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

профессиональной переподготовки

Наименование программы	Безопасность автоматизированных систем
Форма обучения	очно-заочная
Выдаваемый документ	диплом о профессиональной переподготовке
Новая квалификация	не присваивается
Центр ДО	Филиал МЭИ в г. Смоленск, Центр подготовки и переподготовки "Энергетик"

Зам. директора ИДДО (должность)
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)
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)

Начальник ФДО (должность)
Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»
Сведения о владельце ЦЭП МЭИ
Владелец: Малич Н.В.
Идентификатор: R13696f6e-MalichNV-45fe3095
(подпись) Н.В. Малич (расшифровка подписи)

Руководитель Филиал МЭИ в г. Смоленск, ЦПП "Энергетик" (должность)
Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»
Сведения о владельце ЦЭП МЭИ
Владелец: Максимкин В.Л.
Идентификатор: R9e14050c-MaximkinVL-G14050C2
(подпись) В.Л. Максимкин (расшифровка подписи)

Москва

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Максимкин В.Л. Идентификатор: R9e14050c-MaximkinVL-G14050C2	В.Л. Максимкин
(должность)	(подпись)	(расшифровка подписи)

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Цель: профессиональная переподготовка путем формирования у слушателей профессиональных компетенций, необходимых для профессиональной деятельности в области информационной безопасности..

Программа составлена в соответствии:

- с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки от 26.11.2020 г. № 145518.02.2021 г. № 62549.
- с Профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах», утвержденным приказом Минтруда 15.09.2016 г. № 522н, зарегистрированным в Минюсте России 28.09.2016 г. № 43857, уровень квалификации 8.

Форма реализации: обучение в МЭИ.

Форма обучения: очно-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 ее наличии. 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: требования к уровню подготовки слушателя, необходимые для освоения программы: лица, желающие освоить дополнительную профессиональную программу, должны иметь высшее или среднее профессиональное образование. Наличие указанного образования должно подтверждаться документом государственного или установленного образца..

Выдаваемый документ: при успешном прохождении программы и сдаче итоговой аттестации выдается диплом о профессиональной переподготовке 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): бессрочно.

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-4: способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Знать: - Современную классификацию средств защиты информации в информационных системах..
	Уметь: - Применять современные программные и аппаратные средства защиты информации..
	Владеть: - Способностью осваивать новые методы обеспечения информационной безопасности..
ОПК-2: способен разрабатывать технический проект системы (подсистемы либо компонента система) обеспечения информационной безопасности	Знать: - Структуры современных информационных сетей; оборудование информационных сетей современного уровня; используемые технологии обеспечения безопасности информационных сетей.
	Уметь: - Разрабатывать информационные сети заданной структуры или заданного предназначения; настраивать компоненты информационных сетей; организовывать эксплуатацию информационных сетей.
	Владеть: - Навыками комплексного подхода к разработке информационной системы, как защищенной сетевой структуры.
ОПК-1: способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Знать: - Основные положения и методы управления коммуникациями в проекте..
	Уметь: - Использовать основные положения и методы управления коммуникациями в проекте..
	Владеть: - Навыками презентации разработанных проектов и их презентаций..

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
06.033 «Специалист по защите информации в автоматизированных системах»	
ПК-843/B/01.6/1 способен осуществлять диагностику систем защиты информации автоматизированных систем	Трудовые действия: - Обнаружение инцидентов в процессе эксплуатации автоматизированной системы; - Идентификация инцидентов в процессе эксплуатации автоматизированной системы; - Оценка защищенности автоматизированных систем с помощью типовых программных средств; - Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы.
	Умения: - Определять источники и причины возникновения инцидентов; - Оценивать последствия выявленных инцидентов; - Обнаруживать нарушения правил разграничения доступа; - Устранять нарушения правил разграничения доступа; - Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах; - Использовать криптографические методы и средства защиты информации в автоматизированных системах.
	Знания: - Нормативные правовые акты в области защиты информации; - Национальные, межгосударственные и международные стандарты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - Организационные меры по защите информации; - Принципы построения средств защиты информации от "утечки" по техническим каналам; - Критерии оценки защищенности автоматизированной системы; - Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах.

ПК-843/В/03.6/1 способен осуществлять основные меры по защите информации в автоматизированных системах	Трудовые действия: - Анализ воздействия изменений конфигурации автоматизированной системы на ее защищенность; - Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе.
	Умения: - Оценивать информационные риски в автоматизированных системах; - Классифицировать и оценивать угрозы безопасности информации; - Определять подлежащие защите информационные ресурсы автоматизированных систем; - Применять нормативные документы по противодействию технической разведке; - Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; - Конфигурировать параметры системы защиты информации автоматизированных систем; - Применять технические средства контроля эффективности мер защиты информации.
	Знания: - Основные методы управления защитой информации; - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Методы защиты информации от "утечки" по техническим каналам; - Нормативные правовые акты в области защиты информации; - Национальные, межгосударственные и международные стандарты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

ПК-843/B/05.6/1 способен осуществлять мониторинг защищенности информации в автоматизированных системах	Трудовые действия: - Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы; - Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний; - Выявление угроз безопасности информации в автоматизированных системах; - Принятие мер защиты информации при выявлении новых угроз безопасности информации; - Анализ недостатков в функционировании системы защиты информации автоматизированной системы; - Устранение недостатков в функционировании системы защиты информации автоматизированной системы.
	Умения: - Классифицировать и оценивать угрозы информационной безопасности; - Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; - Применять нормативные документы по противодействию технической разведке; - Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем; - Контролировать события безопасности и действия пользователей автоматизированных систем; - Применять технические средства контроля эффективности мер защиты информации; - Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы.

	Знания: - Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; - Программно-аппаратные средства обеспечения защиты информации автоматизированных систем; - Методы защиты информации от "утечки" по техническим каналам; - Нормативные правовые акты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - Организационные меры по защите информации.
ПК-843/С/01.6/1 способен осуществлять установку и настройку средств защиты информации в автоматизированных системах	Трудовые действия: - Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы; - Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы; - Проведение приемочных испытаний системы защиты информации автоматизированной системыс.
	Умения: - Администрировать программные средства системы защиты информации автоматизированных систем; - Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации; - Применять нормативные документы по противодействию технической разведке; - Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; - Проводить анализ структурных и функциональных схем защищенной автоматизированной системы; - Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы.

	Знания: - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; - Основные меры по защите информации в автоматизированных системах; - Нормативные правовые акты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.
ПК-843/С/03.6/1 способен осуществлять анализ уязвимостей внедряемой системы защиты информации	Трудовые действия: - Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем; - Проведение анализа уязвимостей автоматизированных и информационных систем; - Уточнение модели угроз безопасности информации автоматизированной системы; - Проведение предварительных испытаний системы защиты информации автоматизированной системы; - Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы.
	Умения: - Классифицировать и оценивать угрозы безопасности информации автоматизированной системы; - Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы; - Проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств; - Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.

	Знания: - Основные методы и средства криптографической защиты информации; - Способы защиты информации от "утечки" по техническим каналам; - Способы контроля эффективности защиты информации от "утечки" по техническим каналам; - Нормативные правовые акты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - Организационные меры по защите информации; - Содержание эксплуатационной документации автоматизированной системы.
ПК-843/D/01.7/1 способен осуществлять тестирование систем защиты информации автоматизированных систем	Трудовые действия: - Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; - Выявление уязвимости информационно-технологических ресурсов автоматизированных систем; - Выявление основных угроз безопасности информации в автоматизированных системах; - Составление методик тестирования систем защиты информации автоматизированных систем; - Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем.
	Умения: - Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации; - Анализировать основные узлы и устройства современных автоматизированных систем; - Применять действующую нормативную базу в области обеспечения безопасности информации; - Контролировать безотказное функционирование технических средств защиты информации.

	Знания: - Принципы построения и функционирования систем и сетей передачи информации; - Эталонная модель взаимодействия открытых систем; - Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; - Основные меры по защите информации в автоматизированных системах; - Особенности защиты информации в автоматизированных системах управления технологическими процессами; - Принципы построения средств защиты информации от "утечки" по техническим каналам; - Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; - Технические каналы "утечки" информации; - Технические средства контроля эффективности мер защиты информации; - Организация защиты информации от "утечки" по техническим каналам на объектах информатизации; - Нормативные правовые акты в области защиты информации; - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

2.2. Характеристика нового вида профессиональной деятельности, новой квалификации

В результате освоения дополнительной образовательной программы *«Безопасность автоматизированных систем»* слушатель должен быть готов к области профессиональной деятельности, объектам и задачам.

Область/сферы профессиональной деятельности слушателя, прошедшего обучение по программе профессиональной переподготовки включает:

- Область профессиональной деятельности слушателя, прошедшего обучение по программе профессиональной переподготовки включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности и защиты информации..

- В результате освоения дополнительной образовательной программы профессиональной переподготовки «Безопасность автоматизированных систем» слушатель должен обладать способностями к выполнению нового вида деятельности в сфере «Информационная безопасность».

Объектами профессиональной деятельности являются:

- Фундаментальные и прикладные проблемы информационной безопасности; объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и

информационно-аналитические системы; средства и технологии обеспечения информационной безопасности и защиты информации; экспертиза, сертификация и контроль защищенности информации и объектов информатизации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации; организация и управление информационной безопасностью..

Выпускник программы должен уметь решать профессиональные ***задачи*** по видам профдеятельности:

организационно-управленческий:

- Профессиональные задачи в соответствии с организационно-управленческой профессиональной деятельностью.

проектный:

- Профессиональные задачи в соответствии с проектной профессиональной деятельностью.

В результате освоения дополнительной образовательной программы слушатель должен обладать способностями к выполнению **нового вида деятельности** соответствующего присваемой **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**:**

- 34,8 зачетных единиц;

1251 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	Защищенные информационные системы	139	76	74			2	63			Зачет с оценкой	
1.1.	Анализ угроз информационной безопасности	15	6	6				9				
1.2.	Политика безопасности	17	8	8				9				
1.3.	Стандарты информационной безопасности	19	10	10				9				
1.4.	Математические модели защищенных информационных систем	21	12	12				9		Расчетное задание		
1.5.	Архитектура защищенной информационной системы	29	20	20				9				
1.6.	Методы оценки рисков информационной безопасности	17	8	8				9				
1.7.	Тестирование защиты	21	12	10			2	9				
2	Управление проектами в сфере информационной безопасности	121	58	56			2	63			Экзамен	
2.1.	Обоснование проекта в сфере информационной безопасности	29	8	8				21				
2.2.	Планирование проекта в сфере информационной безопасности	55	34	34				21				
2.3.	Фазы исполнения и внедрения проекта сфере информационной безопасности	37	16	14			2	21				
3	Технологии обеспечения информационной безопасности	121	58	56			2	63			Экзамен	
3.1.	Общие проблемы информационной безопасности	24	8	8				16				
3.2.	Технологии защиты данных	28	12	12				16				
3.3.	Технологии защиты	4	24	24				16				

	межсетевого обмена данными	0										
3.4.	Технологии обнаружения вторжений	29	14	12			2	15				
4	Информационно-аналитические системы безопасности	121	58	56			2	63			Экзамен	
4.1.	Информационно-аналитическая деятельность в системе безопасности	39	18	18				21				
4.2.	Организация противодействия злоумышленной деятельности	41	20	20				21				
4.3.	Технологии информационно-аналитического обеспечения безопасности	41	20	18			2	21				
5	Современные технологии информационных сетей	139	76	74			2	63			Экзамен	
5.1.	Введение в современные технологии информационных сетей	20	8	8				12				
5.2.	Организация информационных сетей	47	34	34				13				
5.3.	Обеспечение защищенности информационных сетей	29	16	16				13				
5.4.	Вопросы обеспечения эффективности информационных сетей	27	14	14				13				
5.5.	Перспективные направления развития информационных сетей	16	4	2			2	12				
6	Технологии и методы защиты информации в сети Интернет	139	76	74			2	63			Зачет с оценкой	
6.1.	Основы безопасной работы в сети	45	24	24				21				

	Интернет											
6.2.	Средства защиты информации в компьютерных сетях	45	24	24				21				
6.3.	Обнаружение и предотвращение вторжений	49	28	26			2	21		Расчетное задание		
7	Информационная безопасность компьютерных сетей	139	76	74			2	63			Зачет с оценкой	
7.1.	Общие вопросы информационной безопасности компьютерных сетей	22	10	10				12				
7.2.	Информационная безопасность IP-сетей	31	18	18				13				
7.3.	Технологии виртуальных защищенных сетей	35	22	22				13				
7.4.	Информационная безопасность промышленных сетей	29	16	16				13				
7.5.	Защита беспроводных сетей передачи информации	22	10	8			2	12				
8	Криптографические методы и средства защиты автоматизированных систем	0	0								Защита курсовой работы	
9	Криптографические методы и средства защиты информации	163	76	74			2	87			Экзамен	
9.1.	Введение в криптографию	16	6	6				10				
9.2.	Математические основы криптографии	19	8	8				11				
9.3.	Симметричная криптография	27	16	16				11				
9.4.	Асимметричная криптография	19	8	8				11				
9.5.	Целостность и установление подлинности	23	12	12				11				
9.6.	Управление криптографическим	19	8	8				11				

	и ключами											
9.7.	Основы современной стеганографии	19	8	8				11				
9.8.	Основы криптоанализа	21	10	8			2	11				
10	Программно-аппаратные средства защиты информации	139	76	74			2	63			Экзамен	
10.1.	Общие вопросы обеспечения безопасности	18	8	8				10				
10.2.	Средства для контроля и управления доступом	35	18	18				17				
10.3.	Средства для предотвращения несанкционированного доступа к программам компьютера	42	24	24				18				
10.4.	Средства обнаружения и организация защиты от утечек информации	44	26	24			2	18				
11	Итоговая аттестация	30	6	2			4	24				Итоговый аттестационный экзамен
	ИТОГО:	**1251**	**636**	**614**	**0**	**0**	**22**	**615**	**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.	Защищенные информационные системы	
1.1.	Анализ угроз информационной безопасности	Проблемы безопасности информационных систем. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Проблемы безопасности IP-сетей. Способы обеспечения информационной безопасности. Пути решения проблемы защиты информации.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
1.2.	Политика безопасности	Основные понятия политики безопасности. Описание проблемы. Область применения. Позиция организации. Распределение ролей и обязанностей. Управленческие меры обеспечения информационной безопасностью. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности.
1.3.	Стандарты информационной безопасности	Роль стандартов информационной безопасности. Роль стандартов информационной безопасности (ИБ). Первое поколение стандартов информационной безопасности. Новое поколение стандартов информационной безопасности. Стандарты ISO/IEC 17799:2002. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Международный стандарт информационной безопасности ISO 15408. Международный стандарт информационной безопасности ISO 15408 «Общие критерии безопасности информационных технологий». Отечественные стандарты безопасности информационных технологий. Российский стандарт ГОСТ Р ИСО/МЭК 15408 «Методы и средства обеспечения безопасности». ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».
1.4.	Математические модели защищенных информационных систем	Основные понятия и определения, используемые при описании моделей безопасности информационных систем. Элементы теории защиты информации. Математические основы моделей безопасности. Классификация моделей безопасности информационных систем. Математические модели дискреционного и мандатного разграничения доступа. Модель Харрисона-Руззо-Ульмана. Модель распространения прав доступа Take-Grant. Модель Белла-ЛаПадула. Модель Биба. Модели ролевого разграничения доступа. Понятие ролевого разграничения доступа (РРД). Базовая модель РРД. Модель администрирования РРД. Модель мандатного РРД. Проблемы применения моделей безопасности при построении защищенных информационных систем. Проблема адекватности реализации модели безопасности в реальной информационной системе. Проблемы реализации политики безопасности. Политика безопасного администрирования.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
1.5.	Архитектура защищенной информационной системы	Концепция глобального управления безопасностью. Концепция GSM (Global Security Management). Основные свойства GSM. Глобальная и локальная политика безопасности. Функционирование системы управления средствами безопасности. Назначение основных средств безопасности. Защита ресурсов. Управление средствами защиты. Управление пользователями и правами доступа. Аудит и мониторинг безопасности информационных систем. Обеспечение безопасности облачных систем. Общие требования к безопасности облачных технологий. Безопасность сетевой части облака. Безопасность серверной части облака. Безопасность хранения данных и приложений. Средства защиты информационных систем. Организация защиты от вирусов. Межсетевые экраны. Средства обнаружения и предотвращения вторжений. Средства предотвращения утечек. Средства шифрования. Средства двухфакторной аутентификации. Однократная аутентификация. Ложные информационные системы.
1.6.	Методы оценки рисков информационной безопасности	Процесс оценки рисков и управления риском информационной безопасности. Процесс оценки рисков ИБ: идентификация рисков, анализ рисков, оценивание рисков, обработка рисков. Процесс управления риском ИБ. Программный инструментарий для управления рисками ИБ. Методика CRAMM. Методика ГРИФ. Методика RiskWatch. Методика CORAS. Методика MSAT.
1.7.	Тестирование защиты	Модель опасностей. Декомпозиция приложения. Ранжирование интерфейсов по степени уязвимости. Атаки по классификации STRIDE. Создание инструментов для поиска дефектов. Создание тест-планов на основании модели опасностей. Создание тест-плана. Определение «поверхности поражения». Определение основных векторов атаки. Тестирование с шаблонами безопасности. Сквозное тестирование.
2.	Управление проектами в сфере информационной безопасности	
2.1.	Обоснование проекта в сфере информационной безопасности	Основные определения в проектном управлении. Инициация проекта.
2.2.	Планирование проекта в сфере информационной безопасности	Разработка содержания проекта. Разработка расписания проекта. Планирование рисков проекта в сфере информационной безопасности. Планирование человеческих ресурсов проекта. Планирование

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		коммуникаций и управления конфигурацией в проекте.
2.3.	Фазы исполнения и внедрения проекта сфере информационной безопасности	Управление проектом на фазе проектирования. Управление проектом на фазе внедрения.
3.	Технологии обеспечения информационной безопасности	
3.1.	Общие проблемы информационной безопасности	Анализ угроз безопасности. Угрозы и уязвимости информационных систем. Способы обеспечения информационной безопасности. Политика безопасности. Стандарты информационной безопасности. Роль стандартов информационной безопасности (ИБ). Международные стандарты ИБ. Отечественные стандарты безопасности информационных технологий.
3.2.	Технологии защиты данных	Технологии обеспечения безопасности операционных систем (ОС). Проблемы обеспечения безопасности ОС. Угрозы безопасности ОС. Понятие защищенной ОС. Архитектура подсистемы защиты ОС. Аудит и мониторинг безопасности. Классификация методов аудита. Технологии аудита безопасности. Анализ системных журналов.
3.3.	Технологии защиты межсетевого обмена данными	Технологии межсетевых экранов. Функции межсетевых экранов (МЭ). Особенности функционирования МЭ на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ. Основы технологии виртуальных защищенных сетей. Концепция построения виртуальных защищенных сетей VPN. Классификация сетей VPN. VPN - решения для построения защищенных сетей. Технологии информационной безопасности на сетевом и транспортном уровнях семиуровневой модели OSI. Обеспечение ИБ на сетевом уровне с помощью протоколов IPSec (Протоколы безопасности AH и ESP, протокол управления ключами IKE). Обеспечение ИБ на транспортном уровне с помощью протоколов SSL/TLS и SOCKS. Защита беспроводных сетей. Технология трансляции сетевых адресов NAT. Инфраструктура защиты на прикладном уровне семиуровневой модели OSI. Протоколы PGP и S/MIME. Организация защищенного удаленного доступа. Протоколы аутентификации удаленных пользователей.
3.4.	Технологии обнаружения вторжений	Анализ защищенности и обнаружение атак. Концепция адаптивного управления безопасностью. Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		защищенности ОС. Технологии обнаружения атак. Классификация систем обнаружения атак.
4.	Информационно-аналитические системы безопасности	
4.1.	Информационно-аналитическая деятельность в системе безопасности	Аналитическая работа по исследованию информационной безопасности. Требования к информационно-аналитической системе обеспечения безопасности. Методические основы сбора и анализа информации в сфере безопасности.
4.2.	Организация противодействия злоумышленной деятельности	Конкурентная разведка. Противодействие промышленному шпионажу. Защита коммерческой тайны на предприятии.
4.3.	Технологии информационно-аналитического обеспечения безопасности	Статистический анализ данных. Инструменты интеллектуального анализа данных. Структура информационно-аналитической системы обеспечения безопасности.
5.	Современные технологии информационных сетей	
5.1.	Введение в современные технологии информационных сетей	Особенности организации информационных сетей. Современные технологии в организации информационных сетей.
5.2.	Организация информационных сетей	Архитектура, компоненты и функционирование информационной сети. Организация коммутации информации в сети. Сетевые коммутаторы. Маршрутизация информации. технические программно-аппаратные средства маршрутизации. Современные беспроводные каналы передачи информации. Средства хранения информации сверхбольшой емкости. Современные приборы и устройства прикладного предназначения, предназначенные для использования в информационных сетях. Информационная сеть системы "Умный дом". Облачные технологии хранения и доступа к информации. Глобальные информационные сети.
5.3.	Обеспечение защищенности информационных сетей	Использование общедоступных каналов передачи информации. Организация персональных и корпоративных сетей и подсетей. Защита информации в каналах общего использования.
5.4.	Вопросы обеспечения эффективности информационных сетей	Администрирование информационных сетей. Системы и средства наблюдения и контроля информационного обмена и содержимого информации. Технологии обеспечивающие эффективное функционирование информационных сетей.
5.5.	Перспективные	Тенденции развития информационных сетей,

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
	направления развития информационных сетей	перспективные сетевые технологии.
6.	Технологии и методы защиты информации в сети Интернет	
6.1.	Основы безопасной работы в сети Интернет	Угрозы информационной безопасности в сети Интернет. Принципы безопасного использования Интернет-ресурсов. Технологии безопасной передачи информации в сети Интернет.
6.2.	Средства защиты информации в компьютерных сетях	Защита от вредоносного программ и спама. Межсетевое экранирование. Организация виртуальных защищенных VPN-сетей.
6.3.	Обнаружение и предотвращение вторжений	Понятие и классификация атак на компьютерные сети. Методы обнаружения атак. Системы обнаружения вторжений.
7.	Информационная безопасность компьютерных сетей	
7.1.	Общие вопросы информационной безопасности компьютерных сетей	Введение в дисциплину. Основные понятия и определения. Проблемы и угрозы информационной безопасности сетей. Отечественные и зарубежные стандарты информационной безопасности компьютерных сетей.
7.2.	Информационная безопасность IP-сетей	Введение в сетевой информационный обмен. Межсетевые экраны (МЭ). Схемы сетевой защиты на базе МЭ. Категории сетевых атак. Технологии обнаружения сетевых вторжений.
7.3.	Технологии виртуальных защищенных сетей	Виртуальные локальные сети. Конфигурирование виртуальных локальных сетей. Виртуальные защищенные сети VPN. Технологии и протоколы VPN. Построение VPN на основе маршрутизаторов.
7.4.	Информационная безопасность промышленных сетей	Понятие и разновидности промышленных информационных сетей. Промышленный Ethernet. Интегрированные системы промышленной автоматизации. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры.
7.5.	Защита беспроводных сетей передачи информации	Защищенные системы беспроводной связи. Беспроводные виртуальные сети.
8.	Криптографические методы и средства защиты информации	
8.1.	Введение в криптографию	Введение в криптографию. Основные определения. История криптографии. Классификация криптоалгоритмов.
8.2.	Математические основы криптографии	Модульная арифметика и алгебраические структуры. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		структуры. Поля Галуа. Генерация и тестирование псевдослучайных последовательностей. Структура генератора псевдослучайных последовательностей (ГПСП). Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП. Тестирование ГПСП.
8.3.	Симметричная криптография	Современные блочные шифры. Стандарт шифрования DES. Режимы работы алгоритма DES. Стандарт шифрования AES. Российский стандарт шифрования. Стандарт шифрования ГОСТ Р 34. 12-2015 (Магма и Кузнечик). Современные шифры потока. Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании. Шифр RC4. Шифрование, использующее современные шифры с симметричным ключом. Применение современных блочных шифров. Использование шифров потока. Методы повышения криптостойкости симметричных криптосистем.
8.4.	Асимметричная криптография	Криптосистема RSA. Принцип работы современных асимметричных криптосистем. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина. Криптосистемы на основе метода эллиптических кривых. Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая криптосистему Эль-Гамаля.
8.5.	Целостность и установление подлинности	Обеспечение целостности передаваемых данных. Целостность сообщения. Случайная модель Oracle. Установление подлинности сообщения. Криптографические хеш-функции. Итеративные хеш-функции. Схема Меркеля-Дамгарда. Хеш- функции, основанные на блочных шифрах. Схема Рабина. Алгоритм безопасного хеширования SHA. Шифр Whirlpool. Российский стандарт хеширования ГОСТ Р 34.11-2012. Электронная цифровая подпись. Алгоритм формирования электронной цифровой подписи (ЭЦП). Схема ЭЦП RSA. ЭЦП Эль-Гамаля. ЭЦП Шнорра. Стандарт цифровой подписи DSS. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10- 2012. Установление подлинности объекта. Аутентификация на основе пароля. Одноразовый пароль. Система установления подлинности «запрос-ответ». Подтверждение с нулевым разглашением. Протокол Фиата-Шамира. Биометрия. Физиологические и

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		поведенческие методы биометрии.
8.6.	Управление криптографическими ключами	Генерация и хранение криптографических ключей. Стандарт ANSI. X9.17. Методы хранения ключевой информации. Алгоритмы безопасного распределения ключей. Прямой обмен ключами между пользователями. Система «запрос-ответ». Алгоритм Ниидома-Шредера. Алгоритм Диффи-Хеллмана. Использование Центра распределения ключей. Инфраструктура PKI. Стандарт X.509. Система Kerberos.
8.7.	Основы современной стеганографии	Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.
8.8.	Основы криптоанализа	Обзор методов криптоанализа. Методы криптоанализа. Криптоанализ блочных шифров. Частотный криптоанализ. Современные методы криптоанализа. Дифференциальный криптоанализ. Линейный криптоанализ. Интерполяционный криптоанализ. Методы криптоанализа, основанные на слабости ключевых разверток.
9.	Программно-аппаратные средства защиты информации	
9.1.	Общие вопросы обеспечения безопасности	Основные сведения об источниках и носителях защищаемой информации. Принципы организации и комплексный подход к средствам защиты. Основные меры противодействия несанкционированному доступу.
9.2.	Средства для контроля и управления доступом	Методы обеспечения идентификации и аутентификации пользователей. Технологии идентификации человека. Носители идентификационных признаков. Биометрические методы идентификации. Принципы построения и функционирования электронных замков. Кодовый замок с таблеткой. Кодовый замок с бесконтактной картой. Регистрация событий.
9.3.	Средства для предотвращения несанкционированного доступа к программам компьютера	Ограничение доступа к компонентам вычислительных систем. Основные принципы и способы защиты программ. Привязка программ к аппаратуре. Методы парольной защиты и PIN-коды. Разделение уровней привилегий. Защита программ привязкой к носителю информации. Защита с помощью электронных ключей. Универсальная электронная карта. Способы определения факта незаконного использования программ. Способы защиты программ от незаконного использования.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		Гарантированное удаление данных.
9.4.	Средства обнаружения и организация защиты от утечек информации	Классификация и структура технических каналов утечки информации. Виды и физическая природа каналов утечки информации при эксплуатации ЭВМ. Особенности утечки информации по техническим каналам. Характеристики технических каналов утечки информации. Оптические каналы утечки информации. Радиоканалы утечки информации. Акустические каналы утечки информации. Вещественные каналы утечки информации. Поиск незаконных устройств утечек информации.
10.	Криптографические методы и средства защиты автоматизированных систем	

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 *итогового аттестационного экзамена*. 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. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / Томский Государственный университет систем управления и радиоэлектроники (ТУСУР) . – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015 . – 284 с. : схем., табл., ил. – Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация . - Библиогр. в кн .;

2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие для вузов по специальностям 090300 "Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем" и направлению 090900 "Информационная безопасность" / П. Н. Девянин . – М. : Горячая Линия-Телеком, 2011 . – 320 с. - ISBN 978-5-9912-0147-6 .;

3. Куроуз, Д. Компьютерные сети. Многоуровневая архитектура Интернета : пер. с англ. / Д. Куроуз, К. Росс . – 2-е изд . – СПб. : Питер, 2004 . – 765 с. - ISBN 5-8046-0093-1 .;

4. Рыбалова, Е. А. Управление проектами : учебно-методическое пособие / Томский Государственный университет систем управления и радиоэлектроники (ТУСУР) ; Кафедра автоматизации обработки информации . – Томск : Факультет дистанционного обучения ТУСУРа, 2015 . – 149 с. : схем., табл., ил. – Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация . - Библиогр. в кн ..

б) литература ЭБС и БД:

Не предусмотрено

в) используемые ЭБС:

1. Научная электронная библиотека https://elibrary.ru/;

2. ЭБС Лань

https://e.lanbook.com/;

3. ЭБС "Университетская библиотека онлайн" http://biblioclub.ru/index.php?page=main_ub_red.

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 актуализирована и утверждена	30.01.2023

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Максимкин В.Л. Идентификатор: R9e14050c-MaximkinVL-G14050C2	В.Л. Максимкин
(должность)	(подпись)	(расшифровка подписи)