Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ И.В. Бабина
«__» _____ 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.10.01 «СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Соляной В.Н. Рабочая программа дисциплины: «Социотехносферная безопасность объектов информационной защиты». – Королев МО: «Технологический университет», 2022.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 17.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

1.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целями изучения дисциплины являются:

1. Дать студентам базовые знания по основам обеспечения социотехносферной безопасности ключевых объектов информационной защиты на предприятиях, организациях и учреждений в современных условиях;

2. Выработать и закрепить у студентов первичные умения и навыки по организации и реализации технологий социотехносферной безопасности объектов информационной защиты на предприятиях (организациях и учреждений) с различными формами собственности с учетом современных подходов обеспечения информационной безопасности.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ПК-1. Способен проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности;

ПК-2. Способен принимать участие в проведении экспериментальных исследований системы защиты информации;

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

Основными **задачами** дисциплины являются:

1. Показать актуальность существующей проблемы обеспечения социотехносферной безопасности функционирования типовых объектов информационной защиты на предприятиях, учреждениях и организациях (современных информационных систем);

2. Изложить, с научно-практической направленностью, теоретические основы социотехносферной безопасности субъектов информационной защиты (индивидуумов, социума);

3. Изложить, с научно-практической направленностью, теоретические основы социотехносферной безопасности функционирования современных технических средств и систем обработки информации;

4. Дать основы моделирования эффективности процессов обеспечения социотехносферной безопасности функцинирования информационных объектов современных социотехнических систем;

5. Сформулировать типовые основы организации обеспечения социотехносферной безопасности функционирования объектов информационной защиты на предприятиях (организациях, учреждениях);

6. Ознакомить с возможными правовыми основами обеспечения социотехносферной (энергоинформационной) безопасности - проектами

концепций обеспечения региональной и глобальной энергоинформационной безопасности государства.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

Необходимые умения:

- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);
- применять действующую нормативную базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;
- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;

Трудовые действия:

- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);
- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;
- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Социотехносферная безопасность объектов информационной защиты» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)»,

прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часа; для студентов очной формы составляет 3 зачетных единицы, 108 часа.

Таблица1

Виды занятий	**Всего часов**	**Семестр 6**	**Семестр …**	**Семестр 7**	**Семестр …**
Общая трудоемкость	108	108		108	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	50	50			
Другие виды контактной работы	10	10			
Практическая подготовка	16	16			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	**Экзамен**	**Экзамен**			

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4.Содержание дисциплины
4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Практическая подготовка, час	Код компетенций
Раздел 1. **Общие теоретические положения по социотехносферной безопасности информационных объектов**					
Тема 1**. Введение в проблему обеспечения социотехносферной безопасности социотехнических систем**	2	4	2	3	ПК-1
Тема 2. **Теоретико-прикладные основы обеспечения социотехносферной безопасности индивидуума и социума**	2	4	4	3	ПК-1
Тема 3. **Теоретические основы обеспечения социотехносферной безопасности технических средств и систем**	2	6	4	3	ПК-2
Раздел 2. **Базовые практические положения по социотехносферной безопасности объектов информационной защиты**					
Тема 4. **Основы моделирования и оценки эффективности процессов по обеспечению социотехносферной безопасности**	2	6	4	3	ПК-2
Тема 5. **Социотехносфер**	4	6	4	2	ПК-3

ная безопасность предприятия (учреждения, организации)					
Тема 6. **Региональная и глобальная социотехносферная безопасность государства**	4	6	2	2	ПК-3
Итого:	16	322	90	162	

4.2. Содержание тем дисциплины

I раздел. *Общие теоретические положения по социотехносферной безопасности информационных объектов*

Тема 1. Введение в проблему обеспечения социотехносферной безопасности социотехнических систем

Понятие о социотехнических системах и основы их обеспечения безопасности.

Базовые положения по обеспечению социотехносферной безопасности информационных объектов социотехнических систем.

Основные направления развития социотехносферной безопасности в современных условиях.

Концептуальная модель обеспечения энергоинформационной безопасности. Мифы и реальности обеспечения энергоинформационной безопасности.

Тема 2. Теоретико-прикладные основы обеспечения социотехносферной безопасности индивидуума и социума

Концептуальные подходы обеспечения энергоинформационной безопасности человека (личности) и социума как субъектов информационной защиты в системе информационной безопасности.

Источники дестабилизирующих энергоинформационных воздействий на индивидуума /социум/ и их возможности: люди; техника и природа.

Энергоинформационные угрозы и их влияние на человека и на социум.

Особенности воздействия скрытых электромагнитных полей на субъекта и на социум.

Типовые признаки и основные этапы энергоинформационных скрытых воздействий на личность и на социум.

Тема 3. Теоретические основы информационные социотехносферной безопасности технических средств и систем

Научные основы влияния деструктивных энергоинформационных воздействий на технические средства и системы объектов информационной защиты.

Особенности обеспечения энергоинформационной безопасности функционирования технических средств.

Базовые положения по обеспечению энергоинформационной безопасности функционирования технических систем.

Возможности использования скрытых энергоинформационных излучений для реализации безопасных информационных технологий (связи, навигации и разведки).

II раздел. *Базовые практические положения по социотехносферной безопасности объектов информационной защиты*

Тема 4. Основы моделирования и оценки эффективности процессов по обеспечению социотехносферной безопасности

Обобщенная модель взаимодействия информации, энергии и материи Вселенной (энергоинформационная модель мирового пространства).

Основы выявления и оценки эффективности деструктивных энергоинформационных воздействий на объекты и субъекты информационной защиты: люди/персонал; техника/технологические процессы и строительные конструкции(помещения, здания и защитные устройства).

Инструментальные методы обнаружения и оценки эффективности скрытых деструктивных энергоинформационных воздействий.

Тема 5. Социотехносферная безопасность предприятия (учреждения, организации)

Общие положения по обеспечению энергоинформационной (социотехносферной) безопасности функционирования предприятия (фирмы).

Особенности влияния скрытых деструкттивных энергоинформационных воздействий малой интенсивности на деятельность фирмы (предприятия) и целесообразные организационно-правовые мероприятия по обеспечения социотехносферной безопасности в системе информационной безопасности предприятия.

Основы технического направления обеспечения социотехносферной безопасность предприятия по противодействию несанкционированному доступу к защищаемому информационному ресурсу (объектам и субъектам) в условиях воздействия скрытых деструктивных энергоинформационных излучений малой интенсивности.

Тема 6. Региональная и глобальная социотехносферная безопасность государства

Проблемы обеспечения глобальной и региональной социотехносферной безопасности государства.

Современные информационные войны между государствами и роль в них социотехносферной безопасности.

Энергоинформационное оружие – главная скрытая информационная угроза национальной безопасности страны с современных условиях.

Эниология (космоэнергетика) в мирной деятельности государства.

Основы разработки Концепции энергоинформационной (социотехносферной) безопасности государства.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

1. «Методические указания для обучающихся по освоению дисциплины», представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

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

Основная литература:

1.Чернов, К. В. Управление техносферной безопасностью / К. В. Чернов. — Санкт-Петербург : Лань, 2023. — 160 с. — ISBN 978-5-507-45029-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book76575 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Титова, Т. С. Система управления техносферной безопасностью : методические указания / Т. С. Титова, Р. Г. Ахтямов. — Санкт-Петербург : ПГУПС, 2017. — 23 с. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book01566 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Управление техносферной безопасностью : учебное пособие / И. С. Мартынов, М. Н. Шапров, Е. Ю. Гузенко [и др.]. — Волгоград : Волгоградский ГАУ, 2019. — 108 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book39210 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.
4.Соколов, А. К. Управление техносферной безопасностью : учебное пособие / А. К. Соколов. — Иваново : ИГЭУ, 2018. — 140 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book54587 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Электронные книги:

1. Энергоинформационная педагогика.
http://library.kpi.kharkov.ua/NEW/Podlasyy_Energo.pdf

2. Информационная безопасность в режиме «сетевой войны»
http://fanread.ru/book/3731798/?page=1

3. Эниология: от догадок к современной науке
http://lib100.com/book/unknown/hf_1/%D4%E8%F0%FC%FF%E7%20%D5%E0%ED%F6%E5%E2%E5%F0%EE%E2,%20%DD%ED%E8%EE%EB%EE%E3%E8%FF,%20%F2%EE%EC%201.pdf

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

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.iso27000.ru/ - портал по управлению информационной безопасностью.

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: *MS Office.*

Информационные справочные системы:

1. Справочно-правовая система «Консультант плюс».
2. Электронные ресурсы образовательной среды Университета.
3. Рабочая программа и методическое обеспечение по дисциплине «Социотехносферная безопасность объектов информационной защиты».

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций/слайдов.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows XP; офисные программы MS Office 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает::		
				Требуемые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способность проводить исследования защищенности информационных объектов на соответствие требованиям нормативно-правовых актов и стандартов в области информационной безопасности	Тема:1 -6	- выполнять обнаружение, идентификацию и устранение инцидентов ИБ (ЗИ);	- выявлять и оценивать источники и последствия инцидентов ИБ (ЗИ);	- нормативно-правовые акты и стандарты в области ИБ и принципы проведения диагностики системы ЗИ;
2.	ПК-2	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	Тема:1,-6	- разрабатывать модели, проекты и предложения в ходе проведения экспериментов деятельности по совершенствованию системы ЗИ;	- применять действующую нормативну ю базу выбирать целесообразные потребные средства и определять структуру системы ЗИ в ходе проведения экспериментов;	- руководящие и методические документы принципы организации по проведению экспериментальной деятельности в области ЗИ;
3.	ПК-3	Способность осуществлять управление с	Темы 1 -6	- анализировать	- оценивать информационные риски	- основные нормативно-правовые акты,

		разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС		воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию	разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;	методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-1,2,3	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно.*** ***Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
ПК-1,2,3	***Доклад***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не</u>***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).***

		сформирована) – 2 и менее баллов	***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).*** ***Максимальная сумма баллов - 5 баллов.***
ПК-1,2,3	***Выполнение контрольной работы***	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Становление эниологии (энергоинформационной безопасности) как новое направлению обеспечения ИБ.
2. Непознанные явления в природе и обществе как основа эниологии.
3. Эниологии как научно-прикладное направление ИБ.
4. Эниология (энергоинформационная безопасность) в системе современного мировоззрения.
5. Научно-прикладные аспекты эниологических явлений информационной безопасности.
6.Обзор и классификация эниофеноменов в системе ИБ.
7. Организационные аспекты эниологии (энергоинформационной безопасности).

8. Эниология и чрезвычайные ситуации в системе ИБ.
9. Законодательные аспекты современной эниологии (энергоинформационной безопасности).
10. Фундаментальные основы содержания эниологических феноменов в системе ИБ.
11. Электромагнитные аспекты сущности эниологических феноменов.

12. Информационно-прикладная интерпретация эниофеноменов в системе ИБ.
13. Экспериментальная проверка эниофеноменов в области ИБ.
14. Геопланитарные эниоявления в ИБ: наличие и влияние геопатогенных мест (зон).

Примерная тематика контрольной работы:
1. Человек как резонатор электромагнитной модели эниофеноменов в системе ИБ.
2. Космический энергоинформационный обмен в системе обеспечения ИБ**.**
3. Космос и эниологии в современной системе ИБ.
4. Энергоинформационная безопасность (эниология) архитектуры (конструкций) объектов информационной защиты.
5. Энергоинформационный контакт с «неизвестным разумом» при обеспечении ИБ.
6. Энергоинформационные ритмы в системе обеспечения ИБ.
7. Биоритмы и обеспечение ИБ.
8. Влияние энергоинформационных ритмов развития общества при обеспечении ИБ государства.
9. Современное информационное оружия XXI века во взаимосвязи с энергоинформационными процессами.
10. Космическое энергоинформационное оружие в системе ИБ.
11. Особенности энергоинформационных воздействий на человека и общество.
12. Эниологическая (энергоинформационная) безопасность и искусственный разум в системе ИБ.
13. Биолокационный метод анализа энергоинформационной обстановки при обеспечении ИБ.
14. Организация энергоинформационного медико-психологического экспресс-метода анализа состояния персонала как субъектов ИБ.
15. Экспертная эниослужба при обеспечении информационной безопасности компьютерных сетей.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Социотехносферная безопасность объектов информационной защиты» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1,2,3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1,2,3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***

Проводится в сроки, установленные графиком образовательного процесса	Экзамен	ПК-1,2,3	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено

						практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Когда возникла компьютерная криптография?
- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

2. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:
- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

3. Сколько уровней в эталонной модели OSI?
- 1
- 13
- 10
- 7

4. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?
- 2000
- 1967
- 1998
- 2008

5. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?
- да
- нет
- для государственных учреждений нет, а для комерческих предприятий да
- только для иностранных компаний, действующих на территории России

6. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)
- канальный

- представления
- прикладной
- сеансовый

7. В каком ГОСТ-е дано определение термину "служебная тайна"?
- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

Типовые вопросы, выносимые на экзамен

1. Понятие о социотехнических системах и основы их обеспечения безопасности.

2. Базовые положения по энергоинформационной безопасности социотехнических систем.

3. Основные направления развития энергоинформационной безопасности в современных условиях.

4. Концептуальная модель обеспечения энергоинформационной безопасности.

5. Мифы и реальности обеспечения энергоинформационной безопасности.

6. Концептуальные подходы обеспечения энергоинформационной безопасности человека (личности).

7. Энергоинформационные угрозы и их влияние на человека.

8. Особенности воздействия электромагнитных волн на субъекта.

9. Типовые признаки и основные этапы энергоинформационных воздействий на личность.

10. Источники дестабилизирующих энергоинформационных воздействий на индивидуумов и их возможности.

11. Научные основы влияния энергоинформационных воздействий на технические средства и системы.

12. Особенности обеспечения энергоинформационной безопасности функционирования технических средств.

13. Базовые положения по обеспечению энергоинформационной безопасности функционирования технических систем.

14. Возможности использования энергоинформационных излучений для реализации безопасных информационных технологий (связи, навигации и разведки).

15. Обобщенная модель взаимодействия информации, энергии и материи Вселенной (энергоинформационная модель мирового пространства).

16. Основы эффективности энергоинформационных воздействий.

17. Инструментальные методы обнаружения и оценки эффективности энергоинформационных воздействий.

18. Общие положения по обеспечению энергоинформационной безопасности функционирования предприятия (фирмы).

19. Особенности влияния энергоинформационных воздействий на деятельность фирмы и привлекаемые технические средства обеспечения энергоинформационной безопасности.

20. Энергоинформационная безопасность бизнеса и противодействие несанкционированному доступу к защищаемому информационному ресурсу в условиях воздействия энергоинформационных излучений.

21. Проблемы обеспечения глобальной/региональной энергоинформационной безопасности государства.

22. Энергоинформационное оружие – главная угроза национальной безопасности страны.

23. Классификация энергоинформационного оружия.

24. Характеристика информационно-технического оружия.

25. Энергоинформационное оружие программно-технического воздействия.

26. Природные энергоинформационные деструктивные воздействия.

27. Современные информационные войны между государствами и роль в них области энергоинформационной безопасности.

28. Основы разработки (базовые положения) Концепции энергоинформационной безопасности государства.

29. Становление энергоинформационной безопасности (эниологии) как область обеспечения ИБ.

30. Неопознанные явления в природе, обществе и на производстве как основы причин становления эниологии.

31. Эниология как научно-прикладное направление ИБ.

32. Эниология (энергоинформационная безопасность) в системе современного мировоззрения.

33. Основные научно-прикладные аспекты эниологических явлений в области ИБ.

34. Обзор и классификация эниофеноменов в системе ИБ.

35. Организационные аспекты эниологии (энергоинформационной безопасности).

36. Соотношение эниологии и чрезвычайных ситуаций в системе ИБ.

37. Законодательные аспекты современной эниологии (энергоинформационной безопасности).

38. Фундаментальные основы сущности и содержания эниологических феноменов в системе ИБ.

39. Электромагнитные аспекты сущности эниологических феноменов.

40. Информационно-прикладная интерпретация эниофеноменов в системе ИБ.

41. Понятие об экспериментальной проверки эниофеноменов в области ИБ.

42. Геопланитарные эниоявления в системе обеспечения ИБ: влияние геопатогенных зон (областей).

43. Человек как резонатор электромагнитной модели эниофеноменов в системе ИБ.

44. Понятие о космическом энергоинформационном обмене в системе обеспечения ИБ.

45. Космос в системе обеспечения энергоинформационной безопасности современных социотехнических систем.

46. Энергоинформационная безопасность (эниологические аспекты) архитектуры (строительных конструкций) объектов информационной защиты.

47. Понятие об энергоинформационном контакте с «неизвестным разумом» при обеспечении ИБ.

48. Понятие об энергоинформационных природных ритмах при обеспечении ИБ.

49. Понятие и роль биоритмов в деятельности человека (коллективов) при обеспечении ИБ.ю

50. Основы влияния энергоинформационных ритмов развития общества при обеспечении ИБ государства.

51.Современное информационное оружие XXI века во взаимосвязи с энергоинформационными процессами.

52. Космическое энергоинформационное оружие (деструктивные воздействия) в системе ИБ.

53. Основы энергоинформационных воздействий на человека и общество.

54. Энергоинформационная безопасность и искусственный разум в системе ИБ.

55. Биологический метод анализа энергоинформационной обстановки при обеспечении ИБ.

56. Экспертная эниослужба при обеспечении ИБ компьютерных сетей.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является: овладеть обучаемыми знаниями, умениями и навыками (профессиональными компетенциями) по обеспечению социотехносферной безопасности функционирования информационных объектов и субъектов современных организаций (предприятий и учреждений) в условиях воздействия скрытых деструктивных энергоинформационных угроз малой интенсивности.

Задачами дисциплины являются:

1. Обосновать актуальность существующей проблемы по обеспечению социотехносферной безопасности современных социотехнических систем (предприятий, учреждений, организаций, фирм и их субъектов);
2. Изложить с научно-практической направленностью основы энергоинформационной безопасности отдельной личности (субъекта) и социума в целом;
3. Дать теоретико-прикладные основы социотехносферной безопасности функционирования технических систем и средств, строительных конструкций и инженерных сооружений в объектах информационной защиты;
4. Довести основы моделирования процессов обеспечения энергоинформационной безопасности социотехнических систем;
5. Сформулировать типовые практические направления обеспечения социотехносферной безопасности современных предприятий, организаций и учреждений;
6. Показать роль, место и содержание социотехносферной безопасности на региональном и глобальном уровнях существования государства как составляющая современной системы информационной войны.

2. Указания по проведению практических занятий

Раздел 1. *Общие теоретические положения по социотехносферной безопасности информационных объектов*

Тема 1. Введение в проблему обеспечения социотехносферной безопасности социотехнических систем

Практическое занятие 1.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания о социотехнических системах и основы их обеспечения безопасности.

Основные положения темы занятия:

Базовые положения по обеспечению социотехносферной безопасности информационных объектов социотехнических систем.

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.

Продолжительность занятия – 5 ч.

Тема 2. Теоретико-прикладные основы обеспечения социотехносферной безопасности индивидуума и социума

Практическое занятие 2.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Изучить концептуальные подходы обеспечения энергоинформационной безопасности человека (личности) и социума как субъектов информационной защиты в системе информационной безопасности.

Основные положения темы занятия:

Источники дестабилизирующих энергоинформационных воздействий на индивидуума /социум/ и их возможности: люди; техника и природа.

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Мифы и реальности обеспечения энергоинформационной безопасности.

Продолжительность занятия – 5 ч.

Тема 3. Теоретические основы информационные социотехносферной безопасности технических средств и систем

Практическое занятие 3.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Изучить научные основы влияния деструктивных энергоинформационных воздействий на технические средства и системы объектов информационной защиты.

Основные положения темы занятия:

Особенности обеспечения энергоинформационной безопасности функционирования технических средств.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Возможности использования скрытых энергоинформационных излучений для реализации безопасных информационных технологий (связи, навигации и разведки).

Продолжительность занятия – 5 ч.

2. раздел. Базовые практические положения по социотехносферной безопасности объектов информационной защиты

Тема 4. Теоретические основы информационные социотехносферной безопасности технических средств и систем

Практическое занятие 4.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Узнать обобщенную модель взаимодействия информации, энергии и материи Вселенной (энергоинформационная модель мирового пространства).

Основные положения темы занятия:

Основы выявления и оценки эффективности деструктивных энергоинформационных воздействий на объекты и субъекты информационной защиты: люди/персонал; техника/технологические процессы и строительные конструкции(помещения, здания и защитные устройства). Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Инструментальные методы обнаружения и оценки эффективности скрытых деструктивных энергоинформационных воздействий.

Продолжительность занятия – 5 ч.

Тема 5. Социотехносферная безопасность предприятия (учреждения, организации)

Практическое занятие 5.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Изучить общие положения по обеспечению энергоинформационной (социотехносферной) безопасности функционирования предприятия (фирмы).

Основные положения темы занятия:

Выявить особенности влияния скрытых деструкттивных энергоинформационных воздействий малой интенсивности на деятельность фирмы (предприятия) и целесообразные организационно-правовые мероприятия по обеспечения социотехносферной безопасности в системе информационной безопасности предприятия.

Учебные вопросы:

Инструментальные методы обнаружения и оценки эффективности скрытых деструктивных энергоинформационных воздействий.

Продолжительность занятия – 6 ч.

Тема 6. Социотехносферная безопасность предприятия (учреждения, организации)

Практическое занятие 6.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Изучить проблемы обеспечения глобальной и региональной социотехносферной безопасности государства.

Основные положения темы занятия:

Выявить современные информационные войны между государствами и роль в них социотехносферной безопасности.

Учебные вопросы:

Энергоинформационное оружие – главная скрытая информационная угроза национальной безопасности страны с современных условиях.

Продолжительность занятия – 6 ч.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Тема 3. **Теоретические основы обеспечения социотехносферной безопасности технических средств и систем**	***Подготовка докладов по темам:*** 1. Становление энергоинформационно безопасности (эниологии) как област обеспечения ИБ. 2. Неопознанные явления в природе, обществе и н производстве как основы причин становлени эниологии.

		3. Эниология как научно-прикладное направлени ИБ. 4. Эниология (энергоинформационна безопасность) в системе современно мировоззрения. 5. Основные научно-прикладные аспект эниологических явлений в области ИБ. 6. Обзор и классификация эниофеноменов в систем ИБ. 7. Организационные аспекты эниологи (энергоинформационной безопасности). 8. Соотношение эниологии и чрезвычайны ситуаций в системе ИБ. 9. Законодательные аспекты современно эниологии (энергоинформационно безопасности). 10. Фундаментальные основы сущности содержания эниологических феноменов системе ИБ.
2.	Тема 4. **Основы моделирования и оценки эффективности процессов по обеспечению социотехносферной безопасности**	***Подготовка докладов по темам:*** 11.. Электромагнитные аспекты сущност эниологических феноменов. 12. Информационно-прикладная интерпретаци эниофеноменов в системе ИБ. 13. Понятие об экспериментальной проверк эниофеноменов в области ИБ. 14. Геопланитарные эниоявления в систем обеспечения ИБ: влияние геопатогенных зо (областей). 15. Человек как резонатор электромагнитной модел эниофеноменов в системе ИБ. 16. Понятие о космическом энергоинформационно обмене в системе обеспечения ИБ. 17. Космос в системе обеспечени энергоинформационной безопасност современных социотехнических систем. 18. Энергоинформационная безопасност (эниологические аспекты) архитектур (строительных конструкций) объекто информационной защиты.

3	Тема 5. **Социотехносферная безопасность предприятия (учреждения, организации)**	***Подготовка докладов по темам:*** 19.Понятие об энергоинформационном контакте «неизвестным разумом» при обеспечении ИБ. 20.Понятие об энергоинформационных природны ритмах при обеспечении ИБ. 21.Понятие и роль биоритмов в деятельност человека (коллективов) при обеспечении ИБ. 22.Основы влияния энергоинформационных ритмо развития общества при обеспечении И государства.
4	Тема 6. **Региональная и глобальная социотехносферная безопасность государства**	***Подготовка докладов по темам:*** 22. Влияние энергоинформационных ритмов развития общества при обеспечении ИБ государства. 23. Современное информационное оружия XXI века во взаимосвязи с энергоинформационными процессами. 23. Космическое энергоинформационное оружие в системе ИБ. 24. Особенности энергоинформационных воздействий на человека и общество. 25. Эниологическая (энергоинформационная) безопасность и искусственный разум в системе ИБ. 26. Биолокационный метод анализа энергоинформационной обстановки при обеспечении ИБ. 27. Организация энергоинформационного медико-психологического экспресс-метода анализа состояния персонала как субъектов ИБ. 28. Экспертная эниослужба при обеспечении информационной безопасности компьютерных сетей.

5. Указания по проведению контрольных работ для студентов

5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую Вами литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

5.4.Примерная тематика контрольных работ:

1. Понятие о социотехнических системах и основы их обеспечения безопасности.
2. Базовые положения по энергоинформационной безопасности социотехнических систем.
3. Основные направления развития энергоинформационной безопасности в современных условиях.
4. Концептуальная модель обеспечения энергоинформационной безопасности.
5. Мифы и реальности обеспечения энергоинформационной безопасности.
6. Концептуальные подходы обеспечения энергоинформационной безопасности человека (личности).
7. Энергоинформационные угрозы и их влияние на человека.
8. Особенности воздействия электромагнитных волн на субъекта.
9. Типовые признаки и основные этапы энергоинформационных воздействий на личность.
10. Источники дестабилизирующих энергоинформационных воздействий на индивидуумов и их возможности.
11. Научные основы влияния энергоинформационных воздействий на технические средства и системы.

12. Особенности обеспечения энергоинформационной безопасности функционирования технических средств.

13. Базовые положения по обеспечению энергоинформационной безопасности функционирования технических систем.

14. Возможности использования энергоинформационных излучений для реализации безопасных информационных технологий (связи, навигации и разведки).

15. Обобщенная модель взаимодействия информации, энергии и материи Вселенной (энергоинформационная модель мирового пространства).

16. Основы эффективности энергоинформационных воздействий.

17. Инструментальные методы обнаружения и оценки эффективности энергоинформационных воздействий.

18. Общие положения по обеспечению энергоинформационной безопасности функционирования предприятия (фирмы).

19. Особенности влияния энергоинформационных воздействий на деятельность фирмы и привлекаемые технические средства обеспечения энергоинформационной безопасности.

20. Энергоинформационная безопасность бизнеса и противодействие несанкционированному доступу к защищаемому информационному ресурсу в условиях воздействия энергоинформационных излучений.

21. Проблемы обеспечения глобальной/региональной энергоинформационной безопасности государства.

22. Энергоинформационное оружие – главная угроза национальной безопасности страны.

23. Классификация энергоинформационного оружия.

24. Характеристика информационно-технического оружия.

25. Энергоинформационное оружие программно-технического воздействия.

26. Природные энергоинформационные деструктивные воздействия.

27. Современные информационные войны между государствами и роль в них области энергоинформационной безопасности.

28. Основы разработки (базовые положения) Концепции энергоинформационной безопасности государства.

29. Становление энергоинформационной безопасности (эниологии) как область обеспечения ИБ.

30. Неопознанные явления в природе, обществе и на производстве как основы причин становления эниологии.

31. Эниология как научно-прикладное направление ИБ.

32. Эниология (энергоинформационная безопасность) в системе современного мировоззрения.

33. Основные научно-прикладные аспекты эниологических явлений в области ИБ.

34. Обзор и классификация эниофеноменов в системе ИБ.

35. Организационные аспекты эниологии (энергоинформационной безопасности).

36. Соотношение эниологии и чрезвычайных ситуаций в системе ИБ.

37. Законодательные аспекты современной эниологии (энергоинформационной безопасности).

38. Фундаментальные основы сущности и содержания эниологических феноменов в системе ИБ.

39. Электромагнитные аспекты сущности эниологических феноменов.

40. Информационно-прикладная интерпретация эниофеноменов в системе ИБ.

41. Понятие об экспериментальной проверки эниофеноменов в области ИБ.

42. Геопланитарные эниоявления в системе обеспечения ИБ: влияние геопатогенных зон (областей).

43. Человек как резонатор электромагнитной модели эниофеноменов в системе ИБ.

44. Понятие о космическом энергоинформационном обмене в системе обеспечения ИБ.

45. Космос в системе обеспечения энергоинформационной безопасности современных социотехнических систем.

46. Энергоинформационная безопасность (эниологические аспекты) архитектуры (строительных конструкций) объектов информационной защиты.

47. Понятие об энергоинформационном контакте с «неизвестным разумом» при обеспечении ИБ.

48. Понятие об энергоинформационных природных ритмах при обеспечении ИБ.

49. Понятие и роль биоритмов в деятельности человека (коллективов) при обеспечении ИБ.ю

50. Основы влияния энергоинформационных ритмов развития общества при обеспечении ИБ государства.

51.Современное информационное оружие XXI века во взаимосвязи с энергоинформационными процессами.

52. Космическое энергоинформационное оружие (деструктивные воздействия) в системе ИБ.

53. Основы энергоинформационных воздействий на человека и общество.

54. Энергоинформационная безопасность и искусственный разум в системе ИБ.

55. Биологический метод анализа энергоинформационной обстановки при обеспечении ИБ.

56. Экспертная эниослужба при обеспечении ИБ компьютерных сетей.

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1.Чернов, К. В. Управление техносферной безопасностью / К. В. Чернов. — Санкт-Петербург : Лань, 2023. — 160 с. — ISBN 978-5-507-45029-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book76575 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Титова, Т. С. Система управления техносферной безопасностью : методические указания / Т. С. Титова, Р. Г. Ахтямов. — Санкт-Петербург : ПГУПС, 2017. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book01566 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Управление техносферной безопасностью : учебное пособие / И. С. Мартынов, М. Н. Шапров, Е. Ю. Гузенко [и др.]. — Волгоград : Волгоградский ГАУ, 2019. — 108 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book39210 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

4.Соколов, А. К. Управление техносферной безопасностью : учебное пособие / А. К. Соколов. — Иваново : ИГЭУ, 2018. — 140 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book54587 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности

http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по курсу «Социотехносферная безопасность объектов информационной защиты».