

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиоп физики и радиоэлектроники



УТВЕРЖДАЮ
Декан физического факультета
/ Н.М. Буднев
2021 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.ДВ.01.02 «Основы информационного противоборства»**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Техническая защита информации**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК:
физического факультета
Протокол № 30 от « 31 » августа 2021 г.

Председатель: д.ф.-м.н., профессор
Н.М. Буднев

Рекомендовано кафедрой
радиоп физики и радиоэлектроники:

Протокол № 1 от «30» августа 2021 г.

И.о.зав.кафедрой
С.Н.

Колесник

Иркутск 2021 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	3
II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО	3
III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	3
IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ	5
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов	5
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине....	7
4.3. Содержание учебного материала	11
4.3.1. Перечень семинарских, практических занятий и лабораторных работ	11
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС).....	13
4.4. Методические указания по организации самостоятельной работы студентов..	14
4.5. Примерная тематика курсовых работ	15
V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	15
VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	15
6.1. Учебно-лабораторное оборудование:	15
6.2. Программное обеспечение:	15
6.3. Технические и электронные средства:	15
VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	16
VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ	16

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Учебная дисциплина «Основы информационного противоборства» обеспечивает формирование углубленного понимания значения информации в современных условиях и знаний в области информационной безопасности автоматизированных систем.

Цели:

- формирование представления и знаний о развитии информационных войн и их влиянии на информационную безопасность;
- формирование умений противостоять информационным атакам, регулировать информационные потоки, осознавать социальную ответственность будущей профессиональной деятельности.

Задачи:

- понимание методов формирования общественного мнения о государственных и частных, коммерческих и некоммерческих организациях, общественных явлениях;
- изучение принципов защиты информации в условиях информационного противоборства;
- подготовка к решению организационно-управленческих, коммуникационных и иных информационных задач.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.В.ДВ.01.02 Основы информационного противоборства относится к части программы, формируемой участниками образовательных отношений. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

Психология социального взаимодействия, саморазвития и самоорганизации

Основы информационной безопасности

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

Организационное и правовое обеспечение информационной безопасности

Психология личности и профессиональное самоопределение

При подготовке специалистов по разработке и эксплуатации современных автоматизированных средств, необходимо уделять особое внимание изучению современного методов ведения и способов противодействия информационным войнам.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-2. Способен проводить анализ уязвимостей системы защиты информации и автоматизированных систем.	ИДК _{ПК2.1} Проводит анализ уязвимостей системы защиты информации	Знать: - основные принципы информационной войны, виды информационного оружия, средства его разработки и методы анализа; - основные методы
	ИДК _{ПК2.2} Проводит анализ уязвимостей автоматизированных систем	

	<p>ИДК_{ПК3.2} Выбирает организационные меры по защите информации в автоматизированных системах.</p>	<p>оценки поражающих факторов информационного оружия, надежных средствах констатации его применения;</p> <p>Уметь:</p> <ul style="list-style-type: none"> - разрабатывать специальные информационные мероприятия и применять их для защиты информации; - оценивать риски и оправданность применения специальных информационных мероприятий; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками быстрого и эффективного отбора исходных материалов для подготовки специальных информационных мероприятий; - навыками быстрого распознавания проводимой информационной войны и определения ее субъектов;
--	--	---

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетных единицы, 144 часа,
 в том числе _____ зачетных единиц, _____ часов на экзамен
 Из них __ часов – практическая подготовка

Форма промежуточной аттестации: Зачет

(экзамен, зачет, зачет с оценкой)

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/п	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)			Самостоятельная работа	Форма текущего контроля успеваемости	
					Контактная работа преподавателя с обучающимися					
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация			
1	2	3	4	5	6	7	8	9	10	
1	Раздел 1. Информационные войны в современном мире.									
2	Тема 1.1. Информационные войны в структуре современной цивилизации	7	15		2	6		14	Устный опрос, письменный опрос на практических занятиях Защита лабораторной	

									работы
3	Тема 1.2. Модель информационной войны и информационные кампании.	7	15		2	6		16	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы
5	Раздел 2. Способы и средства информационной войны.								
6	Тема 2.1. Информационные войны в мирное и военное время.	7	15		2	6		16	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы
7	Тема 2.2. Инструментарий информационной войны.	7	18		2	8		14	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы
9	Раздел 3. Информационная безопасность в условиях информационной войны.								
10	Тема 3.1. Информационная война в интернете и средствах массовой информации.	7	16		2	6		11	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы

11	Тема 3.2. Информационная составляющая национальной безопасности.	7	16		2	6		14	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы
----	--	---	----	--	---	---	--	----	---

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
7	Тема 1.1. Информационные войны в структуре современной цивилизации	Работа с учебником, справочной литературой, первоисточниками, конспектом	1-ая неделя	14	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
7	Тема 1.2. Модель информационной войны и информационные кампании.	Работа с учебником, справочной литературой, первоисточниками, конспектом	4-ая неделя	16	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
7	Тема 2.1. Информационные войны в мирное и военное время.	Работа с учебником, справочной литературой, первоисточниками, конспектом	8-ая неделя	16	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
7	Тема 2.2. Инструментарий информационной войны.	Работа с учебником, справочной литературой, первоисточниками, конспектом	12-ая неделя	14	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
7	Тема 3.1. Информационная война в интернете и средствах массовой информации.	Работа с учебником, справочной литературой, первоисточниками, конспектом	16-ая неделя	11	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
7	Тема 3.2. Информационная составляющая национальной безопасности.	Работа с учебником, справочной литературой, первоисточниками, конспектом	19-ая неделя	14	Устный опрос, письменный опрос на практических занятиях	Источники 1-4 из основной и 1-3 из дополнительной литературы. Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ
Общий объем самостоятельной работы по дисциплине (час)				81		

4.3. Содержание учебного материала

Раздел 1. Информационные войны в современном мире.

Тема 1.1. Информационные войны в структуре современной цивилизации.

История информационного противоборства. Становление информационного общества. Понятие «информационная война». Отличия информационной войны от войн, ведущихся традиционными средствами.

Тема 1.2. Модель информационной войны и информационные кампании.

Модели управления общественным мнением. Уровни информационного воздействия. Модель переноса экономической нестабильности в политическую. Молодежь как целевая группа информационных войн. Законы и принципы ведения информационных войн. Информационное воздействие на личность. Информационно-психологические операции, как организационная форма реализации концепции информационной войны.

Раздел 2. Способы и средства информационной войны.

Тема 2.1. Информационные войны в мирное и военное время.

Основные технологии информационных войн. Информационно-психологическое воздействие на кризисные ситуации, социально-политические конфликты. Терроризм как инструмент информационной войны. Особенности информационных войн в мирное и военное время.

Тема 2.2. Инструментарий информационной войны.

Классификация информационного оружия: наступательное и оборонительное, информационно-психологическое и информационно-техническое. Средства поражения техники, программного обеспечения, каналов связи. Особенности информационного оружия. Борьба за контроль и использование информационного пространства.

Раздел 3. Информационная безопасность в условиях информационной войны.

Тема 3.1. Информационная война в интернете и средствах массовой информации.

СМИ и Интернет как информационное оружие. Способы и средства отражения информационного нападения в Интернет. Тематические интернет-форумы, как целевые аудитории информационных войн. Особенности восприятия информации в зависимости от типа СМИ. Средства поражения техники, программного обеспечения, каналов связи.

Тема 3.2. Информационная составляющая национальной безопасности.

Глобализация мира и информационная война. Возможные угрозы суверенитету и национальной безопасности. Информационная безопасность государства. Основные направления государственной политики в информационной сфере. Стратегия запрета информации. Понятие и значение информационной безопасности в структуре национальной безопасности.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	Раздел 1. Информационные войны в современном мире. Тема 1.1. Информационные войны в структуре современной цивилизации.	ПЗ. 1. Виды информационных войн. ЛР. 1. Исторические исследования	2 4	4	Устный опрос, письменный опрос на практических занятиях Защита	ПК-2

	ые войны в структуре современной цивилизации.	информационных войн			лабораторной работы	
2	Тема 1.2. Модель информационной войны и информационных кампаний.	ПЗ. 2. Информационно - психологическая война в современном мире. ЛР 2. Обнаружение и нейтрализации пропагандистских кампаний.	2 4	2 4	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы	ПК-2
3	Раздел 2. Способы и средства информационной войны. Тема 2.1. Информационные войны в мирное и военное время.	ПЗ 3. «Холодная война»: анализ информационного противостояния двух систем. ЛР 3. Исследование эффективности информационного пространства.	2 4	4	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы	ПК-2
4	Тема 2.2. Инструментарий информационной войны.	ПЗ. 4. Анализ способов и средств информационной войны. ЛР 4. Исследование характеристик информационного оружия.	2 6	2 4	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы	ПК-3
5	Раздел 3. Информационная безопасность в условиях информационной войны. Тема 3.1. Информационная война в интернете и средствах массовой информации.	ПЗ 5. Информационные войны в интернет и манипуляции в СМИ ЛР 5. Влияние новых информационных технологий на картину мира современного человека.	2 4		Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы	ПК-3

6	Тема 3.2. Информационная составляющая национальной безопасности.	ПЗ 6. Способы и эффективность защиты от информационного оружия. ЛР 6. Исследование способов защиты от информационного оружия и их эффективности.	2	2	Устный опрос, письменный опрос на практических занятиях Защита лабораторной работы	ПК-3
			4	4		

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	2	3	4	5
1	Тема 1.1. Информационные войны в структуре современной цивилизации.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет ресурсов -	ПК-2	ИДК _{ПК2.1} ИДК _{ПК2.2}
2	Тема 1.2. Модель информационной войны и информационные кампании.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет ресурсов -	ПК-2	ИДК _{ПК2.1} ИДК _{ПК2.2}
3	Тема 2.1. Информационные войны в мирное и военное время.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта	ПК-2	ИДК _{ПК2.1} ИДК _{ПК2.2}

		лекций, литературы, Интернет ресурсов	-		
4	Тема 2.2. Инструментарий информационной войны.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет ресурсов	-	ПК-3	ИДК _{ПК3.1} ИДК _{ПК3.2}
5	Тема 3.1. Информационная война в интернете и средствах массовой информации.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет ресурсов	-	ПК-3	ИДК _{ПК3.1} ИДК _{ПК3.2}
6	Тема 3.2. Информационная составляющая национальной безопасности.	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет ресурсов	-	ПК-3	ИДК _{ПК3.1} ИДК _{ПК3.2}

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе, которой студент активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. В процессе проведения самостоятельной работы формируются компетенции ПК-2, ПК-3.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Тема 1.1. Информационные войны в структуре современной цивилизации (7 ч).
Проработка лекционного материала и материала практического занятия (7 ч).

Тема 1.2. Модель информационной войны и информационные кампании (7 ч).
Проработка лекционного материала и материала практического занятия (7 ч).

Тема 2.1. Информационные войны в мирное и военное время (7 ч). Проработка лекционного материала и материала практического занятия (7 ч).

Тема 2.2. Инструментарий информационной войны (8 ч). Проработка лекционного материала и материала практического занятия (8 ч).

Тема 3.1. Информационная война в интернете и средствах массовой информации (8 ч).
Проработка лекционного материала и материала практического занятия (8 ч).

Тема 3.2. Информационная составляющая национальной безопасности (8 ч).
Проработка лекционного материала и материала практического занятия (8 ч).

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Воронова О. Е. Современные информационные войны: типология и технологии: монография: Рязанский государственный университет имени С. А. Есенина, 2018, - 188 с. <https://e.lanbook.com/book/164490>.

2. Лингвистика информационно-психологической войны. Книга II: Монография / А. А. Бернацкая и др. Сибирский Федеральный Университет, 2019, - 488 с. <https://e.lanbook.com/book/157702>.

3. Лингвистика информационно-психологической войны. Книга III: Монография / А. А. Бернацкая и др. Сибирский Федеральный Университет, 2020, - 344 с. <https://e.lanbook.com/book/181614>.

б) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.

2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

6.2. Программное обеспечение:

1. Microsoft PowerPoint

2. Microsoft Windows.

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия 1-6 проводятся в интерактивной форме.

Наименование тем занятий с указанием форм/ методов/ технологий обучения:

№ п/п	Тема занятия	Вид занятия	Форма / Методы//технологии дистанционного, интерактивного обучения	Количество часов
1	2	3	4	5
1	Виды информационных войн.	Практическое занятие	Дискуссия	2
2	Информационно-психологическая война в современном мире.	Практическое занятие	Дискуссия	2
3	«Холодная война»: анализ информационного противостояния двух систем.	Практическое занятие	Дискуссия	2
4	Анализ способов и средств информационной войны.	Практическое занятие	Дискуссия	2
5	Информационные войны в интернет и манипуляции в СМИ	Практическое занятие	Дискуссия	2
6	Способы и эффективность защиты от информационного оружия.	Практическое занятие	Дискуссия	2
Итого часов:				12

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

№	Вид контроля	Контролируемые темы (разделы)	Контролируемые компетенции/ индикаторы
1	2	3	4
1	Текущий контроль	Тема 1.1. Информационные войны в структуре современной цивилизации.	ПК-2 ИДК _{ПК2.1} ИДК _{ПК2.2}
2	Текущий контроль	Тема 1.2. Модель информационной войны и информационные кампании.	ПК-2 ИДК _{ПК2.1} ИДК _{ПК2.2}
3	Текущий контроль	Тема 2.1. Информационные	ПК-2 ИДК _{ПК2.1}

		войны в мирное и военное время.	ИДК _{ПК2.2}
4	Текущий контроль	Тема 2.2. Инструментарий информационной войны.	ПК-3 ИДК _{ПК3.1} ИДК _{ПК3.2}
5	Текущий контроль	Тема 3.1. Информационная война в интернете и средствах массовой информации.	ПК-3 ИДК _{ПК3.1} ИДК _{ПК3.2}
6	Текущий контроль	Тема 3.2. Информационная составляющая национальной безопасности.	ПК-3 ИДК _{ПК3.1} ИДК _{ПК3.2}
7	Промежуточный контроль - Зачет	Разделы 1-3	ПК-2 ИДК _{ПК2.1} ИДК _{ПК2.2} ПК-3 ИДК _{ПК3.1} ИДК _{ПК3.2}

8.1. Оценочные материалы (ОМ)

8.1.1. Оценочные материалы для входного контроля

Не предусмотрено

8.1.2 Оценочные материалы текущего контроля

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ6. Текущий контроль направлен на выявление сформированности компетенций ПК-2, ПК-3. Для реализации текущего контроля используется балльно-рейтинговая система оценки, принятая в университете.

Усвоение студентом изучаемой дисциплины максимально оценивается 100 баллами. Максимальное количество баллов за текущую работу в семестре ограничивается 60-ю баллами, на оценку экзамена максимально предусмотрено 30 баллов. Возможны «премиальные» баллы (от 0 до 10), которые могут быть добавлены студенту за активные формы работы, высокое качество выполненных практических работ и т.д.

За посещение одного вида занятия дается 1.1 балла (23 занятия (Л+Пз) * 1.13 балл = 25.99 балла), максимальное количество баллов за письменный контроль на ЛР и Пз – 2.1 балла (10 занятий (ПЗ)*2.1 балл = 21 балл).

Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ6.

Критерии оценки	Оценка / баллы			
	Отлично 2.1 балла.	Хорошо 1.4 балла	Удовлетв. 0.7 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и

				допущено более 3-х ошибок.
--	--	--	--	----------------------------

Вопросы для письменного текущего контроля приведены ниже:

- Пз. 1 Разновидности информационных войн и их особенности.
- Пз. 2 1. Примеры пропагандистских кампаний, цели и результаты.
2. Отличительные черты информационно-психологической войны в современном мире.
- Пз. 3 Анализ информационного противостояния в «Холодной войне», результаты и уроки.
- Пз. 4 Что разрушает информационное оружие?
- Пз. 5 1. Объекты и результаты воздействия в информационной войне.
Влияние новых информационных технологий на проведение информационной войны.
- Пз.6 Инструменты отражения информационного нападения в Интернет.
Оценка эффективности защиты от информационного оружия.
Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ6.

Критерии оценки	Оценка / баллы			
	Отлично/ 2.1 балла.	Хорошо/ 1.4 балла	Удовлетв. / 0.7 балла.	Неудовл. / 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок.

8.1.3 Оценочные материалы для промежуточной аттестации

Промежуточная аттестация проводится в форме зачета. Форма проведения зачета – устный по билетам или письменный по билетам. Зачеты проводятся во время экзаменационных сессий в соответствии с расписанием.

Экзаменационный билет состоит из двух теоретических вопросов и одного практического. Экзаменационные задания (билеты) для приема экзаменов выполнены многовариантными, чтобы исключить возможность списывания и обмена информацией в ходе экзамена. Вопросы для самостоятельной подготовки студентов к экзамену приведены в приложении 1.

Студент допускается к экзамену в том случае, если в течение семестра за текущую работу набрано 40 баллов и более. В противном случае выставляется 0 сессионных баллов. Во время экзамена студент может набрать до 30 баллов. Если на экзамене ответ студента оценивается менее чем 10-ю баллами, то экзамен считается не сданным, студенту выставляется 0 баллов, а в ведомость выставляется оценка «неудовлетворительно».

Если на экзамене студент набирает 10 и более баллов, то они прибавляются к сумме баллов за текущую работу и переводятся в академическую оценку, которая фиксируется в ведомости и зачетной книжке студентов.

Итоговый семестровый рейтинг	Академическая оценка
60-70 баллов	«удовлетворительно»
71-85 баллов	«хорошо»
86-100 баллов	«отлично»

Преподаватель имеет право выставить экзаменационную оценку (с согласия студента) без процедуры сдачи экзамена, если сумма баллов, набранная студентом за текущую работу составит 70 баллов. В этом случае к набранному студентом количеству баллов за текущую работу автоматически добавляется 20 баллов и выставляется соответствующая академическая оценка.

Критерии	Оценка			
	Отлично	Хорошо	Удовлетв.	Неудовлетв.
Знание	Всесторонние глубокие знания (10 -11 баллов)	Знание материала в пределах программы (7 -9 баллов)	Отмечены пробелы в усвоении программного материала (4 -6 баллов)	Не знает основное содержание дисциплины (0-3 балла)
Понимание	Полное понимание материала, приводит примеры, дополнительные вопросы не требуются (8 -10 баллов)	Понимает материал, приводит примеры, но испытывает затруднения с выводами, однако достаточно полно отвечает на дополнительные вопросы (6 -8 баллов)	Суждения поверхностны, содержат ошибки, примеры не приводит, ответы на дополнительные вопросы неуверенные (4 -6 баллов)	С трудом формулирует свои мысли, не приводит примеры, не дает ответа на дополнительные вопросы (0-3 балла)
Применение проф. терминологии	Дает емкие определения основных понятий, корректно использует профессиональную терминологию (3-5 баллов)	Допускает неточности в определении понятий, не в полном объеме использует профессиональную терминологию (2-3 балла)	Путает понятия, редко использует профессиональную терминологию (1-2 балла)	Затрудняется в определении основных понятий дисциплины, некорректно использует профессиональную терминологию (0-2 балла)
Соблюдение норм литературного языка	Соблюдает нормы литературного языка, преобладает научный стиль изложения (3-4 балла)	Соблюдает нормы литературного языка, допускает единичные ошибки (2-3 балла)	Допускает множественные речевые ошибки при изложении материала (1-2 балл)	Косноязычная речь искажает смысл ответа (0-1 балл)

Демонстрационный вариант теста

Тестовые вопросы для проверки сформированности компетенции

ПК-2. Способен проводить анализ уязвимостей системы защиты информации и

автоматизированных систем.

1. Не являются методами информационной войны ...

- | | | |
|----|----------------------|-------------|
| А) | деятельность | хакеров |
| Б) | террористические | провокации |
| В) | электронно-магнитное | воздействие |

2. Внутренние источники угроз информационной безопасности Российской Федерации (укажите все правильные варианты ответов)

- А) снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- Б) недостаточный государственный контроль за развитием информационного рынка;
- В) разработка рядом государств концепции информационных войн

3. Информационная война – это ...

- А) действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты
- Б) любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты
- В) любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты

4. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

- А) информационная война
- Б) информационное оружие
- В) информационное превосходство

5. Поражающее воздействие информационного оружия, прежде всего направлено на

- А) информационные системы
- Б) мозг человека
- В) информационные продукты

6. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

- А) информационная война
- Б) информационное оружие
- В) информационное превосходство

7. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:

- А) Защита информации
- Б) Безопасность
- В) Информационная безопасность

8. Возможность сбора, обработки и распространения непрерывного потока информации при восприятии использования информации противником это:

- А) Информационная война
- Б) Информационное оружие
- В) Информационное превосходство

9. Внешние источники угроз информационной безопасности Российской Федерации... (укажите все правильные варианты ответов)

- А) увеличение технологического отрыва ведущих стран мира, их противодействие созданию конкурентоспособных информационных технологий
- Б) недостаточная экономическая мощь государства
- В) обострение международной конкуренции за обладание информационными технологиями и ресурсами

10. К национальным интересам РФ в информационной сфере относятся:

- А) Реализация конституционных прав на доступ к информации
- Б) Политическая экономическая и социальная стабильность
- В) Сохранение и оздоровлении окружающей среды

11. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие? (укажите все правильные варианты ответов)

- А) Информационный саботаж
- Б) Физический саботаж
- В) Информационные инфекции

12. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:

- А) Информационная безопасность
- Б) Защита информации
- В) Национальная безопасность

ПК-3. Способен внедрять организационные меры по защите информации в автоматизированных системах.

1. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

- А) Безопасность АС
- Б) Угрозы информационной безопасности
- В) Политика безопасности

2. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений

- А) Информационная сфера
- Б) Информационные услуги
- В) Информационные продукты

3. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками...»

- А) Информация с ограниченным доступом

- Б) Информация, распространение которой наносит вред интересам общества
- В) Объект интеллектуальной собственности

4. Защищенность от негативных информационно-психологических и информационно-технических воздействий:

- А) Защита информации
- Б) Компьютерная безопасность
- В) Защищенность потребителей информации

5. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:

- А) Интересы личности в информационной сфере
- Б) Интересы общества
- В) Интересы общества в информационной сфере

6. Какова основная цель коммерческих информационных агентств?

- А) Получение и продажа информации;
- Б) Оперативное донесение достоверной информации до власти и общественности;
- В) Развитие образования и повышение интеллектуального уровня населения.

7. Меняет ли полученная людьми информация на их повседневное поведение?

- А) Нет, не меняет, за исключением рекламного воздействия на индивидов;
- Б) Да, меняет, хотя люди не всегда это ясно осознают;
- В) Слабо меняет под воздействием отечественного и зарубежного кино.

8. Что понимается под термином «независимый источник информации»?

- А) информатор из финансовых кругов, обладающий инсайдерскими данными.
- Б) информатор из состава спецслужб иностранного государства;
- В) информатор, лично не заинтересованный в замалчивании или приукрашивании передаваемых в СМИ сведений;

9. Является ли сознательное искажение информации об истории государства правонарушением?

- А) государства является правонарушением, тяжесть которого зависит от намерений лица (или лиц), фальсифицирующих историю и распространяющих данные сведения;
- Б) является шуткой, пародией и не считается правонарушением;
- В) является троллингом ответственных лиц;

10. Является ли детское кино и мультфильмы инструментом воспитания детей и юношества?

- А) Нет, не является, поскольку мультфильмы, а также кинокартины для детей и юношества не несут в себе чуждых ценностей;
- Б) Детское кино и мультфильмы воспитывают и перевоспитывают людей среднего возраста и пенсионеров;
- В) Да, является, поскольку в детском и юношеском возрасте наиболее активно формируется характер, ценности человека;

11. Являются ли вредоносные программы информационным продуктом?

- А) Да, являются, поскольку могут быть объектом купли-продажи на информационных рынках;
- Б) Нет, не являются, поскольку компьютерные программы не являются товаром, предназначенном для реализации;

В) Вредоносные программы предназначены для причинения ущерба или вымогательства денежных средств, а не для продажи всем желающим, поэтому информационным продуктом не являются.

12. Помогает ли адекватное управление информацией поддерживать конкурентоспособность государствам, компаниям, силовым структурам, физлицам?

А) Нет, не помогает, поскольку конкурентоспособность государства и компаний зависит от силы армии, мощи экономики, имиджа и репутации на мировой арене;

Б) Должным образом подобранная конфиденциальная информация помогает телефонным мошенникам обманывать рядовых граждан;

В) Да, помогает, поскольку правильно подобранная информация необходима в рекламе, пропаганде, продвижении торговых марок, в формировании имиджа людям и событиям;

Примерный перечень вопросов и заданий к зачету

1. Информационные войны в структуре современной цивилизации
2. Статус информации в современной информационной цивилизации.
3. Модели управления общественным мнением.
4. Междисциплинарный характер проблематики информационных войн.
5. Информационная борьба и информационная безопасность.
6. Информационный суверенитет государства.
7. Информационная война как коммуникативная технология.
8. Дестабилизирующая информация.
9. Цели и роль новых моделей поведения информационных войн.
10. Информационная кампания.
11. Информационная война и методы планирования кампании.
14. Методы создания резонанса в информационной кампании.
15. Классификации целевой аудитории информационной кампании.
16. Холодная война СССР-США как пример информационной войны.
17. Рост возможностей информационного воздействия на массовое сознание.
18. Отличие категории информационная война от категории психологическая война.
19. Примеры успешных информационных войн в современном мире.
20. Модель переноса экономической нестабильности в политическую.
21. Информационно-культурная агрессия, отбор информационных сообщений для СМИ.
22. Молодежь как целевая группа информационных войн.
23. Отличие войны в обычном понимании этого термина и войны информационной.
24. Факторы увеличения эффективности информационной операции.
25. Информационные операции как часть военной стратегии государства.
26. Информационная составляющая национальной безопасности
27. Возможные угрозы суверенитету и национальной безопасности.
28. Информационная безопасность государства.
29. Основные направления государственной политики в информационной сфере.
30. Информационное пространство государства: потоки формирования
31. Информационная безопасность: контроль, санкции, креативность, позитив.
32. Пропагандистские кампании
33. Инструментарий информационной войны
34. Новые возможности использования информации в современном обществе.
35. Роль техники и СМИ в информационной войне.
36. Свойства информационного пространства и построение инструментария.
37. Трансформаторы информационного пространства.

38. Информационное оружие в контексте основных видов коммуникативного воздействия
39. Особенности информационного оружия
40. Особенности ведения информационной войны в Интернете.
41. Информационное оружие и возможности нового этапа развития цивилизации.
42. Борьба за контроль и использование информационного пространств.
43. Характеристики информационного оружия.

Разработчики:



(подпись) профессор _____ Ерохин В.В. _____
(занимаемая должность) (Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «30» августа 2021 г. Протокол № 1

И.О. зав. кафедрой  Колесник С.Н.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.