Содержание дисциплины	Ошибка! Закладка не определена.
4. Образовательные технологии	Ошибка! Закладка не определена.
5. Оценка планируемых результатов обучения.....	Ошибка! Закладка не определена.
5.1 Система оценивания	Ошибка! Закладка не определена.
5.2 Критерии выставления оценки по дисциплине	Ошибка! Закладка не определена.
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	Ошибка! Закладка не определена.
6. Учебно-методическое и информационное обеспечение дисциплины.....	Ошибка! Закладка не определена.
6.1 Список источников и литературы	Ошибка! Закладка не определена.
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».	14
6.3 Профессиональные базы данных и информационно-справочные системы	14
7. Материально-техническое обеспечение дисциплины	15
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов	15
9. Методические материалы.....	17
9.1 Планы практических занятий	17
Приложение 1. Аннотация рабочей программы дисциплины	18

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка магистров, необходимая для освоения методов и организации и планирования защиты государственной тайны.

Задачи дисциплины:

дать знания:

– о нормативных правовых актах, регламентирующих защиту государственной тайну;

– методы, средства и способы комплексирования систем защиты информации составляющей государственную тайну;

– способы планирования и бюджетирования работ по комплексной защите информации, содержащей государственную тайну.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-5 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлению процессом их реализации	ПК-5.1 – Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации	Знать: процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, составляющей государственную тайну, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
	ПК-5.2 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	Уметь: разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы комплексной защиты информации, составляющей государственную тайну
	ПК-5.3 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Владеть: навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по комплексной защите информации, составляющей государственную тайну
ПК-6 – Способен организовывать технологический	ПК-6.1 – Знает технологический процесс защиты информации и	Знать: технологический процесс защиты информации и процедуру разработки

<p>процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами</p>	<p>технических заданий, планов и графиков проведения работ по защите информации, составляющей государственную тайну, в соответствии с действующим нормативными и методическими документами</p>
	<p>ПК-6.2 – Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке</p>	<p>Уметь: применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, составляющей государственную тайну, читать и понимать нормативные и методические документы по информационной безопасности на английском языке</p>
	<p>ПК-6.3 – Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации</p>	<p>Владеть: навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации, составляющей государственную тайну</p>

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Планирование и финансирование работ по комплексной защите информации, составляющей государственную тайну» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Технологии обеспечения информационной безопасности», «Система защиты государственной тайны», «Законодательные и нормативные документы в области защиты государственной тайны».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 4 з.е., 144 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
4	Лекции	32
4	Практическая работа	46
Всего:		78

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 66 академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Нормативные документы в области защиты государственной тайны	Основные нормативные документы, термины в области защиты государственной тайны. Угрозы безопасности информации, содержащей государственную тайну. Классификация угроз. Источники угроз безопасности информации, содержащей государственную тайну. Модель угроз и модель нарушителя безопасности информации, содержащей государственную тайну. Принципы добывания и защиты информации. Их взаимосвязь.
2.	Автоматизированные системы обработки информации, содержащей государственную тайну	Виды автоматизированных систем обработки информации, содержащей государственную тайну. Классификация автоматизированных систем и средств вычислительной техники, предназначенных для обработки информации, содержащей государственную тайну. Защищённые сетевые устройства, классификация.
3.	Средства защиты информации, содержащей государственную тайну	Средства инженерной защиты информации, содержащей государственную тайну. Рубежи защиты. Средства технической защиты информации, содержащей государственную тайну. Программно-аппаратные средства защиты информации, содержащей государственную тайну. Криптографические средства защиты информации, содержащей государственную тайну. Организационные средства защиты информации,

		содержащей государственную тайну.
4.	Организация работ по защите информации, содержащей государственную тайну	Планирование работ по защите информации, содержащей государственную тайну. Финансирование работ по комплексной защите информации, содержащей государственную тайну.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Нормативные документы в области защиты государственной тайны	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование посредством электронной почты
2	Автоматизированные системы обработки информации, содержащей государственную тайну	Лекция 2.1 Лекция 2.2 Лекция 2.3 Лекция 2.4 Лекция 2.5 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование посредством электронной почты
3	Средства защиты информации, содержащей государственную тайну	Лекция 3.1 Лекция 3.2 Лекция 3.3 Лекция 3.4 Лекция 3.5 Лекция 3.6 Лекция 3.7 Лекция 3.8 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
4	Организация работ по защите информации, содержащей государственную тайну	Лекция 4.1 Лекция 4.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Работа с литературой Консультирование и проверка заданий посредством электронной почты
9	Практическое занятие 1. Разработка модели угроз и нарушителя объекта информатизации	Практическое занятие 1. Самостоятельная работа	Выполнение и защита практического задания

10	Практическое занятие 2. Выбор СВТ и разработка макета АС	Практическое занятие 2. Самостоятельная работа	Выполнение и защита практического задания
11	Практическое занятие 3. Обеспечение комплексной защиты информации на объекте информатизации	Практическое занятие 3. Самостоятельная работа	Выполнение и защита практического задания
12	Практическое занятие 4. Организация защиты информации на объекте информатизации	Практическое занятие 4. Самостоятельная работа	Выполнение и защита практического задания

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Максимальное количество баллов
Текущий контроль:	
– опрос или письменное тестирование	8 баллов (4 темы по 2 балла)
– практическое задание 1	8
– практическое задание 2	18
– практическое задание 3	18
– практическое задание 4	8
Промежуточная аттестация (зачёт с оценкой)	40 баллов
Итого за семестр	100 баллов

Текущий контроль (опрос, в том числе в виде выполнения интерактивных заданий, участие в дискуссии) проводится в устном или письменном виде; контрольная работа, реферат — в письменном виде.

Система текущего и промежуточного контроля знаний студентов по дисциплине предусматривает проверку сформированности компетенций ПК-5; ПК-6.

Промежуточная аттестация (зачет) проводится в форме коллоквиума в устном виде.

Полученный совокупный результат (максимум 100 баллов) конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82			C
56 – 67	D		
50 – 55	удовлетворительно		E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и

рассчитанное на выяснение объема знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Примерный перечень устных вопросов для проверки знаний

№	Вопрос
1.	Основной документ по защите гостайны.
2.	Область применения основного документа по защите гостайны.
3.	Основные угрозы безопасности информации, составляющей гостайну
4.	Основные нарушители безопасности информации, составляющей гостайну
5.	Назовите классы АСЗИ
6.	Какие классы АСЗИ используются при обработке информации, составляющей гостайну
7.	Какие классы СВТ используются при обработке информации, составляющей гостайну
8.	Какие классы МЭ используются при обработке информации, составляющей гостайну
9.	Назовите технические средства ПАЗИ, составляющей гостайну
10.	Назовите основные рубежи охраны
11.	Что относится к средствам инженерной защиты?
12.	Методы планирования работ по созданию системы защиты информации, составляющей гостайну
13.	Источники финансирования работ по созданию КЗИ, составляющей гостайну

Примерные вопросы тестовых заданий

(проверка сформированности компетенций ПК-5 и ПК-6)

1. Какое постановление Правительства РФ определяет процедуру лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну?
2. Какой официальный документ, разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока?
3. Органом, уполномоченными на ведение лицензионной деятельности по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, является:
4. Органами, уполномоченными на ведение лицензионной деятельности на право проведения работ, связанных с созданием средств защиты информации являются:
5. Органами, уполномоченными на ведение лицензионной деятельности на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны являются:
6. Работа органов, уполномоченных на ведение лицензионной деятельности по защите государственной тайны, координируется:
7. Может ли заявитель для получения лицензии представить в соответствующий орган, уполномоченный на ведение лицензионной деятельности, документы в электронном виде?
8. Кто несет ответственность за достоверность представляемых документов для получения лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну?
 Ответственность за достоверность представляемых документов для получения лицензии
 В течение какого срока со дня получения заявления со всеми необходимыми документами орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии?
9. На какой срок может быть продлен срок принятия решения о выдаче или об отказе в выдаче лицензии в зависимости от сложности и объема подлежащих специальной

экспертизе материалов? руководитель органа, уполномоченного на ведение лицензионной деятельности, до ...

10. Наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности, является обязательным условием получения лицензии?

11. Соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений является обязательным условием получения лицензии?

Промежуточная аттестация (зачёт с оценкой)

Примерные вопросы к зачёту с оценкой:

№	Вопрос
1.	Основные нормативные документы, термины в области защиты государственной тайны
2.	Угрозы безопасности информации, содержащей государственную тайну.
3.	Классификация угроз безопасности информации, содержащей государственную тайну. Нарушители угроз безопасности информации, содержащей государственную тайну.
4.	Модель угроз и модель нарушителя безопасности информации, содержащей государственную тайну.
5.	Принципы добывания и защиты информации. Их взаимосвязь.
6.	Классификация автоматизированных систем, предназначенных для обработки информации, содержащей государственную тайну.
7.	Классификация средств вычислительной техники, предназначенных для обработки информации, содержащей государственную тайну.
8.	Защищённые сетевые устройства, классификация.
9.	Средства инженерной защиты информации, содержащей государственную тайну. Рубежи защиты.
10.	Средства технической защиты информации, содержащей государственную тайну.
11.	Программно-аппаратные средства защиты информации, содержащей государственную тайну.
12.	Криптографические средства защиты информации, содержащей государственную тайну.
13.	Комплексирование средств защиты информации, содержащей государственную тайну.
14.	Планирование работ по комплексной защите информации, содержащей государственную тайну.
15.	Финансирование работ по комплексной защите информации, содержащей государственную тайну.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основные источники

Закон РФ "О государственной тайне" от 21.07.1993 № 5485-1 [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_2481/

Указ Президента РФ от 30.11.1995 № 1203 "Об утверждении Перечня сведений, отнесенных к государственной тайне" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_8522/

Дополнительные источники

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный.

Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.

ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс] : Режим доступа : <http://gostrf.com/normadata/1/4294818/4294818891.pdf>, свободный.

Рекомендации стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (По состоянию на 8 июля 2018 г.) [Электронный ресурс]: Режим доступа: <https://pdf.standartgost.ru/catalog/Data2/1/4293850/4293850561.pdf>, свободный.

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/component/attachments/download/296>, свободный.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/component/attachments/download/297>, свободный.

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : <https://fstec.ru/component/attachments/download/295>, свободный.

Основная литература

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1021578>

Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1844364>

Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1865598>

Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2022. — 204 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/21158>. - ISBN 978-5-369-01603-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1851140>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

ФГУ НИЦ «Охрана» ФСНВГ России. Нормативные документы [Электронный ресурс] :
Режим доступа : <http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html>. –
Загл. с экрана.

Сайт ФСТЭК России. [Электронный ресурс] : <https://fstec.ru/>
Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Состав программного обеспечения (ПО)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическое занятие 1

Тема – Разработка модели угроз и нарушителя объекта информатизации

Продолжительность – 6 ч.

Задания:

1. Построить вербальную модель объекта защиты для указанного преподавателем помещения организации, работающей со сведениями, составляющими государственную тайну.
2. Описать объект защиты, предположительные каналы утечки информации,
3. Описать модель поведения внешнего и внутреннего нарушителей, методы, способы и технические средства съёма информации.
4. Составить экспликацию помещений объекта информатизации, где предполагается обработка информации, составляющей государственную тайну

Указания по выполнению заданий:

1. Изучить теоретический материал по теме, нормативные документы.
2. Преподавателем выдаётся описание организации и группы помещений (от двух до четырёх), в которых планируется обрабатывать информацию, составляющую государственную тайну и гриф секретности информации.
3. Схемы помещений рекомендуется создавать в MS Visio или любом графическом редакторе.
4. Составить отчёт о выполнении практического задания
5. Ответить на теоретические вопросы в конце практического занятия
6. Защитить практическое задание
7. Данная работа является базовой основой для выполнения последующих практических работ

Практическое занятие 2

Тема – Выбор СВТ и разработка макета АС

Продолжительность – 14 ч.

Задания:

1. Провести макетирование автоматизированной системы в защищённом исполнении. Присвоить требуемый класс защиты АС от НСД.
2. Выбрать необходимые средства вычислительной техники (оконечные, сетевые и периферийные устройства) и программное обеспечение, сертифицированные ФСТЭК и ФСБ России.
3. Провести разграничение доступа между предполагаемыми пользователями системы.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме и руководящие документы ФСТЭК России.
2. Выбрать необходимые СВТ и ПО для компьютеров.
3. Составить отчёт о выполнении практического задания
4. Ответить на теоретические вопросы в конце практического занятия
5. Защитить практическое задание.

Практическое занятие 3

Тема – Обеспечение комплексной защиты информации на объекте информатизации

Продолжительность – 20 ч.

Задания:

1. Предложить меры по инженерной защите объекта информатизации.
2. Выбрать с сайта продавцов необходимые технические средства, определённые в ходе выполнения практического задания 2.
3. Выбрать средства технической защиты информации
4. Выбрать средства криптографической защиты информации

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Разместить средства на экспликации объектов и общем плане объекта.
3. Составить отчёт о практическом занятии.
4. Ответить на теоретические вопросы в конце практического занятия.
5. Защитить практическое задание.

Практическое занятие 4

Тема – Организация комплексной защиты информации на объекте информатизации

Продолжительность – 10 ч.

Задания:

1. Составить план проведения мероприятий по защите объекта информатизации.
2. Провести бюджетирование затрат по защите объекта информатизации, где обрабатывается информация, составляющая государственную тайну.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Цены брать с сайтов продавцов.
3. Составить отчёт о практическом занятии.
4. Ответить на теоретические вопросы в конце практического занятия.
5. Защитить практическое задание.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины - профессиональная подготовка магистрантов, необходимая для освоения методов и организации и планирования защиты государственной тайны.

Задачи: дать знания о нормативных правовых актах, регламентирующих защиту государственной тайны; методы, средства и способы комплексирования систем защиты информации составляющей государственную тайну; способы планирования и бюджетирования работ по комплексной защите информации, содержащей государственную тайну.

Дисциплина направлена на формирование следующих компетенций:

- ПК-5 – Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлению процессом их реализации
 - ПК-5.1 – Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
 - ПК-5.2 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
 - ПК-5.3 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
- ПК-6 – Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
 - ПК-6.1 – Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами
 - ПК-6.2 – Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке
 - ПК-6.3 – Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации

В результате освоения дисциплины обучающийся должен:

Знать: процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, составляющей государственную тайну, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации; технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации, составляющей государственную тайну, в соответствии с действующим нормативными и методическими документами

Уметь: разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы комплексной защиты информации, составляющей государственную тайну; применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, составляющей государственную тайну, читать и понимать нормативные и методические документы по информационной безопасности на английском языке

Владеть: навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по комплексной защите информации, составляющей государственную тайну; навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации, составляющей государственную тайну.

По дисциплине предусмотрена промежуточная аттестация в форме *зачёта с оценкой*.

Общая трудоёмкость освоения дисциплины составляет 4 зачётные единицы.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлена основная литература</i>	17.03.2023	9

Обновление основной литературы (2023 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

1. Дополнить раздел **Основная литература**

Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1900721>

Баранова Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1861657>

Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1912992>

Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1912987>

Составитель:

К.т.н., доцент, доцент, Н.В.Гришина