МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(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»
«Комплексная защита объектов информатизации»

Уровень квалификации выпускника (*бакалавр*)
Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

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
№ 5 от 24.01.2017

ОГЛАВЛЕНИЕ

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)*:

Коды компе-тенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	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; ставить цели и выбирать пути эффективного решения задач в области защиты информации Владеть: навыками определения угроз информации применительно к объектам защиты в условиях информационного противоборства; опытом выявления причин, обстоятельств и условий дестабилизирующего воздействия на защищаемую информацию со стороны источников воздействия.

ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	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-5	способность использовать нормативные правовые акты в профессиональной деятельности	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», «Защита информационных процессов в автоматизированных системах».

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

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 44 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Информационные средства и способы воздействия на	8	4		2			8	опрос

	противника в современных условиях								
2	Современные взгляды на роль и способы ведения информационного противоборства	8	2		2			8	опрос
3	Информационное противоборство в технической сфере	8	6		4			14	опрос
4	Информационное противоборство в психологической сфере	8	6		4			14	опрос, контрольная работа
5	Зачет	8							Зачет по билетам
	Итого		**16**		**12**			**44**	

3. Содержание дисциплины (модуля)

№	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 противоборства	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.
3	Информационное противоборство в технической сфере	Классификация базового информационно-технического оружия. Основные классы обеспечивающего информационно-техническое 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

При реализации рабочей программы дисциплины используются следующие образовательные технологии:

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1	**2**	**3**	**5**
1.	Информационные средства и способы воздействия на противника в современных условиях	Лекция 1 Семинар 1	Вводная лекция с использованием видеоматериалов Опрос
2.	Современные взгляды на роль и способы ведения информационного противоборства	Лекция 2 Семинар 2	Лекция с использованием видеоматериалов опрос
3.	Информационное противоборство в технической сфере	Лекция 3 Семинар 3	Лекция с использованием видеоматериалов опрос

4.	Информационное противоборство в психологической сфере	Лекция 4 Семинар 4 Контрольная работа	Лекция с использованием видеоматериалов опрос Подготовка к контрольной с использованием материалов лекций и литературы

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*
Итого за семестр *зачёт*		*100 баллов*

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

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	1	ОК-5, ОПК-4	План практического занятия
2.	2	ОК-5	План практического занятия
3.	3	ОПК-4, ОПК-5	План практического занятия
4.	4	ОПК-4, ОПК-5	План практического занятия Контрольная работа

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		A
83 – 94		зачтено	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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	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 выставляются 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

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются 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 выставляются 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 *(модулю)*

Текущий контроль (вариант опросного задания)

Вопросы	***Реализуемая компетенция***
1. Базовые объекты информационной войны.	***ОК-5***
2. Основные свойства средств информационного воздействия.	***ОПК-4***
3. Базовые задачи информационных операций.	***ОК-5***
4. Основные типы информационно-технического воздействия на информацию.	***ОПК-4***

Примерная тематика контрольной работы - проверка сформированности компетенций ОК-5, ОПК-4, ОПК-5

1. Основные способы реализации информационно-технического воздействия.
2. Классификация средств оборонительных информационно-технических воздействий.
3. Основные средства психофизического оружия.

4. Классификация удалённых сетевых атак.
5. Основные стадии жизненного цикла компьютерных вирусов.
6. Классификация программных закладок.
7. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки.
8. Социальные сети как новый инструмент для активации протестных настроений.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций ОК-5, ОПК-4, ОПК-5

1. Особенности стратегического информационного противоборства.
2. Основные концепции информационного противоборства США.
3. Базовые цели информационного противоборства.
4. Основные направления ведения информационного противоборства.
5. Базовые цели информационных операций.
6. Основные сферы информационного противоборства.
7. Базовые объекты воздействия в ходе информационных операций.
8. Классификация информационных операций.
9. Основные виды и способы информационного воздействия.
10. Базовые виды информационного оружия.
11. Основные группы технологий, обеспечивающих разработку и применение наступательного информационного оружия.
12. Основные группы технологий, обеспечивающих разработку и применение оборонительного информационного оружия.
13. Задачи информационных операций в соответствии с концепцией "Единые силы-2020" США.
14. Основные силы Китая для проведения кибероперацій.
15. Классификация информационно-технического оружия.
16. Базовые типы информационно-технического воздействия на информацию.
17. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки.
18. Классификация способов реализации удалённых сетевых атак.
19. Основные классы программных закладок.
20. Виды психологического оружия.
21. Основные средства психофизического оружия.
22. Базовые психотропные средства, используемые в военных целях.

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: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9034#008124909983936601

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://www.consultant.ru/document/cons_doc_LAW_216363/

б) основная литература:

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

2. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060

в) дополнительная литература:

Гришина, Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-105165-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/612572

г) базы данных, информационно-справочные и поисковые системы:

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

2. Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

3. Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru

д) Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press

	ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	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.

Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	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, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - *проверка сформированности компетенций ОК-5, ОПК-4, ОПК-5*

Планы практических занятий

Практическое занятие 1. (Тема 1). Особенности информационных операций - **(2 часа)** - ***проверка сформированности компетенций ОК-5, ОПК-4***

Вопросы для изучения и обсуждения:

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

Контрольные вопросы:

1. В чём отличие информационной войны от компьютерного преступления?
2. Классификация информационных операций по целям и задачам.
3. В чём сущность стратегии ассиметричного противодействия противнику?
4. Какие используются основные мероприятия наступательных информационных операций?

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:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9034#008124909983936601

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://www.consultant.ru/document/cons_doc_LAW_216363/

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

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

Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru

Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru

Практическое занятие 2. (Тема 2). Особенности национальных концепций информационного противоборства - **(2 часа) - *проверка сформированности компетенций* - ОК-5**

Вопросы для изучения и обсуждения:

1. Базовые принципы доктрины информационного противоборства США.
2. Базовые компоненты французской концепции информационной войны.
3. Отличия представлений об информационной войне в ФРГ от американского.
4. Особенности китайской концепции информационного противоборства.

Контрольные вопросы:

1. Основные задачи командования США в киберпространстве.
2. В чём особенности немецкой концепции информационной войны?
3. Особенности радиоэлектронной борьбы.
4. Какие существуют основные подразделения армии Китая для проведения кибероперaций?

Список литературы:

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

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

Практическое занятие 3. (Тема 3). Классификация информационно-технического оружия - **(2 часа) - *проверка сформированности компетенций* - ОПК-4, ОПК-5**

Вопросы для изучения и обсуждения:

1. Классификация атакующего информационно-технического оружия.
2. Основные классы обеспечивающего информационно-технического оружия.
3. Классификация информационно-технического оружия по способу реализации.
4. Основные способы противодействия уничтожению командных структур противника.

Контрольные вопросы:

1. Основные уязвимости ИС, позволяющие проводить против них успешные удалённые сетевые атаки.
2. Базовые типы информационно-технического воздействия на информацию.
3. Классификация средств оборонительных информационно-технических воздействий.
4. Основные способы реализации информационно-технического воздействия

Список литературы

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

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

Практическое занятие 4. (Тема 4). Особенности информационного противоборства в психологической сфере - **(2 часа)** - ***проверка сформированности компетенций*** - **ОПК-4, ОПК-5**

Вопросы для изучения и обсуждения:

1. Основные задачи, решаемые с помощью психологического оружия.
2. Базовые типы психофизического оружия, основанные на суггестии.
3. Использование Интернет и социальных сетей как нового средства информационно-психологического оружия.
4. Основные средства информационно-психологического оружия.

Контрольные вопросы:

1. Базовые возможности психотропных средств, используемых для информационно-психологического воздействия на человека.
2. Особенности когнитивного оружия.
3. Основные средства психотронного оружия.
4. Какие способы манипулирования информацией используют средства массовой информации?

Список литературы

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

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

10. Методические рекомендации по организации самостоятельной работы

Трудоемкость освоения дисциплины «Гуманитарные аспекты информационной безопасности. Информационное противоборство» составляет 72 часа, из них 44 часа отведены на самостоятельную работу студента (СР).

Вид работы	**Содержание (перечень вопросов)**	**Трудоемкость самостоятельной работы (в часах)**	**Рекомендации**
Подготовка к практическому занятию Тема 1. «Особенности информационных операций»	Основные задачи информационных операций. Классификация информационных операций по целям и задачам. Отличия информационной войны от компьютерного преступления. Классификация информационных операций по характеру решаемых задач.	8	Проанализировать материал из законодательных, нормативных документов, учебников: ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М.: Стандартинформ, 2007. — 11 с. - Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=90341#008124909983936601 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://www.consultant.ru/document/cons_doc_LAW_216363/

			Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: http://znanium.com/catalog/product/1013794 Национальный открытый университет ИНТУИТ. URL: Режим доступа: http://www.intuit.ru Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru
Подготовка к практическому занятию Тема 2 «Особенности национальных концепций информацион-ного противоборства»	Основные принципы доктрины информационного противоборства США. Базовые компоненты французской концепции информационной войны. Отличия представления об информационной войне в ФРГ от американского. Особенности китайской концепции информационного противоборства.	8	Проанализировать материал из законодательных, нормативных документов, учебников: Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: http://znanium.com/catalog/product/1013794 Поликарпов В.С., Шибанов В.Е., Поликарпова Е.В., Румянцев К.Я. Философские Национальный открытый университет ИНТУИТ. URL: Режим доступа: http://www.intuit.ru
Подготовка к	Классификация	14	Проанализировать

практическому занятию Тема 3 «Классификация информационно-технического оружия»	атакующего информационно-технического оружия. Основные классы обеспечивающего информационно-технического оружия. Классификация информационно-технического оружия по способу реализации. Основные способы противодействия уничтожению командных структур противника.		материал из законодательных, нормативных документов, учебников: Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: http://znanium.com/catalog/product/1013794 Национальный открытый университет ИНТУИТ. URL: Режим доступа: http://www.intuit.ru
Подготовка к практическому занятию Тема 4 «Особенности информационного противоборства в психологической сфере»	Основные задачи, решаемые с помощью психологического оружия. Базовые типы психофизического оружия, основанные на суггестии. Использование Интернет и социальных сетей как нового средства информационно-психологического оружия. Основные средства информационно-психологического оружия.	14	Проанализировать материал из законодательных, нормативных документов, учебников: Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. Режим доступа: URL: http://znanium.com/catalog/product/1013794 Национальный открытый университет ИНТУИТ. URL: Режим доступа: http://www.intuit.ru

Приложение 1

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 следующих компетенций:

- ОК-5 - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- ОПК-4 - способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен:

***Знать**:*

- базовый понятийный аппарат в области защиты информации, информационных войн и информационного оружия;
- основные нормативно-правовые документы в профессиональной деятельности;
- состав, классификацию информационного оружия и основные способы его применения;
- основные методы и приемы информационного противоборства.

***Уметь**:*

- пользоваться нормативно-правовыми документами в области защиты информации;
-применять полученные знания в научно-исследовательской работе;
- применять способы и средства защиты информации в условиях информационного противоборства;
- ставить цели и выбирать пути эффективного решения задач в области защиты информации.

***Владеть**:*

- навыками работы с нормативно-правовыми актами в сфере защиты информации;
- навыками определения угроз информации применительно к объектам защиты в условиях информационного противоборства;
- опытом выявления причин, обстоятельств и условий дестабилизирующего воздействия на защищаемую информацию со стороны источников воздействия;
- навыками определения направлений защиты информации с учетом характера защищаемой информации и задач по ее защите.

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

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

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017 г.*	***10***
2	*Обновлена основная и дополнительная литература*	*26.06.2018 г.*	***20***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***20***
4	*Обновлена основная и дополнительная литература*	*29.08.2019 г.*	***1***
5	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	***1***
6	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020 г*	***14***
7	*Обновлена основная и дополнительная литература*	*23.06.2020 г*	***14***
8	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020 г*	***14***
9	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020 г*	***14***

Приложение 1
к листу изменений

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
д.т.н, профессор В.В. Арутюнов

Приложение 2
к листу изменений

2.Обновление основной и дополнительной литературы (2018 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

2. Дополнить раздел ***Основная литература***

Поликарпов В.С., Шибанов В.Е., Поликарпова Е.В., Румянцев К.Я. Философские проблемы информационного противоборства: учебное пособие. - Ростов-на-Дону: Издательство Южного федерального университета, 2018. - 210 с. - Режим доступа: URL: http://znanium.com/bookread2.php?book=1021754

3.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

1. Перечень ПО

Таблица 1

№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 Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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

2. Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г.

	Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

д.т.н, профессор, В.В. Арутюнов

Приложение 3
к листу изменений

4.Обновление основной и дополнительной литературы (2019 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Дополнительная литература*

Марков А.А., Быстрянцев С.Б., Краснова Г.В. Информационное общество. Информационная безопасность. Информационные войны. Санкт-Петербург: Санкт-Петербургский государственный экономический университет. 2019. - 124 с. - Режим доступа: URL: https://elibrary.ru/download/elibrary_37614822_10040872.pdf

Миронов С.И., Шангараев Р.Н. Психологические аспекты информационного противоборства противодействие террористической идеологии // Научно-аналитический журнал Обозреватель - Observer. 2019. № 1 (348). С. 66-75. - Режим доступа: URL: https://elibrary.ru/download/elibrary_36881475_88487374.pdf

5.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень 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 Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г.

	Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 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

Составитель:

д.т.н, профессор, В.В. Арутюнов

Приложение 4
к листу изменений

6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Информационные средства и способы воздействия на противника в современных условиях	8	4		2			8	опрос
2	Современные взгляды на роль и способы ведения информационного противоборства	8	2		2			8	опрос
3	Информационное противоборство в технической сфере	8	6		4			14	опрос
4	Информационное противоборство в психологической сфере	8	4		4			18	опрос, контрольная работа
	Итого		**16**		**12**			**48**	

7. Обновление дополнительной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

1. Дополнить раздел **Дополнительная литература**

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

Муза Д.Е., Артамонов В.С. Актуальное геополитическое информационное противоборство Запада и России // Национальная безопасность и стратегическое планирование. 2020. № 1 (29). С. 66-70. - Режим доступа: URL: https://elibrary.ru/download/elibrary_42745677_73291909.pdf

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

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.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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 Statisctics 22	IBM	лицензионное

7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 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

Составитель:

д.т.н, профессор, В.В. Арутюнов