

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение  
высшего образования

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
Факультет информационных систем и безопасности  
Кафедра информационной безопасности

## **ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**10.03.01 Информационная безопасность**

*Код и наименование направления подготовки/специальности*

**Организация и технологии защиты информации  
(по отрасли или в сфере профессиональной деятельности)**

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2024

ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
Рабочая программа дисциплины

Составитель(и):

Доктор технических наук, профессор В.В. Арутюнов

Ответственный редактор

канд. ист. наук, доц., заведующая кафедрой  
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры  
Информационной безопасности  
№ 11 от 18.03.2024

## ОГЛАВЛЕНИЕ

1. Пояснительная записка .....	4
1.1. Цель и задачи дисциплины .....	4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций .....	4
1.3. Место дисциплины в структуре образовательной программы .....	6
2. Структура дисциплины .....	6
3. Содержание дисциплины .....	6
4. Образовательные технологии .....	8
5. Оценка планируемых результатов обучения .....	9
5.1 Система оценивания .....	9
5.2 Критерии выставления оценки по дисциплине .....	10
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине .....	11
6. Учебно-методическое и информационное обеспечение дисциплины .....	11
6.1 Список источников и литературы .....	15
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ....	15
6.3 Профессиональные базы данных и информационно-справочные системы .....	16
7. Материально-техническое обеспечение дисциплины .....	16
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов .....	16
9. Методические материалы .....	17
9.1 Планы практических занятий .....	17
Приложение 1. Аннотация рабочей программы дисциплины .....	17

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины - формирование у обучающихся знаний о сущности информационных войн и информационного оружия, методов и способов их реализации, а также о возможностях информационного противоборства потенциальному противнику.

Задачи дисциплины:

- раскрытие основных категорий информационной войны и базовых факторов, оказывающих влияние на её содержание;
- определение основных принципов, отражающих закономерности информационной войны;
- анализ базовых уровней общественного сознания, выступающего в качестве поля сражения;
- выявление основных классов и практических видов информационного оружия;
- установление базовых мероприятий по предотвращению или нейтрализации последствий применения информационного оружия;
- раскрытие практических мероприятий программного характера по защите от информационного оружия.

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

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
<i>УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений</i>	УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач	Знать: основные особенности Интернета как современной коммуникационной среды; Уметь: пользоваться основными сервисами Интернета; Владеть: основными элементами делового общения в сети
	УК-2.2 Способность использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.	Знать: принципы функционирования социальных сервисов в сети Интернет Уметь: пользоваться знаниями о преимуществе и недостатках использования социальных сетей

		Владеть: правилами этикета при работе в сети Интернет
<i>УК-3 - Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде</i>	УК-3.1 Понимает эффективность использования стратегии сотрудничества для достижения поставленной цели; определяет роль каждого участника в команде;	Знать: понятия информации и информационной безопасности; Уметь: пользоваться основополагающими правовыми документами, определяющими место и роль информационной безопасности в системе национальной безопасности России Владеть: навыками применения полученных знаний в научно-исследовательской работе;
	УК-3.2 Эффективно взаимодействует с членами команды; участвует в обмене информацией, знаниями и опытом; содействует презентации результатов работы команды; соблюдает этические нормы взаимодействия	Знать: основные источники угроз информационной безопасности; Уметь: оценивать и классифицировать угрозы информационной безопасности;
<i>ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</i>	ОПК-1.1 Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации	Владеть: навыками определения угроз информации применительно к объектам защиты в условиях информационного противоборства
	ОПК-1.2 Умеет классифицировать и оценивать угрозы информационной безопасности	Знать: базовый понятийный аппарат в области информационного противоборства, информационной войны; основные методы и приемы информационного противоборства;
	ОПК-1.3 Владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности	Уметь: ставить цели и выбирать пути эффективного решения задач в области защиты

	личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире	информации Владеть: навыками работы при использовании основных социальных сервисов.
--	---	--

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина (модуль) «Гуманитарные аспекты информационной безопасности» относится к базовой части блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Надёжность информационных систем».

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения преддипломной практики и подготовки и защиты ВКР.

## 2. Структура дисциплины

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

### Структура дисциплины для очной формы обучения

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

Семестр	Тип учебных занятий	Количество часов
7	Лекции	20
7	Практические занятия	22
8	Лекции	20
8	Практические занятия	22
Всего:		84

Объём дисциплины в форме самостоятельной работы обучающихся составляет 60 академических часов.

## 3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
<b>7 семестр</b>		
1	Особенности сети Интернет как коммуникационной среды	Основные понятия и определения. История возникновения, становления и развития сети Интернет. Основные классы сервисов Интернета. Эволюция "Всемирной паутины" от Web 1.0 к Web 3.0. Особенности и преимущества Web 2.0.

		Основные факторы, способствующие в наше время повышению уязвимости информации в сети. Базовые негативные аспекты, возникающие в связи с развитием современных информационных технологий и глобальных сетей. Прошлое, настоящее и будущее Всемирной паутины.
2	Семантический Web как одно из направлений семантических технологий	Семантические технологии как один из видов современных инновационных технологий. Особенности инновационных технологий. Основные направления становления и развития семантических технологий. Базовые компоненты семантического Web. Преимущества Web 3.0 по сравнению с Web 2.0 и Web 1.0. Формула ценности Всемирной паутины с учётом сетевого эффекта.
3	Особенности современных социальных сетевых сервисов	Социальные поисковые системы. Современные социальные сети (Facebook, ВКонтакте, Одноклассники, Мой Круг, Twitter). Гендерный и возрастной анализ аудитории социальных сетей. Общий сценарий поведения пользователей для сетевых сервисов. Коллективные и персональные блоги. Вики-сервисы (Wikipedia, Letopisi). Социальные медиохранилища (Picasa, Flickr, Youtube). Особенности географических сервисов. Использование социальных сетевых сервисов в образовании.
4	Специфика деловой коммуникации в сетевых сообществах	Основные классы сетевых сообществ. Социальные, профессиональные и коммерческие сообщества. Особенности профессионально-ориентированных сетевых сообществ. Основные роли участников сетевых сообществ. Особенности корпоративных блогов. Базовые параметры интеллектуальных агентов в рамках деловой коммуникации. Особенности автономных интеллектуальных агентов.
<b>8 семестр</b>		
№	Наименование раздела дисциплины	Содержание
1	Информационные средства и способы воздействия на противника в современных условиях	Основные понятия и определения. Актуальность развития информационных средств и способов воздействия в современных информационных войнах. Развитие подходов к месту и роли информационного противоборства в современных информационных войнах. Концепция стратегического информационного доминирования. Концепции «стратегического паралича» и «навязанной стоимости». Операции на основе эффектов — третье поколение методов информационного противоборства. Общая классификация информационного оружия. Классификация технологий информационного противоборства, обеспечивающих разработку и применение информационного оружия.
2	Современные взгляды на роль и способы ведения информационного	Основные принципы доктрины информационного противоборства США. Стратегии кибербезопасности западноевропейских стран. Отличия представлений об информационной войне в ФРГ от американского.

	противоборства	Основные компоненты французской концепции информационной войны. Особенности китайской концепции информационной войны. Основные силы информационного противоборства за рубежом.
3	Информационное противоборство в технической сфере	Классификация базового информационно-технического оружия. Основные классы обеспечивающего информационно-технического оружия. Разновидности атакующего информационно-технического оружия. Основные способы реализации информационно-технического оружия. Использование информационно-технического оружия для борьбы с системами военного управления. Основные виды информационно-технических воздействий. Базовые классы основных средств информационно-технических воздействий. Особенности удалённых сетевых атак.
4	Информационное противоборство в психологической сфере	Основные задачи и области ведения информационно-психологического противоборства. Классификация психологических операций. Основные мероприятия психологических операций. Базовые эффекты, широко применяемые в психологических операциях. Основные области организации информационно-психологического воздействия. Классификация средств и методов информационно-психологического воздействия. Основные типы психологического оружия.

#### 4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
<b>7 семестр</b>			
1.	Особенности сети Интернет как коммуникационной среды	Лекция 1  Практическое занятие 1	Вводная лекция с использованием видеопроектора  опрос
2.	Семантический Web как одно из направлений семантических технологий	Лекция 2  Практическое занятие 2	Лекция с использованием видеопроектора  опрос
3.	Особенности современных социальных сетевых сервисов	Лекция 3  Практическое занятие 3	Лекция с использованием видеопроектора  опрос
4.	Специфика деловой коммуникации в сетевых сообществах	Лекция 4	Лекция с использованием видеопроектора  опрос



		Практическое занятие 4 Контрольная работа	Подготовка к контрольной с использованием материалов лекций и литературы
8 семестр			
№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Информационные средства и способы воздействия на противника в современных условиях	Лекция 1 Практическое занятие 1	Вводная лекция с использованием видеоматериалов Опрос
2.	Современные взгляды на роль и способы ведения информационного противоборства	Лекция 2 Практическое занятие 2	Лекция с использованием видеоматериалов опрос
3.	Информационное противоборство в технической сфере	Лекция 3 Практическое занятие 3	Лекция с использованием видеоматериалов опрос
4.	Информационное противоборство в психологической сфере	Лекция 4 Практическое занятие 4 Контрольная работа	Лекция с использованием видеоматериалов опрос Подготовка к контрольной с использованием материалов лекций и литературы

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

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

## 5. Оценка планируемых результатов обучения

### 5.1 Система оценивания

7 семестр

Форма контроля	Макс. количество баллов	
	За одну	Всего

	<b>работу</b>	
Текущий контроль: - <i>опрос</i> - <i>контрольная работа (темы 3-4)</i>	<i>10 баллов</i> <i>20 баллов</i>	<i>40 баллов</i> <i>20 баллов</i>
Промежуточная аттестация (традиционная форма)		<i>40 баллов</i>
<b>Итого за семестр</b> <i>зачёт</i>		<i>100 баллов</i>

## 8 семестр

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - <i>опрос</i> - <i>контрольная работа (темы 3-4)</i>	<i>10 баллов</i> <i>20 баллов</i>	<i>40 баллов</i> <i>20 баллов</i>
Промежуточная аттестация (традиционная форма)		<i>40 баллов</i>
<b>Итого за семестр</b> <i>зачёт</i>		<i>100 баллов</i>

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

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

## 5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

<b>Баллы/ Шкала ECTS</b>	<b>Оценка по дисциплине</b>	<b>Критерии оценки результатов обучения по дисциплине</b>
82-68/ С	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

#### ***Примерная тематика опросного задания***

1. Отличительные особенности защиты информации и информационной безопасности - ОПК-1.
2. На каком принципе построены практически все услуги сети Интернет? - УК-3.
3. Постройте иерархическую систему из понятий защита информации, компьютерная безопасность, информация, информационная безопасность - ОПК-1.
4. Особенности сетевого эффекта - ОПК-1.
5. Основные технологии, используемые для виртуального делового общения - УК-3.
6. Базовые отличия профессиональных сетевых сообществ от социальных - УК-3.

#### ***Примерная тематика контрольной работы***

1. Основные ресурсы сети Интернет - ОПК-1.
2. Базовые причины уязвимости информации в XXI веке - ОПК-1.
3. Основные негативные последствия при использовании современных технологий и сетей - ОПК-1.
4. Формула ценности Всемирной паутины с учётом сетевого эффекта - ОПК-1.
5. Основные задачи, решаемые сетевыми социальными сервисами социальных - УК-3.
6. Классификация блогов по авторскому составу социальных - УК-3.
7. Основные цели корпоративного блога социальных - УК-3.
  
8. Базовые параметры интеллектуальных агентов в рамках деловой коммуникации социальных - УК-3.

***Промежуточная аттестация (примерные контрольные вопросы по курсу)***

1. Особенности Web 2.0 - ОПК-1.
2. Классификация сервисов сети Интернет - ОПК-1.
3. Основные направления семантических технологий - ОПК-1.
4. Характеристика эпохи Интернет-2 в России - ОПК-1.
5. Основные правила нетикета - УК-3.
6. Базовые типы интернет-зависимости - ОПК-1.
7. Основные негативные аспекты, возникающие в связи с развитием современных информационных технологий и глобальных сетей - ОПК-1.
8. Основные симптомы зависимости от социальных сетей - ОПК-1.
9. Особенности Web 3.0 - ОПК-1.
10. Основные виды социальных сетевых сервисов - УК-3.
11. Базовые задачи, решаемые сетевыми социальными сервисами - УК-3.
12. Основные социальные поисковые системы - УК-3.
13. Особенности YouTube - УК-3.
14. Основные социальные медиохранилища - УК-3.
15. Использование социальных сетевых сервисов в образовании - УК-3.
16. Особенности сети ВКонтакте - УК-3.
17. Классификация сетевых сообществ - УК-3.
18. Особенности профессиональных сетевых сообществ - УК-3.
19. Основные роли участников профессиональных сетевых сообществ - УК-3.
20. Особенности корпоративных блогов - УК-3.

**Примерная тематика опросных заданий**

1. Базовые объекты информационной войны - УК-2.

2. Основные свойства средств информационного воздействия - ОПК-1.
3. Базовые задачи информационных операций - ОПК-1.
4. Основные типы информационно-технического воздействия на информацию - ОПК-1.
5. Классификация информационно-технического оружия- УК-2.
6. Основные виды информационного оружия - УК-2.

***Примерная тематика контрольной работы***

9. Основные способы реализации информационно-технического воздействия - ОПК-1.
10. Классификация средств оборонительных информационно-технических воздействий - ОПК-1.
11. Основные средства психофизического оружия - ОПК-1.
12. Классификация удалённых сетевых атак - УК-2.
13. Основные стадии жизненного цикла компьютерных вирусов - УК-2.
14. Классификация программных закладок - УК-2.
15. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - УК-2.
16. Социальные сети как новый инструмент для активации протестных настроений - ОПК-1.

***Промежуточная аттестация (примерные контрольные вопросы по курсу)***

21. Особенности стратегического информационного противоборства - ОПК-1.
22. Основные концепции информационного противоборства США - ОПК-1.
23. Базовые цели информационного противоборства - УК-2.
24. Основные направления ведения информационного противоборства - УК-2.
25. Базовые цели информационных операций - УК-2.
26. Основные сферы информационного противоборства - УК-2.
27. Базовые объекты воздействия в ходе информационных операций - УК-2.
28. Классификация информационных операций - УК-2.
29. Основные виды и способы информационного воздействия - ОПК-1.
30. Базовые виды информационного оружия - ОПК-1.
31. Основные группы технологий, обеспечивающих разработку и применение наступательного информационного оружия - ОПК-1.
32. Основные группы технологий, обеспечивающих разработку и применение оборонительного информационного оружия - ОПК-1.
33. Задачи информационных операций в соответствии с концепцией "Единые силы-

2020" США - УК-2.

34. Основные силы Китая для проведения киберопераций - УК-2.
35. Классификация информационно-технического оружия - ОПК-1.
36. Базовые типы информационно-технического воздействия на информацию - ОПК-1.
37. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - ОПК-1.
38. Классификация способов реализации удалённых сетевых атак - УК-2.
39. Основные классы программных закладок - УК-2.
40. Виды психологического оружия - УК-2.
41. Основные средства психофизического оружия - УК-2.
42. Базовые психотропные средства, используемые в военных целях - УК-2.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Список источников и литературы

а) источники:

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006, № 149-ФЗ. - Режим доступа: URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

2. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 гг. (утверждена Указом Президента Российской Федерации от 9 мая 2017 г., № 203).- Режим доступа: URL: <http://publication.pravo.gov.ru/Document/View/0001201705100002>

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М.: Стандартинформ, 2007. — 11 с. - Режим доступа: URL: <https://internet-law.ru/gosts/gost/8419/>

б) основная литература:

Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2024. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2131865>

Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography\_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2052391>

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2082642>

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

1. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: <http://www.intuit.ru>

2. Система "Академик". - Режим доступа: URL: <https://dic.academic.ru/dic.nsf/ruwiki/1334827>

3. Государственная публичная научно-техническая библиотека России. - Режим доступа: URL: <http://www.gpntb.ru>

Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)  
 ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)  
 Электронная библиотека Grebennikon.ru [www.grebennikon.ru](http://www.grebennikon.ru)

### 6.3 Профессиональные базы данных и информационно-справочные системы

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

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

### 7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, компьютером или ноутбуком, проектором (стационарным или переносным) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

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

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

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

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

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

При необходимости предусматривается увеличение времени для подготовки ответа.

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

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



использоваться собственные технические средства.

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

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

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

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

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA SE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1 Планы практических занятий**

Тема 1 (4 ч.). Интернет как коммуникационная среда

Вопросы для обсуждения:

1. Основные этапы развития сети Интернет - ОПК-1.
2. Отличия, существующие между сервисами Web 1.0 и Web 2.0 - ОПК-1.
3. Эволюция "Всемирной паутины" от Web 1.0 к Web 3.0 - УК-3.
4. Прошлое, настоящее и будущее Всемирной паутины - ОПК-1.
5. Каковы особенности Web 2.0? - УК-3.
6. Сущность закона Р. Меткалфа для сети - УК-3.
7. В чём особенности сетевого эффекта? - УК-3.
8. В чём заключаются негативные последствия при использовании современных технологий и сетей? - ОПК-1.

Тема 2 (6 ч.). Особенности семантического Web как разновидности семантических технологий

Вопросы для обсуждения:

1. Основные положительные аспекты, возникающие в связи с развитием современных информационных технологий и глобальных сетей - ОПК-1.
2. Базовые направления развития семантических технологий -УК-3.
3. Основные компоненты семантического Web -УК-3.

4. Преимущества Web 3.0 по сравнению с Web 2.0 и Web 1.0 -УК-3.
5. Формула ценности Всемирной паутины с учётом сетевого эффекта -УК-3.
6. Характеристика эпохи Интернет-2 в России -УК-3.
7. Базовые типы интернет-зависимости - ОПК-1.

Основные симптомы зависимости от социальных сетей - ОПК-1.

Тема 3 (6 ч.). Социальные сети в Интернете

Вопросы для обсуждения:

1. Современные зарубежные и российские социальные сети - ОПК-1.
2. Гендерный и возрастной анализ аудитории социальных сетей - ОПК-1.
3. Коллективные и персональные блоги - УК-3.
4. Особенности географических сервисов - УК-3.
5. В чём заключаются особенности сервиса WikiMapia?
6. Социальное медиохранилище Picasa - УК-3.
7. Особенности использования социальных сетевых сервисов в образовании - ОПК-1.
8. Характеристика сети ВКонтакте - УК-3.

Тема (4 ч.). Социальные, профессиональные и коммерческие сообщества в сети Интернет

Вопросы для обсуждения:

1. Особенности профессионально-ориентированных сетевых сообществ - УК-3.
2. Базовые параметры интеллектуальных агентов в рамках деловой коммуникации - ОПК-3.
3. Особенности корпоративных блогов - УК-3.
4. Особенности автономных интеллектуальных агентов - ОПК-3.
5. Характеристика сетевого социального сервиса как набора средств для взаимодействия коммуникантов - ОПК-3.
6. Основные классы сетевых сообществ - УК-3.
7. Особенности корпоративных блогов - УК-3.
8. Основные роли участников профессиональных сетевых сообществ - ОПК-3.

## **8 семестр**

Тема 1 (4 ч.). Особенности информационных операций

Вопросы для обсуждения:

1. Основные задачи информационных операций - ОПК-1.
2. Классификация информационных операций по целям и задачам - ОПК-1.
3. Отличия информационной войны от компьютерного преступления - УК-2.
4. Классификация информационных операций по характеру решаемых задач - ОПК-1.

5. В чём отличие информационной войны от компьютерного преступления? - УК-2.
6. Классификация информационных операций по целям и задачам - УК-2.
7. В чём сущность стратегии асимметричного противодействия противнику? - ОПК-1.
8. Какие используются основные мероприятия наступательных информационных операций? - УК-2.

Тема 2 (6 ч.). Особенности национальных концепций информационного противоборства

Вопросы для обсуждения:

8. Базовые принципы доктрины информационного противоборства США - УК-2.
9. Базовые компоненты французской концепции информационной войны - ОПК-1.
10. Отличия представлений об информационной войне в ФРГ от американского - ОПК-1.
11. Особенности китайской концепции информационного противоборства - УК-2.
12. Основные задачи командования США в киберпространстве - УК-2.
13. В чём особенности немецкой концепции информационной войны? - ОПК-1.
14. Особенности радиоэлектронной борьбы - УК-2.
15. Какие существуют основные подразделения армии Китая для проведения киберопераций? - ОПК-1.

Тема 3 (6 ч.). Классификация информационно-технического оружия

Вопросы для изучения и обсуждения:

9. Классификация атакующего информационно-технического оружия - УК-2.
10. Основные классы обеспечивающего информационно-технического оружия - УК-2.
11. Классификация информационно-технического оружия по способу реализации - УК-2.
12. Основные способы противодействия уничтожению командных структур противника - ОПК-1.
13. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - УК-2.
14. Базовые типы информационно-технического воздействия на информацию - ОПК-1.
15. Классификация средств оборонительных информационно-технических воздействий - ОПК-1.
16. Основные способы реализации информационно-технического воздействия - ОПК-1.

Тема 4 (4 ч.). Особенности информационного противоборства в психологической сфере

Вопросы для обсуждения:

1. Основные задачи, решаемые с помощью психологического оружия - УК-2.
2. Базовые типы психофизического оружия, основанные на суггестии - ОПК-1.
3. Использование Интернет и социальных сетей как нового средства информационно-психологического оружия - ОПК-1.
4. Основные средства информационно-психологического оружия - УК-2.
5. Базовые возможности психотропных средств, используемых для информационно-психологического воздействия на человека - УК-2.
6. Особенности когнитивного оружия - ОПК-1.
7. Основные средства психотронного оружия - УК-2.
8. Какие способы манипулирования информацией используют средства массовой информации? - ОПК-1.

9.2. Методические рекомендации по организации самостоятельной работы

Вид работы	Содержание (перечень вопросов)	Трудоем- кость самостоя- тельной работы (в часах)	Рекомендации
Подготовка к практическому занятию Тема 1. «Интернет как коммуникационная среда»	<p>Основные этапы развития сети Интернет.</p> <p>Отличия, существующие между сервисами Web 1.0 и Web 2.0.</p> <p>Эволюция "Всемирной паутины" от Web 1.0 к Web 3.0.</p> <p>Прошлое, настоящее и будущее Всемирной паутины.</p>	4	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006, № 149-ФЗ. - Режим доступа: URL: <a href="http://www.consultant.ru/document/cons_doc_LAW_61798/">http://www.consultant.ru/document/cons_doc_LAW_61798/</a></p> <p>Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы (утверждена Указом Президента Российской Федерации от 9 мая 2017г., № 203). Режим</p>

			<p>доступа: URL:  <a href="http://publication.pravo.gov.ru/Document/View/0001201705100002">http://publication.pravo.gov.ru/Document/View/0001201705100002</a></p> <p>Национальный открытый университет ИНТУИТ. -  Режим доступа: URL:  <a href="http://www.intuit.ru">http://www.intuit.ru</a></p>
<p>Подготовка к практическому занятию</p> <p>Тема 2.  «Особенности семантического Web как разновидности семантических технологий»</p>	<p>Основные положительные аспекты, возникающие в связи с развитием современных информационных технологий и глобальных сетей.</p> <p>Базовые направления развития семантических технологий.</p> <p>Основные компоненты семантического Web.</p> <p>Преимущества Web 3.0 по сравнению с Web 2.0 и Web 1.0.</p>	8	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Малинина Т.Б., Смертина Д.А. <a href="#">Феномен социальной сети в информационном обществе // Наука и бизнес: пути развития.</a> 2019, № 2 (92). С. 246-250.  - Режим доступа: URL: <a href="https://elibrary.ru/download/elibrary_37057075_65422952.pdf">https://elibrary.ru/download/elibrary_37057075_65422952.pdf</a></p> <p>Таратухина Ю.А. Деловая коммуникация в сфере информационных технологий: учебное пособие. М.: «ART-менеджер», 2011. — 200 с.  Режим доступа: URL: <a href="https://publications.hse.ru/mirror/pubs/share/folder/1n4rgl8r04/direct/67760217">https://publications.hse.ru/mirror/pubs/share/folder/1n4rgl8r04/direct/67760217</a></p> <p>Национальный открытый университет ИНТУИТ. -  Режим доступа: URL:  <a href="http://www.intuit.ru">http://www.intuit.ru</a></p> <p>1. Система "Академик". -  Режим доступа: URL:  <a href="https://dic.academic.ru/dic.nsf/ruwiki/1334827">https://dic.academic.ru/dic.nsf/ruwiki/1334827</a></p> <p>2. Государственная публичная научно-техническая библиотека России. -  Режим доступа: URL:  <a href="http://www.gpntb.ru">http://www.gpntb.ru</a></p>

<p>Подготовка к практическому занятию</p> <p>Тема 3. «Социальные сети в Интернете»</p>	<p>Современные зарубежные и российские социальные сети.</p> <p>Гендерный и возрастной анализ аудитории социальных сетей.</p> <p>Коллективные и персональные блоги.</p> <p>Особенности географических сервисов.</p>	8	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Далворт М. Социальные сети. Руководство по эксплуатации. - М.: Добрая книга. 2010 - 248 с. - Режим доступа: URL: <a href="https://ozon-st.cdn.ngenix.net/multimedia/1012301032.PDF">https://ozon-st.cdn.ngenix.net/multimedia/1012301032.PDF</a></p> <p>1. Леонтьев В. Социальные сети: ВКонтакте, Facebook и другие. Издательство: Литагент «Олма Медиа», 2012. - 170 с. - Режим доступа: URL: <a href="https://www.libfox.ru/544773-vitaliy-leontev-sotsialnye-seti-vkontakte-facebook-i-drugie.html">https://www.libfox.ru/544773-vitaliy-leontev-sotsialnye-seti-vkontakte-facebook-i-drugie.html</a></p> <p>Национальный открытый университет ИНТУИТ. - Режим доступа: URL: <a href="http://www.intuit.ru">http://www.intuit.ru</a></p> <p>Система "Академик". - Режим доступа: URL: <a href="https://dic.academic.ru/dic.nsf/ruwiki/1334827">https://dic.academic.ru/dic.nsf/ruwiki/1334827</a></p> <p>Государственная публичная научно-техническая библиотека России. - Режим доступа: URL: <a href="http://www.gpntb.ru">http://www.gpntb.ru</a></p>
<p>Подготовка к практическому занятию</p> <p>Тема 4. «Социальные, профессиональные и коммерческие сообщества в сети Интернет»</p>	<p>Особенности профессионально-ориентированных сетевых сообществ.</p> <p>Базовые параметры интеллектуальных агентов в рамках деловой коммуникации.</p> <p>Особенности корпоративных блогов.</p> <p>Особенности</p>	10	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Далворт М. Социальные сети. Руководство по эксплуатации. - М.: Добрая книга. 2010 - 248 с. - Режим доступа: URL: <a href="https://ozon-st.cdn.ngenix.net/multimedia">https://ozon-st.cdn.ngenix.net/multimedia</a></p>

	<p>автономных интеллектуальных агентов.</p>	<p><a href="#">/1012301032.PDF</a></p> <p>Таратухина Ю.А. Деловая коммуникация в сфере информационных технологий: учебное пособие. М.: «ART-менеджер», 2011. — 200 с. Режим доступа: URL: <a href="https://publications.hse.ru/mirror/pubs/share/folder/1n4rgl8r04/direct/67760217">https://publications.hse.ru/mirror/pubs/share/folder/1n4rgl8r04/direct/67760217</a></p> <p>Национальный открытый университет ИНТУИТ. - Режим доступа: URL: <a href="http://www.intuit.ru">http://www.intuit.ru</a></p> <p>Система "Академик". - Режим доступа: URL: <a href="https://dic.academic.ru/dic.nsf/ruwiki/1334827">https://dic.academic.ru/dic.nsf/ruwiki/1334827</a></p> <p>Государственная публичная научно-техническая библиотека России. - Режим доступа: URL: <a href="http://www.gpntb.ru">http://www.gpntb.ru</a></p>
--	---	--

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Цель дисциплины: формирование у обучающихся знаний о сущности информационных войн и информационного оружия, методов и способов их реализации, а также о возможностях информационного противоборства потенциальному противнику.

Задачи:

- раскрытие основных категорий информационной войны и базовых факторов, оказывающих влияние на её содержание;
- определение основных принципов, отражающих закономерности информационной войны;
- анализ базовых уровней общественного сознания, выступающего в качестве поля сражения;
- выявление основных классов и практических видов информационного оружия;
- установление базовых мероприятий по предотвращению или нейтрализации последствий применения информационного оружия;
- раскрытие практических мероприятий программного характера по защите от информационного оружия.

Дисциплина направлена на формирование следующих компетенций:

УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1 Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач

УК-2.2 Способность использования знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.

УК-3 - Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

УК-3.1 Понимает эффективность использования стратегии сотрудничества для достижения поставленной цели; определяет роль каждого участника в команде;

УК-3.2 Эффективно взаимодействует с членами команды; участвует в обмене информацией, знаниями и опытом; содействует презентации результатов работы команды; соблюдает этические нормы взаимодействия

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-1.1 Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации

ОПК-1.2 Умеет классифицировать и оценивать угрозы информационной безопасности

ОПК-1.3 Владеет основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.