



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

03.03.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИКЕ

Направление подготовки (специальность)
13.06.01 ЭЛЕКТРО- И ТЕПЛОТЕХНИКА

Направленность (профиль/специализация) программы
Электротехнические комплексы и системы

Уровень высшего образования - подготовка кадров высшей квалификации

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Электроснабжения промышленных предприятий
Курс	3
Семестр	5

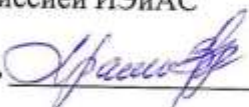
Магнитогорск
2021 год

Рабочая программа составлена на основе ФГОС ВО по направлению подготовки 13.06.01 ЭЛЕКТРО- И ТЕПЛОТЕХНИКА (уровень подготовки кадров высшей квалификации). (приказ Минобрнауки России от 30.07.2014 г. № 878)

Рабочая программа рассмотрена и одобрена на заседании кафедры Электроснабжения промышленных предприятий
10.02.2021 г., протокол № 4

Зав. кафедрой  Г.П. Корнилов


Рабочая программа одобрена методической комиссией ИЭиАС
03.03.2021 г., протокол № 5

Председатель  В.Р. Храмшин

Рабочая программа составлена:

зав. кафедрой ЭПП, д-р техн. наук  Г.П. Корнилов

Рецензент:

Проректор по учебной работе, профессор кафедры «Мехатроника и автоматизация» ФГАОУ ВО «ЮУрГУ (НИУ)», д-р техн. наук  А.А. Радионов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.П. Корнилов

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.П. Корнилов

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ Г.П. Корнилов

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Информационная безопасность в электроэнергетике» является получение аспирантами основных научно-практических, общесистемных знаний в области информационной безопасности и защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность в электроэнергетике входит в вариативную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Методология и информационные технологии в научных исследованиях

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Научно-исследовательская деятельность и подготовка НКР

Подготовка к сдаче и сдача государственного экзамена

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Информационная безопасность в электроэнергетике» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОПК-2 владением культурой научного исследования в том числе, с использованием новейших информационно-коммуникационных технологий	
Знать	-основные понятия информационной безопасности ; -основные направления защиты информации; -законодательство Российской Федерации в области защиты информации.
Уметь	-использовать нормативные документы по защите информации; – использовать знания основ ИБ в профессиональной деятельности; – использовать источники информации и осуществлять сбор и обработку статистических данных при принятии организационно-управленческих решений по обеспечению ИБ в рамках своей профессиональной деятельности;
Владеть	-профессиональным языком предметной области знания; -навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности; -навыками организации и обеспечения режима секретности; -навыками аналитической работы и содержательной интерпретации информационных процессов, подлежащих защите.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетных единиц 72 акад. часов, в том числе:

- контактная работа – 13 акад. часов;
- аудиторная – 13 акад. часов;
- внеаудиторная – 0 акад. часов
- самостоятельная работа – 59 акад. часов;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. 1. Основные понятия информационной безопасности								
1.1 1.1. Информационная безопасность в системе национальной безопасности РФ.	5	2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2
1.2 1.2 Современная доктрина информационной безопасности Российской Федерации. Политика информационной безопасности России.		2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2
1.3 1.3 Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.		2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2
Итого по разделу		6			24			
2. 2. Компьютерные вирусы и защита от них.								
2.1 2.1. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов, проблемы при определении компьютерного вируса	5	2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2

2.2	2.2.	Профилактика компьютерных вирусов наиболее распространенные пути заражения компьютеров вирусами, правила защиты от компьютерных вирусов	2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2	
Итого по разделу			4			16				
3. 3. Защита информации										
3.1	3.1	Понятие электронно-цифровой подписи	5	2			8	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2
3.2	3.2	Безопасность работы в сети Интернет для пользователя.		1			11	Подготовка к устному опросу, выполнению теста-задания	Устный опрос, выполнение теста-задания	ОПК-2
Итого по разделу			3			19				
Итого за семестр			13			59		зачёт		
Итого по дисциплине			13			59		зачет	ОПК-2	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Информационная безопасность в электроэнергетике» используются традиционная и модульно-компетентностная технологии.

Передача необходимых теоретических знаний и формирование основных представлений по курсу «Информационная безопасность в электроэнергетике» происходит с использованием мультимедийного оборудования. Для аудиторных занятий используются технологии обзорной лекции (для систематизации знаний по дисциплине); лекции визуализации (для наглядного представления изучаемого материала); проблемной лекции (для развития исследовательских навыков аспирантов).

Самостоятельная работа аспирантов проявляется в непосредственной подготовке к зачету. В качестве оценочных средств на зачете используются устные ответы.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1137902> (дата обращения: 22.09.2020)

б) Дополнительная литература:

1. Чернова, Е. В. Информационная безопасность : учебное пособие / Е. В. Чернова ; МГТУ. - [2-е изд., подгот. по печ. изд. 2011 г.]. - Магнитогорск : МГТУ, 2015. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=1453.pdf&show=dcatalogues/1/1123976/1453.pdf&view=true> (дата обращения: 25.09.2020). - Макрообъект. - Текст: электронный. - Сведения доступны также на CD-ROM.

2. Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи : материалы внутривузовской конференции 9-12 октября 2015 г. / МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL:

<https://magtu.informsystema.ru/uploader/fileUpload?name=3223.pdf&show=dcatalogues/1/1136764/3223.pdf&view=true> (дата обращения: 25.09.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

3. Журнал «Вестник ЮУрГУ. Серия «Энергетика»
<https://vestnik.susu.ru/power/issue/archive>

4. Журнал «Электротехнические системы и комплексы» <http://esik.magtu.ru/ru/>

5. Журнал "Вестник Ивановского государственного энергетического университета"
<http://vestnik.ispu.ru/taxonomy/term/102#> .

в) Методические указания:

1. Чернова, Е. В. Информационная безопасность в образовании : учебное пособие / Е. В. Чернова, Л. Ф. Ганиева ; МГТУ. - Магнитогорск : МГТУ, 2016. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=2499.pdf&show=dcatalogues/1/1130272/2499.pdf&view=true> (дата обращения: 25.09.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

г) Программное обеспечение и Интернет-ресурсы:**Программное обеспечение**

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows 7 Professional (для классов)	Д-757-17 от 27.06.2017	27.07.2018
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

В соответствии с учебным планом по дисциплине «Информационная безопасность в электроэнергетике» предусмотрены следующие виды занятий: лекции и самостоятельная работа и зачет.

Учебные аудитории для проведения занятий лекционного типа: Мультимедийные средства хранения, передачи и представления информации.

Помещения для самостоятельной работы обучающихся: Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

Помещение для хранения и профилактического обслуживания учебного оборудования Стеллажи, сейфы для хранения учебного оборудования

Инструменты для ремонта лабораторного оборудования

ПРИЛОЖЕНИЕ 1

(обязательное)

Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем для самостоятельной работы и устного опроса:

1. Информационная безопасность в системе национальной безопасности РФ.
2. Нормативно-правовые основы информационной безопасности общества;
3. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.
4. Концепция национальной безопасности РФ.
5. Важнейшие задачи обеспечения национальной безопасности в информационной сфере.
6. Доктрина информационной безопасности.
7. Ответственность за нарушения в сфере информационной безопасности.
8. Компьютерные вирусы и их классификации. Примеры.
9. Профилактика компьютерных вирусов
10. Наиболее распространенные пути заражения компьютеров вирусами. Правила защиты от компьютерных вирусов
11. Классификации антивирусных программ. Примеры.
12. Понятие электронно-цифровой подписи.
13. Безопасность работы в сети Интернет для пользователя.

ПРИЛОЖЕНИЕ 2

(обязательное)

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОПК-2 - владением культурой научного исследования в том числе, с использованием новейших информационно-коммуникационных технологий		
Знать	<ul style="list-style-type: none"> – основные понятия информационной безопасности; – основные направления защиты информации; – законодательство российской федерации в области защиты информации. 	<p>Перечень тем и заданий для подготовки к промежуточной аттестации:</p> <ol style="list-style-type: none"> 1. Информационная безопасность в системе национальной безопасности РФ. 2. Нормативно-правовые основы информационной безопасности общества; 3. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. 4. Концепция национальной безопасности РФ. 5. Важнейшие задачи обеспечения национальной безопасности в информационной сфере. 6. Доктрина информационной безопасности. 7. Ответственность за нарушения в сфере информационной безопасности. 8. Компьютерные вирусы и их классификации. Примеры. 9. Профилактика компьютерных вирусов 10. Наиболее распространенные пути заражения компьютеров вирусами. Правила защиты от компьютерных вирусов 11. Классификации антивирусных программ. Примеры. 12. Понятие электронно-цифровой подписи. 13. Безопасность работы в сети Интернет для пользователя.
Уметь	<ul style="list-style-type: none"> – использовать нормативные документы по защите информации; – использовать знания основ иб в профессиональной деятельности; – использовать источники информации и 	<p>Перечень тем для самостоятельной работы:</p> <ol style="list-style-type: none"> 1. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Влияние данных нормативных актов на правовые аспекты в электроэнергетике 2. Концепция национальной безопасности РФ.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	<p>осуществлять сбор и обработку статистических данных при принятии организационно- управленческих решений по обеспечению иб в рамках своей профессиональной деятельности.</p>	<p>3. Важнейшие задачи обеспечения национальной безопасности (в контексте электроэнергетики) в информационной сфере. 4. Доктрина информационной безопасности. 5. Ответственность за нарушения в сфере информационной безопасности. 6. Цифровизация в электроэнергетике: влияние информационной и кибербезопасности на надежности электроснабжения</p>
<p>Владеть</p>	<p>– профессиональным языком предметной области знания; – навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности; – навыками организации и обеспечения режима секретности; – навыками аналитической работы и содержательной интерпретации информационных процессов, подлежащих защите.</p>	<p>Задания на решение задач из профессиональной области, комплексные задания 1. Изучить нормативные правовые акты в области обеспечения информационной безопасности; 2. Изучить вопросы организации и обеспечения режима секретности; 3. Выполнить профилактику компьютерных вирусов на заданном объекте исследования. 4. Владеть навыками применения электронно-цифровой подписи.</p>

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Информационная безопасность в электроэнергетике» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, выявляющие степень сформированности умений и владений, проводится в форме зачета.

Зачет по данной дисциплине проводится в устной форме. Критерии оценки:

– **«зачтено»** – обучающийся демонстрирует высокий или средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации;

– **«не зачтено»** – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.