



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

04.02.2025 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

***ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИКЕ***

Научная специальность  
2.4.2. 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                                               |

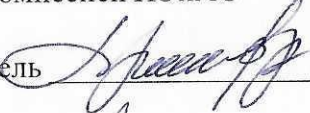
Магнитогорск  
2025 год

Рабочая программа составлена на основе ФГТ (приказ Минобрнауки России от 20.10.2021 г. № 951)

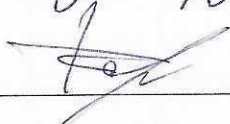
Рабочая программа рассмотрена и одобрена на заседании кафедры  
Электроснабжения промышленных предприятий  
30.01.2025 г., протокол № 4

Зав. кафедрой  А.В. Варганова

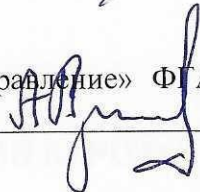
Рабочая программа одобрена методической комиссией ИЭиАС  
04.02.2025 г., протокол № 3

Председатель  В.Р. Храмшин

Рабочая программа составлена:

профессор кафедры ЭПП, д-р техн. наук  Г.П. Корнилов

Рецензент:

Заведующий кафедрой «Автоматика и управление» ФГАОУ ВО «Московский  
политехнический университет», д-р техн. наук  А.А. Радионов

## Лист актуализации рабочей программы

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от \_\_\_\_ 20\_\_ г. № \_\_\_\_  
Зав. кафедрой \_\_\_\_\_ А.В.Варганова

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от \_\_\_\_ 20\_\_ г. № \_\_\_\_  
Зав. кафедрой \_\_\_\_\_ А.В.Варганова

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от \_\_\_\_ 20\_\_ г. № \_\_\_\_  
Зав. кафедрой \_\_\_\_\_ А.В.Варганова

---

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Электроснабжения промышленных предприятий

Протокол от \_\_\_\_ 20\_\_ г. № \_\_\_\_  
Зав. кафедрой \_\_\_\_\_ А.В.Варганова

### **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 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:

|                                                                                                                                                                                                                   |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                                                                                                                                                                                                                   |  |
| КНС-3 Способен широко использовать методы математического и IT-моделирования при разработке и эксплуатации электротехнических и электроэнергетических комплексов и систем в нормальных и аварийных режимах работы |  |

### 3. Структура, объём и содержание дисциплины (модуля)

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

- контактная работа – 44 акад. часов;
- аудиторная – 44 акад. часов;
- внеаудиторная – 0 акад. часов;
- самостоятельная работа – 28 акад. часов;

Форма аттестации - зачет

| Раздел/ тема дисциплины                                                                                                                                                                    | Семестр | Аудиторная контактная работа (в акад. часах) |             | Самостоятельная работа студента | Форма текущего контроля успеваемости и промежуточной аттестации |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|----------------------------------------------|-------------|---------------------------------|-----------------------------------------------------------------|
|                                                                                                                                                                                            |         | Лек.                                         | практ. зан. |                                 |                                                                 |
| 1. 1. Основные понятия информационной безопасности                                                                                                                                         | 5       |                                              |             |                                 |                                                                 |
| 1.1 1.1. Информационная безопасность в системе национальной безопасности РФ.                                                                                                               |         | 4                                            | 4           | 4                               | Устный опрос, выполнение теста-задания                          |
| 1.2 1.2 Современная доктрина информационной безопасности Российской Федерации. Политика информационной безопасности России.                                                                |         | 4                                            | 4           | 4                               | Устный опрос, выполнение теста-задания                          |
| 1.3 1.3 Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. |         | 3                                            | 3           | 4                               | Устный опрос, выполнение теста-задания                          |
| Итого по разделу                                                                                                                                                                           |         | 11                                           | 11          | 12                              |                                                                 |
| 2. 2. Компьютерные вирусы и защита от них.                                                                                                                                                 | 5       |                                              |             |                                 |                                                                 |
| 2.1 2.1. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов, проблемы при определении компьютерного вируса                                              |         | 3                                            | 3           | 4                               | Устный опрос, выполнение теста-задания                          |
| 2.2 2.2. Профилактика компьютерных вирусов наиболее распространенные пути заражения компьютеров вирусами, правила защиты от компьютерных вирусов                                           |         | 2                                            | 2           | 4                               | Устный опрос, выполнение теста-задания                          |
| Итого по разделу                                                                                                                                                                           |         | 5                                            | 5           | 8                               |                                                                 |
| 3. 3. Защита информации                                                                                                                                                                    | 5       |                                              |             |                                 |                                                                 |
| 3.1 3.1 Понятие электронно-цифровой подписи                                                                                                                                                |         | 3                                            | 3           | 4                               | Устный опрос, выполнение теста-задания                          |
| 3.2 3.2 Безопасность работы в сети Интернет для пользователя.                                                                                                                              |         | 3                                            | 3           | 4                               | Устный опрос, выполнение теста-задания                          |
| Итого по разделу                                                                                                                                                                           |         | 6                                            | 6           | 8                               |                                                                 |
| Итого за семестр                                                                                                                                                                           |         | 22                                           | 22          | 28                              | зачёт                                                           |
| Итого по дисциплине                                                                                                                                                                        |         | 22                                           | 22          | 28                              | зачет                                                           |

#### 4 Оценочные средства для проведения текущей и промежуточной аттестации

Представлены в приложении 1.

#### 5 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: 30.04.2025)

#### б) Дополнительная литература:

1. Чернова Елена Владимировна. Информационная безопасность человека : учебное пособие для вузов / Елена Владимировна Чернова ; Е. В. Чернова. - 3-е изд. - Москва : Юрайт, 2024. - 327 с. - (Высшее образование). - URL: <https://urait.ru/bcode/542739> (дата обращения: 23.09.2024). - URL: <https://urait.ru/bcode/542739>. - URL: <https://urait.ru/book/cover/D2E0974D-0199-44E7-ACF9-A79F28E16236>. - ISBN 978-5-534-16772-6. - дата обращения: 30.04.2025

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). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/20564>. - Текст : электронный. - дата обращения: 30.04.2025

3. Журнал «Вестник ЮУрГУ. Серия «Энергетика» <https://www.powervestniksusu.ru/index.php/PVS>

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

5. Журнал «Вестник Ивановского государственного энергетического университета» <http://vestnik.ispu.ru/>

#### в) Программное обеспечение и Интернет-ресурсы:

##### Программное обеспечение

| Наименование ПО              | № договора                   | Срок действия лицензии |
|------------------------------|------------------------------|------------------------|
| MS Office 2007 Professional  | № 135 от 17.09.2007          | бессрочно              |
| 7Zip                         | свободно распространяемое ПО | бессрочно              |
| MS Office 2003 Professional  | № 135 от 17.09.2007          | бессрочно              |
| FAR Manager                  | свободно распространяемое ПО | бессрочно              |
| STATISTICA в.6               | К-139-08 от 22.12.2008       | бессрочно              |
| Adobe Reader                 | свободно распространяемое ПО | бессрочно              |
| Calculate Linux Desktop Xfce | свободно распространяемое ПО | бессрочно              |

|       |          |           |
|-------|----------|-----------|
| Linux | свободно | бессрочно |
|-------|----------|-----------|

### Профессиональные базы данных и информационные справочные системы

| Название курса                                                                                       | Ссылка                                                                                              |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Электронная база периодических изданий East View Information                                         | <a href="https://dlib.eastview.com/">https://dlib.eastview.com/</a>                                 |
| Национальная информационно-аналитическая система – Российский индекс                                 | URL: <a href="https://elibrary.ru/project_risc.asp">https://elibrary.ru/project_risc.asp</a>        |
| Федеральное государственное бюджетное учреждение «Федеральный институт                               | URL: <a href="http://www1.fips.ru/">http://www1.fips.ru/</a>                                        |
| Российская Государственная библиотека. Каталоги                                                      | <a href="https://www.rsl.ru/ru/4readers/catalogues/">https://www.rsl.ru/ru/4readers/catalogues/</a> |
| Электронные ресурсы библиотеки МГТУ им. Г.И. Носова                                                  | <a href="https://host.megaprolib.net/MP0109/Web">https://host.megaprolib.net/MP0109/Web</a>         |
| Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer Nature» | <a href="https://www.nature.com/siteindex">https://www.nature.com/siteindex</a>                     |

## **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) Оценочные средства для проведения текущей и промежуточной аттестации:

**КНС-3: Способен широко использовать методы математического и IT-моделирования при разработке и эксплуатации электротехнических и электроэнергетических комплексов и систем в нормальных и аварийных режимах работы**

**Перечень тем и заданий для подготовки к промежуточной аттестации:**

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.

**Перечень тем для самостоятельной работы:**

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.
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

**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.

**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.