

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.  
ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»  
Профили: Организация и технология защиты информации (по отрасли  
или в сфере профессиональной деятельности)  
Безопасность автоматизированных систем (по отрасли  
или в сфере профессиональной деятельности)  
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2021

Гуманитарные аспекты информационной безопасности.  
Информационное противоборство  
Рабочая программа дисциплины  
Составитель:  
д.т.н, профессор В.В. Арутюнов

Ответственный редактор  
к.и.н., доцент, заведующая кафедрой  
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО  
Протокол заседания кафедры информационной безопасности  
№ 10 от 20.05.2021

## **ОГЛАВЛЕНИЕ**

### **1. Пояснительная записка**

### **2. Пояснительная записка**

1.1 Цель и задачи дисциплины (*модуля*)

1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

### **2. Структура дисциплины (*модуля*)**

### **3. Содержание дисциплины (*модуля*)**

### **4. Образовательные технологии**

### **5. Оценка планируемых результатов обучения**

5.1. Система оценивания

5.2. Критерии выставления оценок

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

### **6. Учебно-методическое и информационное обеспечение дисциплины**

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### **7. Материально-техническое обеспечение дисциплины (*модуля*)**

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

### **9. Методические материалы**

9.1. Планы практических занятий

## **Приложения**

Приложение 1. Аннотация дисциплины

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля): 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. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (модулю):

Компетенция (код и название)	Индикаторы компетенций (код и наименование)	Результаты обучения
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	Знать: основные способы реализации информационно-технического воздействия; Уметь: пользоваться нормативно-правовыми документами в сфере защиты информации; Владеть: навыками работы с нормативно-правовыми документами в сфере защиты информации;
	УК-2.2 способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов	Знать: нормы действующего российского права для определения круга задач профессиональной деятельности; Уметь: ставить цели и выбирать пути эффективного решения задач в области защиты информации;

		Владеть: навыками применения норм российского законодательства в профессиональной деятельности;
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	Знать: базовый понятийный аппарат в области защиты информации, информационных войн и информационного оружия; основные методы и приемы информационного противоборства Уметь: применять полученные знания в научно-исследовательской работе; Владеть: навыками определения угроз информации применительно к объектам защиты в условиях информационного противоборства;
	ОПК-1.2 умеет классифицировать и оценивать угрозы информационной безопасности	Знать: состав, классификацию информационного оружия и основные способы его применения; Уметь: применять способы и средства защиты информации в условиях информационного противоборства; Владеть: навыками определения направлений защиты информации с учетом характера защищаемой информации и задач по ее защите.
	ОПК-1.3 владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формами их проявления в современном мире	Знать: основные нормативно-правовые документы в профессиональной деятельности; Уметь: пользоваться нормативно-правовыми документами в области защиты информации; Владеть: навыками работы с нормативно-правовыми документами в сфере защиты информации.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина (модуль) «Гуманитарные аспекты информационной безопасности. Информационное противоборство» 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 (модуля)

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)					Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная						
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Информационные средства и способы воздействия на противника в современных условиях	8	4		4			4	опрос
2	Современные взгляды на роль и способы ведения информационного противоборства	8	2		6			8	опрос
3	Информационное противоборство в технической сфере	8	4		6			8	опрос
4	Информационное противоборство в психологической сфере	8	6		8			10	опрос, контрольная работа
	<b>Итого</b>		<b>16</b>		<b>24</b>			<b>36</b>	

## 3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
1	Информационные средства и способы воздействия на противника в современных условиях	<p>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.</p> <p>Общая классификация информационного оружия. Классификация технологий информационного противоборства, обеспечивающих разработку и применение информационного оружия.</p>
2	Современные взгляды на роль и способы ведения информационного противоборства	<p>Основные принципы доктрины информационного противоборства США. Стратегии кибербезопасности западноевропейских стран. Отличия представлений об информационной войне в ФРГ от американского. Основные компоненты французской концепции информационной войны. Особенности китайской концепции информационной войны. Основные силы информационного противоборства за рубежом.</p>
3	Информационное противоборство в технической сфере	<p>Классификация базового информационно-технического оружия. Основные классы обеспечивающего информационно-технического оружия. Разновидности атакующего информационно-технического оружия. Основные способы реализации информационно-технического оружия.</p> <p>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.</p>
4	Информационное противоборство в психологической сфере	<p>Основные задачи и области ведения информационно-психологического противоборства. Классификация психологических операций. Основные мероприятия психологических операций. Базовые эффекты, широко применяемые в психологических операциях.</p> <p>Основные области организации информационно-психологического воздействия.</p> <p>Классификация средств и методов информационно-психологического воздействия. Основные типы психологического оружия.</p>

#### 4. Образовательные технологии

При реализации рабочей программы дисциплины используются следующие образовательные технологии:

№ 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

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

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

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
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	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ С	зачтено	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F, FX	не зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

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

**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**

1. Основные способы реализации информационно-технического воздействия - ОПК-1.
2. Классификация средств оборонительных информационно-технических воздействий - ОПК-1.
3. Основные средства психофизического оружия - ОПК-1.
4. Классификация удалённых сетевых атак - УК-2.
5. Основные стадии жизненного цикла компьютерных вирусов - УК-2.
6. Классификация программных закладок - УК-2.
7. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - УК-2.
8. Социальные сети как новый инструмент для активации протестных настроений - ОПК-1.

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

1. Особенности стратегического информационного противоборства - ОПК-1.
2. Основные концепции информационного противоборства США - ОПК-1.
3. Базовые цели информационного противоборства - УК-2.
4. Основные направления ведения информационного противоборства - УК-2.
5. Базовые цели информационных операций - УК-2.
6. Основные сферы информационного противоборства - УК-2.
7. Базовые объекты воздействия в ходе информационных операций - УК-2.
8. Классификация информационных операций - УК-2.
9. Основные виды и способы информационного воздействия - ОПК-1.
10. Базовые виды информационного оружия - ОПК-1.
11. Основные группы технологий, обеспечивающих разработку и применение

наступательного информационного оружия - ОПК-1.

12. Основные группы технологий, обеспечивающих разработку и применение оборонительного информационного оружия - ОПК-1.
13. Задачи информационных операций в соответствии с концепцией "Единые силы-2020" США - УК-2.
14. Основные силы Китая для проведения киберопераций - УК-2.
15. Классификация информационно-технического оружия - ОПК-1.
16. Базовые типы информационно-технического воздействия на информацию - ОПК-1.
17. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - ОПК-1.
18. Классификация способов реализации удалённых сетевых атак - УК-2.
19. Основные классы программных закладок - УК-2.
20. Виды психологического оружия - УК-2.
21. Основные средства психофизического оружия - УК-2.
22. 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. 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/>

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

б) основная литература:

1. Макаренко С.П. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. — СПб.: Научные технологии, 2017. — 546с. Режим доступа: URL: <https://sccs.intelgr.com/editors/Makarenko/Makarenko-InfPro.pdf>

2. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: <http://znanium.com/catalog/product/1013794>

в) дополнительная литература:

1. Расторгуев С.П., Литвиненко М.В. Информационные операции в сети Интернет / Под общ. ред. А.Б. Михайловского. — М.: АНО ЦСОиП, 2014. — 128 с. - Режим доступа: URL: <http://csef.ru/media/articles/5173/5173.pdf>
2. Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с. - Режим доступа: URL: <https://www.litmir.me/br/?b=276514&p=1>
3. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. - 90 с. - Режим доступа: URL: <https://mgimo.ru/upload/iblock/486/%D0%A1%D1%83%D0%BB%D0%B5%D0%B9%D0%BC%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0%20%D0%A8.%D0%A1.%20%D0%9D%D0%B0%D0%B7%D0%B0%D1%80%D0%BE%D0%B2%D0%B0%20%D0%95.%D0%90.%20-%D0%98%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%98%D0%9E%D0%9D%D0%9D%D0%AB%D0%95%20%D0%92%D0%9E%D0%99%D0%9D%D0%AB.pdf>
4. Добрышин М.М. Особенности применения информационно-технического оружия при ведении современных гибридных войн // I-methods. 2020. Т. 12. № 1. С. 1-11. - Режим доступа: [https://elibrary.ru/download/elibrary\\_43130611\\_41634805.pdf](https://elibrary.ru/download/elibrary_43130611_41634805.pdf)

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

1. Национальный открытый университет ИНТУИТ. - Режим доступа: URL: <http://www.intuit.ru>
2. Димлевич Н. Информационные войны в киберпространстве - США // Pentagonus. 2010. — Режим доступа: URL: [http://pentagonus.ru/publ/informacionnye\\_vojny\\_v\\_kiberprostranstve\\_ssha\\_i/80-1-0-1610](http://pentagonus.ru/publ/informacionnye_vojny_v_kiberprostranstve_ssha_i/80-1-0-1610)
3. Манойло А. В. Объекты и субъекты информационного противоборства // Пси-Фактор. 2003. — Режим доступа: URL: <https://psyfactor.org/lib/psywar24.htm>

#### Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г.

	Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

### 7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

### Состав программного обеспечения (ПО)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

## **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 CE;
  - 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.). 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.

Список источников и литературы:

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/>

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

Макаренко С.П. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. — СПб.: Научные технологии, 2017. — 546с. Режим доступа: URL: <https://sccs.intelgr.com/editors/Makarenko/Makarenko-InfPro.pdf>

Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. — М.: Международный издательский центр «Этносоциум», 2017. — 90 с. — Режим доступа: URL: <https://mgimo.ru/upload/iblock/486/%D0%A1%D1%83%D0%BB%D0%B5%D0%B9%D0%BC%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0%20%D0%A8.%D0%A1.%20%D0%9D%D0%B0%D0%B7%D0%B0%D1%80%D0%BE%D0%B2%D0%B0%20%D0%95.%D0%90.%20-%D0%98%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%98%D0%9E%D0%9D%D0%9D%D0%AB%D0%95%20%D0%92%D0%9E%D0%99%D0%9D%D0%AB.pdf>

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

Димлевич Н. Информационные войны в киберпространстве - США // Pentagonus. 2010. — Режим доступа: URL: [http://pentagonus.ru/publ/informacionnye\\_vojny\\_v\\_kiberprostranstve\\_ssha\\_i/80-1-0-1610](http://pentagonus.ru/publ/informacionnye_vojny_v_kiberprostranstve_ssha_i/80-1-0-1610)

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

Вопросы для обсуждения:

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

Список литературы:

Макаренко С.П. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. — СПб.: Научно-технические технологии, 2017. — 546с. - Режим доступа: URL: <https://sccs.intelgr.com/editors/Makarenko/Makarenko-InfPro.pdf>

Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с. - Режим доступа: URL: <https://www.litmir.me/br/?b=276514&p=1>

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

Димлевич Н. Информационные войны в киберпространстве - США // Pentagonus. 2010. — Режим доступа: URL: [http://pentagonus.ru/publ/informacionnye\\_vojny\\_v\\_kiberprostranstve\\_ssha\\_i/80-1-0-1610](http://pentagonus.ru/publ/informacionnye_vojny_v_kiberprostranstve_ssha_i/80-1-0-1610)

Манойло А. В. Объекты и субъекты информационного противоборства // Пси-Фактор. 2003. — Режим доступа: URL: <https://psyfactor.org/lib/psywar24.htm>

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

Вопросы для изучения и обсуждения:

1. Классификация атакующего информационно-технического оружия - УК-2.
2. Основные классы обеспечивающего информационно-технического оружия - УК-2.
3. Классификация информационно-технического оружия по способу реализации - УК-2.

4. Основные способы противодействия уничтожению командных структур противника - ОПК-1.

5. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки - УК-2.

6. Базовые типы информационно-технического воздействия на информацию - ОПК-1.

7. Классификация средств оборонительных информационно-технических воздействий - ОПК-1.

8. Основные способы реализации информационно-технического воздействия - ОПК-1.

#### Список литературы

Макаренко С.П. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. — СПб.: Научно-технологические технологии, 2017. — 546с. - Режим доступа: URL: <https://sccs.intelgr.com/editors/Makarenko/Makarenko-InfPro.pdf>

Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/catalog/product/1013794>

Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с. - Режим доступа: URL: <https://www.litmir.me/br/?b=276514&p=1>

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

Димлевич Н. Информационные войны в киберпространстве - США // Pentagonus. 2010. — Режим доступа: URL: [http://pentagonus.ru/publ/informacionnye\\_vojny\\_v\\_kiberprostranstve\\_ssha\\_i/80-1-0-1610](http://pentagonus.ru/publ/informacionnye_vojny_v_kiberprostranstve_ssha_i/80-1-0-1610)

Добрышин М.М. Особенности применения информационно-технического оружия при ведении современных гибридных войн // I-methods. 2020. Т. 12. № 1. С. 1-11. - Режим доступа: [https://elibrary.ru/download/elibrary\\_43130611\\_41634805.pdf](https://elibrary.ru/download/elibrary_43130611_41634805.pdf)

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.

#### Список литературы

Макаренко С.П. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. — СПб.: Научные технологии, 2017. — 546 с. - Режим доступа: URL: <https://scs.intelgr.com/editors/Makarenko/Makarenko-InfPro.pdf>

Расторгуев С. П., Литвиненко М. В. Информационные операции в сети Интернет / Под общ. ред. А.Б. Михайловского. — М.: АНО ЦСОиП, 2014. — 128 с. - Режим доступа: URL: <http://csef.ru/media/articles/5173/5173.pdf>

Ларина Е.С., Овчинский В.С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. — М.: Книжный мир, 2014. — 352 с. - Режим доступа: URL: <https://www.litmir.me/br/?b=276514&p=1>

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

Манойло А. В. Объекты и субъекты информационного противоборства // Пси-Фактор. 2003. — Режим доступа: URL: <https://psyfactor.org/lib/psywar24.htm>

## АННОТАЦИЯ

Дисциплина (модуль) «Гуманитарные аспекты информационной безопасности. Информационное противоборство» реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.

Цель дисциплины (модуля): 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.

Дисциплина (модуль) направлена на формирование следующей компетенции:

- 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;
- В результате освоения дисциплины (модуля) обучающийся должен:
- Анализирует имеющиеся ресурсы и ограничения, оценивает и выбирает оптимальные способы решения поставленных задач
  - способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов

- ОПК-1 - способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

В результате освоения дисциплины (модуля) обучающийся должен:

- знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации
- умеет классифицировать и оценивать угрозы информационной безопасности
- владеет основными понятиями, связанные с обеспечением информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формами их проявления в современном мире

По дисциплине (модулю) предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины (модуля) составляет 2 зачетные единицы.