Министерство науки
и высшего образования РФ
ФГБОУ ВО «НИУ «МЭИ»
Институт дистанционного
и дополнительного образования

УТВЕРЖДАЮ:
Директор ИДДО

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Шиндина Т.А.
Идентификатор	Rd0ad64b2-ShindinaTA-e12224c9

(подпись)

Т.А. Шиндина
(расшифровка подписи)

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

повышения квалификации

Наименование программы	Основы кибербезопасности микропроцессорных устройств релейной защиты и автоматики
Форма обучения	очная
Выдаваемый документ	удостоверение о повышении квалификации
Новая квалификация	не присваивается
Центр ДО	ОДПО, Центр профессиональной переподготовки преподавателей "Управление в высшем образовании"

Зам. директора ИДДО	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Усманова Н.В. Идентификатор: R3b653adc-UsmanovaNatV-90b3fa4	Н.В. Усманова
Начальник ОДПО	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крохин А.Г. Идентификатор: R6d4610d5-KrokhinAG-aa301f84	А.Г. Крохин
Руководитель ОДПО, ЦПП УВО	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Максимова А.А. Идентификатор: R6a033f13-VorozhtsovaAA-daecd82	А.А. Максимова
Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Сафронов Б.А. Идентификатор: Ra01acb9f-SafronovBA-92cc47d9	Б.А. Сафронов

Москва

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Цель: повышение квалификации путем формирования повышения у слушателей профессиональных компетенций, необходимых для выполнения профессиональной деятельности в области кибербезопасности микропроцессорных устройств релейной защиты и автоматики..

Программа составлена в соответствии:

- с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 13.03.02 Электроэнергетика и электротехника, утвержденным приказом Минобрнауки от 28.02.2018 г. № 14422.03.2018 г. № 50467.
- с Профессиональным стандартом 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденным приказом Минтруда 01.11.2016 г. № 598н, зарегистрированным в Минюсте России 28.11.2016 г. № 44464, уровень квалификации 8.

Форма реализации: обучение с применением дистанционных образовательных технологий.

Форма обучения: очная.

Режим занятий:

Расписание занятий по дополнительной образовательной программе может устанавливаться в зависимости от набора в группы. Конкретные даты проведения занятий указываются в договоре на оказание образовательных услуг. При любом графике занятий учебная нагрузка устанавливается не более 40 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

Требования к уровню подготовки слушателя, необходимые для освоения программы: лица, желающие освоить дополнительную образовательную программу, должны иметь среднее профессиональное или высшее образование. Наличие указанного образования должно подтверждаться документом государственного или установленного образца..

Выдаваемый документ: при успешном прохождении программы и сдаче итоговой аттестации выдается удостоверение о повышении квалификации установленного образца.

Срок действия итоговых документов

Срок действия итоговых документов регламентируется на основе правил по работе с персоналом в сфере деятельности данной программы, устанавливается на основе содержания программы и составляет (в годах): 5.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

2.1. Компетенции

В результате освоения дополнительной образовательной программы слушатель должен обладать компетенциями (табл. 1).

Таблица 1

Компетентностно-ориентированные требования к результатам освоения программы

Компетенция	Требования к результатам
ОПК-1: Способен понимать принципы работы современных информационных технологий и использования их для решения задач профессиональной деятельности	Знать: - Технические средства реализации протоколов передачи данных устройств РЗА; - Принципы передачи информации между РЗА; - Возможные уязвимости и точки проникновения устройств РЗА; - Способы защиты информации устройств РЗА.
	Уметь: - Шифровать программное обеспечение устройств РЗА; - Настраивать защищенные соединения РЗА; - Выстраивать модель уязвимостей РЗА; - На основе анализа находить решения по защите от проникновения РЗА.
	Владеть:

В результате освоения программы слушатель должен быть способен реализовывать трудовые функции в соответствии с профессиональным стандартом (табл. 2).

Уровень квалификации 7.

Таблица 2

Практико-ориентированные требования к результатам освоения программы

Трудовые функции	Требования к результатам
06.032 «Специалист по безопасности компьютерных систем и сетей»	
ПК-842/С/03.7/1 способен осуществлять проведение анализа безопасности компьютерных систем	Трудовые действия: - Оценка рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; - Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам.
	Умения: - Анализировать компьютерную систему с целью определения уровня защищенности и доверия; - Прогнозировать возможные пути развития действий нарушителя информационной безопасности; - Производить анализ политики безопасности на предмет адекватности.

	Знания: - Принципы построения компьютерных систем и сетей; - Криптографические методы защиты информации; - Уязвимости компьютерных систем и сетей; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - Нормативные правовые акты в области защиты информации; - Национальные, межгосударственные и международные стандарты в области защиты информации.

2.2. Характеристика нового вида профессиональной деятельности, новой квалификации

Не предусмотрено

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ (РАБОЧИЕ ПРОГРАММЫ ДИСЦИПЛИН (МОДУЛЕЙ)

3.1. Трудоемкость программы

Трудоемкость программы включая все виды аудиторной и внеаудиторной (самостоятельной) работы составляет**:**

- 2 зачетных единиц;

72 ак. ч.

Структура программы с указанием наименования дисциплин (модулей) и их трудоемкости представлена в табл. 3.

Учебный план дополнительной образовательной программы представлен в приложение А., являющийся неотъемлемой частью программы.

Таблица 3

Структура программы и формы аттестации

№	Наименование дисциплин (модулей)	всего	Контактная работа, ак. ч					Самостоятельная работа, ак. ч	Стажировка, ак. ч	Форма аттестации		
			всего	аудиторные занятия	электронное обучение	обучение с ДОТ	контроль			текущий контроль (тест, опрос и пр.)	промежуточная аттестация (зачет, экзамен, защита отчета о стажировке)	итоговая аттестация (итоговый зачет, итоговый экзамен, доклад по результатам стажировки, итоговый аттестационный экзамен, итоговая аттестационная работа)
1	2	3	4	5	6	7	8	9	11	12	13	14
1	Основы кибербезопасности микропроцессорны	70	50	24		26		20			Нет	

	х устройств релейной защиты и автоматики											
1.1.	Введение в учебный курс	2	2			2						
1.2.	Обзор нормативно-правого и нормативно-технического регулирования в сфере защиты информации, безопасности критической информационной инфраструктуры РФ при переходе к цифровизации электроэнергетической отрасли РФ	10	6			6		4				
1.3.	Вопросы защиты информации в автоматизированных системах управления, системах релейной защиты и противоаварийной автоматики активно-адаптивных сетей (Smart Grid)	24	18			18		6				
1.4.	Работа с проектами с открытым кодом. Реализация взаимодействия по протоколу MMS. Применение протокола TLS 1.2 для защиты протокола MMS. Изучение объекта защиты ИЭУ РЗА. Разработка Модели угроз кибербезопасности ИЭУ РЗА. Разработка требований к встроенным в ИЭУ РЗА средствам защиты информации	34	24	24				10				
2	Итоговая аттестация	2	2				2					Итоговый зачет

	ИТОГО:	**72**	**52**	**24**	**0**	**26**	**2**	**20**	**0**			

3.2. Содержание программы (рабочие программы дисциплин (модулей)
Содержание дисциплин (модулей) представлено в табл. 4.

Таблица 4

Содержание дисциплин (модулей)

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
1.	Основы кибербезопасности микропроцессорных устройств релейной защиты и автоматики	
1.1.	Введение в учебный курс	Введение в предмет: Основные понятия предметной области.
1.2.	Обзор нормативно-правого и нормативно-технического регулирования в сфере защиты информации, безопасности критической информационной инфраструктуры РФ при переходе к цифровизации электроэнергетической отрасли РФ	Частные вопросы нормативно-правового регулирования в сфере обеспечения безопасного функционирования Объектов КИИ при переходе к Цифровизации электроэнергетической отрасли РФ.Частные вопросы нормативно-технического регулирования, обеспечивающего реализацию концепции активно-адаптивной сети (Smart Grid), создания цифровых питающих центров (Цифровых подстанций).Вопросы международного нормативно-технического регулирования, обеспечивающего реализацию концепции активно-адаптивной сети (Smart Grid), создания цифровых питающих центров (Цифровых подстанций).
1.3.	Вопросы защиты информации в автоматизированных системах управления, системах релейной защиты и противоаварийной автоматики активно-адаптивных сетей (Smart Grid)	Частные методические вопросы анализа угроз безопасности информации в автоматизированных системах управления, системах релейной защиты и противоаварийной автоматики активно-адаптивных сетей (Smart Grid).Обзор основных концепций построения защищенных компьютерных систем (цифровых систем) Smart Grid.Обзор основных механизмов защиты, реализуемых в защищенных встроенных операционных системах. Вводная лекция в криптологию. Понятия: криптология, криптография, криптоанализ. Частные вопросы теории одноключевых алгоритмов. Частные вопросы теории двуключевых алгоритмов.Криптографические хеш функции. Коды аутентичности сообщений. Распределение и управление криптографическими ключами.Обзор криптографических протоколов, применение которых возможно в систем релейной защиты и противоаварийной автоматики активно-адаптивных

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		сетей (Smart Grid). Теоретические и практические способы криптографической защиты информации при реализации межсетевого взаимодействия в ЦПС в соответствии со стандартом МЭК 61850 и МЭК 62351.Вопросы реализации и применения встроенных СЗИ в современных Интеллектуальных Электронных Устройствах.Введение в организацию процессов разработки безопасного программного обеспечения комплексов систем управления Smart Grid (РЗА и ПА).
1.4.	Работа с проектами с открытым кодом. Реализация взаимодействия по протоколу MMS. Применение протокола TLS 1.2 для защиты протокола MMS. Изучение объекта защиты ИЭУ РЗА. Разработка Модели угроз кибербезопасности ИЭУ РЗА. Разработка требований к встроенным в ИЭУ РЗА средствам защиты информации	Работа с проектами с открытым кодом. Реализация взаимодействия по протоколу MMS. Применение протокола TLS 1.2 для защиты протокола MMS. Изучение объекта защиты ИЭУ РЗА. Разработка Модели угроз кибербезопасности ИЭУ РЗА. Разработка требований к встроенным в ИЭУ РЗА средствам защиты информации.

Аннотации рабочих программ дисциплин (модулей) представлены в приложении Б.

4. ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Информация о практической подготовке в структуре дополнительной образовательной программы представлена в приложение В.

В рамках учебного плана дополнительной образовательной программы используются традиционные образовательные технологии, а также интерактивные технологии, представленные в табл. 5.

Таблица 5

Характеристика образовательной технологии

Наименование	Краткая характеристика
Не предусмотрено	

5. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

5.1. Текущий контроль

Текущий контроль проводится в соответствии с характеристиками контрольных заданий и представлен в Таблице 1 приложения Г.

5.2. Промежуточная аттестация

Промежуточная аттестация по программе проводится в форме зачета, экзамена или отчета о стажировке в соответствии с учебным планом. Характеристика заданий представлена в Таблице 2 приложения Г.

5.3. Итоговая аттестация

Итоговая аттестация по программе проводится в форме . Характеристика заданий представлена Таблице 3 приложения Г.

5.4. Независимый контроль качества обучения

Порядок независимой оценки качества дополнительной образовательной программы представлен в приложении Г.

6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

6.1. Учебно-методическое и информационное обеспечение

а) литература НТБ МЭИ:

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. 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;

3. 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)) ..

б) литература ЭБС и БД:

1. 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.

в) используемые ЭБС:

1. База данных Scopus http://www.scopus.com;
2. База данных Web of Science http://webofscience.com/ ;
3. Научная электронная библиотека https://elibrary.ru/;
4. Национальная электронная библиотека https://rusneb.ru/;
5. ЭБС Лань https://e.lanbook.com/;
6. ЭБС "Университетская библиотека онлайн" http://biblioclub.ru/index.php?page=main_ub_red;
7. Электронная библиотека МЭИ (ЭБ МЭИ) http://elib.mpei.ru/login.php.

6.2. Кадровое обеспечение

Для реализации дополнительной образовательной программы привлекаются преподаватели из числа штатных научно-педагогических работников ФГБОУ ВО «НИУ «МЭИ» и лица, представители работодателей или объединений работодателей. Информация о кадровом обеспечении дополнительной образовательной программы представлена в приложении Д.

Сведения о руководителе дополнительной образовательной программы представлены в приложение Е.

6.3. Финансовое обеспечение

План расходов и расчет обоснования стоимости по дополнительной образовательной программе представлены в приложение Ж.

Финансирование программы осуществляется за счет личных средств слушателей или заказчиков, по направлению которых проводится обучение. В качестве заказчика могут выступать работодатели, университеты (в том числе МЭИ), государственные структуры и прочие участники образовательного рынка.

6.4. Материально-техническое обеспечение

Материально-технические условия реализации дополнительной образовательной программы представлены в Приложении З.

Календарный график учебного процесса разрабатывается с учетом требований к качеству освоения и по запросам обучающихся (Приложение И). Расписание занятий разрабатывается на каждую реализуемую программу.

ЛИСТ ИЗМЕНЕНИЙ (АКТУАЛИЗАЦИИ)

№ п/п	Содержание изменения (актуализации)	Дата утверждения изменений
1	Программа утверждена	09.10.2023

Руководитель образовательной программы

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»
Сведения о владельце ЦЭП МЭИ
Владелец: Сафронов Б.А.
Идентификатор: Ra01acb9f-SafronovBA-92cc47d9

Б.А. Сафронов