МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
Технологий обработки и защиты информации
А.А. Сирота

_____
03.05.2023.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.44 Гуманитарные аспекты информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

направленность (профиль) № 1 "Безопасность компьютерных систем" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация выпускника: Бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Филиппова Неля Викторовна, к.ю.н, доцент

7. Рекомендована: протокол НМС № 7 от 03.05.2023

8. Учебный год: 2024-2025 **Семестр(ы)/Триместр(ы):** 4

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:
изучение теоретических основ гуманитарных аспектов информационной безопасности, а также овладение практическими навыками применения методов и способов обеспечения информационно-психологической безопасности личности, общества и государства.
Задачи дисциплины:
– усвоение обучающимися системы понятий и категорий в области гуманитарных аспектов информационной безопасности личности, общества и государства;
– привитие навыков и умений правильного выявления угроз информационно-психологического воздействия и манипулирования сознанием;
- привитие навыков и умений обоснованного применения методов и способов обеспечения информационно-психологической безопасности;
- формирование у обучающихся практических навыков анализа и оценки гуманитарных аспектов информации, ее политического, правового, экономического и социального содержания с позиции общенациональной безопасности государства.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относиться к обязательной части Блок 1. Дисциплины (модули).

Входные знания в области основ информационной безопасности.

Дисциплина является предшествующей для дисциплины «Техническая защита информации».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
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-1.5	знает основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире	Знать: понятия в области информационного управления, информационного воздействия, их роль в информационном обществе, основные типы и содержание технологий информационного воздействия, информационные операции в сети Интернет, основные положения государственной политики Российской Федерации в области информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире Уметь: определять и классифицировать субъекты, объекты и источники угроз информационно безопасности, информационные воздействия в различных коммуникативных ситуациях; использовать технологии скрытого управления личностью и обществом с помощью информационных воздействий, применять способы психологической самозащиты; Владеть: навыками информационного управления информационной безопасностью, способами манипулирования в массовых информационных процессах; навыками применения моделей, ресурсов, технологий защиты от информационных воздействий.

12. Объем дисциплины в зачетных единицах/час. — 3/108.

Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра - 4	№ семестра	итого
Аудиторные занятия		50	50		50
в том числе:	лекции	16	16		16
	практические	34	34		34
	лабораторные				
Самостоятельная работа		22	22		22
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – 36 час.)*		36	36		36
Итого:		108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Место и роль проблем информационной безопасности в становлении современного информационного общества.	Предмет, цели, методы изучения дисциплины «Гуманитарные аспекты информационной безопасности» и рекомендованная литература. Понятийный аппарат гуманитарных аспектов информационной безопасности. Информационная безопасность: краткая характеристика основных гуманитарных проблем. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации.	
1.2	Информационное общество в России: стратегия развития и перспективы.	Глобальное информационное общество: основные понятия и история становления и развития. Роль Интернета и других информационно-коммуникационных технологий. Проблемы цифрового разрыва и пути решения. Результаты на современном этапе. Стратегии развития информационного общества в Российской Федерации. Правовая основа развития информационного общества в Российской Федерации. Информационно-телекоммуникационная инфраструктура информационного общества. Информационная сфера как системообразующий фактор жизни общества. Основные направления обеспечения безопасности в информационном обществе.	
1.3	Концептуальные основы информационной безопасности России.	Содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность». Национальная безопасность России в условиях информационного общества. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Понятие международной информационной безопасности. Информационные угрозы, интересы РФ в информационной сфере, информационное противоборство, информационное противодействие.	
1.4	Основные понятия теории систем и системного ана-	История развития теории систем и системного анализа	

	лиза	Основные элементы теории систем и системного анализа Семья как элемент государственной системы	
1.5	Сознание человека как объект угроз информационного воздействия и манипулирования	Мысль, мышление, способности и виды мышления. Особенности творческого мышления, сравнение, анализ и синтез. Мышление и язык. Особенности строения головного мозга человека История изучения воздействия СМИ. Тенденции освещения экстремальных событий в СМИ. Способы привлечения массовой и специализированной аудиторий. Манипуляция сознанием, признаки выявления манипуляции Манипуляция сознанием в деструктивных культах и техника религиозной безопасности. Понятие и структура информационно-психологической безопасности. Субъекты, объекты и источники угроз информационно-психологической безопасности.	
1.6	Основные технологии информационно-психологического воздействия	Психологическое воздействие как средство управляющего воздействия в социальных системах. Виды информационно-психологического воздействия. Технологии информационно-психологического воздействия в массовых информационных процессах. Технологии информационного воздействия как инструмент социального управления в системе государственной информационной политики. Информационно-психологические конфликты в современном информационном обществе: условия, тенденции и закономерности возникновения и эволюционного развития острых конфликтных ситуаций в сфере информационно-психологических отношений. Основные этапы возникновения и развития конфликтов в современном информационном обществе. Информационно-психологический конфликт как средство достижения политических целей. Информационно-психологическая безопасность современного информационного общества.	
1.7	Информационно-психологическая война как средство манипуляции общественным сознанием	Информационно-психологическая война как социальное явление. Эволюция политических форм, средств и методов информационно-психологического противоборства. Информационно-психологическая война как форма эскалации межгосударственных конфликтов. Виды информационной войны. Средства и способы ведения информационно-психологической войны. Информационное оружие. Информационные войны в сети Интернет. Основные теории информационных войн. Общие понятия о принципах информационной защиты.	
1.8	Основы обеспечения информационно-психологической безопасности личности	Общие сведения об информационно-психологической защите личности. Основные направления обеспечения информационно-психологической безопасности личности. Понятие и виды психологической защиты личности. Понятие и структура системы психологической защиты личности. Основные формы психологической самозащиты. Способы повышения стрессоустойчивости личности.	
2. Практические занятия			
2.1	Место и роль проблем	Предмет, цели, методы изучения дисциплины «Гу-	

	информационной безопасности в становлении современного информационного общества.	манитарные аспекты информационной безопасности» и рекомендованная литература. Понятийный аппарат гуманитарных аспектов информационной безопасности. Информационная безопасность: краткая характеристика основных гуманитарных проблем. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации.	
2.2	Информационное общество в России: стратегия развития и перспективы.	Глобальное информационное общество: основные понятия и история становления и развития. Роль Интернета и других информационно-коммуникационных технологий. Проблемы цифрового разрыва и пути решения. Результаты на современном этапе. Стратегии развития информационного общества в Российской Федерации. Правовая основа развития информационного общества в Российской Федерации. Информационно-телекоммуникационная инфраструктура информационного общества. Информационная сфера как системообразующий фактор жизни общества. Основные направления обеспечения безопасности в информационном обществе.	
2.3	Концептуальные основы информационной безопасности России.	Содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность». Национальная безопасность России в условиях информационного общества. Стратегия национальной безопасности РФ. Доктрина информационной безопасности РФ. Понятие международной информационной безопасности. Информационные угрозы, интересы РФ в информационной сфере, информационное противоборство, информационное противодействие.	
2.4	Основные понятия теории систем и системного анализа	История развития теории систем и системного анализа Основные элементы теории систем и системного анализа Семья как элемент государственной системы	
2.5	Сознание человека как объект угроз информационного воздействия и манипулирования	Мысль, мышление, способности и виды мышления. Особенности творческого мышления, сравнение, анализ и синтез. Мышление и язык. Особенности строения головного мозга человека История изучения воздействия СМИ. Тенденции освещения экстремальных событий в СМИ. Способы привлечения массовой и специализированной аудиторий. Манипуляция сознанием, признаки выявления манипуляции Манипуляция сознанием в деструктивных культах и техника религиозной безопасности. Понятие и структура информационно-психологической безопасности. Субъекты, объекты и источники угроз информационно-психологической безопасности.	
2.6	Основные технологии информационно-психологического воздействия	Психологическое воздействие как средство управляющего воздействия в социальных системах. Виды информационно-психологического воздействия. Технологии информационно-психологического воздействия в массовых информационных процессах. Технологии информационного воздействия как ин-	

		струмент социального управления в системе государственной информационной политики. Информационно-психологические конфликты в современном информационном обществе: условия, тенденции и закономерности возникновения и эволюционного развития острых конфликтных ситуаций в сфере информационно-психологических отношений. Основные этапы возникновения и развития конфликтов в современном информационном обществе. Информационно-психологический конфликт как средство достижения политических целей. Информационно-психологическая безопасность современного информационного общества.	
2.7	Информационно-психологическая война как средство манипуляции общественным сознанием	Информационно-психологическая война как социальное явление. Эволюция политических форм, средств и методов информационно-психологического противоборства. Информационно-психологическая война как форма эскалации межгосударственных конфликтов. Виды информационной войны. Средства и способы ведения информационно-психологической войны. Информационное оружие. Информационные войны в сети Интернет. Основные теории информационных войн. Общие понятия о принципах информационной защиты.	
2.8	Основы обеспечения информационно-психологической безопасности личности	Общие сведения об информационно-психологической защите личности. Основные направления обеспечения информационно-психологической безопасности личности. Понятие и виды психологической защиты личности. Понятие и структура системы психологической защиты личности. Основные формы психологической самозащиты. Способы повышения стрессоустойчивости личности.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Место и роль проблем информационной безопасности в становлении современного информационного общества.	2	4		2	8
2	Информационное общество в России: стратегия развития и перспективы.	2	4		2	8
3	Концептуальные основы информационной безопасности России.	2	4		2	8
4	Основные понятия теории систем и системного анализа	2	2		2	6
5	Сознание человека как объект угроз информационного воздействия и манипулирования.	2	4		2	8
6	Основные технологии информационно-психологического воздействия.	2	8		4	14

7	Информационно-психологическая война как средство манипуляции общественным сознанием	2	4		4	10
8	Основы обеспечения информационно-психологической безопасности личности.	2	4		4	10
	Итого:	16	34		22	72

14. Методические указания для обучающихся по освоению дисциплины: 1) При освоении дисциплины рекомендуется использовать следующие средства:

- изучение рекомендуемой основной и дополнительной литературы методических указаний и пособий;
- работа с текстом конспекта лекций;
- систематическая подготовка к практическим занятиям;
- выполнение контрольных заданий для закрепления теоретического материала;
- работа с электронными версиями учебников и методических указаний для выполнения лабораторно-практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и лабораторных работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Основы информационной безопасности : учебное пособие / С.А. Нестеров .— Изд. 4-е, стер. — Санкт-Петербург ; Москва ; Краснодар : Лань, 2018 .— 321 с. : ил., табл. — (Учебники для вузов. Специальная литература) (Библиотека высшей школы) .— Библиогр.: с. 319-321.*
2	Кармановский Н.С., Михайличенко О.В., Савков С.В. Организационно-правовое и методическое обеспечение информационной безопасности / Учебное пособие. – СПб: НИУ ИТМО, 2013. – 148 с.

б) дополнительная литература:

№ п/п	Источник
1	Организационно-правовое обеспечение информационной безопасности : учеб. пособие для студ. высш. учеб. заведений / А. А. Стрельцов и др.; под ред. А. А. Стрельцова. – М.: Издательский центр «Академия», 2008. — 256 с.
2	Соловьев, А .В. Культура информационного общества [Электронный ресурс] : учеб. пособие / А. В. Соловьев. - Москва : ДиректМедиа, 2013. - 276 с. - ISBN 978-54458-3851-7.
3	Чугунов, А. В. Социальная информатика [Электронный ресурс] : учеб. и практикум для акад. бакалавриата / А. В. Чугунов. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2017. - 259 с. - (Университеты России). - ISBN 978-5-534-01233-0.
4	Бирюков В.Д., Теплов Э.П. Гуманитарные аспекты информационной безопасности: понятие о системах и функциях, управлении и системно-логических операциях анализа и синтеза. Учебное пособие. - СПб.: ГУМРФ имени адмирала С.О.Макарова, 2013.
5	Бирюков В.Д., Теплов Э.П. Информационно-психологическая война: гуманитарные аспекты. –

	СПб, 2012.
6	Бирюков В.Д., Теплов Э.П. Информационно-психологическая война: гуманитарные аспекты. – СПб, 2012.
7	Делягин М.Г. Драйв человечества. Глобализация и мировой кризис. – М., 2008.
8	Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита. - 3-е. – М, 2005. Расторгуев С.П. Информационная война. - М., 2005
9	Федоров Д.Ю. Гуманитарные аспекты информационной безопасности : учебное пособие / Д.Ю. Федоров, С.К. Морозов. – СПб. : Изд-во СПбГЭУ, 2017. – 65 с.
10	Теплов Э.П., Гатчин Ю.А., Нырков А.П., Сухостат В.В. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций: Учебное пособие. - РИО Университета ИТМО, 2016
11	Расторгуев С.П. Математические модели в информационном противоборстве: Учебное пособие М.: АНО ЦСОиП, 2014
12	Тарасов А.М. Электронное правительство и информационная безопасность: учеб. пособие М.: ГАЛАРТ, 2011
13	Ярочкин Владимир Иванович. Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин .– М. : Академический Проект, 2003.– 638,[1] с. : ил. – (Gaudeamus.Учебник для вузов).– Библиогр.: с.633-637.– ISBN 5-8291-0292-7.– ISBN 5-902357-02-0.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022 (срок предоставления с 12.01.2023 по 11.01.2024)
2	ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)
3	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)
4	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
5	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
6	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
	Справочно-информационная система «КонсультантПлюс» [Электронный ресурс]. – URL: http://www.consultant.ru.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:
1. ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2.При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет

18. Материально-техническое обеспечение дисциплины:

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 477
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 505п
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 292
Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для ви-деоконференций Logitech ConferenceCam
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380
Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17", мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 305п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 307п
Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран
ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

Перечень программного обеспечения, используемого в образовательном процессе

№ пп	Наименование ПО	Производитель ПО (или торговая марка, Или правообладатель) при наличии
	ОС Windows v.7, 8, 10	Microsoft (прим. 1)
2	СУБД Oracle Database 11g Express Edition	Oracle
3	Microsoft Visio, Access, OneNote v. 2010-2019	Microsoft
4	Visual Studio, v. 2010-2019	Microsoft
5	Набор утилит (архиваторы, файл-менеджеры)	GNU, BSD
6	ОС GNU/Linux (CentOS) v.6-8	RedHat, GNU
7	LibreOffice v.5-7	The Document Foundation, GNU
8	Среда разработки Eclipse	Eclipse Foundation
9	GlassFish Java EE	Eclipse Foundation
10	Python ver 3.8	Python Software Foundation
11	MySQL Workbench Community	GNU
12	PyCharm Community	JetBrains
13	IntelliJ IDEA	JetBrains
14	Среда разработки NetBeans IDE	ORACLE
15	Дистрибутив Anaconda/Python	BSD
16	Системы моделрования системной Динамики Vensim	Ventana Systemms Inc.
17	Системы моделирования бизнес процессов BizAgi	BizAgi
18	Системы управления проектами Wrike	Wrike Inc.
19	Системы моделирования Modelio	Modeliosoft
20	MATLAB “Total Academic Headcount – 25”	MathWorks (прим. 2)
21	HUGIN EXPERT / HUGIN Lite (open-source)	HUGIN EXPERT A/S

22	Справочно-правовая система (СПС) Консультант+ для образования	Консультант+ (прим. 7)
23	Microsoft SQL Server	Microsoft
24	Virtual Box	ORACLE
25	Microsoft Windows Virtual PC	Microsoft
26	VLC media player	VideoLAN, GNU
27	Google Workspace for Education Fundamentals (ранее G Suite for Education и Google-Apps for Education)	Google Inc.
28	SecretNet Studio 8 (демоверсия)	ООО Код Безопасности
29	Dr. Web Enterprise Security Suite	Компания «Доктор Веб» (прим. 3)
30	XSpider	Компания Positive Technologies (прим. 4)
31	СКЗИ «КриптоПро Рутокен CSP»	Компания КриптоПро (прим. 5)
32	ViPNet	ОАО ИнфоТеКС (прим. 6)
33	ERwin Data Modeler Standard Edition	CA Technologies (лицензия до 2025 г., Contract#: 40217535)
34	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License
35	PHP	PHP Group
36	Notepad++	GNU
37	PuTTY	MIT
38	Ramus Educational	Алексей Чижевский
39	ОС GNU/Linux (Ubuntu)	Canonical Ltd, GNU
40	Foxit PDF Reader	корпорация FOXIT SOFTWARE INC., проприетарная бесплатная лицензия
41	Операционная система РЕД ОС	ООО Ред Софт (прим. 9)
42	Система виртуализации РЕД Виртуализация	ООО Ред Софт (прим. 9)

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Место и роль проблем информационной безопасности в становлении современного информационного общества.	ОПК-1	ОПК-1.5	Устный опрос
2.	Информационное общество в России: стратегия развития и перспективы.	ОПК-1	ОПК-1.5	Устный опрос Тест № 1
3.	Концептуальные основы информационной безопасности России.	ОПК-1	ОПК-1.5	Устный опрос Тест № 2 Практическое задание
4.	Основные понятия теории систем и системного анализа	ОПК-1	ОПК-1.5	Устный опрос Тест № 3
5.	Сознание человека как объект угроз информационного воздействия и манипулирования.	ОПК-1	ОПК-1.5	Устный опрос Тест № 4 Практическое задание
6.	Основные технологии информационно-психологического воз-	ОПК-1	ОПК-1.5	Устный опрос Тест № 5

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	действия.			Практическое задание
7.	Информационно-психологическая война как средство манипуляции общественным сознанием	ОПК-1	ОПК-1.5	Устный опрос Тест № 6 Практическое задание
8.	Основы обеспечения информационно-психологической безопасности личности.	ОПК-1	ОПК-1.5	Устный опрос Тест № 7 Практическое задание
Промежуточная аттестация форма контроля – экзамен				Комплект КИМ

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными;

3) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Тест	Теоретические вопросы по темам/разделам дисциплины	Содержит 4 тестовых вопроса, за правильный ответ на каждый из которых дается 1 балл
3	Практическое задание	Практические задачи	Оценка «отлично» выставляется студенту, если он исчерпывающе и свободно справляется с практическими заданиями, дает правильное обоснование принятого решения; Оценка «хорошо» выставляется студенту, если он правильно, но недостаточно полно выполняет задания, не допускает существенных неточностей; Оценка «удовлетворительно» выставляется студенту, если он допускает неточности в ответе, испытывает затруднения в выполнении практических заданий, при указании на существенные ошибки может их исправить; Оценка «неудовлетворительно» выставляется студенту, если он допускает существенные ошибки и неправильно выполняет практические задания

Примерный перечень вопросов для устного опроса

1. В чем сущность гуманитарных аспектов информационной безопасности.

2. Раскройте содержание термина «информационная агрессия».

3. Что такое глобальное информационное общество.

4. Охарактеризуйте роль Интернета и других информационно-коммуникационных технологий для современного общества.

5. Охарактеризуйте основные проблемы цифрового разрыва и пути решения.

6. Каковы перспективы развития информационного общества в России.

7. Раскройте содержание термина «мышление».

8. Охарактеризуйте виды мышления.

9. Что такое манипуляция сознанием.

10. Перечислите признаки манипуляции сознанием.

11. Охарактеризуйте методы противодействия манипуляции сознанием.

Примерные тесовые задания

1. Что такое «национальная безопасность»?

а) совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер;

б) система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу;

в) состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

2. Информационная безопасность Российской Федерации – это:

а) состояние защищенности информации, циркулирующей в обществе;

б) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

г) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

3. В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

а) искать и распространять информацию любым способом;

б) искать, получать, передавать, производить и распространять информацию любым законным способом;

в) искать, получать, передавать, производить и распространять информацию любым способом;

г) получать и распространять информацию любым способом.

Примерные практические задания

1. Приведите примеры взаимодействия социальных систем, исходя из их целей.

2. Постройте «интеллект-карту» (mind map) безопасность семьи.

3. Приведите по 3 примера негативного (манипулятивного) и позитивного информационно-психологического воздействия в повседневной жизни.

4. Постройте «интеллект-карту» (mind map) с примерами скрытой рекламы.

5. Заполните таблицу «Исторические этапы развития информационного противоборства».

№ п/п	Наименование этапа	Основной носитель и средства доведения информации	Объект воздействия	Способы ведения информационного противоборства

6. Приведите по одному историческому примеру информационного противоборства, соответствующему каждому этапу его развития.

7. В научной литературе имеется множество различных формулировок термина «информационной войны», которые по своей сути объединены в три подхода. Раскройте сущность данного термина в соответствии с данными подходами. Какого подхода придерживаетесь Вы. Свой ответ аргументируйте.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине

Компетенция ОПК-1.5

Вопросы с выбором

1. Понятие информационной безопасности Российской Федерации установлено:
а) доктриной информационной безопасности, утвержденной Указом Президента №646 от 5 декабря 2016;
б) федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
в) федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
в) федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. «Гуманитарные аспекты информационной безопасности» - это отрасль научного знания, которая:
а) выявляет и изучает информационные угрозы для социокультурного потенциала нации, вскрывает закономерности переформатирования информационным агрессором сознания и подсознания членов нации в целях ее самоликвидации;
б) прогнозирует опасные последствия реализации различных информационных угроз и вырабатывает практические рекомендации по предотвращению, локализации и устранению ущерба, причиненного этой информационной агрессией;
в) формулирует цели, содержание, средства, результат активного информационного и иного воздействия на информационного агрессора и тех
групп населения, которые попали под его влияние.
г) все перечисленное.

3. Что такое фрагментарное (клиповое) мышление?
а) вид понятийно-логического мышления, характеризующийся использованием определенной логической основы (таблиц, графиков, объективных закономерностей, системы принципов) для последующего анализа, исследования, сравнения, прогнозирования и т.д;
б) вид мышления, характеризующийся быстротой протекания, отсутствием четко выраженных этапов, является минимально осознанным.
в) это обобщенное познание человеком действительности, т. е. получение знаний о ней в форме понятий и идей;
г) алогичное мышление, при котором человек не видит логической связи и между разделенными по времени историческими событиями, и между событиями современной жизни, потому что понимает их образно и фрагментами.

4. К социальным проблемам информационной безопасности относятся:
а) электронная слежка за политическими лидерами;
б) новая информационная культура общества;
в) информационная преступность;
г) информационные факторы деструктивного поведения.

5. К геополитическим проблемам информационной безопасности не относятся:
а) электронная слежка за политическими лидерами;

б) глобальное наблюдение» за населением;
в) энергоинформационная безопасность;
г) информационные и «гибридные» войны.

6. К сдерживающим факторам развития информационного общества нельзя отнести:
а) слабая подготовленность населения к жизни в информационном обществе, отсутствие мотивации для использования современных информационно-телекоммуникационных технологий из-за плохой осведомленности об их возможностях, традиционной пассивности и инерции в использовании информации;
б) отсутствие инвестиционной политики для финансирования перспективных программ и проектов, реализующих стратегию развития информационного общества в России;
в) наличие высокого научного, образовательного и культурного потенциала, сохранившегося в России, а также самобытной многонациональной культуры;
г) более низкий по сравнению с ведущими странами уровень развития информационно-коммуникационной инфраструктуры и производства информационных и коммуникационных средств, продуктов и услуг.

7. Преимущества Российской федерации в развитии информационного общества:
а) наличие высокого научного, образовательного и культурного потенциала, сохранившегося в России, а также самобытной многонациональной культуры;
б) наличие серьезных теоретических разработок мирового уровня в области информатики;
в) опережающие темпы развития всех видов российских телекоммуникаций по сравнению с другими областями экономической деятельности;
г) все вышеперечисленное.

8. К положительным последствиям информатизации не относится:
а) совершенствование информационно-вычислительного обеспечения
экономических и социальных процессов;
б) интернет зависимость;
в) рост и развитие информационных потребностей населения за счет
доступности ресурсов и их многообразия, расширения спектра средств доступа;
г) развитие электронной демократии и электронного правительства.

9. Целью психологической войны является:
а) расширение экономического влияния государства;
б) дестабилизация общества, его внутренняя разобщенность,
дезинформация, нарушение оптимального функционирования;
в) достижение мирового превосходства и, как следствие, контроль инноваций;
г) контроль информационного пространства и обеспечение защиты своей информации от вражеских действий.

10. К последствиям эмоционального воздействия на аудиторию следует отнести:
а) искусственное создание сенсаций, погоня за новостями;
б) создание из любой социальной проблемы шоу, зрелища, которое развлекает аудиторию;
в) нет правильного ответа;
г) все вышеперечисленное.

11. К стадиям реагирования на моральную панику в СМИ не относится:
а) осознание опасности;
б) поиск врага;
в) концептуализация будущего;
г) осознание безисходности.

12. К признакам скрытой манипуляции относится:
а) сокращение контактов;
б) сенсационность и срочность;
в) изменение темпа;
г) создание искусственной непредсказуемости реакции.

13. К методам противодействия манипуляции следует отнести:
а) предсказуемость;
б) непредсказуемость;
в) повторение;
г) дробление.

14. Информационный контроль (отсечение или клевета на внешние источники информации) как прием, используемый деструктивными культурами имеет следствием:
а) понижает психологическую защиту;
б) мешает информированному принятию решений и таким образом предотвращает критическую оценку;
в) прививает чувство вины;
г) ослабляет способность критически оценивать ситуацию.

15. Информационно-психологический конфликт это:
а) столкновение интересов двух или нескольких субъектов информационно-психологических отношений с целью обострения или разрешения противоречий по поводу власти и осуществления политического руководства в информационно-психологическом пространстве, а также по поводу перераспределения их роли, места и функций в социально политической системе информационного общества;
б) вооружённое противоборство между государствами или социальными общностями внутри отдельных государств, имеющее целью разрешение экономических, политических, национально-этнических и иных противоречий через ограниченное применение военной силы;
в) противоборство субъектов социального взаимодействия (наций, государств, классов и т.д.) на основе противоположных экономических интересов, обусловленных положением и ролью в системе общественных отношений;
г) ситуация, при которой личная заинтересованность (прямая или косвенная) служащего влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им должностных обязанностей.

16. К основным направлениям реализации информационно-психологической безопасности не относится:
а) экспертиза;
б) обучение;
в) научное консультирование по проблемам;
г) фальсификация.

17. К прямым методам воздействия на сознание не относится:
а) метод закрепления установок;
б) метод инициализация нарушений мозговой деятельности путем повышения потребления алкоголя;
в) метод рекламы;
г) метод опосредованного воздействия средств массовой информации на общественное сознание через межличностные неформальные каналы информации.

18. Количество этапов информационного противоборства:
а) 3;
б) 4;
в) 5;
г) 8.

19. Стратегическая информационная война:
а) применяется в военных операциях;
б) применяется в психологических операциях;
в) применяется в обоих случаях;
г) нет правильного ответа.

20. В чем сущность дозирования информации как приема манипулирования информацией?
а) сообщается гигантское количество информации, основную часть которой составляют абстрактные рассуждения, ненужные подробности, различные пустяки и т.п. «мусор»;
б) сообщается только часть сведений, а остальные тщательно скрываются, что приводит к тому, что картина реальности искажается в ту или иную сторону, либо вообще становится непонятной;
в) под различными предлогами оттягивать обнародование действительно важных сведений до того момента, когда будет уже поздно что-то изменить;
г) вымышленную (естественно, выгодную для себя) версию тех или иных событий через подставных лиц, нейтральных по отношению к обеим конфликтующим сторонам.

Вопросы с коротким ответом

21. Сведения, сообщения, данные независимо от их представления – это …?

22. В каком нормативном правовом документе закреплено понятие информационная безопасность Российской Федерации?

23. Как называется психическое воздействие, которое производится тайно, а следовательно, и в ущерб тем лицам, на которых оно направлено?

24. Совокупность средств, методов, способов и технологий информационно-психологического воздействия, специально созданных для тайного управления информационной сферой противника, процессами и системами, функционирующими на основе информации, а также – для нанесения им ущерба – это…?

25. Способ оказания влияние на людей (на отдельных индивидов и на группы), осуществляемое с целью изменения идеологических и психологических структур их сознания и подсознания, трансформации эмоциональных состояний, стимулирования определенных типов поведения с использованием различных способов явного и скрытого психологического принуждения– это…?

Вопросы с развернутым ответом

26. Перечислите этапы психологического воздействия.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное перечисление этапов психологического воздействия.	Отлично (90-100 баллов)
Обучающийся приводит перечисление этапов психологического воздействия. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся приводит неполное перечисление этапов психологического воздействия. Допускаются неточности.	Удовлетворительно (50-70 баллов)
Обучающийся приводит неполное перечисление этапов психологического воздействия. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

27. Какие нормативные правовые документы составляют правовую основу Стратегии национальной безопасности?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень нормативных правовых документов, составляющих правовою основу Стратегии национальной безопасности.	Отлично (90-100 баллов)
Обучающийся приводит полный перечень нормативных правовых документов, составляющих правовою основу Стратегии национальной безопасности. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся приводит неполный перечень нормативных правовых документов, составляющих правовою основу Стратегии национальной безопасности.	Удовлетворительно (50-70 баллов)
Обучающийся не приводит перечень нормативных правовых документов, составляющих правовою основу Стратегии национальной безопасности. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

28. Какие группы включают гуманитарные проблемы информационной безопасности?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень групп гуманитарных проблем информационной безопасности.	Отлично (90-100 баллов)
Обучающийся приводит перечень групп гуманитарных проблем информационной безопасности. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся приводит неполный перечень групп гуманитарных проблем информационной безопасности Допускаются неточности.	Удовлетворительно (50-70 баллов)
Обучающийся не приводит перечень групп гуманитарных проблем информационной безопасности. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

29. На какие виды разделяются конфликты по количеству участников?

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень видов конфликтов по количеству участников.	Отлично (90-100 баллов)
Обучающийся приводит перечень видов конфликтов по количеству участников. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся приводит неполный перечень видов конфликтов по количеству участников. Допускаются неточности.	Удовлетворительно (50-70 баллов)

Обучающийся не приводит перечень видов конфликтов по количеству участников. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

30. Перечислите сферы ведения информационного противоборства.

Критерии оценивания	Шкала оценок
Обучающийся приводит полный и безошибочный перечень сфер ведения информационного противоборства.	Отлично (90-100 баллов)
Обучающийся приводит перечень сфер ведения информационного противоборства. Допускаются незначительные неточности.	Хорошо (70-80 баллов)
Обучающийся приводит неполный перечень сфер ведения информационного противоборства Допускаются неточности.	Удовлетворительно (50-70 баллов)
Обучающийся не приводит перечень сфер ведения информационного противоборства. Присутствуют грубые ошибки или неточности.	Неудовлетворительно (менее 50 баллов)

20.2. Промежуточная аттестация

Примерный перечень вопросов к экзамену

№	Содержание
1	Понятие о системном анализе, его логике, этапах, количественно-качественных характеристиках и закономерностях.
2	Системное содержание понятия «национальная безопасность» и типология угроз этой безопасности.
3	Главные цели и закономерности информационно-психологической войны.
4	Информационная сфера как системообразующий фактор жизни общества.
5	Доктрина информационной безопасности Российской Федерации.
6	Информационное обеспечение государственной политики.
7	Сохранение культурно-нравственных ценностей российского народа.
8	Подходы к оцениванию информационной безопасности России.
9	Информационные взаимосвязи личности, общества и государства.
10	Информационные воздействия на личность, общество и государство.
11	Возможности применения информационных воздействий деструктивного характера для нанесения ущерба личности, обществу и государству.
12	Понятие и структура информационно-психологической безопасности.
13	Субъекты, объекты и источники угроз информационно-психологической безопасности.
14	Информационное противоборство и информационная война.
15	Понятия информационного и рефлексивного управления, их роль в информационном обществе.
16	Модели информационного и рефлексивного управления.
17	Понятия информационного и информационно-психологического противоборства.
18	Информационная война как средство достижения политических целей. Информационное оружие.
19	Взгляды иностранных государств на информационную войну.
20	Информационные войны в новейшей истории.
21	Модели, ресурсы, технологии и мишени информационных воздействий.
22	Основные типы и содержание технологий информационного воздействия.
23	Способы манипулирования в массовых информационных процессах, в ходе обсуждений и дискуссий, в межличностном общении.
24	Технологии скрытого управления личностью и обществом с помощью информационных воздействий.
25	Информационные операции в сети Интернет.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
«____»_____ 2023

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.Б.44 Гуманитарные аспекты информационной безопасности
Форма обучения Очное

Вид контроля экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Информационно-психологическая безопасность как составляющая информационной безопасности.
2. Информационная война как средство достижения политических целей.

Преподаватель _____ Н.В. Филиппова

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше.