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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«13» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Политические и социальные аспекты 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 компетенций:

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**ОПК-1. ПСАИБ**. Способен оценивать роль информации и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**Знания:** особенности восприятия человеком информации; место и функции информации в социальных системах; основные политические и социальные факторы, влияющие на обеспечение информационной безопасности социальных систем; основные компоненты и структуру информационного пространства, как сферы действия политических и социальных факторов обеспечения информационной безопасности социальных систем; технологии воздействия на общественное сознание; принципы и виды информационно-психологического воздействия; сущность и содержание информационного противоборства современных государств; объекты информационного противоборства; субъекты информационного противоборства; средства, способы и технологии информационно-психологического воздействия; методы противодействия информационно-психологической агрессии; содержание основных мероприятий по противодействию психологическим операциям и срыву информационно-психологического воздействия; основные направления совершенствования государственной политики в социально-культурном пространстве и СМИ.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		Умения: оценивать роль информации и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства; анализировать социальные конфликты в современном обществе с точки зрения информационного противоборства; вырабатывать рекомендации по организации защите социальных от информационных воздействий. **Опыт деятельности:** подготовки докладов и рефератов по вопросам обеспечения информационной безопасности.

В результате изучения дисциплины студент должен:

Знать:

- основные политические и социальные факторы, влияющие на обеспечение информационной безопасности социальных систем;
- основные компоненты и структуру информационного пространства как сферы действия политических и социальных факторов обеспечения информационной безопасности социальных систем;
- особенности системы социально-политических отношений современного информационного общества;
- место и функции информации в социальных системах;
- политическое и социальное значение массовой коммуникации в социальных системах;
- технологии воздействия на общественное сознание через органы СМИ;
- социально-информационный подход к выявлению особенностей влияния на человека деструктивного информационного воздействия;
- информационное воздействие, как способ влияния на поведение людей;
- особенности восприятия человеком информации;
- информационно-психологическое воздействие, как средство управляющего воздействия в социальных системах;
- принципы и виды информационно-психологического воздействия;
- политико-правовое понимание информационной безопасности государства;
- особенности обеспечения информационной безопасности в современных условиях;
- сущность и содержание информационного противоборства современных государств;
- объекты информационного противоборства;

- субъекты информационного противоборства;
- основные виды информационного противоборства и их характеристику;
- средства, способы и технологии информационно-психологического воздействия, как инстумент политической борьбы в современном информационном обществе;
- технологии информационно-психологического воздействия;
- методы, силы и средства ведения информационно-психологической войны;
- виды и способы психологического воздействия на человека;
- формы ведения информационно-психологической борьбы;
- социальные сети, как среду проведения тайных информационных операций
- систему обеспечения информационного суверенитета России;
- содержание основных мероприятий по эффективному противодействию психологическим операциям и срыву информационно-психологического воздействия;
- системный подход к организации эффективной защиты социальных систем и силовых структур от информационных воздействий;
- содержание государственной информационной политики в условиях информационно-психологической войны;
- основные направления государственной информационной политики в условиях информационно-психологической войны;
- методы противодействия информационно-психологической агрессии;
- основные направления совершенствования государственной политики в социально-культурном пространстве и СМИ;
- технологии противодействия вовлечению социальных объектов в деструктивные организации;
- патриотизм, как важнейший фактор обеспечения информационной безопасности государства в условиях информационно-психологической войны.

Уметь:

- оценивать роль информации и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;
- анализировать социальные конфликты в современном обществе с точки зрения информационного противоборства;
- вырабатывать рекомендации по организации защите социальных от информационных воздействий.

Иметь опыт деятельности:

- подготовки докладов и рефератов по вопросам обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Политические и социальные аспекты информационной безопасности» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и

читается на 4-м курсе в 7-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении следующих дисциплин: «Правоведение», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Знания и умения, полученные в результате изучения дисциплины, используются в дисциплине «Основы управления информационной безопасностью», учебной, производственной практиках и 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		
4	7	5	180	80	32	-	32	16	64	Экз. (36 ч)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
Модуль 1. «Политические и социальные факторы обеспечения информационной безопасности»	12	-	12	6	24	Компьютерный тест КТ-1. Защита реферата
Модуль 2. «Информационная война в системе политических отношений современного информационного общества»	12	-	12	6	24	Компьютерный тест КТ-2. Защита реферата

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
Модуль 3. «Основные направления противодействия информационному воздействию в интересах обеспечения информационной безопасности личности, общества и государства в современных условиях»	8	-	8	4	16	Компьютерный тест КТ-3. Защита реферата

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1	1.	2	**Лекция 1. Основные политические и социальные факторы, влияющие на обеспечение информационной безопасности социальных систем** Политические факторы обеспечения информационной безопасности. Социальные факторы обеспечения информационной безопасности. Актуальные проблемы обеспечения информационной безопасности в современных социальных системах. Основные компоненты и структура информационного пространства как сферы действия политических и социальных факторов обеспечения информационной безопасности социальных систем. Особенности управления социальными системами в контексте обеспечения их информационной безопасности.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	2.	2	**Лекция 2. Система социальных и политических отношений как среда организации и проведения операций информационной войны** Особенности системы социально-политических отношений современного информационного общества. Информация и ее место и функции в социальных системах. Информационное пространство с позиций синергетики. Политическое и социальное значение массовой коммуникации в социальных системах. Технологии воздействия на общественное сознание через органы СМИ.
	3.	2	**Лекция 3. Личность как объект информационного воздействия в социальных системах** Социально-информационный подход к выявлению особенностей влияния на человека деструктивного информационного воздействия Информационное воздействие как способ влияния на поведение людей Социально-психологический подход к пониманию человека Человек как объект информационного воздействия Особенности восприятия человеком информации
	4.	2	**Лекция 4. Социально-политические особенности информационно-психологического воздействия на личность и социальные системы** Информационно-психологическое воздействие как средство управляющего воздействия в социальных системах Принципы информационно-психологического воздействия Виды информационно-психологического воздействия Психологические манипуляции Дезинформирование Лоббирование Пропаганда Управление кризисами Шантаж
	5.	2	**Лекция 5. Политологический подход к информационной безопасности в системе национальной безопасности России** Политико-правовое понимание информационной безопасности государства Безопасность информационного пространства как политическое явление и процесс Системный подход к информационной безопасности Особенности обеспечения информационной безопасности в современных условиях Информационно-психологическая безопасность РФ

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	6.	2	**Лекция 6. Сущность и содержание информационного противоборства современных государств** Эволюция политических форм, средств и методов информационного противоборства Сущность информационного противоборства Принцип информационной асимметрии Принцип информационного доминирования Объекты информационного противоборства Субъекты информационного противоборства
2	7.	2	**Лекция 7. Основные виды информационного противоборства и их характеристика** Приоритеты геополитической конкуренции в информационном пространстве Внешнее управление информационно-психологическими процессами... Информационно-психологическая экспансия Информационно-психологическая агрессия Информационная война Информационно-психологические операции Информационное сдерживание
	8.	2	**Лекция 8. Информационная война как политическое и социальное явление и средство достижения политических целей** Сущность информационной войны Современное понимание содержания информационной войны. Политическое и социальное содержание информационной войны Информационные войны как разновидность информационных социальных технологий
	9.	2	**Лекция 9. Средства, способы и технологии информационно-психологического воздействия как инстумент политической борьбы в современном информационном обществе** Технологии информационно-психологического воздействия. Силы и средства ведения информационно-психологической войны. Методы информационной войны Тайные операции как организованная форма реализации целей информационно-психологической войны. Характеристика операций информационно-психологической войны

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	10.	2	**Лекция 10. Информационно-психологическое воздействие при ведении психологических операций в условиях информационно-психологической войны** Особенность информационного противоборства в современном мире. Пропагандистское воздействие в ходе проведения психологических операций Психологическое воздействие в ходе проведения психологических операций. Содержание психологического воздействия Виды психологического воздействия **Способы психологического воздействия**
	11.	2	**Лекция 11. Формы ведения информационно-психологической борьбы** Информационно-психологическое воздействие печатными средствами Информационно-психологическое воздействие с помощью электронных средств. Информационно-психологическое воздействие с помощью радиовещания. Информационно - психологическое воздействие с помощью телевещания. Информационно - психологическое воздействие с помощью компьютерных социальных сетей Информационно-психологическое воздействие через непосредственное или опосредованное общение Информационно-психологическое воздействие изобразительными средствами
	12.	2	**Лекция 12. Социальные сети как среда проведения тайных информационных операций** Общая характеристика социальных сетей в мире Информационно-психологическое воздействие с помощью компьютерных социальных сетей Опыт США по использованию социальных сетей в целях осуществления «мягкого» перехвата власти Сетецентрические операции против России Блогосфера как новый инструмент общения Основные направления НИОКР, проводимых США в целях достижения подавляющего информационного превосходства Цели создания методов и средств проведения информационных операций в открытых (закрытых) ресурсах Интернет

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
3	13.	2	**Лекция 13. Системный подход к противодействию информационно-психологического воздействия на социум** Система обеспечения информационного суверенитета России Содержание основных мероприятий по эффективному противодействию психологическим операциям и срыву информационно-психологического воздействия Особенности прогнозирования психологических операций Профилактика эффективного психологического воздействия противника Срыв психологического воздействия противника **Системный подход к организации эффективной защиты социальных систем и силовых структур от информационных воздействий**
	14.	2	**Лекция 14. Современная государственная информационная политика в условиях информационно-психологической войны** Содержание государственной информационной политики в условиях информационно-психологической войны Особенность государственной информационной политики в условиях информационно-психологической войны Основные направления государственной информационной политики в условиях информационно-психологической войны Государственная система информационного противоборства Противодействие информационно-психологической агрессии (войне) на ранней стадии Быстрое реагирование на внезапно выявленные акции и мероприятия информационно-психологической войны Формирование системы государственной информационной политики в особых условиях

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	15.	2	**Лекция 15. Государственная политика и безопасность в информационно-культурной сфере и противодействие информационным операциям, реализуемые неформальными объединениями и деструктивными культами** Культурное пространство страны и целостного мира личности как объекты информационной безопасности Информационное противоборство как культурно-информационное противоборство Социокультурная значимость деятельности СМИ Основные направления совершенствования государственной политики в социально-культурном пространстве и СМИ Влияние телевидения на духовно-нравственное состояние общества Неформальное движение как канал проведения информационно-психологической операции Факторы, способствующие успешности деятельности деструктивных культов в России Процесс установления контроля над сознанием адептов в деструктивном культе Фазы введения нового члена в деструктивный культ Технологии противодействия вовлечению социальных объектов в деструктивные организации
	16.	2	**Лекция 16. Патриотизм как важнейший фактор обеспечения информационной безопасности государства в условиях информационно-психологической войны** Сущность и содержание патриотизма. Этапы становления российской государственности и формирования российской нации и развитие патриотизма Факторы и условия формирования патриотизма граждан Российской Федерации Роль и значение патриотизма в государственной информационной политике как средство обеспечения национальной безопасности Государственная программа «Патриотическое воспитание граждан Российской Федерации»

4.2. Практические занятия

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
1	1.	4	**Практическое занятие (семинар). Актуальные политические и социальные проблемы обеспечения информационной безопасности в современных социальных системах.** Политические факторы обеспечения информационной безопасности Особенности управления социальными системами в контексте обеспечения их информационной безопасности. Система социальных и политических отношений как среда организации и проведения операций информационной войны
	2.	4	**Практическое занятие (семинар 2). Информационное воздействие как способ влияния на поведение людей и социальные системы** Социально-информационный подход к выявлению особенностей влияния на человека деструктивного информационного воздействия Человек как объект информационного воздействия Социально-политические особенности информационно-психологического воздействия на человека и социальные системы
	3.	4	**Практическое занятие (семинар). Безопасность информационного пространства как политическое явление и процесс в условиях информационных войн.** Политико-правовое понимание информационной безопасности государства Особенности обеспечения информационной безопасности в современных условиях Эволюция политических форм, средств и методов информационного противоборства
2	4.	4	**Практическое занятие (семинар). Основы информационного противоборства социальных систем и их характеристика** Приоритеты геополитической конкуренции в информационном пространстве Информационно-психологическая агрессия Сущность и содержание информационной войны.
	5.	4	**Практическое занятие (семинар). Информационно-психологическое воздействие как инструмент политической борьбы в современном информационном обществе** Силы и средства ведения информационно-психологической войны Тайные операции как организованная форма реализации целей информационно-психологической войны Информационно-психологическое воздействие при ведении психологических операций

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
	6.	4	**Практическое занятие (семинар). Формы, технологии, методы и способы ведения психологической борьбы** Основные виды информационно-психологического воздействия Информационно-психологическое воздействие с помощью электронных средств Информационно-психологическое воздействие через непосредственное или опосредованное общение
3	7.	4	**Практическое занятие. Система мероприятий по эффективному противодействию психологическим операциям и срыву информационно-психологического воздействия** Содержание основных мероприятий по эффективному противодействию психологическим операциям и срыву информационно-психологического воздействия Профилактика эффективного психологического воздействия противника Содержание государственной информационной политики в условиях информационно-психологической войны
	8.	4	**Практическое занятие (семинар). Государственная политика и безопасность в информационно-культурной сфере и противодействие информационным операциям** Культурное пространство страны и целостного мира личности как объекты информационной политики и безопасности Основные направления совершенствования государственной политики в социально-культурном пространстве и СМИ Неформальное движение как канал проведения информационно-психологической операции

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	4	**Подготовка к практическому занятию (семинару) № 1.** Изучение материалов лекции 1-2 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 3-4 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 5-6 и рекомендованной литературы. Изучение плана проведения семинара 3. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к компьютерному тесту КТ-1.** Изучение материалов лекции 1-6 и рекомендованной литературы.
2	4	**Подготовка к практическому занятию (семинару) № 4:** Изучение материалов лекции 7-8 и рекомендованной литературы. Изучение плана проведения семинара 4. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к практическому занятию (семинару) № 5:** Изучение материалов лекции 9-10 и рекомендованной литературы. Изучение плана проведения семинара 5. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к практическому занятию (семинару) № 6:** Изучение материалов лекции 11-12 и рекомендованной литературы. Изучение плана проведения семинара 6. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к компьютерному тесту КТ-2.** Изучение материалов лекции 7-12 и рекомендованной литературы.
3	4	**Подготовка к практическому занятию (семинару) № 7:** Изучение материалов лекции 13-14 и рекомендованной литературы. Изучение плана проведения семинара 7. Подготовка доклада и презентации по одному из вопросов семинара.
	4	**Подготовка к практическому занятию (семинару) № 8:** Изучение материалов лекции 15-16 и рекомендованной литературы. Изучение плана проведения семинара 8. Подготовка доклада и презентации по одному из вопросов семинара
	4	**Подготовка к компьютерному тесту КТ-2.** Изучение материалов лекции 13-16 и рекомендованной литературы.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1-3	20	**Подготовка реферата**

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

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. «Политические и социальные факторы обеспечения информационной безопасности»:

Тексты лекций № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 1 - 3. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. «Информационная война в системе политических отношений современного информационного общества».

Тексты лекций № 6 – 12. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 4 - 6. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 3. «Основные направления противодействия информационному воздействию в интересах обеспечения информационной безопасности личности, общества и государства в современных условиях»:

Тексты лекций № 13 – 66. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 7 и 8. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Макаров В.Е. Политические и социальные аспекты информационной безопасности : Монография / В.Е. Макаров. - М. ; Таганрог : Изд-ль С.А. Ступин, 2015. - 352 с. - ISBN 978-5-9906281-5-1.
2. Малюк, А. А Защита информации в информационном обществе / А. А. Малюк. -

Москва : Горячая линия-Телеком, 2017. - 230 с. - URL: https://e.lanbook.com/book/111078 (дата обращения: 15.03.2021). - ISBN 978-5-9912-0481-1. - Текст : электронный.

3. 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.
4. 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.
5. 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.

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 Методика определения актуальных угроз безопас-

ности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.
8. 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.
9. 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.
10. 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.
11. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
12. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
13. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Общие положения; Национальный стандарт РФ : Введ. 09.02.1995: М.: Издательство стандартов (Переиздание) Стандартинформ, август 2006 -URL: https://docs.cntd.ru/document/1200004675 (дата обращения: 15.03.2021) -Текст: электронный.
14. 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.
15. 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.
16. 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.
17. 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.-12 л. - Текст: непосредственный.
18. 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.-20 л.- Текст: непосредственный.

Периодические издания

1. 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.
2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 - 2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.
3. Information Security / Информационная безопасность». – URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Режим доступа: свободный.
4. Вопросы кибербезопасности./. – URL: http://cyberrus.com/ (дата обращения: 15.03.2021). – Режим доступа: свободный.
5. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 10.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный
6. Jet Info./ «Инфосистемы Джет». – URL: http://www.jetinfo.ru (дата обращения: 15.03.2021). – Режим доступа: свободный.
7. 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.

4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.

5. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Режим доступа: свободный.

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).	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	Учебная доска.	
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. 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: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-1. ПСАИБ. Способен оценивать роль информации и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

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 (семинары) и подготовка реферата.

В процессе изучения курса предполагается самостоятельная работа студента при подготовке к лекционным, практическим занятиям, подготовке реферата. При этом студент использует методические разработки, рекомендуемую литературу, библиотеку электронных модулей в электронной информационной образовательной среде ОРИОКС, Интернет-ресурсы, информационно-справочные системы.

Максимальная эффективность освоения материалов ***лекций*** достигается при предварительной подготовке к ней. Студенту рекомендуется заранее ознакомиться с предстоящей темой лекции и основными ее тезисами, подготовить вопросы к лектору по заинтересовавшим разделам.

Для закрепления лекционного материала проводятся ***практические занятия***. Для повышения эффективности практических занятий (семинаров) студенту также необходимо предварительно ознакомиться с методическими указаниями, прочитать конспект лекций по данной

тематике и соответствующие главы учебника (учебного пособия).

Одной из форм обучения является ***консультация*** у преподавателя. Обращаться к помощи преподавателя следует в любом случае, когда студенту не ясно изложение какого-либо вопроса в учебной литературе или требуется помощь в подборе необходимой дополнительной литературы.

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 рефератов

Реферат представляет собой отчет об изучении студентом конкретной задачи (вопроса).

Перечень возможных тем рефератов

1. Политические факторы обеспечения информационной безопасности.
2. Социальные факторы обеспечения информационной безопасности.
3. Актуальные проблемы обеспечения информационной безопасности в современных социальных системах
4. Основные компоненты и структура информационного пространства как сферы действия политических и социальных факторов обеспечения информационной безопасности социальных систем
5. Особенности управления социальными системами в контексте обеспечения их информационной безопасности
6. Особенности системы социально-политических отношений современного информационного общества
7. Информация и ее место и функции в социальных системах.
8. Информационное пространство с позиций синергетики.
9. Политическое и социальное значение массовой коммуникации в социальных системах
10. Технологии воздействия на общественное сознание через органы СМИ
11. Социально-информационный подход к выявлению особенностей влияния на человека деструктивного информационного воздействия

12. Информационное воздействие как способ влияния на поведение людей
13. Социально-психологический подход к пониманию человека
14. Человек как объект информационного воздействия
15. Особенности восприятия человеком информации
16. Информационно-психологическое воздействие как средство управляющего воздействия в социальных системах
17. Принципы информационно-психологического воздействия
18. Виды информационно-психологического воздействия
19. Психологические манипуляции
20. Дезинформирование
21. Лоббирование
22. Пропаганда
23. Управление кризисами
24. Шантаж
25. Политико-правовое понимание информационной безопасности государства
26. Безопасность информационного пространства как политическое явление и процесс.
27. Системный подход к информационной безопасности
28. Особенности обеспечения информационной безопасности в современных условиях
29. Информационно-психологическая безопасность РФ
30. Эволюция политических форм, средств и методов информационного противоборства
31. Сущность информационного противоборства.
32. Принцип информационной асимметрии
33. Принцип информационного доминирования
34. Объекты информационного противоборства
35. Субъекты информационного противоборства
36. Приоритеты геополитической конкуренции в информационном пространстве.
37. Внешнее управление информационно-психологическими процессами...
38. Информационно-психологическая экспансия.
39. Информационно-психологическая агрессия.
40. Информационная война.
41. Информационно-психологические операции.
42. Информационное сдерживание.
43. Сущность информационной войны.
44. Современное понимание содержания информационной войны.
45. Политическое и социальное содержание информационной войны
46. Информационные войны как разновидность информационных социальных технологий
47. Технологии информационно-психологического воздействия.
48. Силы и средства ведения информационно-психологической войны...
49. Методы информационной войны
50. Тайные операции как организованная форма реализации целей информационно-психологической войны.
51. Характеристика операций информационно-психологической войны
52. Особенность информационного противоборства в современном мире..
53. Пропагандистское воздействие в ходе проведения психологических операций

54. Психологическое воздействие в ходе проведения психологических операций.
55. Содержание психологического воздействия.
56. Виды психологического воздействия
57. Способы психологического воздействия.
58. Информационно-психологическое воздействие печатными средствами.
59. Информационно-психологическое воздействие с помощью электронных средств.
60. Информационно - психологическое воздействие с помощью радиовещания..
61. Информационно - психологическое воздействие с помощью телевещания.
62. Информационно - психологическое воздействие с помощью компьютерных социальных сетей.
63. Информационно-психологическое воздействие через непосредственное или опосредованное общение
64. Информационно-психологическое воздействие изобразительными средствами.
65. Система обеспечения информационного суверенитета России….
66. Содержание основных мероприятий по эффективному противодействию психологическим операциям и срыву информационно-психологического воздействия..
67. Особенности прогнозирования психологических операций …
68. Профилактика эффективного психологического воздействия противника.
69. Срыв психологического воздействия противника.
70. Системный подход к организации эффективной защиты силовых структур (войск) от информационных воздействий
71. Содержание государственной информационной политики в условиях информационно-психологической войны
72. Особенность государственной информационной политики в условиях информационно-психологической войны.
73. Основные направления государственной информационной политики в условиях информационно-психологической войны..
74. Государственная система информационного противоборства.....
75. Противодействие информационно-психологической агрессии (войне) на ранней стадии
76. Быстрое реагирование на внезапно выявленные акции и мероприятия информационно-психологической войны.
77. Информационно-психологическая борьба в условиях информационной войны.
78. Формирование системы государственной информационной политики в особых условиях

Реферат должен состоять из следующих частей (структурных элементов):

Титульный лист является первым листом в реферате.

Перечень условных обозначений и сокращений. Принятые в реферате 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 реферата включает введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования), заключение, список использованных ис-

точников и наименование приложений с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки.

Введение должно содержать развернутую оценку современного состояния решаемой задачи. Объем введения 1 − 3 страницы.

Основная часть. Основная часть включает два – три раздела.

Первый раздел носит обычно просветительский характер и посвящен описанию основных положений, методов, способов и подходов, используемых для решения поставленной задачи. В этот раздел включается только то, что необходимо в качестве исходной основы для понимания сути проведенных исследований, описанных в последующих разделах. Остальные разделы содержат конкретные результаты исследований.

Заключение должно содержать краткие выводы по результатам выполнений работы. Типовой объем заключения составляет 1-2 страницы.

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

Приложения. В приложения рекомендуется включать материалы, связанные с выполненной работой, которые по каким-либо причинам не могут быть включены в основную часть. Все приложения нумеруются и располагаются в конце пояснительной записки в порядке ссылок на них. Каждое приложение начинается с новой страницы и имеет содержательный заголовок. При необходимости текст приложения может быть разбит на разделы, подразделы, пункты и подпункты, которые следует нумеровать в пределах каждого приложения в соответствии с требованиями для основной части записки.

Общий объем реферат составляет до 24 страниц (без приложений). Не следует объем делать более 30 страниц (с приложениями).

При изложении текста реферата следует руководствоваться ГОСТ 7.32-2017 «Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления».

Реферат оформляется в редакторе Word, шрифт Times New Roman размер – 12-14 интервал – полуторный (30 строк по 60 печатных знаков в каждой строке, считая пробелы). Размеры полей следующие: левое – 30 мм, правое — не менее 10 мм, верхнее - не менее 20 мм, нижнее — не менее 20 мм. Отступ красной строки 1,25 см.

Изложение реферата должно быть выдержано в строгом литературном стиле, принятом для научно-технических отчетов и научных публикаций. Не следует использовать жаргоны и вульгаризмы. Это относится как к авторскому тексту, так и к текстам, заимствованным из различных не рецензируемых и не проходящих корректуру электронных публикаций в Internet. Не следует в пределах реферата применять для одних и тех же понятий различные термины. Нежелательно также применение иностранных слов и терминов при наличии равнозначных общепринятых в данной области русскоязычных слов и терминов. При первом упоминании термина его синонимы, используемые в данной области, можно перечислить, а затем пользоваться только одним из них. Следует использовать только общепринятые аббревиатуры, сокращения, условные обозначения, символы, единицы и термины.

Рефераты размещаются в разделе «Портфолио» электронной информационной обра-

зовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11.3. 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, доклады с рефератами), 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

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
2	Практическое занятие (семинар) № 1	5	3
4	Практическое занятие (семинар) № 2	5	3
6	Практическое занятие (семинар) № 3	5	3
6	Компьютерный тест (КТ-1)	5	2
8	Практическое занятие (семинар) № 4	5	3
10	Практическое занятие (семинар) № 5	5	3
12	Практическое занятие (семинар) № 6	5	3
12	Компьютерный тест (КТ-2)	5	2
14	Практическое занятие (семинар) № 7	5	3
16	Практическое занятие (семинар) № 8	5	3
16	Компьютерный тест (КТ-3)	5	2
16	Посещаемость, активность	5	2
17	Реферат	12	4
	Итого за текущий контроль	***72***	***36***
	Итоговый контроль	***28***	***14***
	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

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

РАЗРАБОТЧИК

Профессор кафедры «Информационная безопасность»
доктор технических наук, доцент _____ /Душкин А.В. /

Рабочая программа дисциплины «Политические и социальные аспекты 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 /