МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.ДВ.04.02 Информационные войны**

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки №4 "Безопасность автоматизированных систем" (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Учебная дисциплина «Информационные войны» обеспечивает формирование углубленного понимания значения информации в современных условиях и знаний в области информационной безопасности автоматизированных систем.

Цели освоения учебной дисциплины «Информационные войны»**:**

1) формирование представления и знаний о развитии информационных войн и их влиянии на информационную безопасность;

2) формирование умений противостоять информационным атакам, регулировать информационные потоки, осознавать социальную ответственность будущей профессиональной деятельности.

Задачи освоения учебной дисциплины**:**

1) понимание методов формирования общественного мнения о государственных и частных, коммерческих и некоммерческих организациях, общественных явлениях;

2) изучение принципов защиты информации в условиях информационного противоборства;

3) подготовка к решению организационно-управленческих, коммуникационных и иных информационных задач.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационные войны» является дисциплиной по выбору вариативной части профессионального цикла. Дисциплина является вводной в проблематику информационных войн и информационного противоборства. Взаимосвязь данной дисциплины через компетенции отражена в рабочем учебном плане и матрице компетенций. Дисциплина опирается на знания, полученные в ходе изучения дисциплин «Математические модели политики информационной безопасности», «Информационная безопасность государственных информационных систем», которая должна быть освоена полностью и студенты должны владеть навыками применения моделей политики информационной безопасности.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Защита объектов критической информационной инфраструктуры», «Комплексное обеспечение информационной безопасности автоматизированных систем», а так же для учебной и производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения принципов обеспечения безопасности автоматизированных систем.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующей компетенции:

ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты.

ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

В результате изучения дисциплины студент должен:

Знать:

- основные принципы информационной войны, виды информационного оружия, средства его разработки и методы анализа;

- основные методы оценки поражающих факторов информационного оружия, надежных средствах констатации его применения;

- алгоритмы различения информационной войны, контрпропаганды, антирекламы;

- особенности проведения информационной войны и возможности адаптации к ней.

Уметь:

- разрабатывать специальные информационные мероприятия и применять их для защиты информации;

- оценивать риски и оправданность применения специальных информационных мероприятий;

- формировать требования к защите информации в условиях ведения информационных войн;

- оценивать значение информационной безопасности в развитии современного общества.

Владеть:

- навыками быстрого и эффективного отбора исходных материалов для подготовки специальных информационных мероприятий;

- навыками быстрого распознавания проводимой информационной войны и определения ее субъектов;

- навыками минимизации ущерба от проведенных в отношении своих или дружественных организаций специальных информационных мероприятий.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		7			
Аудиторные занятия (всего)	52/1,44	52/1,44			
В том числе:	-	-	-	-	-
Лекции	26/0,72	26/0,72			
Практические занятия (ПЗ)	26/0,72	26/0,72			
Семинары (С)					
Лабораторные работы (ЛР)					
КСР	4/0,11	4/0,11			
Контроль					
Самостоятельная работа (всего)	88/2,45	88/2,45			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	56/1,55	56/1,55			
Общая трудоемкость часы	144	144			
зачетные единицы	4	4			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

РАЗДЕЛ 1 Информационные войны в современном мире.

Тема 1.1. Информационные войны в структуре современной цивилизации.

История информационного противоборства. Становление информационного общества. Понятие «информационная война». Отличия информационной войны от войн, ведущихся традиционными средствами.

Тема 1.2. Информационная кампания.

Законы и принципы ведения информационных войн. Информационное воздействие на личность. Информационно-психологические операции, как организационная форма реализации концепции информационной войны.

Тема 1.3. Модель информационной войны.

Модели управления общественным мнением. Уровни информационного воздействия. Модель переноса экономической нестабильности в политическую. Молодежь как целевая группа информационных войн.

РАЗДЕЛ 2 Способы и средства информационной войны.

Тема 2.1. Информационные войны в мирное и военное время.

Основные технологии информационных войн. Информационно-психологическое воздействие на кризисные ситуации, социально-политические конфликты. Терроризм как инструмент информационной войны. Особенности информационных войн в мирное и военное время.

Тема 2.2. Инструментарий информационной войны.

Классификация информационного оружия: наступательное и оборонительное, информационно-психологическое и информационно-техническое. Средства поражения техники, программного обеспечения, каналов связи. Особенности информационного оружия. Борьба за контроль и использование информационного пространства.

Тема 2.3. Стратегии трансформации информационного пространства.

Информационная война как комплекс активных методов трансформации информационного пространства. Изменения структуры информационного пространства. Замедление или ускорение информационных процессов.

РАЗДЕЛ 3. Информационная безопасность в условиях информационной войны.

Тема 3.1. Информационная война в интернете и средствах массовой информации.

СМИ и Интернет как информационное оружие. Способы и средства отражения информационного нападения в Интернет. Тематические интернет-форумы, как целевые аудитории информационных войн. Особенности восприятия информации в зависимости от типа СМИ. Средства поражения техники, программного обеспечения, каналов связи.

Тема 3.2. Информационная составляющая национальной безопасности.

Глобализация мира и информационная война. Возможные угрозы суверенитету и национальной безопасности. Информационная безопасность государства. Основные направления государственной политики в информационной сфере. Стратегия запрета информации.

Тема 3.3. Информационные войны и безопасность в будущем.

Понятие и значение информационной безопасности в структуре национальной безопасности. Пути предотвращения информационных войн. Противодействие информационному нападению. Эффективность защиты. Направленность удара информационного оружия на человеческий разум. Защита от физических атак и защита от

атак на каналы восприятия человеческого мозга. Информационная война как атака на структуры порождения информации. Роль простых средств коммуникативного воздействия. Глобальное информационное пространство. Информационные войны в будущем.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Защита объектов критической информационной инфраструктуры	2 (2.1-2.3) 3 (3.1-3.3)
2	Комплексное обеспечение информационной безопасности автоматизированных систем	1 (1.1-1.3) 3 (3.1-3.3)
3	Практика по получению первичных профессиональных умений и навыков	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)
4	Эксплуатационная практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)
5	Проектно-технологическая практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3)

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1.1	2	2			9	13
2.	***Раздел 1***	Тема 1.2	2	2			9	13
3.	***Раздел 1***	Тема 1.3	2	4			10	16
4.	***Раздел 2***	Тема 2.1	2	2			10	14
5.	***Раздел 2***	Тема 2.2	2	2			10	14

6.	***Раздел 2***	Тема 2.3	4	4			10	18
7.	***Раздел 3***	Тема 3.1	4	2			10	16
8.	***Раздел 3***	Тема 3.2	4	4			10	18
9.	***Раздел 3***	Тема 3.3	4	4			10	18

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1. Тема 1.1.***	ПЗ. 1. Виды информационной войны.	2	Тестовый контроль по теме	ПК-3 ПК-10
2.	***Раздел 1. Тема 1.2.***	ПЗ. 2. Пропагандистские кампании в истории и современности.	2	Тестовый контроль по теме	ПК-3 ПК-10
3.	***Раздел 1. Тема 1.3.***	ПЗ. 3. Информационно-психологическая война в современном мире.	4	Тестовый контроль по теме	ПК-3 ПК-10
4.	***Раздел 2. Тема 2.1.***	ПЗ 4. «Холодная война»: анализ информационного противостояния двух систем.	2	Тестовый контроль по теме	ПК-3 ПК-10
5.	***Раздел 2. Тема 2.2.***	ПЗ 5. Характеристики информационного оружия.	2	Тестовый контроль по теме	ПК-3 ПК-10
6.	***Раздел 2. Тема 2.3.***	ПЗ 6. Эффективность информационного пространства.	4	Тестовый контроль по теме	ПК-3 ПК-10
7.	***Раздел 3. Тема 3.1.***	ПЗ 7. Информационные войны в интернет и манипуляции в СМИ.	2	Тестовый контроль по теме	ПК-3 ПК-10
8.	***Раздел 3. Тема 3.2.***	ПЗ 8. Влияние новых информационных технологий на картину мира современного человека.	4	Тестовый контроль по теме	ПК-3 ПК-10
9.	***Раздел 3. Тема 3.3.***	ПЗ 9. Способы и эффективность защиты от информационного оружия.	4	Тестовый контроль по теме	ПК-3 ПК-10

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1.1-1.3**	Решение задач к практическим занятиям	Повторение и углубленное изучение	Учебный сайт	28

		Подготовка к защите лабораторных работ	учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов		
8-15	**2.1-2.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	30
16-20	**3.1-3.3**	Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	30
21		Подготовка доклада с презентацией		Учебный сайт	
22		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Информационная безопасность государственных информационных систем», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка рефератов;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Информационные войны», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

1. Воронова О. Е. Современные информационные войны: типология и технологии: монография: Рязанский государственный университет имени С. А. Есенина, 2018, - 188 с. https://e.lanbook.com/book/164490.

2. Лингвистика информационно-психологической войны. Книга II: Монография / А. А. Бернацкая и др. Сибирский Федеральный Университет**,** 2019, - 488 с. https://e.lanbook.com/book/157702.

3. Лингвистика информационно-психологической войны. Книга III: Монография / А. А. Бернацкая и др. Сибирский Федеральный Университет, 2020, - 344 с. https://e.lanbook.com/book/181614.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225,

оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Информационные войны» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при

выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (9 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

Пз. 1 Разновидности информационных войн и их особенности.
.

Пз. 2 Примеры пропагандистских кампаний, цели и результаты.

Пз. 3 Отличительные черты информационно-психологической войны в современном мире.

Пз. 4 Анализ информационного противостояния в «Холодной войне», результаты и уроки.

Пз. 5 Что разрушает информационное оружие?

Пз.6 Объекты и результаты воздействия в информационной войне.

Пз.7 Инструменты отражения информационного нападения в Интернет.

Пз. 8 Влияние новых информационных технологий на проведение информационной войны.

Пз. 9 Оценка эффективности защиты от информационного оружия.

11.3. Оценочные средства для текущего контроля в форме тестирования

Тестовые вопросы для проверки сформированности компетенций

ПК-3. Способность администрировать подсистемы информационной безопасности объекта защиты.

1. Не являются методами информационной войны …

А) деятельность хакеров

Б) террористические провокации

В) электронно-магнитное воздействие

2. Внутренние источники угроз информационной безопасности Российской Федерации (укажите все правильные варианты ответов)

А) снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

Б) недостаточный государственный контроль за развитием информационного рынка;

В) разработка рядом государств концепции информационных войн

3. Информационная война – это …

А) действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты

Б) любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты

В) любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты

4. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….

А) информационная война

Б) информационное оружие

В) информационное превосходство

5. Поражающее воздействие информационного оружия, прежде всего направлено на

А) информационные системы

Б) мозг человека

В) информационные продукты

6. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

А) информационная война

Б) информационное оружие

В) информационное превосходство

7. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:

А) Информационная безопасность

Б) Безопасность

В) Защита информации

8. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником это:

А) Информационная война

Б) Информационное оружие

В) Информационное превосходство

9. Внешние источники угроз информационной безопасности Российской Федерации…(укажите все правильные варианты ответов)

А) увеличение технологического отрыва ведущих стран мира, их противодействие созданию конкурентоспособных информационных технологий

Б) недостаточная экономическая мощь государства

В) обострение международной конкуренции за обладание информационными технологиями и ресурсами

10. К национальным интересам РФ в информационной сфере относятся:

А) Реализация конституционных прав на доступ к информации

Б) Политическая экономическая и социальная стабильность

В) Сохранение и оздоровлении окружающей среды

11. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие? (укажите все правильные варианты ответов)

А) Информационный саботаж
Б) Физический саботаж
В) Информационные инфекции

12. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:

А) Информационная безопасность
Б) Защита информации
В) Национальная безопасность

ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

1. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

А) Безопасность АС
Б) Угрозы информационной безопасности
В) Политика безопасности

2. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а так же системы регулирования возникающих при этом общественных отношений

А) Информационная сфера
Б) Информационные услуги
В) Информационные продукты

3. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…»

А) Информация с ограниченным доступом
Б) Информация, распространение которой наносит вред интересам общества
В) Объект интеллектуальной собственности

4. Защищенность от негативных информационно-психологических и информационно-технических воздействий:

А) Защита информации
Б) Компьютерная безопасность
В) Защищенность потребителей информации

5. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:

А) Интересы личности в информационной сфере
Б) Интересы общества
В) Интересы общества в информационной сфере

6. Какова основная цель коммерческих информационных агентств?

А) Получение и продажа информации;
Б) Оперативное донесение достоверной информации до власти и общественности;
В) Развитие образования и повышение интеллектуального уровня населения.

7. Меняет ли полученная людьми информация на их повседневное поведение?

А) Нет, не меняет, за исключением рекламного воздействия на индивидов;

Б) Да, меняет, хотя люди не всегда это ясно осознают;

В) Слабо меняет под воздействием отечественного и зарубежного кино.

8. Что понимается под термином «независимый источник информации»?

А) информатор из финансовых кругов, обладающий инсайдерскими данными.

Б) информатор из состава спецслужб иностранного государства;

В) информатор, лично не заинтересованный в замалчивании или приукрашивании передаваемых в СМИ сведений;

9. Является ли сознательное искажение информации об истории государства правонарушением?

А) является шуткой, пародией и не считается правонарушением;

Б) государства является правонарушением, тяжесть которого зависит от намерений лица (или лиц), фальсифицирующих историю и распространяющих данные сведения;

В) является троллингом ответственных лиц;

10. Является ли детское кино и мультфильмы инструментом воспитания детей и юношества?

А) Нет, не является, поскольку мультфильмы, а также кинокартины для детей и юношества не несут в себе чуждых ценностей;

Б) Да, является, поскольку в детском и юношеском возрасте наиболее активно формируется характер, ценности человека;

В) Детское кино и мультфильмы воспитывают и перевоспитывают людей среднего возраста и пенсионеров;

11. Являются ли вредоносные программы информационным продуктом?

А) Да, являются, поскольку могут быть объектом купли-продажи на информационных рынках;

Б) Нет, не являются, поскольку компьютерные программы не являются товаром, предназначенном для реализации;

В) Вредоносные программы предназначены для причинения ущерба или вымогательства денежных средств, а не для продажи всем желающим, поэтому информационным продуктом не являются.

12. Помогает ли адекватное управление информацией поддерживать конкурентоспособность государствам, компаниям, силовым структурам, физлицам?

А) Нет, не помогает, поскольку конкурентоспособность государства и компаний зависит от силы армии, мощи экономики, имиджа и репутации на мировой арене;

Б) Да, помогает, поскольку правильно подобранная информация необходима в рекламе, пропаганде, продвижении торговых марок, в формировании имиджа людям и событиям;

В) Должным образом подобранная конфиденциальная информация помогает телефонным мошенникам обманывать рядовых граждан;

11.4. Оценочные средства для промежуточной аттестации

(в форме зачета).

Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Примерный перечень вопросов и заданий к зачету

1. Информационные войны в структуре современной цивилизации
2. Статус информации в современной информационной цивилизации.
3. Модели управления общественным мнением.
4. Междисциплинарный характер проблематики информационных войн.
5. Информационная борьба и информационная безопасность.
6. Информационный суверенитет государства.
7. Информационная война как коммуникативная технология.
8. Дестабилизирующая информация.
9. Цели и роль новых моделей поведения информационных войн.
10. Информационная кампания.
11. Информационная война и методы планирования кампании.
14. Методы создания резонанса в информационной кампании.
15. Классификации целевой аудитории информационной кампании.
16. Холодная война СССР-США как пример информационной войны.
17. Рост возможностей информационного воздействия на массовое сознание.
18. Отличие категории информационная война от категории психологическая война.
19. Примеры успешных информационных войн в современном мире.
20. Модель переноса экономической нестабильности в политическую.
21. Информационно-культурная агрессия, отбор информационных сообщений для СМИ.
22. Молодежь как целевая группа информационных войн.
23. Отличие войны в обычном понимании этого термина и войны информационной.
24. Факторы увеличения эффективности информационной операции.
25. Информационные операции как часть военной стратегии государства.
26. Информационная составляющая национальной безопасности
27. Возможные угрозы суверенитету и национальной безопасности.
28. Информационная безопасность государства.
29. Основные направления государственной политики в информационной сфере.
30. Информационное пространство государства: потоки формирования
31. Информационная безопасность: контроль, санкции, креативность, позитив.
32. Пропагандистские кампании
33. Инструментарий информационной войны
34. Новые возможности использования информации в современном обществе.
35. Роль техники и СМИ в информационной войне.
36. Свойства информационного пространства и построение инструментария.
37. Трансформаторы информационного пространства.
38. Информационное оружие в контексте основных видов коммуникативного воздействия
39. Особенности информационного оружия
40. Особенности ведения информационной войны в Интернете.
41. Информационное оружие и возможности нового этапа развития цивилизации.
42. Борьба за контроль и использование информационного пространств.
43. Характеристики информационного оружия.

Разработчики:

_____	профессор	Ерохин В.В.
(подпись)	(занимаемая должность)	(Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«20» 03 2020 г. Протокол № 8

И.о.зав. кафедрой  Колесник С.Н.