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	Организация и технологии защиты информации: новое в отрасли
Форма обучения	очно-заочная
Выдаваемый документ	удостоверение о повышении квалификации
Новая квалификация	не присваивается
Центр ДО	Кафедра "Безопасности и информационных технологий", Центр подготовки и переподготовки "Кибербезопасности"

Зам. директора ИДДО (должность, ученая степень, ученое звание)	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Усманова Н.В. Идентификатор: R3b653adc-UsmanovaNatV-90b3fa4 (подпись)	Н.В. Усманова (расшифровка подписи)
Начальник ОДПО (должность, ученая степень, ученое звание)	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Крохин А.Г. Идентификатор: R6d4610d5-KrokhinAG-aa301f84 (подпись)	А.Г. Крохин (расшифровка подписи)
Руководитель кафедра БИТ, ЦПП ИИЭБП (должность, ученая степень, ученое звание)	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Кунбутаев Л.М. Идентификатор: R7a759843-KunbutayevLM-28fc24a (подпись)	Л.М. Кунбутаев (расшифровка подписи)
Руководитель образовательной программы (должность, ученая степень, ученое звание)	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d (подпись)	А.Ю. Невский (расшифровка подписи)

Москва

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Цельповышение квалификации слушателей путем формирования у них профессиональных компетенций, необходимых для профессиональной деятельности в области организации и технологий защиты информации..

Программа составлена в соответствии:

- с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Минобрнауки от 17.11.2020 г. № 142718.02.2021 г. № 62548.

Форма реализации: обучение с применением дистанционных образовательных технологий.

Форма обученияочно-заочная.

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. Данные расписания хранятся в электронной системе учета хода реализации программы. 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 программылица, желающие освоить дополнительную образовательную программу должны иметь высшее образование.

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 оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Знать: - законодательные и нормативные акты по информационной безопасности; - особенности и приоритеты практической подготовки студентов по программам бакалавриата и магистратуры для повышения конкурентоспособности выпускников.
	Уметь: - решать задачи управления информационной безопасностью организации.
	Владеть: - системным подходом при организации подготовки бакалавров и магистров.

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

_____.

Таблица 2

Практико-ориентированные требования к результатам освоения программы

Трудовые функции	Требования к результатам

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**:**

- 1 зачетных единиц;

36 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	лекции	семинары, практические и лабораторные занятия	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	Актуальное правовое и нормативное регулирование информационной безопасности	3	2	2				1			Нет	
1.1.	Актуальное правовое и нормативное регулирование информационной безопасности	3	2	2				1				
2	Управление информационной безопасностью	6	5	2		3		1			Нет	
2.1.	Управление информационной безопасностью	6	5	2		3		1				
3	Менеджмент рисков информационной безопасности	6	5	2		3		1			Нет	
3.1.	Менеджмент рисков информационной безопасности	6	5	2		3		1				
4	Компьютерная безопасность	6	5	2		3		1			Нет	
4.1.	Компьютерная безопасность	6	5	2		3		1				
5	Современные аспекты безопасности информационных технологий	6	5	2		3		1			Нет	
5.1.	Современные аспекты безопасности	6	5	2		3		1				

	информационных технологий											
6	Образовательные и профессиональные стандарты по защите информации	3	2	1		1		1			Нет	
6.1.	Образовательные и профессиональные стандарты по защите информации	3	2	1		1		1				
7	Методика практической подготовки специалистов в сфере информационной безопасности	4	3	1		2		1			Нет	
7.1.	Методика практической подготовки специалистов в сфере информационной безопасности	4	3	1		2		1				
8	Итоговая аттестация	2	2				2					Итоговый зачет
	ИТОГО:	**36**	**29**	**12**	**0**	**15**	**2**	**7**	**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.	Актуальное правовое и нормативное регулирование информационной безопасности	
1.1.	Актуальное правовое и нормативное регулирование информационной безопасности	Тема № 1. Правовое обеспечение ИБ Основы правового обеспечения ИБ в РФ. Система правового регулирования отношений в информационной области. Правовое регулирование отношений в области: - служебной и профессиональной тайн; - персональных данных; - информационной безопасности объектов критической информационной инфраструктуры энергетики; - интеллектуальной собственности; - технического регулирования; - массовой информации, телекоммуникаций и связи. Тема № 2. Организационное обеспечение ИБ Основы организационного обеспечения

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		ИБ предприятия. Конфиденциальная информация (КИ). Допуск персонала к КИ и работа с этим персоналом. Пропускной и внутренний режим предприятия. Охрана и физическая защита предприятия. Защита информации при: - проведении совещаний; - в рекламной и публикационной деятельности. Контроль защиты КИ на предприятии. Организация и проведение служебных расследований по фактам разглашения КИ и утраты носителей КИ.
2.	Управление информационной безопасностью	
2.1.	Управление информационной безопасностью	Тема № 1. Национальные стандарты в области ИБ. Управление ИБ предприятия на основе стандартов ГОСТ Р ИСО/МЭК 27000 в области менеджмента ИБ Требования национальных стандартов по управлению ИБ: комплекс стандартов СТО БР ИББС-1.0-2014; ГОСТ Р ИСО/МЭК 27001:2006; ГОСТ Р ИСО/МЭК 27002:2021; ГОСТ Р ИСО/МЭК 27005:2010. Тема № 2. Управление физической защитой информационных активов предприятия и контроль доступа к ним Реализация политик «чистого стола» и «чистого экрана». Хранение носителей информации. Обеспечение сохранности компьютерной и оргтехники. Прием и отправка корреспонденции. Доступ к копировальным устройствам. Тема № 3. Управление программно-аппаратной защитой активов предприятия Защита программного обеспечения и массивов информации от внедрения вредоносного кода. Реализация политик резервного копирования, журнальной регистрации событий информационной системы и ошибочных действий пользователей. Защита от неавторизованного доступа. Обеспечение безопасности информационных активов при использовании облачных сервисов. Безопасность сменных носителей. Утилизация носителей информации. Тема №4. Управление безопасностью процедур обработки и обмена информацией между организациями Организация процедур обработки и хранения информации. Обеспечение безопасного обмена информацией, программным обеспечением и носителями информации между организациями. Безопасность электронной почты. Тема № 5. Разработка, внедрение и совершенствование системы менеджмента ИБ на предприятии Определение области действия СМИБ на предприятии и разработка политики СМИБ:

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		концепция, предъявляемые к СМИБ требования, управление рисками и критерии их оценки. Организация мониторинга и анализа СМИБ. Совершенствование СМИБ на основе полученных результатов. Тема №6. Оценка эффективности СМИБ предприятия с помощью программных средств Связь СМИБ с жизненным циклом информационных технологий предприятия. Общая характеристика программного комплекса.
3.	Менеджмент рисков информационной безопасности	
3.1.	Менеджмент рисков информационной безопасности	Тема № 1. Термины и определения. Моделирование угроз информационной безопасности Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков. Цели и задачи моделирования угроз информационной безопасности. Базовая модель угроз. Тема № 2. Управление рисками в концепциях отечественных и зарубежных стандартов Управление рисками в концепции ГОСТ ИСО/МЭК 27005: Управление рисками в концепции стандарта США NIST 800-30, COBIT 5,0.
4.	Компьютерная безопасность	
4.1.	Компьютерная безопасность	Тема № 1. Классификация угроз безопасности информации при обработке и хранении на ПК Виды и источники угроз ИБ. Виды сетевых атак. Снижение вероятности угрозы сниффинга пакетов. Меры по ликвидации угрозы IP-спуффинга. Тема № 2. Технические аспекты безопасности компьютерных данных Борьба с атаками на уровне приложений. Безопасность локальных вычислительных сетей. Распределенное хранение файлов. Уровни ЗИ. Аутентификация пользователя. Тема № 3. Атаки снаружи и изнутри Что включает ЗИ от НСД. Атаки снаружи и изнутри Достоинства и недостатки программно-аппаратных средств ЗИ. Механизмы защиты при идентификации и аутентификации пользователя. Система управления доступом. Система протоколирования аудита. Виды механизмов защиты для обеспечения конфиденциальности данных и сообщений. Контроль участников взаимодействия. Служба регистрации и наблюдения. Программа «Логическая бомба». Тема №4. Направления работ по защите информационной системы объекта Требования к автоматизированным системам защиты 3-й, 2-й и 1-й групп. Классы ЗИ от НСД для вычислительной техники.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		Выбор класса защищенности. Межсетевые экраны: требования и показатели защищенности. Программы-вирусы, пути их распространения, методы их обнаружения и противодействия им.
5.	Современные аспекты безопасности информационных технологий	
5.1.	Современные аспекты безопасности информационных технологий	Тема № 1. Безопасность персональных данных. Новый взгляд на старые проблемы Новое в законодательстве РФ и нормативном регулировании защиты персональных данных. Угрозы персональным данным в современном информационном пространстве. Оценка рисков, связанных с утечкой персональных данных. Тема № 2. Безопасность критической информационной инфраструктуры и проблема импортозамещения Организация защиты значимых объектов ключевой информационной инфраструктуры (ЗО КИИ) на основе современных требований законодательства РФ. Подключение субъектов КИИ к ГосСОПКА. Перечень используемых программно-аппаратных и программных средств защиты информации для обеспечения безопасности ЗОО КИИ с учетом требований импортозамещения
6.	Образовательные и профессиональные стандарты по защите информации	
6.1.	Образовательные и профессиональные стандарты по защите информации	Тема № 1. Общие положения Основы безопасности ИТ. Угрозы безопасности ИТ. Тема № 2. Основные принципы и меры по обеспечению безопасности ИТ. Правовые основы обеспечения безопасности ИТ Тема № 3. Обеспечение безопасности информационных технологий Организационная структура системы обеспечения безопасности ИТ. Обязанности конечных пользователей и ответственных за обеспечение безопасности ИТ в подразделениях. Документы, регламентирующие правила парольной и антивирусной защиты. Тема № 4. Обеспечение безопасности компьютерных систем и сетей
7.	Методика практической подготовки специалистов в сфере информационной безопасности	
7.1.	Методика практической подготовки специалистов в сфере информационной безопасности	Тема № 1. Круглый стол: Концептуальные основы подготовки специалистов по информационной безопасности Поколение стандартов ФГОС ВО 3++. Профессиональные стандарты. Практическая реализация в информационной системе «Электронный МЭИ». Актуальные знания, необходимые специалисту по информационной безопасности (программа «Эталон»)

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		Тема № 2. Аналитический обзор существующих подходов к построению процесса подготовки специалистов в области защиты информации Тема № 3. Краткосрочные формы обучения специалистов в области информационной безопасности

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

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 -*итоговый зачет*. 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. Бабаш, А. В. Информационная безопасность: лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников . – 2-е изд., стереотип . – М. : КноРус, 2013 . – 136 с. + CD . – (Бакалавриат) . - ISBN 978-5-406-02760-8 .

2. Информационная безопасность открытых систем. В 2 т. Т.1. Угрозы, уязвимости, атаки и подходы к защите : учебник для вузов по специальности 075500(090105) "Комплексное обеспечение информационной безопасности автоматизированных систем" / С. В. Запечников, и др. – М. : Горячая Линия-Телеком, 2006 . – 536 с. - ISBN 5-935172-91-1 .

3. Информационная безопасность открытых систем. В 2 т. Т.2. Средства защиты в сетях : учебник для вузов по специальности 075500(090105) "Комплексное обеспечение информационной безопасности автоматизированных систем" / С. В. Запечников, и др. – М. : Горячая Линия-Телеком, 2008 . – 558 с. - ISBN 978-5-9912003-4-9 .

4. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для вузов по специальности 075400 "Комплексная защита объектов информации" / А. А. Малюк . – М. : Горячая Линия-Телеком, 2004 . – 280 с. - ISBN 5-935171-97-X .

5. Партыка, Т. Л. Информационная безопасность : учебное пособие для среднего профессионального образования по специальностям информатики и вычислительной техники / Т. Л. Партыка, И. И. Попов . – 5-е изд., перераб. и доп . – М. : Форум : ИНФРА-М, 2014 . – 432 с. – (Профессиональное образование) . - ISBN 978-5-91134-627-0 .

6. Федеральный закон "Об информации, информационных технологиях и защите информации: вступил в силу с 9 авг. 2006 г. – Новосибирск : Сиб. унив. изд-во, 2006 . – 16 с. – (Кодексы и законы России) . - ISBN 5-940877-41-9 .

7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для среднего профессионального образования по группе специальностей "Информатика и вычислительная техника" / В. Ф. Шаньгин . – М. : Форум : ИНФРА-М, 2012 . – 416 с. – (Профессиональное образование) . - ISBN 978-5-8199-0331-5 .

8. Ярочкин, В. И. Информационная безопасность : учебник для вузов по гуманитарным и социально-экономическим специальностям / В. И. Ярочкин ; Отв. ред. Л. И. Филиппенко . – 5-е изд . – М. : Академический проект, 2008 . – 544 с. – (Gaudeamus) . - ISBN 978-5-8291-0987-5 .

б) литература ЭБС и БД:

в) используемые ЭБС:

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	27.06.2022

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)