**Министерство науки и высшего образования РФ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Национальный исследовательский университет «МЭИ»**

---

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

# Рабочая программа дисциплины
# СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

| | |
|---|---|
| **Блок:** | **Блок 1 «Дисциплины (модули)»** |
| **Часть образовательной программы:** | **Часть, формируемая участниками образовательных отношений** |
| **№ дисциплины по учебному плану:** | **Б1.Ч.07** |
| **Трудоемкость в зачетных единицах:** | **8 семестр - 4;** |
| **Часов (всего) по учебному плану:** | **144 часа** |
| **Лекции** | **8 семестр - 28 часа;** |
| **Практические занятия** | **8 семестр - 56 часа;** |
| **Лабораторные работы** | **не предусмотрено учебным планом** |
| **Консультации** | **8 семестр - 2 часа;** |
| **Самостоятельная работа** | **8 семестр - 57,5 часа;** |
| **в том числе на КП/КР** | **не предусмотрено учебным планом** |
| **Иная контактная работа** | **проводится в рамках часов аудиторных занятий** |
| **включая:**<br>**Контрольная работа**<br>**Коллоквиум**<br>**Тестирование** | |
| **Промежуточная аттестация:** | |
| **Экзамен** | **8 семестр - 0,5 часа;** |

**Москва 2021**

**ПРОГРАММУ СОСТАВИЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность) | (подпись) | (расшифровка подписи) |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |
| Заведующий выпускающей кафедры | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** Целью освоения дисциплины является освоение общекультурных и профессиональных компетенций по системному анализу назначения, организации, построению и структуры системы обеспечения информационной безопасности (СОИБ) на предприятии, а также по вопросам управления ею и порядку оценки ее эффективности

**Задачи дисциплины**

- изучение теории по вопросам назначения, целей, решаемых задач, структуры СОИБ и организации ее функционирования в концепции системного подхода;;
- формирование готовности и способности к активной профессиональной деятельности по организации и обеспечению функционирования СОИБ в условиях современного информационного противоборства;;
- приобретение навыков системного анализа и синтеза сложных организационно-иерархических систем..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|---|---|
| ПК-1 Готов обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации | ПК-1.2$_{ПК-1}$ Управляет защитой информации в автоматизированных системах | знать:<br>- комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия;<br>- нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО;.<br><br>уметь:<br>- правильно разработать и оформить документы политики информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики;;<br>- применять системный подход к управлению информационной безопасностью предприятия;. |
| ПК-2 Готов к внедрению систем защиты информации автоматизированных систем | ПК-2.2$_{ПК-2}$ Разрабатывает организационно-распорядительные документы по защите информации в автоматизированных системах | знать:<br>- комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности;.<br><br>уметь:<br>- организовать технологический процесс защиты информационных |

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|---|---|
| | | активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины;<br>- применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных решений;. |
| ПК-2 Готов к внедрению систем защиты информации автоматизированных систем | ПК-2.3$_{ПК-2}$ Внедряет организационные меры по защите информации в автоматизированных системах | знать:<br>- методы и средства защиты систем управления технологическим оборудованием;<br>- психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности.<br><br>уметь:<br>- осуществлять поиск, анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП;;<br>- на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности. |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

| № п/п | Разделы/темы дисциплины/формы промежуточной аттестации | Всего часов на раздел | Семестр | Распределение трудоемкости раздела (в часах) по видам учебной работы | | | | | | | | | | Содержание самостоятельной работы/ методические указания |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Контактная работа | | | | | | | | СР | | |
| | | | | Лек | Лаб | Пр | Консультация | | ИКР | | ПА | Работа в семестре | Подготовка к аттестации /контроль | |
| | | | | | | | КПР | ГК | ИККП | ТК | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | Основы организации и функционирования СОИБ предприятия | 38 | 8 | 10 | - | 20 | - | - | - | - | - | 8 | - | ***Подготовка реферата:*** Разработка модели информационной системы ХС с позиций безопасности. |
| 1.1 | Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | ***Самостоятельное изучение теоретического материала:*** Политика информационной безопасности предприятия. Основные положения и документы Политики ИБ. ***Подготовка расчетных заданий:*** Внутренние организационно-распорядительные документы СОИБ, их состав и содержание. Деловая игра |
| 1.2 | Система обеспечения информационной безопасности предприятия. | 14 | | 4 | - | 8 | - | - | - | - | - | 2 | - | ***Самостоятельное изучение теоретического материала:*** Внутренние организационно-распорядительные документы СОИБ, их состав и содержание. |
| 1.3 | Перечень факторов, влияющих на организацию СОИБ предприятия | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | ***Подготовка реферата:*** Разработка проекта перечня сведений, составляющих коммерческую тайну. |
| 1.4 | Политика информационной безопасности. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | ***Самостоятельное изучение теоретического материала:*** Выявление состава информационных активов предприятия. Определение перечня информации, составляющей коммерческую тайну. ***Самостоятельное изучение теоретического материала:*** Сущность и задачи СОИБ предприятия, принципы |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | организации, этапы разработки и факторы, влияющие на организацию СОИБ<br>***Изучение материалов литературных источников:***<br>[1], 22-45<br>[2], 60-74<br>[3], 13-19<br>[4], 26-45 |
| 2 | Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия | 70 | | 18 | - | 36 | - | - | - | - | - | 16 | - | ***Изучение материалов литературных источников:***<br>[1], 56-68<br>[2], 88-95<br>[3], 64-66 |
| 2.1 | Правовые основы функционирования СОИБ предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.2 | Организационные основы функционирования СОИБ предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.3 | Кадровое обеспечение СОИБ предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.4 | Финансово-экономическое обеспечение функционирования СОИБ предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.5 | Инженерно-техническое обеспечение СОИБ. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.6 | Программно-аппаратное обеспечение функционирования СОИБ предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.7 | Подсистема аудита информационной системы предприятия. | 8 | | 2 | - | 4 | - | - | - | - | - | 2 | - | |
| 2.8 | Управление СОИБ | 14 | | 4 | - | 8 | - | - | - | - | - | 2 | - | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | предприятия. | | | | | | | | | | | | | |
| | Экзамен | 36.0 | | - | - | - | - | 2 | - | - | 0.5 | - | 33.5 | |
| | **Всего за семестр** | **144.0** | | **28** | **-** | **56** | **-** | **2** | **-** | **-** | **0.5** | **24** | **33.5** | |
| | **Итого за семестр** | **144.0** | | **28** | **-** | **56** | **2** | | **-** | | **0.5** | **57.5** | | |

**Примечание:** Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

**3.2 Краткое содержание разделов**

*1. Основы организации и функционирования СОИБ предприятия*

1.1. Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта.

Основы системного подхода к обеспечению информационной безопасности предприятия малого и среднего бизнеса. Этапы реализации системного подхода..

1.2. Система обеспечения информационной безопасности предприятия.

Понятие, сущность, назначение и задачи СОИБ предприятия. Методологические основы организации СОИБ. Основные требования, предъявляемые к СОИБ и содержательная характеристика этапов ее разработки..

1.3. Перечень факторов, влияющих на организацию СОИБ предприятия

Форма собственности предприятия, организационно-правовая форма и характер основной деятельности хозяйствующего субъекта; состав, объем и степень конфиденциальности защищаемой информации; структура и территориальное расположение; режим функционирования, ресурсообеспечение и уровень автоматизации (цифровизации) основных информационных процессов..

1.4. Политика информационной безопасности.

Политика информационной безопасности. Политика по управлению информационной безопасностью..

*2. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия*

2.1. Правовые основы функционирования СОИБ предприятия.

Структура правового обеспечения ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации. Лицензирование, сертификация и аттестация в области информационной безопасности..

2.2. Организационные основы функционирования СОИБ предприятия.

Назначение, цели и задачи организационного обеспечения. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности..

2.3. Кадровое обеспечение СОИБ предприятия.

Назначение, цели и задачи кадрового обеспечения. Основные мероприятия, проводимые при подборе, работе, увольнении сотрудников подразделений ИБ. Программы повышения осведомленности в области ИБ. Особенности профессиональной этики специалиста в области ИБ..

2.4. Финансово-экономическое обеспечение функционирования СОИБ предприятия.

Экономические основы СОИБ. Модели для оценки экономической эффективности инвестиций в СОИБ предприятия..

2.5. Инженерно-техническое обеспечение СОИБ.

Инженерно-техническая защита территорий, зданий и помещений предприятия. Организация защиты информации от утечки по техническим каналам. Методы и средства защиты информации от утечки по техническим каналам..

2.6. Программно-аппаратное обеспечение функционирования СОИБ предприятия.

Назначение, цели и задачи подсистемы программно-аппаратного обеспечения СОИБ. Силы и программные средства защиты информации..

2.7. Подсистема аудита информационной системы предприятия.

Назначение, цели и задачи подсистемы аудита информационной безопасности. Направления деятельности подсистемы аудита. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита..

2.8. Управление СОИБ предприятия.

Понятие и цели управления. Сущность процессов управления СОИБ. Принципы управления и анализ системы управления СОИБ. Структура и содержание управления СОИБ организации..

**3.3. Темы практических занятий**

1. Направления деятельности подсистемы аудита информационной безопасности. Технологии проведения аудита. Этапы проведения аудита ИБ. Особенности активного аудита;
2. Организация защиты компьютерной (цифровой) информации в информационной системе предприятия. Программно-аппаратное обеспечение функционирования СОИБ предприятия;
3. Организация инженерно-технической защиты территорий, зданий и помещений предприятия. Организация мероприятий защиты информации предприятия от утечки по техническим каналам;
4. Моделирование и оценка экономической эффективности инвестиций в СОИБ предприятия.;
5. Кадровое обеспечение функционирования КСОИБ. Особенности работы с персоналом СОИБ. Особенности профессиональной этики специалиста в области ИБ;
6. Организация эффективного функционирования СОИБ на основе Политики информационной безопасности. Моделирование информационной системы предприятия с позиций безопасности;
7. Правовые основы функционирования СОИБ предприятия. Структура законодательства РФ в сфере ИБ. Стандартизация в области ИБ. Комплекс внутренней нормативно-организационной документации СОИБ;
8. Моделирование и оценка экономической эффективности инвестиций в СОИБ предприятия.;
9. Внутренние организационно-распорядительные документы СОИБ, их состав и содержание;
10. Выявление состава информационных активов предприятия. Определение перечня информации, составляющей коммерческую тайну. Разработка проекта перечня сведений, составляющих коммерческую тайну. Политика информационной безопасности предприятия. Основные положения и документы Политики ИБ. Разработка модели информационной системы ХС с позиций безопасности.;
11. Основы организации и функционирования СОИБ предприятия.

**3.4. Темы лабораторных работ**

не предусмотрено

**3.5 Консультации**

*Групповые консультации по разделам дисциплины (ГК)*

1. Обсуждение материалов по кейсам раздела "Основы организации и функционирования СОИБ предприятия"
2. Обсуждение материалов по кейсам раздела "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия"

*Текущий контроль (ТК)*

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы организации и функционирования СОИБ предприятия"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия"

**3.6 Тематика курсовых проектов/курсовых работ**

Курсовой проект/ работа не предусмотрены

**3.7. Соответствие разделов дисциплины и формируемых в них компетенций**

| Запланированные результаты обучения по дисциплине (в соответствии с разделом 1) | Коды индикаторов | Номер раздела дисциплины (в соответствии с п.3.1) | | Оценочное средство (тип и наименование) |
|---|---|---|---|---|
| | | 1 | 2 | |
| **Знать:** | | | | |
| нормативные и организационно-распорядительные документы в области обеспечения своей профессиональной деятельности, включая и документы по обеспечению безопасности АСУТП КВО; | ПК-1.2$_{ПК-1}$ | | + | Коллоквиум/Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности |
| комплекс мер по менеджменту информационной безопасности предприятия на основе разработанной политикой информационной безопасности и других локальных нормативных актов предприятия | ПК-1.2$_{ПК-1}$ | + | | Тестирование/Организация функционирования СОИБ предприятия на основе системного подхода. |
| комплекс мер по обеспечению информационной безопасности с учетом его правовой обоснованности, технической реализуемости и экономической целесообразности; | ПК-2.2$_{ПК-2}$ | | + | Контрольная работа/Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия |
| психологические особенности работы в коллективах предприятий малого и среднего бизнеса с учётом принципов профессиональной этики в области информационной безопасности | ПК-2.3$_{ПК-2}$ | | + | Контрольная работа/Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия |
| методы и средства защиты систем управления технологическим оборудованием | ПК-2.3$_{ПК-2}$ | | + | Коллоквиум/Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности |
| **Уметь:** | | | | |
| применять системный подход к управлению информационной безопасностью предприятия; | ПК-1.2$_{ПК-1}$ | + | | Контрольная работа/Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) |
| правильно разработать и оформить документы политики | ПК-1.2$_{ПК-1}$ | + | | Контрольная работа/Назначение и общая |

| | | | | |
|---|---|---|---|---|
| информационной безопасности предприятия в различных сферах деятельности, в том числе и на объектах энергетики; | | | | характеристика видов обеспечения (подсистем) СОИБ предприятия |
| применять комплексный подход к защите технологических процессов в АСУ ТП с применением инженерно-технических и программно-аппаратных решений; | ПК-2.2$_{ПК-2}$ | | + | Коллоквиум/Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности |
| организовать технологический процесс защиты информационных активов предприятия в соответствии с принятыми в РФ правилами и нормами с применением системного анализа и системного подхода в предметной области дисциплины | ПК-2.2$_{ПК-2}$ | | + | Коллоквиум/Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности |
| на практике применять способности научной организации работы коллектива исполнителей на предприятии малого и среднего бизнеса в профессиональной деятельности | ПК-2.3$_{ПК-2}$ | | + | Тестирование/Организация функционирования СОИБ предприятия на основе системного подхода. |
| осуществлять поиск, анализ, выбор и установку программных компонентов комплексной системы защиты технологической информации в АСУ ТП; | ПК-2.3$_{ПК-2}$ | | + | Коллоквиум/Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности |

## 4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

### 4.1. Текущий контроль успеваемости

**8 семестр**

Форма реализации: Выполнение задания

1. Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности (Коллоквиум)

Форма реализации: Компьютерное задание

1. Организация функционирования СОИБ предприятия на основе системного подхода. (Тестирование)

Форма реализации: Письменная работа

1. Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)
2. Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

### 4.2 Промежуточная аттестация по дисциплине

*Экзамен (Семестр №8)*

Итоговая оценка по курсу выставляется исходя из данных БАРС по семестровой и экзаменационной составляющей

В диплом выставляется оценка за 8 семестр.

**Примечание:** Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

## 5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 5.1 Печатные и электронные издания:

1. Невский, А. Ю. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие / А. Ю. Невский, О. Р. Баронов ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2009 . – 372 с. - ISBN 978-5-383-00375-6 .
http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=1468;
2. Минзов, А. С. Профессиональная этика в сфере информационной и экономической безопасности : [монография] / А. С. Минзов, Нац. исслед. ун-т "МЭИ", Ин-т информац. и экономич. безопасности . – М. : ВНИИгеосистем, 2013 . – 132 с. - ISBN 978-5-8481-0135-5 .;
3. Минзов, А. С. Методика выполнения дипломных работ : учебное пособие для института безопасности бизнеса / А. С. Минзов, А. Ю. Невский, Н. В. Унижаев ; Ред. Л. М. Кунбутаев ; Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2007 . – 100 с. - ISBN 978-5-383-00024-3 .;

4. А. А. Камардина- "Профессиональная этика", Издательство: "Оренбургский государственный университет", Оренбург, 2013 - (167 с.) https://biblioclub.ru/index.php?page=book&id=258824.

**5.2 Лицензионное и свободно распространяемое программное обеспечение:**
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

**5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:**
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных ВИНИТИ online** - http://www.viniti.ru/
5. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
6. **Портал открытых данных Российской Федерации** - https://data.gov.ru
7. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
8. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
9. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
10. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
11. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
12. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
13. **Официальный сайт Федерального агентства по техническому регулированию и метрологии** - http://protect.gost.ru/
14. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
15. **Официальный сайт Министерства науки и высшего образования Российской Федерации** - https://minobrnauki.gov.ru
16. **Официальный сайт Федеральной службы по надзору в сфере образования и науки** - https://obrnadzor
17. **Федеральный портал "Российское образование"** - http://www.edu.ru

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|---|---|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | Н-204, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран |
| | К-601, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран |
| Учебные аудитории для проведения | К-301, Учебная аудитория | стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска |

| | | |
|---|---|---|
| практических занятий, КР и КП | | маркерная, кондиционер |
| Учебные аудитории для проведения промежуточной аттестации | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| | К-301, Учебная аудитория | стол преподавателя, стол учебный, стул, мультимедийный проектор, экран, доска маркерная, кондиционер |
| Помещения для самостоятельной работы | НТБ-303, Компьютерный читальный зал | стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер |
| Помещения для консультирования | А-300, Учебная аудитория "А" | кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор |
| Помещения для хранения оборудования и учебного инвентаря | К-202/2, Склад кафедры БИТ | стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования |

**Приложение А**

# БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Система обеспечения информационной безопасности предприятия

(название дисциплины)

**8 семестр**

**Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:**

КМ-1 Сущность и порядок реализации системного подхода к обеспечению информационной безопасности предприятия (организации) (Контрольная работа)

КМ-2 Организация функционирования СОИБ предприятия на основе системного подхода. (Тестирование)

КМ-3 Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия (Контрольная работа)

КМ-4 Разработка модели информационной системы предприятия энергетической отрасли с позиции безопасности (Коллоквиум)

**Вид промежуточной аттестации –** Экзамен.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
|---|---|---|---|---|---|---|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Основы организации и функционирования СОИБ предприятия | | | | | |
| 1.1 | Роль и место информационной безопасности в обеспечении комплексной безопасности хозяйствующего субъекта. | | + | | | |
| 1.2 | Система обеспечения информационной безопасности предприятия. | | + | | | |
| 1.3 | Перечень факторов, влияющих на организацию СОИБ предприятия | | + | | | |
| 1.4 | Политика информационной безопасности. | | + | + | + | |
| 2 | Назначение и общая характеристика видов обеспечения (подсистем) СОИБ предприятия | | | | | |
| 2.1 | Правовые основы функционирования СОИБ предприятия. | | | | + | + |
| 2.2 | Организационные основы функционирования СОИБ предприятия. | | | | | + |
| 2.3 | Кадровое обеспечение СОИБ предприятия. | | | + | + | |
| 2.4 | Финансово-экономическое обеспечение функционирования СОИБ предприятия. | | | | + | |
| 2.5 | Инженерно-техническое обеспечение СОИБ. | | | | | + |
| 2.6 | Программно-аппаратное обеспечение функционирования СОИБ предприятия. | | | | | + |

| | | | | | |
|---|---|---|---|---|---|
| 2.7 | Подсистема аудита информационной системы предприятия. | | | | + |
| 2.8 | Управление СОИБ предприятия. | | | | + |
| | Вес КМ, %: | 25 | 25 | 25 | 25 |