Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Соляной В.Н. Рабочая программа дисциплины: «Социотехносферная безопасность объектов информационной защиты». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Сухотерин А.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 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)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

2

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

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.

Общепрофессиональные компетенции:

(ОПК-4) способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Профессиональные компетенции:

(ПК-14) способность организовывать работу малого коллектива исполнителей в профессиональной деятельности.

Основными **задачами** дисциплины являются:

- Показать актуальность существующей проблемы обеспечения социотехносферной безопасности функционирования типовых объектов информационной защиты на предприятиях, учреждениях и организациях (современных информационных систем);
- Изложить, с научно-практической направленностью, теоретические основы социотехносферной безопасности субъектов информационной защиты (индивидуумов, социума);
- Изложить, с научно-практической направленностью, теоретические основы социотехносферной безопасности функционирования современных технических средств и систем обработки информации;
- Дать основы моделирования эффективности процессов обеспечения социотехносферной безопасности функцинирования информационных объектов современных социотехнических систем;

- Сформулировать типовые основы организации обеспечения социотехносферной безопасности функционирования объектов информационной защиты на предприятиях (организациях, учреждениях);
- Ознакомить с возможными правовыми основами обеспечения социотехносферной (энергоинформационной) безопасности - проектами концепций обеспечения региональной и глобальной энергоинформационной безопасности государства.

После завершения освоения данной дисциплины студент должен:

Знать:

- понятий аппарат в области энергоинформационной безопасности;
- существующие проблемы по энергоинформационной безопасности социотехнических систем;
- энергоинформационные угрозы и их влияние на персонал;
- основы обеспечения энергоинформационной безопасности;
- технологии обнаружения и оценки эффективности деструктивных энергоинформационных воздействий;
- влияния энергоинформационных воздействий на деятельность фирмы и привлекаемые технические средства обеспечения энергоинформационной безопасности.

Уметь:

- выявлять и аргументировать существующие и возникающие проблемы (задачи) по энергоинформационной безопасности деятельности современных предприятий (организаций и учреждений);
- разрабатывать и аргументировать предложения, направленные на повышение эффективности энергоинформационной безопасности деятельности современных предприятий (организаций и учреждений;
- реализовывать принятые меры по противодействию возможных деструктивных социотехносферных воздействий на объекты информационной защиты.

Владеть навыками:

- использования организационно-правовых методов по обеспечению социотехносферной безопасности функционирования объектов информационной защиты;

- применения располагаемых инструментальных технологий обнаружения и оценки эффективности деструктивных социотехносферных воздействий на объекты информационной защиты.

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», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6, ОПК-2,4,6 и ПК-4,14.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Национальная система по противодействию легализации преступных доходов и финансированию терроризма», «Актуальные проблемы финансов», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетные единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр …	Семестр …	Семестр …
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
КСР	-	-			
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**			

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	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	ОПК-4 ПК-14
Тема 2. **Теоретико-прикладные основы обеспечения социотехносферной безопасности индивидуума и социума**	2	4	4	ОПК-4 ПК-14
Тема 3. **Теоретические основы обеспечения социотехносферной безопасности технических средств и систем**	2	6	4	ОПК-4 ПК-14
Раздел 2. **Базовые практические положения по социотехносферной безопасности объектов информационной защиты**				
Тема 4. **Основы моделирования и оценки эффективности процессов по обеспечению социотехносфер**	2	6	4	ОПК-4 ПК-14

ной безопасности				
Тема 5. **Социотехносферная безопасность предприятия (учреждения, организации)**	4	6	4	ОПК-4 ПК-14
Тема 6. **Региональная и глобальная социотехносферная безопасность государства**	4	6	2	ОПК-4 ПК-14
Итого:	16	32	18	

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 деструктивных 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. Воронцова Л.Ф. и др. История и современность информационного противоборства. М.: Горячая линия-Телеком, 2006.

2. Остапенко Г.А. и др. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты противодействия. Учебное пособие. М.: Горячая линия-Телеком, 2008.

Дополнительная литература:

1. Манойло А.В. и др. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия-Телеком, 2013.
2. Грибунин В.Г. Комплексная система защиты информации на предприятии. Учебное пособие – М.: «Академия», 2009.

Рекомендуемая литература:

1. Баранова Е.К. и др. Моделирование систем защиты информации. Учебное пособие. М.: Инфра-М, 2015.
2. Бухарин С.Н. Методы и технологии информационных войню М.: Академический Проект, 2007.
3. Волобуев С.В. Философия безопасности социотехнических систем: информационные аспекты. М.: Вузовская книга, 2004.
5. Ионин С.В. Параллельное оружие, или чем и как будут убивать в 21 веке. М.: Звонница-МГ, 2009.
6. Новиков В.К. Информационное оружие – оружие современных и будущих войн. М.: Горячая линия-Телеком, 2011.
7. Переездчиков И.В. Анализ опасностей промышленных систем «человек-машина-среда» и основы защиты. Учебное пособие. М.: КНОРУС, 2011.
8. Петров В.П. и др. Информационная безопасность человека и общества. Учебное пособие. М.: ЭНАС,2007.
9. Попов Ю.П. Ресурсы безопасности промышленного предприятия. Практическое пособие. М.: ЭНАС, 2007.
10. Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание. М.: СИНТЕГ, 2003.
11. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика. Учебное пособие. М.: Гелиос РВ, 2006.
12. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МНЦМО, 2002.

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. Ресурсы информационно-образовательной среды МГОТУ
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

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тема:1,4,6	эталонную модель взаимодействия открытых систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах	разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; классифицировать защищаемую ин-формацию по видам тайны и степеням конфиденциальности;	Навыками исследования эффективности создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;
2.	ПК-14	способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Тема:2,3,4,5	состав системы управления и требова-ния к ее элементам;;	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем	методами формирования требований по защите информации;

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-14	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).

			4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

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 оружие 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

Согласно учебному плану	тестирование	ОПК-4 ПК-14	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-4 ПК-14	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-4 ПК-14	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 практически

						х занятиях; «**Неудовлетворительно**»: • 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.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант 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 коммерческих 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

4.2 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 проверке 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.

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.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ СОЦИОТЕХНОСФЕРНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

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.

Задачи дисциплины:

- Обосновать актуальность существующей проблемы по обеспечению социотехносферной безопасности современных социотехнических систем (предприятий, учреждений, организаций, фирм и их субъектов);
- Изложить с научно-практической направленностью основы энергоинформационной безопасности отдельной личности (субъекта) и социума в целом;
- Дать теоретико-прикладные основы социотехносферной безопасности функционирования технических систем и средств, строительных конструкций и инженерных сооружений в объектах информационной защиты;
- Довести основы моделирования процессов обеспечения энергоинформационной безопасности социотехнических систем;
- Сформулировать типовые практические направления обеспечения социотехносферной безопасности современных предприятий, организаций и учреждений;
- 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**:** *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 – 4 ч.

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

Практическое занятие 2.

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 – 4 ч.

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

Практическое занятие 3.

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 – 6 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**:** *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 – 6 ч.

Тема 5. Социотехносферная безопасность предприятия (учреждения, организации)

Практическое занятие 5.

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 обеспечению 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**:** *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

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**60**
Вопросы, выносимые на самостоятельное изучение	12
Подготовка к практическим занятиям	32
Подготовка к лабораторным занятиям	-
Подготовка докладов	8
Выполнение практических заданий	8

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Становление энергоинформационной безопасности (эниологии) как область обеспечения ИБ.
2. Неопознанные явления в природе, обществе и на производстве как основы причин становления эниологии.
3. Эниология как научно-прикладное направление ИБ.
4. Эниология (энергоинформационная безопасность) в системе современного мировоззрения.
5. Основные научно-прикладные аспекты эниологических явлений в области ИБ.
6. Обзор и классификация эниофеноменов в системе ИБ.
7. Организационные аспекты эниологии (энергоинформационной безопасности).
8. Соотношение эниологии и чрезвычайных ситуаций в системе ИБ.
9. Законодательные аспекты современной эниологии (энергоинформационной безопасности).
10. Фундаментальные основы сущности и содержания эниологических феноменов в системе ИБ.
11. Электромагнитные аспекты сущности эниологических феноменов.
12. Информационно-прикладная интерпретация эниофеноменов в системе ИБ.
13. Понятие об экспериментальной проверке эниофеноменов в области ИБ.
14. Геопланитарные эниоявления в системе обеспечения ИБ: влияние геопатогенных зон (областей).
15. Человек как резонатор электромагнитной модели эниофеноменов в системе ИБ.
16. Понятие о космическом энергоинформационном обмене в системе обеспечения ИБ.
17. Космос в системе обеспечения энергоинформационной безопасности современных социотехнических систем.
18. Энергоинформационная безопасность (эниологические аспекты) архитектуры (строительных конструкций) объектов информационной защиты.
19. Понятие об энергоинформационном контакте с «неизвестным разумом» при обеспечении ИБ.
20. Понятие об энергоинформационных природных ритмах при обеспечении ИБ.
21. Понятие и роль биоритмов в деятельности человека (коллективов) при обеспечении ИБ.
22. Основы влияния энергоинформационных ритмов развития общества при обеспечении ИБ государства.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	12	Изучение открытых источников
2.	Подготовка к практическим занятиям	32	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	
4.	Тематика докладов	8	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	8	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Становление эниологии (энергоинформационной безопасности), как новое направление 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).
15. Человек как резонатор электромагнитной модели эниофеноменов в системе ИБ.
16. Космический энергоинформационный обмен в системе обеспечения ИБ**.**
17**.** Космос и эниологии в современной системе ИБ.
18**.** Энергоинформационная безопасность (эниология) архитектуры (конструкций) объектов информационной защиты.

19. Энергоинформационный контакт с «неизвестным разумом» при обеспечении ИБ.
20. Энергоинформационные ритмы в системе обеспечения ИБ.
21. Биоритмы и обеспечение ИБ.
22. Влияние энергоинформационных ритмов развития общества при обеспечении ИБ государства.
23. Современное информационное оружие 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 факультета заочного обучения

Не предусмотрено учебным планом.

6. Перечень основной и дополнительной учебной литературы

Основная:

1. Бабаш. А.В. Криптографические методы защиты информации. Том 1.Учебно - метод. пособие. – 2-е изд.-М.: ИНФРА-М, 2013 - 413.
2. Горбатов В.С. Основы технологии PKI-2-е издание, стереотип. – М. Горячая линия – Телеком, 2011.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.Технические средства и методы защиты информации. Учебное пособие для вузов: - 4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

Дополнительная:

1. Афанасьев А.А., Веденньев Л.Т. и др.Аутентификация.Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.
2. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.
3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стенографии – 2-е издание –М. Горячая линия – Телеком, 2013.

Рекомендуемая:

1. Фирьяз Ханцеверов, Эниология, том 1;
2. Фирьяз Ханцеверов, Эниология, том 2;
3. Фирьяз Ханцеверов, Эниология, том 3.

Электронные книги:

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.
http://biblioclub.ru/index.php?page=book_view&book_id=231673
2. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.
http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html
3. Жданов О.Н., Золотарев В.В. МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ // Успехи современного естествознания. – 2010.
www.rae.ru/use/?section=content&op=show_article&article_id=7784920
4. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.Технические средства и методы защиты информации. Учебное пособие для вузов.:-4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.
http://biblioclub.ru/index.php?page=book&id=253208&sr=1

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Социотехносферная безопасность объектов информационной защиты».