Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 13.04.02 Электроэнергетика и электротехника

Наименование образовательной программы: Интеллектуальные системы защиты, автоматики и управления энергосистемами

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ РЗА ЭНЕРГОСИСТЕМ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.09**
Трудоемкость в зачетных единицах:	**3 семестр - 4;**
Часов (всего) по учебному плану:	**144 часа**
Лекции	**3 семестр - 32 часа;**
Практические занятия	**3 семестр - 16 часов;**
Лабораторные работы	**3 семестр - 16 часов;**
Консультации	**3 семестр - 2 часа;**
Самостоятельная работа	**3 семестр - 77,5 часа;**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: **Отчет**	
Промежуточная аттестация:	
Экзамен	**3 семестр - 0,5 часа;**

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Карантаев В.Г. Идентификатор: Rb72a6d42-KarantayevVG-03f56ea	В.Г. Карантаев

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Волошин А.А. Идентификатор: Ra915003b-VoloshinAA-408ebd73	А.А. Волошин
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Волошин А.А. Идентификатор: Ra915003b-VoloshinAA-408ebd73	А.А. Волошин

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение различных криптографических способов защиты информации устройств релейной защиты и автоматики изучение типов и алгоритмов шифрования микропроцессорных устройств релейной защиты и автоматики

Задачи дисциплины

- формирование представления обучающихся о разнообразных видах и способах криптографической защиты информации устройств релейной защиты и автоматики;
- обучение методам программно-технических мер защиты информации устройств релейной защиты и автоматики, их сравнительного анализа;
- обучение основным алгоритмам шифрования информации микропроцессорных устройств релейной защиты;
- обучение программно-техническим мерам защиты информации микропроцессорных устройств релейной защиты и автоматики.

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-2 Способен осуществить информационный обмен между устройствами релейной защиты и автоматики	ИД-1$_{ПК-2}$ Демонстрирует знание протоколов информационного обмена	знать: - принципы передачи информации между РЗА; - технические средства реализации протоколов передачи данных устройств РЗА. уметь: - настраивать защищенные соединения РЗА; - шифровать программное обеспечение устройств РЗА.
ПК-2 Способен осуществить информационный обмен между устройствами релейной защиты и автоматики	ИД-2$_{ПК-2}$ Демонстрирует знание нормативно-технической документации	знать: - способы защиты информации устройств РЗА; - возможные уязвимости и точки проникновения устройств РЗА. уметь: - на основе анализа находить решения по защите от проникновения РЗА; - выстраивать модель уязвимостей РЗА.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Интеллектуальные системы защиты, автоматики и управления энергосистемами (далее – ОПОП), направления подготовки 13.04.02 Электроэнергетика и электротехника, уровень образования: высшее образование - магистратура.

Требования к входным знаниям и умениям:

- знать основы высшей математики

- знать основы информатики и вычислительной техники
- знать основы программирования
- знать основы построения ЛВС
- знать основы проектирования релейной защиты и автоматики энергосистем
- знать основы релейной защиты
- уметь работать с операционной системой Windows
- уметь работать с операционной системой Linux
- уметь составлять программы

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	Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА	28	3	8	4	4	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА" ***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Защита лабораторной работы №1. Тема –
1.1	Основы информационной безопасности. Понятия, определения	14		4	2	2	-	-	-	-	-	6	-	
1.2	Программная защита информации устройств РЗА	14		4	2	2	-	-	-	-	-	6	-	

														«Настройка защищенного соединения между устройствами РЗА" ***<u>Изучение материалов литературных источников:</u>*** [2], 10-50
2	Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»	28		8	4	4	-	-	-	-	-	12	-	***<u>Подготовка к текущему контролю:</u>*** Повторение материала по разделу "Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»" ***<u>Подготовка к лабораторной работе:</u>*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»" материалу. ***<u>Подготовка к аудиторным занятиям:</u>*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***<u>Подготовка к практическим занятиям:</u>*** Изучение материала по разделу "Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»" подготовка к выполнению заданий на практических занятиях ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»" ***<u>Изучение материалов литературных источников:</u>*** [4], 34-67
2.1	Способы обеспечения защиты информации	14		4	2	2	-	-	-	-	-	6	-	
2.2	Организационные меры защиты информации	14		4	2	2	-	-	-	-	-	6	-	

3	Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты	28		8	4	4	-	-	-	-	-	12	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты"
3.1	Особенности реализации защиты устройств РЗА	14		4	2	2	-	-	-	-	-	6	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты" ***Изучение материалов литературных источников:*** [3], 5-86
3.2	Техническая защита информации устройств РЗА	14		4	2	2	-	-	-	-	-	6	-	
4	Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850	24		8	4	4	-	-	-	-	-	8	-	***Подготовка к текущему контролю:*** Повторение материала по разделу "Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850"
4.1	Криптографические методы защиты	14		4	2	2	-	-	-	-	-	6	-	***Подготовка к лабораторной работе:*** Для выполнения заданий по лабораторной работе

	информации												необходимо предварительно изучить тему и задачи выполнения лабораторной работы, а так же изучить вопросы вариантов обработки результатов по изученному в разделе "Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850" материалу. ***Подготовка к аудиторным занятиям:*** Проработка лекции, выполнение и подготовка к защите лаб. работы ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850" ***Изучение материалов литературных источников:*** [1], 70-92
4.2	Программно-технические меры защиты информации	10		4	2	2	-	-	-	-	-	2	-
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**32**	**16**	**16**	-	**2**	-	-	**0.5**	**44**	**33.5**	
	Итого за семестр	**144.0**		**32**	**16**	**16**	**2**		**-**		**0.5**	**77.5**		

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. Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА

1.1. Основы информационной безопасности. Понятия, определения

«Информационная безопасность». «Доступностью» как соответственно обеспечение доступа к информации. «Целостность» обеспечение достоверности и полноты информации. «Конфиденциальность» обеспечение доступа к информации только авторизованным пользователям. «Угроза» потенциальная возможность тем или иным способом нарушить информационную безопасность. Попытка реализации угрозы называется «атакой», а тот, кто реализует данную попытку, называется «злоумышленником.

1.2. Программная защита информации устройств РЗА

Встроенные средства защиты информации. Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом. Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. Межсетевые экраны (также называемые брандмауэрами или файрволами). Между локальной и глобальной сетями создаются специальные промежуточные серверы, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой. Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript). VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec.

2. Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»

2.1. Способы обеспечения защиты информации

Препятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора. Управление - оказание управляющих воздействий на элементы защищаемой системы. Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника. Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов. Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия

обработки информации под угрозой ответственности (материальной, уголовной, административной) Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

2.2. Организационные меры защиты информации

Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов. Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации. Организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации. Законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности. Психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

3. Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты

3.1. Особенности реализации защиты устройств РЗА

Безопасность данных включает обеспечение достоверности данных и защиту данных и программ от несанкционированного доступа, копирования, изменения. Технологический контроль заключается в организации многоуровневой системы защиты программ и данных как средствами проверки паролей, электронных подписей, электронных ключей, скрытых меток файла. Обеспечение безопасного хранения бинарных файлов устройств РЗА. Обеспечение безопасной передачи данных по протоколу МЭК61850.

3.2. Техническая защита информации устройств РЗА

Технические каналы утечки информации (ТКУИ) и их характеристики; утечка речевой информации. Акустика, виброакустика, акустоэлектропреобразование, высокочастотное навязывание и облучение; утечка информации за счет побочных электромагнитных излучений и наводок. Эфир, токопроводящие материалы, высокочастотное навязывание и облучение.

4. Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850

4.1. Криптографические методы защиты информации

Криптография с симметричными ключами В криптографии с симметричными ключами (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных. Криптография с открытыми ключами Для решения задач распределения ключей и ЭЦП используются идеи асимметричности преобразований и открытого распределения ключей Диффи и Хеллмана.

Шифрование. Реализация схемы ЭЦП с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией. Доверие к открытому ключу и цифровые сертификаты Центральным вопросом схемы открытого распределения ключей является вопрос доверия к полученному открытому ключу партнера, который в процессе передачи или хранения может быть модифицирован или подменен.

4.2. Программно-технические меры защиты информации

Создание препятствий на возможных путях проникновения и доступа потенциальных нарушителей к системе и защищаемой информации. Идентификация и аутентификация пользователей. Разграничение доступа к ресурсам. Регистрация событий. Криптографическая защита информации.

3.3. Темы практических занятий

1. Шифрование дешифрование бинарных файлов и текстовой информации;
2. Разработка защиты информации с применением блокчейн;
3. Хэширование данных;
4. Электронные деньги, безопасность в экономической сфере.

3.4. Темы лабораторных работ

1. Настройка защищенного соединения между устройствами РЗА;
2. Обеспечение защиты информации и конфигурационных файлов устройств РЗА;
3. Взлом и подмена настроек устройств релейной защиты;
4. Криптозащита передачи данных по протоколу МЭК61850.

3.5 Консультации

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850"

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	3	4	
Знать:						
технические средства реализации протоколов передачи данных устройств РЗА	ИД-1$_{ПК-2}$	+				Отчет/КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА
принципы передачи информации между РЗА	ИД-1$_{ПК-2}$	+				Отчет/КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА
возможные уязвимости и точки проникновения устройств РЗА	ИД-2$_{ПК-2}$		+			Отчет/КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА
способы защиты информации устройств РЗА	ИД-2$_{ПК-2}$		+			Отчет/КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА
Уметь:						
шифровать программное обеспечение устройств РЗА	ИД-1$_{ПК-2}$			+		Отчет/КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты
настраивать защищенные соединения РЗА	ИД-1$_{ПК-2}$			+		Отчет/КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты
выстраивать модель уязвимостей РЗА	ИД-2$_{ПК-2}$				+	Отчет/КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850
на основе анализа находить решения по защите от проникновения РЗА	ИД-2$_{ПК-2}$				+	Отчет/КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850

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

4.1. Текущий контроль успеваемости

3 семестр

Форма реализации: Выполнение задания

1. КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА (Отчет)
2. КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850 (Отчет)
3. КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА (Отчет)
4. КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты (Отчет)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №3)

Промежуточная аттестация по итогам освоения дисциплины: средняя оценка по всем оценочным средствам на каждой контрольной неделе. Оценки за все контрольные недели используется при допуске к экзамену

В диплом выставляется оценка за 3 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш . – 3-е изд., перераб. и доп . – М. : РИОР : ИНФРА-М, 2017 . – 322 с. – (Высшее образование) . - ISBN 978-5-369-01450-9 .;
2. Барабанов А. В., Дорофеев А. В., Марков А. С., Цирлов В. Л.- "Семь безопасных информационных технологий", Издательство: "ДМК Пресс", Москва, 2017 - (224 с.) https://e.lanbook.com/book/97352;
3. Карантаев, В. Г. Основы анализа и синтеза требований кибербезопасности ИЭУ подсистемы релейной защиты ЦПС : учебное пособие по курсу "Специальные вопросы электроэнергетики" для студентов, обучающихся по направлению 13.04.02 "Электроэнергетика и электротехника" / В. Г. Карантаев, В. И. Карпенко, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ") . – Москва : Изд-во МЭИ, 2021 . – 100 с. - ISBN 978-5-7046-2448-6 . http://elib.mpei.ru/elib/view.php?id=11521;
4. Папков, Б. В. Проблемы кибербезопасности электроэнергетики / Б. В. Папков, А. Л. Куликов, В. Л. Осокин . – М. : Энергопрогресс, 2017 . – 96 с. – (Библиотечка электротехника, приложение к журналу "Энергетик" ; вып.9(225)) ..

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. Office / Российский пакет офисных программ;
2. Windows / Операционная система семейства Linux;

3. Видеоконференции (Майнд, Сберджаз, ВК и др).

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 Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
7. **Портал открытых данных Российской Федерации** - https://data.gov.ru
8. **База открытых данных Министерства труда и социальной защиты РФ** - https://rosmintrud.ru/opendata
9. **База открытых данных профессиональных стандартов Министерства труда и социальной защиты РФ** - http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/
10. **База открытых данных Министерства экономического развития РФ** - http://www.economy.gov.ru
11. **База открытых данных Росфинмониторинга** - http://www.fedsfm.ru/opendata
12. **Электронная открытая база данных "Polpred.com Обзор СМИ"** - https://www.polpred.com

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Д-107, Аудитория кафедры РЗиАЭ	стол, стул, шкаф, мультимедийный проектор, экран, доска маркерная, журналы, книги, учебники, пособия
Учебные аудитории для проведения практических занятий, КР и КП	Д-107, Аудитория кафедры РЗиАЭ	стол, стул, шкаф, мультимедийный проектор, экран, доска маркерная, журналы, книги, учебники, пособия
Учебные аудитории для проведения лабораторных занятий	Г-101в-1, Лаборатория Автоматики кафедры РЗиАЭ	стул, шкаф для документов, компьютерная сеть с выходом в Интернет, мультимедийный проектор, оборудование специализированное, компьютер персональный, кондиционер
Учебные аудитории для проведения промежуточной аттестации	Д-107, Аудитория кафедры РЗиАЭ	стол, стул, шкаф, мультимедийный проектор, экран, доска маркерная, журналы, книги, учебники, пособия
Помещения для самостоятельной работы	Д-114, Компьютерный класс кафедры РЗиАЭ	стол, стул, компьютерная сеть с выходом в Интернет, компьютер персональный
	Д-105, Компьютерный класс кафедры РЗиАЭ	стол, стул, компьютерная сеть с выходом в Интернет, доска маркерная, компьютер персональный
Помещения для консультирования	Д-108, Кабинет сотрудников каф.	кресло рабочее, стол, стул, компьютерная сеть с выходом в Интернет, доска

	"РЗиАЭ"	маркерная, компьютер персональный, принтер
	Д-106, Кабинет сотрудников каф. "РЗиАЭ"	кресло рабочее, стол, стул, шкаф, компьютерная сеть с выходом в Интернет, компьютер персональный
	Д-103/1, Помещение каф. "РЗиАЭ"	кресло рабочее, стол, стул, шкаф для документов, компьютерная сеть с выходом в Интернет, доска маркерная, компьютер персональный, принтер
	Д-210, Помещение сотрудников кафедры РЗиАЭ	кресло рабочее, стол, шкаф для документов, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер
	Д-208, Помещение кафедры РЗиАЭ	стол, стул, компьютер персональный
	Д-211, Помещение кафедры РЗиАЭ	кресло рабочее, стол, стул, шкаф для документов, компьютер персональный, принтер
	г-101в-3, Рабочее помещение сотрудников кафедры РЗиАЭ	кресло рабочее, стул, шкаф для документов, компьютерная сеть с выходом в Интернет, компьютер персональный, кондиционер
Помещения для хранения оборудования и учебного инвентаря	Д-103/2, Склад кафедры РЗиАЭ	компьютерная сеть с выходом в Интернет, оборудование специализированное

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Основы кибербезопасности РЗА энергосистем

(название дисциплины)

3 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 КМ -1. ЛР Настройка защищенного соединения между устройствами РЗА (Отчет)
КМ-2 КМ-2 ЛР Обеспечение защиты информации и конфигурационных файлов устройств РЗА (Отчет)
КМ-3 КМ-3 ЛР Взлом и подмена настроек устройств релейной защиты (Отчет)
КМ-4 КМ -4 ЛР Криптозащита передачи данных по протоколу МЭК61850 (Отчет)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	16
1	Защита лабораторной работы №1. Тема – «Настройка защищенного соединения между устройствами РЗА					
1.1	Основы информационной безопасности. Понятия, определения		+			
1.2	Программная защита информации устройств РЗА		+			
2	Защита лабораторной работы №2. Тема – «Обеспечение защиты информации и конфигурационных файлов устройств РЗА»					
2.1	Способы обеспечения защиты информации			+		
2.2	Организационные меры защиты информации			+		
3	Защита лабораторной работы №3. Тема – «Взлом и подмена настроек устройств релейной защиты					
3.1	Особенности реализации защиты устройств РЗА				+	
3.2	Техническая защита информации устройств РЗА				+	
4	Защита лабораторной работы №4. Тема – «Криптозащита передачи данных по протоколу МЭК61850					
4.1	Криптографические методы защиты информации					+
4.2	Программно-технические меры защиты информации					+
		Вес КМ, %:	25	25	25	25