Федеральное государственное образовательное бюджетное учреждение
высшего образования
**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**
(Финансовый университет)

Кафедра информационной безопасности

Факультета информационных технологий и анализа больших данных

УТВЕРЖДАЮ

Проректор по учебной
и методической работе
_____Е.А. Каменева

«18» ноября 2024 г.

Цацкина Е.П.

Информационное противоборство

Рабочая программа дисциплины
для студентов, обучающихся по направлению подготовки
10.04.01 – Информационная безопасность,
направленность программы:
«Управление информационной безопасностью в кредитно-финансовой сфере»

Рекомендовано Учёным советом
Факультета информационных технологий и анализа больших данных
(протокол от «30» октября 2024 г. №48)

Одобрено на заседании Кафедры информационной безопасности
(протокол от «05» сентября 2024 г. №7)

Москва, 2024

СОДЕРЖАНИЕ

1. Наименование дисциплины

«Информационное противоборство»

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПКН-1	Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов	1. Использует отечественные и зарубежные стандарты в области обеспечения информационной безопасности.	*Знать:* отечественные и зарубежные стандарты в области обеспечения информационной безопасности *Уметь*: применять нормативно-правовые акты, научную литературу и методические рекомендации регуляторов при решении профессиональных задач
		2. Разрабатывает требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности.	*Знать:* требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности *Уметь:* использовать требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности в осуществлении информационных процессов
		3. Демонстрирует навыки разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	*Знать:* процедуру и технологии разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности в решении задач профессиональной деятельности *Уметь:* уметь практически реализовать решение задач моделирования и проектирования защищенных автоматизированных

			информационных систем и систем обеспечения информационной безопасности
ПКН-3	Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	1. Применяет нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации	*Знать:* нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации *Уметь: применить* нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации
		2. Использует необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	*Знать:* в решении каких профессиональных задачах необходимо применение нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации *Уметь:* применить требования нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации в решении профессиональных задач
		3. Составляет организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	*Знать:* содержание требований нормативно-правовых актов, необходимых при составлении организационно-распорядительных документов, нормативные и методических документов, регламентирующих деятельность по защите информации в организации *Уметь:* составлять

			организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации
УК-1	Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий	1. Использует методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности.	*Знать:* методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности *Уметь:* применять методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности
		2. Демонстрирует способы осмысления и критического анализа проблемных ситуаций.	*Знать:* методику осмысления и критического анализа проблемных ситуаций в профессиональной деятельности *Уметь:* применить методику осмысления и критического анализа проблемных ситуаций в профессиональной деятельности
		3. Предлагает нестандартное решение проблем, новые оригинальные проекты, вырабатывает стратегию действий на основе системного подхода.	*Знать:* методики нестандартного решения проблем, направления возможно новых оригинальных проектов, вырабатывать стратегию действий на основе системного подхода *Уметь:* строить методики нестандартного решение проблем, разрабатывать новые оригинальные проекты, вырабатывать стратегию действий на основе системного подход
ПК-3	Способность разрабатывать архитектуры системы защиты информации	1 Проводит оценку показателей качества и эффективности работы вычислительных	*Знать:* методики и критерии оценки показателей качества и эффективности работы вычислительных систем,

	автоматизированной системы кредитно-финансовой сферы	систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации	программных и программно-аппаратных средств, используемых для построения систем защиты информации *Уметь:* разработать и реализовать методику и критерии оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации
		2 Проводит технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы	*Знать:* методики и критерии технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы *Уметь:* разработать и реализовать технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы
		3 Определяет порядок обработки информации в автоматизированной системе кредитно-финансовой сферы	*Знать:* порядок обработки информации в автоматизированной системе кредитно-финансовой сферы *Уметь:* разработать и реализовать порядок обработки информации в автоматизированной системе кредитно-финансовой сферы

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационное противоборство» является дисциплиной модуля дисциплин по выбору, углубляющих освоение программы магистратуры «Управление информационной безопасностью в кредитно-финансовой сфере» по направлению подготовки 10.04.01 «Информационная безопасность».

4. Объем дисциплины(модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 2

Вид учебной работы по дисциплине	**Всего (в з.е и часах)**	**Модуль 5**
Общая трудоемкость дисциплины	**4 з.е. , 144ч**	**4 з.е. , 144ч**
Контактная работа - Аудиторные занятия	**32**	**32**
Лекции	8	8
Семинары, практические занятия	24	24
Самостоятельная работа	**112**	**112**
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Информационное противоборство в начале XXI века

1. Использование авторитетов (групп влияния).
2. Имитационная дезинформация.
3. Псевдологические выводы.
4. Принуждающая пропаганда.
5. Наклеивание ярлыков.

Тема 2. Информационно-психологическая война как средство агрессии и достижения целей

1. Место психологической войны в системе информационной войны.
2. Основные структурные элементы информационно-психологического воздействия.
3. Дезинформирование, лоббирование, манипулирование, пропаганда, управление кризисами, шантаж.
4. Основные этапы мероприятий и аксиомы психологической войны.

Тема 3. Кибервойна как вид информационных войн. Сетевые войны и их особенности

1. Понятия сетевого общества и сети. Особенности сетевого общества.
2. Естественные и искусственные сети.
3. Сети, построенные на основе этнического принципа.
4. Концепция сетецентричной войны.
5. Возможные направленияподготовки сетецентричной войны.
6. Принципы ведения сетевых войн.

Тема 4. Направления деятельности Российского государства в сфере обеспечения информационной безопасности

1. Межгосударственные конфликты и информационная безопасность России.
2. Концептуальные основы обеспечения информационной безопасностив условиях непрямых действий.
3. Угрозы информационной безопасности Российской Федерации.
4. Органы, обеспечивающие информационную безопасность.
5. Информационно-психологическая защита личности и общества.

Тема 5. Конкурентная разведка и стратегическая аналитика

1. Понятие конкурентной разведки и ее роль в обеспечении экономической безопасности предприятия.
2. Понятие информационно-аналитической работы и ее роль в обеспечении экономической безопасности предприятия.
3. Организационное, методологическое и технологическое обеспечение информационно-аналитической работы.
4. Возможности и ограничения конкурентной разведки для ведения информационно-аналитической работы, сбора информации о конкурентах, анализа рисков и прогноза.

Тема 6. Автоматизация методов выявления деструктивных текстов

1. Алгоритм ИАР и характеристики ее этапов.
2. Изменение подходов к поиску информации в Интернете путем применения методов конкурентной разведки.
3. Автоматизация процессов информационно-аналитической работы, применение технологий Big Data.
4. Современные информационно-аналитические системы в ЭБ.
5. Сбор и анализ информации о партнерах и контрагентах.
6. Соблюдение принципов должной осмотрительности.

5.2. Учебно – тематический план

Таблица 2

№ п/п	Наименование тем (разделов) дисциплины	Трудоёмкость в часах					Формы текущего контроля успеваемости
		Всего	Контактная работа* - Аудиторная работа			Самостоятельная работа	
			Общая,в т.ч.	Лекции	Семинары, практические занятия		
1.	Тема 1. Информационное противоборство в начале XXI века	18	6	2	4	12	доклады презентации дискуссии
2.	Тема 2. Информационно-психологическая война как средство	26	6	2	4	20	доклады презентации дискуссии

	агрессии и достижения целей						
3.	Тема 3. Кибервойна как вид информационных войн. Сетевые войны и их особенности	26	6	2	4	20	доклады презентации дискуссии
4.	Тема 4. Направления деятельности Российского государства в сфере обеспечения информационной безопасности	26	6	2	4	20	доклады презентации дискуссии
5.	Тема 5. Конкурентная разведка и стратегическая аналитика	24	4		4	20	доклады практико-ориентированные задания, дискуссии
6.	Тема 6. Автоматизация методов выявления деструктивных текстов	24	4		4	20	доклады практико-ориентированные задания, дискуссии
	В целом по дисциплине	144	32	8	24	112	Согласно учебному плану: контрольная работа
	Итого в %		22	25	75	78	

*Объем контактной работы в очно-заочной/заочной формах обучения и индивидуальных учебных планах определяется соответствующими учебными планами. Темы, реализуемые в виде контактной работы, определяются преподавателем самостоятельно, исходя из уровня их сложности.

5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование тем (разделов) дисциплины	**Перечень вопросов для обсуждения на семинарах, практических занятиях, рекомендуемые источники из разделов 8,9 (указывается раздел и порядковый номер источника)**	**Формы проведения занятий**
Информационное противоборство в начале XXI века	Использование информационных технологий для свержения законных правительств. Информационная война и вооруженное вторжение коалиционных силво главе с США в Ирак (2003 г.). Роль информационных технологий в «оранжевой» революции (2004-2005 гг.) на Украине. Информационная война и вооруженное вмешательство международныхвооруженных	доклады презентации дискуссии

	сил в гражданскую войну в Ливии. Гражданская война в Сирии и информационная война. Революция «Евромайдана» и противостояние на Украине (2014-2016 гг.). Источники: 8.1, 8.3, 8.6, 8.7 9.1, 9.5, 9.6, 9.12, 9.13, 9.21, 9.22	
Информационно-психологическая война как средство агрессии и достижения целей	Алгоритм самозащиты личности от информационно- психологического воздействия. Основы нейролингвистического программирования. Угрозы информационного воздействия через СМИ и рекламную деятельность. Роль органов управления и пресс-служб в недопущении деструктивных информационных воздействий через СМИ и рекламно-выставочную деятельность. Источники: 8.1, 8.2, 8.3, 8.4, 8.5,8.6, 8.7 9.1, 9.2, 9.3, 9.7, 9.8, 9.10, 9.23	доклады презентации дискуссии
Кибервойна как вид информационных войн. Сетевые войны и их особенности	Участие частных военных компаний и неправительственныхорганизаций в сетевых войнах. « Цветные» («бархатные») революции. Цели кибервойн: дестабилизация компьютерных систем, нарушение доступа к Интернету государственных учреждений и деловых центров, создание беспорядка и хаоса в жизни стран. Формы проявления кибервойн: вандализм, пропаганда, шпионаж, атаки на компьютерные системы и серверы. Источники: 8.1, 8.2, 8.3, 8.4, 8.5,8.6, 8.7 9.2, 9.3, 9.14, 9.20, 9.23	доклады презентации дискуссии
Направления деятельности Российского государства в сфере обеспечения информационной безопасности	Развитие технологической основы обеспечения защиты информации всетях связи специального назначения. Кадровое обеспечение информационной безопасности. Коллективные меры государств ОДКБ в сфере обеспеченияинформационной безопасности. Источники: 8.1, 8.2, 8.3, 8.4, 8.5,8.6, 8.7 9.1, 9.2, 9.3, 9.10, 9.11, 9.17, 9.18	доклады презентации дискуссии
Конкурентная разведка и стратегическая аналитика	Конкурентная разведка в стратегическом управлении. Методы в конкурентной разведке. Профессиональный портрет конкурентного аналитика. Отличие конкурентной разведки и	доклады практико-ориентированные задания дискуссии

	промышленного шпионажа. Источники: 8.1, 8.2, 8.3, 8.4, 8.5, 8.7 9.15, 9.16, 9.17, 9.18, 9.19	
Автоматизация методов выявления деструктивных текстов	Методы контент-анализа, инвент-анализа, когнитивной психологии, когнитивной лингвистики, корпусной лингвистики Источники: 8.1, 8.2, 8.3, 8.4, 8.7 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10	доклады практико-ориентированные задания дискуссии

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Информационное противоборство в начале XXI века	Информационное противоборство, причины его возникновения. Правовые средства противодействия вредоносному использованию информационных технологий государствами. Правовые средства противодействия использованию системы массовой информации для вмешательства во внутренние дела других государств.	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Информационно-психологическая война как средство агрессии и достижения целей	Методы и средства информационной войны против России. Роль СМИ, социальных сетей Виды информационно-психологического воздействия	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Кибервойна как вид информационных войн. Сетевые войны и их особенности	Освещение проблем противодействию информационным войнам в российских и зарубежных научных исследованиях	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме
Направления деятельности Российского государства в	Характеристика общего международного правового нормативного обеспечения в сфере защиты от информационных войн Характеристика общих	- работа с учебной, научной и справочной литературой; - конспект;

сфере обеспечения информационной безопасности	межгосударственных правовых нормативных документов СНГ в области защиты от информационных войн Характеристика общих правовых нормативных документов по защите от информационных войн в области информационной безопасности РФ	- подготовка докладов по теме; - подготовка презентаций по теме
Конкурентная разведка и стратегическая аналитика	Практики применения конкурентной разведки в российских и зарубежных научных исследованиях Особенности информационно-аналитической работы: организационное, методологическое и технологическое обеспечение Технология OSINT	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение практико-ориентированного задания
Автоматизация методов выявления деструктивных текстов	Практики применения методов контент-анализа, инвент-анализа, когнитивной психологии, когнитивной лингвистики, корпусной лингвистики в российских и зарубежных научных исследованиях	- работа с учебной, научной и справочной литературой; - конспект; - подготовка докладов по теме; - подготовка презентаций по теме; - выполнение практико-ориентированного задания

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерный перечень вопросов для подготовки к контрольной работе:

1. Цель обеспечения информационной безопасности.
2. Принципы информационной безопасности.
3. Основные свойства информации как предмета защиты.Характеристики секретной и конфиденциальной информации.
4. Основные понятия, применяемые при анализе информационных войн.
5. Исследование феномена «информационные войны» в современной науке.
6. Информационная война и психологическая война: общее и особенное.
7. Информационное противоборство в начале XXI века.
8. Психологическая война как вид информационной войны.
9. Психологическое воздействие на массовое и индивидуальнойсознание как средство психологической войны.
10. Цели и объекты психологических операций.
11. Пропаганда в системе психологической войны.
12. Сетевые войны и их особенности.

13. Сущность, структура и функции сетей в сетевом обществе.
14. История создания концепции сетевых войн.
15. Кибервойна как вид информационной войны.
16. Психологическая война и кибервойна: общие и особенные черты.
17. Подготовка к кибервойне ведущих государств мира.
18. Информационная безопасность и национальные интересы России.
19. Угрозы информационной безопасности России и их виды.
20. Система обеспечения информационной безопасности России.
21. Методы обеспечения информационной безопасности России.
22. Правовые аспекты информационных войн.
23. Государственная информационная политика в условияхинформационной войны.
24. Информационное противоборство в Интернете – приемы, методы, технологии.
25. Методы и технологии вмешательства США в информационное пространство РФ в ходе президентских кампаний 1996–2018 гг.

Примерный перечень вопросов для дискуссий

1. Проблемы и перспективы развития общего правового нормативного обеспечения по защите от информационных войн в сфере информационной безопасности
2. Освещение проблем противодействию информационным войнам в российских и зарубежных научных исследованиях
3. Международный опыт обеспечения цифровой суверенизации: США, Китай, Индонезия.
4. Цифровая суверенизация: проблемы России, пути разрешения.
5. Система угроз в информационном противоборстве России с НАТО.

Примерный перечень докладов (с презентациями):

1. Цифровая суверенизация: сущность, содержание.
2. Информационное противоборство: принципы, признаки, средства.
3. Современные теории ведения информационных войн.
4. Виды защиты от информационно-психологического воздействия и их содержание.
5. Направления деятельности различных государств по противодействию кибератакам.
6. Приемы информационного противоборства и воздействия на аудиторию в социальных сетях.
7. Методы ведения конкурентной разведки.
8. Информационная безопасность и национальные интересы России.
9. Угрозы информационной безопасности России и их виды.
10. Состояние информационной безопасности России.

11. Система обеспечения информационной безопасности России.
12. Методы обеспечения информационной безопасности России.
13. Государственная информационная политика Российской Федерации в условиях информационной войны.
14. Информационное противоборство в идеологической сфере: особенности, силы, средства
15. Теория Франсуа де Клюзеля «Когнитивное оружие»

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры информационной безопасности.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине содержится в разделе «2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине».

Таблица 6

Наименование компетенции	**Наименование индикаторов достижения компетенции**	**Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции**	**Типовые контрольные задания**
ПКН-1 Способность выявлять угрозы и оценивать уязвимости, разрабатывать требования и критерии оценки информационной безопасности конкретных объектов	1. Использует отечественные и зарубежные стандарты в области обеспечения информационной безопасности.	*Знать:* отечественные и зарубежные стандарты в области обеспечения информационной безопасности *Уметь*: применять нормативно-правовые акты,	1. Цель и принципы обеспечения информационной безопасности. 2. Информационное противоборство: принципы, признаки, средства. 3. Составьте план исследования на тему «Кибервойна в системе

		научную литературу и методические рекомендации регуляторов при решении профессиональных задач	обеспечения цифровой суверенизации РФ».
	2. Разрабатывает требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности.	*Знать:* требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности *Уметь:* использовать требования к системе обеспечения информационной безопасности и критерии оценки ее эффективности в осуществлении информационных процессов	1. Цифровая суверенизация: сущность, содержание. 2. Направления деятельности различных государств по противодействию кибератакам. 3. Установите зависимость эффективности информационного противоборства от уровня цифровой суверенизации.
	3. Демонстрирует навыки разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности.	*Знать:* процедуру и технологии разработки стратегий решения задач моделирования и проектирования защищенных автоматизированных информационных систем и систем обеспечения информационной безопасности в решении задач профессиональной деятельности *Уметь:* уметь практически реализовать решение задач моделирования и проектирования защищенных автоматизированных информационных	1. Методы ведения конкурентной разведки. 2. Методы обеспечения информационной безопасности России. 3. Разработайте техническое задание по обеспечению защиты системы управления доступом.

		систем и систем обеспечения информационной безопасности	
ПКН-3 Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	1. Применяет нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации	*Знать:* нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации *Уметь:* применить нормативные правовые акты, нормативные и методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования и сертификации средств защиты информации	1. Проблемы и перспективы развития общего правового нормативного обеспечения по защите от информационных войн в сфере информационной безопасности. 2. Разработайте глоссарий терминов для общего правового нормативного обеспчения защиты от информационных войн с сфере ИБ.
	2. Использует необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	*Знать:* в решении каких профессиональных задачах необходимо применение нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в организации *Уметь:* применить требования нормативных правовых актов, нормативных и	1. Информационная безопасность и национальные интересы России. 2. Угрозы информационной безопасности России и их виды. 3. Разработайте документное обеспечение защиты от информационных войн в сфере ИБ.

	3. Составляет организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	методических документов, регламентирующих деятельность по защите информации в организации в решении профессиональных задач *Знать:* содержание требований нормативно-правовых актов, необходимых при составлении организационно-распорядительных документов, нормативные и методических документов, регламентирующих деятельность по защите информации в организации *Уметь:* составлять организационно-распорядительные документы, нормативные и методические документы, регламентирующие деятельность по защите информации в организации	1. Государственная информационная политика Российской Федерации в условиях информационной войны. 2. Информационное противоборство в идеологической сфере: особенности, силы, средства. 3. Разработайте систему социально-психологической защиты персонала организации в условиях информационного противоборства с противников.
УК-1 Способность к абстрактному мышлению, критическому анализу проблемных ситуаций на основе системного подхода, выработке стратегии действий	1. Использует методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности.	*Знать:* методы абстрактного мышления, анализа информации и синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности *Уметь:* применять методы абстрактного мышления, анализа информации и	1. Психологическое воздействие на массовое и индивидуальной сознание как средство психологической войны. 2. Разработайте модель психологической структуры человека, способного быть невосприимчивым к

		синтеза проблемных ситуаций, формализованных моделей процессов и явлений в профессиональной деятельности	социально-психологическим воздействиям противника.
	2. Демонстрирует способы осмысления и критического анализа проблемных ситуаций.	*Знать:* методику осмысления и критического анализа проблемных ситуаций в профессиональной деятельности *Уметь:* применить методику осмысления и критического анализа проблемных ситуаций в профессиональной деятельности	1. Освещение проблем противодействию информационным войнам в российских и зарубежных научных исследованиях. 2. Разработайте план исследования на тему: «Психологические операции в системе информационного противоборства».
	3. Предлагает нестандартное решение проблем, новые оригинальные проекты, вырабатывает стратегию действий на основе системного подхода.	*Знать:* методики нестандартного решения проблем, направления возможно новых оригинальных проектов, вырабатывать стратегию действий на основе системного подхода *Уметь:* строить методики нестандартного решения проблем, разрабатывать новые оригинальные проекты, вырабатывать стратегию действий на основе системного подход	1. Психологические операции в системе информационного противоборства: цель, задачи, объекты. 2. Социальные сети в информационном противоборстве: виды, эффективность, российские проблемы. 3. Разработайте модель психологической структуры человека, способного быть невосприимчивым к социально-психологическим воздействиям противника.
ПК-3 Способность разрабатывать архитектуры системы защиты информации автоматизированной системы кредитно-финансовой сферы	1. Проводит оценку показателей качества и эффективности работы вычислительных систем, программных и	*Знать:* методики и критерии оценки показателей качества и эффективности работы вычислительных систем,	1. Информационное противоборство: принципы, признаки, средства. 2. Виды защиты от информационно-психологического воздействия и их

	программно-аппаратных средств, используемых для построения систем защиты информации	программных и программно-аппаратных средств, используемых для построения систем защиты информации	содержание.
		Уметь: разработать и реализовать методику и критерии оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации	3. Разработайте алгоритм применения методов корпусной лингвистики к выявлению деструктивного контента в социальных сетях и СМИ
	2. Проводит технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы	*Знать:* методики и критерии технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы	1. Направления деятельности различных государств по противодействию кибератакам.
			2. Приемы информационного противоборства и воздействия на аудиторию в социальных сетях.
		Уметь: разработать и реализовать технико-экономическую оценку целесообразности создания системы защиты информации автоматизированной системы кредитно-финансовой сферы	3. Разработайте систему оценки эффективности комплексной защиты ИБ организации.
	3. Определяет порядок обработки информации в автоматизированной системе кредитно-	*Знать:* порядок обработки информации в автоматизированной системе кредитно-	1. Методы ведения конкурентной разведки.
			1. Современные теории ведения информационных войн.

	финансовой сферы	финансовой сферы *Уметь:* разработать и реализовать порядок обработки информации в автоматизированной системе кредитно-финансовой сферы	2. Реализуйте алгоритм применения методов корпусной лингвистики к выявлению деструктивного контента в социальных сетях и СМИ .

Примерный перечень вопросов и заданий для подготовки к экзамену

Теоретические вопросы

1. Информационное противоборство: сущность, содержание.
2. Цифровая суверенизация: сущность, содержание.
3. Информационное противоборство: принципы, силы, средства.
4. Цифровая суверенизация: проблемы России, пути разрешения.
5. Зависимость эффективности информационного противоборства от уровня цифровой суверенизации.
6. Порядок анализа качества информационного противоборства.
7. Деятельность российского государственного руководства по обеспечению цифровой суверенизации.
8. Информационное противоборство в идеологической сфере: особенности, силы, средства.
9. Информационная война и психологическая война: общее и частное.
10. Информационное противоборство в системе оборонного сознания молодежи.
11. Игформационное протитвоборство в обеспечении цифровой суверенизации.
12. Принцыпы ведения информационного противоборства странами Запада.
13. Психологическая война в системе обеспечения цифровой суверенизации России.
14. Социально-психологические методы воздействия на противника в условиях ведения информационного противоборства.
15. Способы обеспечения цифровой суверенизации России.
16. Психологические операции в системе информационного противоборства: виды, содержание, практика.

17. Международный опыт обеспечения цифровой суверенизации: США, Китай, Индонезия.
18. Психологические операции в системе информационного противоборства: цель, задачи, объекты.
19. Пропаганда и агитация в системе информационного противоборства: сущность, советский опыт.
20. Социальные сети в информационном противоборстве: виды, эффективность, российские проблемы.
21. Социальные сети в информационном противоборстве: сущность, популярность, практика регулирования.
22. Кибервойна в системе обеспечения цифровой суверенизации России: цель, задачи, методы.
23. Особенности американской стратегии кибервойны в системе обеспечения цифровой суверенизации: политический, экономический факторы.
24. Ассиметричное информационное противоборство: сущность, принципы, методы.
25. Силы и средства современной кибервойны: опыт России.
26. Система угроз в информационном противоборстве России с НАТО,
27. Информационная безопасность России: проблемы, пути их разрешения.
28. Разведка в информационном противоборстве и обеспечении цифровой суверенизации: силы, средства Росии.
29. Информационное противоборство в Интернете: методы, технологии, регулирование.
30. Правовое регулирование обеспечения цифровой суверенизации РФ.

Практико-ориентированные (ситуационные) задания

1. Составьте план исследования на тему «Кибервойна в системе обеспечения цифровой суверенизации РФ»
2. Разработайте техническое задание по обеспечению защиты системы управления доступом
3. Разработайте систему социально-психологической защиты персонала организации в условиях информационного противоборства с противников

4. Разработайте документное обеспечение защиты от информационных войн в сфере ИБ
5. Разработайте глоссарий терминов для общего правового нормативного обеспчения защиты от информационных войн с сфере ИБ
6. Разработайте модель психологической структуры человека, способного быть невосприимчивым к социально-психологическим воздействиям противника
7. Сформируйте систему контроля деятельности персонала организации в социальных сетях
8. Разработайте алгоритм применения методов корпусной лингвистики к выявлению деструктивного контента в социальных сетях и СМИ
9. Разработайте систему оценки эффективности комплексной защиты ИБ организации
10. Разработайте план исследования на тему: «Психологические операции в системе информационного противоборства»

Пример экзаменационного билета

Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

Кафедра информационной безопасности

Дисциплина «Информационное противоборство»

Факультет информационных технологий и анализа больших данных

Форма обучения очная

Направление подготовки «Информационная безопасность»

Направленность программы «Управление информационной безопасностью в кредитно-финансовой сфере»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № ___

1.	Информационное противоборство: принципы, методы, средства	(15 баллов)
2.	Социальные сети в информационном противоборстве: виды, задачи, российские проблемы	(15 баллов)
3.	Разработайте систему социально-психологической защиты	(30 баллов)

	персонала организации в условиях информационного противоборства с противников	

Подготовил _____(Цацкина Е.П.)

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1. Кафтан, В. В. Теории и технологии современной информационной войны : монография / В. В. Кафтан. — Москва : КноРус, 2022. — 287 с. — ЭБС BOOK.ru. — URL: https://book.ru/book/945102 (дата обращения: 04.10.2024). — Текст : электронный.

2. Целых, А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие / А. Н. Целых, Э. М. Котов ; Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2023. - 116 с. - ЭБС ZNANIUM. - URL: https://znanium.ru/catalog/product/2146710 (дата обращения: 04.10.2024). – Текст: электронный.

3. Торба, О. И. Правовое нормативное обеспечение защиты от информационных войн в области информационной безопасности : монография / О. И. Торба, Д. О. Торба, Ю. И. Коваленко, М. М. Тараскин. — Москва : Русайнс, 2021. — 582 с. — ЭБС BOOK.ru. — URL: https://book.ru/book/942308 (дата обращения: 04.10.2024). — Текст : электронный.

б) дополнительная литература

4. Белоус, А. И. Технологии, методы и инструменты войн XXI века: монография / А. И. Белоус. — Москва : Техносфера, 2023 — 528 с.: ил., табл. — ЭБС Университетская библиотека ONLINE. — URL:https://biblioclub.ru/index.php?page=book&id=707794 (дата обращения: 04.10.2024). - Текст : электронный.

5. Леопа, А. В. Информационно-психологическая война в философском и лингвистическом осмыслении : монография / А. В. Леопа, О. В. Фельде, К. В. Волчок. - Красноярск : Сибирский федеральный университет, 2022. - 152 с. - ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/2091871 (дата обращения: 04.10.2024). – Текст : электронный.

6. Основы национальной безопасности: учебник / П. А. Бышков, К. К. Гасанов, С. А. Егоров, М. Ю. Зеленков, О. В. Зиборов; под ред. К. К. Гасанов; под ред. О. В. Зиборов; под ред. Н. Д. Эриашвили. — 2-е изд., перераб. и доп. — Москва : Юнити-Дана, 2022 — 352 с. — ЭБС Университетская библиотека ONLINE. — URL: https://biblioclub.ru/index.php?page=book&id=690542 (дата обращения: 04.10.2024). – Текст : электронный.

7. Ларионова, С. Л. Информационная безопасность дистанционного банковского обслуживания: учебное пособие / С. Л. Ларионова; Финуниверситет. — Москва : Прометей, 2022. — 296 с. - Текст : непосредственный. - То же. - ЭБС Лань. - URL: https://e.lanbook.com/book/290516 (дата обращения: 04.10.2024). — Текст : электронный.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт Центрального банка Российской Федерации: www.cbr.ru;

2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru;

3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.

4. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/

5. Электронно-библиотечная система BOOK.RU http://www.book.ru

6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» http://biblioclub.ru/

7. Электронно-библиотечная система Znanium http://www.znanium.com

8. Электронно-библиотечная система издательства «ЮРАЙТ» https://urait.ru/

9. Электронно-библиотечная система издательства Проспект

http://ebs.prospekt.org/books

10. Электронно-библиотечная система издательства Лань https://e.lanbook.com/

11. Деловая онлайн-библиотека Alpina Digital http://lib.alpinadigital.ru/

12. Электронная библиотека Издательского дома «Гребенников» https://grebennikon.ru/

13. Научная электронная библиотека eLibrary.ru http://elibrary.ru

14. Национальная электронная библиотека http://нэб.рф/

15. Финансовая справочная система «Финансовый директор» http://www.1fd.ru/

16. СПАРК https://spark-interfax.ru/

17. Библиотека онлайн Лекций по Бизнесу и Маркетингу издательства Henry Stewart Talks

18. CNKI. Academic Reference https://ar.oversea.cnki.net/

19. CNKI. China Academic Journals Full-text Database https://oversea.cnki.net/kns?dbcode=CFLQ

20. Электронные продукты издательства Elsevier http://www.sciencedirect.com

21. Коллекция научных журналов Oxford University Press https://academic.oup.com/journals/

22. Электронные коллекции книг и журналов издательства Springer: http://link.springer.com/

23. База данных научных журналов издательства Wiley https://onlinelibrary.wiley.com/

10. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов реализуется в соответствии с приказом Финансового университета от 11.05.2021 № 1040/о «Об утверждении Методических рекомендаций по планированию и организации внеаудиторной самостоятельной работы студентов по образовательным программам бакалавриата и магистратуры в Финансовом университете». Промежуточная аттестация проводится в соответствии с приказом Финансового университета от 23.03.2017 № 0557/о «Об утверждении Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по программам бакалавриата и магистратуры в

Финансовом университете». Кафедрой могут разрабатываться дополнительные методические рекомендации для отдельных форм проведения аудиторных занятий и самостоятельной работы студентов.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11. 1. Комплект лицензионного программного обеспечения

1.Windows, Microsoft Office

2. Антивирус Kaspersky

11.2. Современные профессиональные базы данных и информационные справочные системы

1. Информационно-правовая система «Гарант»

2. Информационно-правовая система «Консультант Плюс»

11.3. Сертифицированные программные и аппаратные средства защиты информации

Не предусмотрены.

12. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Занятия по дисциплине проводятся в аудиториях, оборудованных мультимедийными комплексами, компьютерами с выходом в Интернет.