



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. начальника  
ОДПО

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Селиверстов Н.Д.
Идентификатор	Rf19596d9-SeliverstovND-39ee0b7

Н.Д.  
Селиверстов

Начальник ОДПО

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Селиверстов Н.Д.
Идентификатор	Rf19596d9-SeliverstovND-39ee0b7

Н.Д.  
Селиверстов

Начальник ФДО

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Малич Н.В.
Идентификатор	R13696f6e-MalichNV-45fe3095

Н.В. Малич

Руководитель Филиал  
МЭИ в г. Смоленск,  
ЦПП "Энергетик"

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Максимкин В.Л.
Идентификатор	R9e14050c-MaximkinVL-G14050C2

В.Л.  
Максимкин

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

Москва



## **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. № 1455, зарегистрированным в Министерстве России 18.02.2021 г. № 62549.

- с Профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах», утвержденным приказом Минтруда 14.09.2022 г. № 525н, зарегистрированным в Министерстве России 14.10.2022 г. № 70543, уровень квалификации 7.

**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	<p>Знать:</p> <ul style="list-style-type: none"><li>- Современную классификацию средств защиты информации в информационных системах..</li></ul> <p>Уметь:</p> <ul style="list-style-type: none"><li>- Применять современные программные и аппаратные средства защиты информации..</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>- Способностью осваивать новые методы обеспечения информационной безопасности..</li></ul>
ОПК-2: Способен разрабатывать технический проект системы (подсистемы, компонента системы) обеспечения информационной безопасности	<p>Знать:</p> <ul style="list-style-type: none"><li>- Структуры современных информационных сетей;</li><li>- Оборудование информационных сетей современного уровня;</li><li>- Используемые технологии обеспечения безопасности информационных сетей.</li></ul> <p>Уметь:</p> <ul style="list-style-type: none"><li>- Разрабатывать информационные сети заданной структуры или заданного предназначения;</li><li>- Настраивать компоненты информационных сетей;</li><li>- Организовывать эксплуатацию информационных сетей.</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>- Навыками комплексного подхода к разработке информационной системы, как защищенной сетевой структуры.</li></ul>
ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	<p>Знать:</p> <ul style="list-style-type: none"><li>- Основные положения и методы управления коммуникациями в проекте..</li></ul> <p>Уметь:</p> <ul style="list-style-type: none"><li>- Использовать основные положения и методы управления коммуникациями в проекте..</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>- Навыками презентации разработанных проектов и их презентаций..</li></ul>

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/В/01.6/1 Способен осуществлять диагностику систем защиты информации автоматизированных систем	<p><b>Трудовые действия:</b></p> <ul style="list-style-type: none"> <li>- Обнаружение инцидентов в процессе эксплуатации автоматизированной системы;</li> <li>- Идентификация инцидентов в процессе эксплуатации автоматизированной системы;</li> <li>- Оценка защищенности автоматизированных систем с помощью типовых программных средств;</li> <li>- Устранение последствий инцидентов, возникших в процессе эксплуатации автоматизированной системы.</li> </ul> <p><b>Умения:</b></p> <ul style="list-style-type: none"> <li>- Определять источники и причины возникновения инцидентов;</li> <li>- Оценивать последствия выявленных инцидентов;</li> <li>- Обнаруживать нарушения правил разграничения доступа;</li> <li>- Устранять нарушения правил разграничения доступа;</li> <li>- Определять источники и причины возникновения инцидентов;</li> <li>- Использовать криптографические методы и средства защиты информации в автоматизированных системах.</li> </ul> <p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Национальные, межгосударственные и международные стандарты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;</li> <li>- Организационные меры по защите информации;</li> <li>- Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам;</li> <li>- Критерии оценки защищенности автоматизированной системы;</li> <li>- Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах.</li> </ul>

<p>ПК-843/В/03.6/1</p> <p>Способен осуществлять управление защитой информации в автоматизированных системах</p>	<p>Трудовые действия:</p> <ul style="list-style-type: none"> <li>- Анализ изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации;</li> <li>- Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе.</li> </ul>
	<p>Умения:</p> <ul style="list-style-type: none"> <li>- Оценивать информационные риски в автоматизированных системах;</li> <li>- Классифицировать и оценивать угрозы безопасности информации;</li> <li>- Определять подлежащие защите информационные ресурсы автоматизированных систем;</li> <li>- Применять нормативные документы по защите от несанкционированного доступа к информации и противодействию технической разведке;</li> <li>- Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем;</li> <li>- Конфигурировать параметры системы защиты информации автоматизированных систем;</li> <li>- Применять технические средства контроля эффективности мер защиты информации.</li> </ul>
	<p>Знания:</p> <ul style="list-style-type: none"> <li>- Основные методы управления защитой информации;</li> <li>- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</li> <li>- Методы защиты информации от несанкционированного доступа и утечки по техническим каналам;</li> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Национальные, межгосударственные и международные стандарты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</li> </ul>

<p>ПК-843/В/05.6/1</p> <p>Способен осуществлять мониторинг защищенности информации в автоматизированных системах</p>	<p>Трудовые действия:</p> <ul style="list-style-type: none"> <li>- Устранение недостатков в функционировании системы защиты информации автоматизированной системы;</li> <li>- Анализ недостатков в функционировании системы защиты информации автоматизированной системы;</li> <li>- Принятие мер защиты информации при выявлении новых угроз безопасности информации;</li> <li>- Выработка рекомендаций для принятия решения о повторной аттестации автоматизированной системы или о проведении дополнительных аттестационных испытаний;</li> <li>- Выявление угроз безопасности информации в автоматизированных системах;</li> <li>- Выработка рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы.</li> </ul>
	<p>Умения:</p> <ul style="list-style-type: none"> <li>- Классифицировать и оценивать угрозы информационной безопасности;</li> <li>- Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах;</li> <li>- Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке;</li> <li>- Контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем;</li> <li>- Контролировать события безопасности и действия пользователей автоматизированных систем;</li> <li>- Применять технические средства контроля эффективности мер защиты информации;</li> <li>- Документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы.</li> </ul>

	<p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>- Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;</li> <li>- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</li> <li>- Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;</li> <li>- Программно-аппаратные средства обеспечения защиты информации автоматизированных систем;</li> <li>- Методы защиты информации от утечки по техническим каналам;</li> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;</li> <li>- Организационные меры по защите информации.</li> </ul>
<p>ПК-843/В/07.6/1</p> <p>Способен осуществлять установку и настройку средств защиты информации в автоматизированных системах</p>	<p><b>Трудовые действия:</b></p> <ul style="list-style-type: none"> <li>- Проведение приемочных испытаний системы защиты информации автоматизированной системы;</li> <li>- Входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы;</li> <li>- Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы.</li> </ul>
	<p><b>Умения:</b></p> <ul style="list-style-type: none"> <li>- Администрировать программные средства системы защиты информации автоматизированных систем;</li> <li>- Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации;</li> <li>- Применять нормативные документы по защите информации от несанкционированного доступа и противодействию технической разведке;</li> <li>- Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации;</li> <li>- Проводить анализ структурных и функциональных схем защищенной автоматизированной системы;</li> <li>- Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы.</li> </ul>

	<p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</li> <li>- Типовые средства, методы и протоколы идентификации, аутентификации и авторизации;</li> <li>- Основные меры по защите информации в автоматизированных системах;</li> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.</li> </ul>
<p>ПК-843/В/09.6/1</p> <p>Способен осуществлять анализ уязвимостей внедряемой системы защиты информации</p>	<p><b>Трудовые действия:</b></p> <ul style="list-style-type: none"> <li>- Выбор и обоснование критериев эффективности функционирования защищенных автоматизированных систем;</li> <li>- Проведение анализа уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы;</li> <li>- Уточнение модели угроз безопасности информации автоматизированной системы;</li> <li>- Проведение предварительных испытаний системы защиты информации автоматизированной системы;</li> <li>- Проведение анализа уязвимостей автоматизированных и информационных систем.</li> </ul>
	<p><b>Умения:</b></p> <ul style="list-style-type: none"> <li>- Классифицировать и оценивать угрозы безопасности информации автоматизированной системы;</li> <li>- Разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы;</li> <li>- Проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств;</li> <li>- Устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации.</li> </ul>

	<p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>- Основные методы и средства криптографической защиты информации;</li> <li>- Способы защиты информации от несанкционированного доступа и утечки по техническим каналам;</li> <li>- Способы контроля эффективности защиты информации от несанкционированного доступа и утечки по техническим каналам;</li> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;</li> <li>- Организационные меры по защите информации;</li> <li>- Содержание эксплуатационной документации автоматизированной системы.</li> </ul>
<p>ПК-843/С/01.7/1</p> <p>Способен осуществлять тестирование систем защиты информации автоматизированных систем</p>	<p><b>Трудовые действия:</b></p> <ul style="list-style-type: none"> <li>- Выявление основных угроз безопасности информации в автоматизированных системах;</li> <li>- Выявление уязвимости информационно-технологических ресурсов автоматизированных систем;</li> <li>- Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;</li> <li>- Составление методик тестирования систем защиты информации автоматизированных систем;</li> <li>- Подбор инструментальных средств тестирования систем защиты информации автоматизированных систем.</li> </ul>
	<p><b>Умения:</b></p> <ul style="list-style-type: none"> <li>- Анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации;</li> <li>- Анализировать основные узлы и устройства современных автоматизированных систем;</li> <li>- Применять действующую нормативную базу в области обеспечения безопасности информации;</li> <li>- Контролировать функционирование технических средств защиты информации.</li> </ul>

	<p><b>Знания:</b></p> <ul style="list-style-type: none"> <li>- Принципы построения и функционирования систем и сетей передачи информации;</li> <li>- Эталонная модель взаимодействия открытых систем;</li> <li>- Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</li> <li>- Основные меры по защите информации в автоматизированных системах;</li> <li>- Особенности защиты информации в автоматизированных системах управления технологическими процессами;</li> <li>- Принципы построения средств защиты информации от несанкционированного доступа и утечки по техническим каналам;</li> <li>- Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;</li> <li>- Технические каналы утечки информации;</li> <li>- Технические средства контроля эффективности мер защиты информации;</li> <li>- Организационные основы защиты информации от несанкционированного доступа и утечки по техническим каналам на объектах информатизации;</li> <li>- Нормативные правовые акты в области защиты информации;</li> <li>- Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;</li> <li>- Организационные меры по защите информации.</li> </ul>
--	--

## **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/сфера** профессиональной деятельности слушателя, прошедшего обучение по программе профессиональной переподготовки включает:

- Область профессиональной деятельности слушателя, прошедшего обучение по программе профессиональной переподготовки включает: связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности)..

- 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 присваиваемой **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	✉	Контактная работа, ак. ч	○	○	Форма аттестации
---	--------------	---	--------------------------	---	---	------------------

дисциплин (модулей)		Состав и структура программы											
1	2	3	4	5	6	7	8	9	11	12	13	14	
1	Защищенные информационные системы	1 4 0. 0	74 3	74			0.3	65. 7			Зачет с оценкой		
1.1.	Анализ угроз информационной безопасности	1 1	6	6				5					
1.2.	Политика безопасности	1 3	8	8				5					
1.3.	Стандарты информационной безопасности	1 5	10	10				5					
1.4.	Математические модели защищенных информационных систем	2 2	12	12				10		Расчетное задание			
1.5.	Архитектура защищенной информационной системы	4 5	20	20				25					
1.6.	Методы оценки рисков информационной безопасности	2 0	10	10				10					
1.7.	Тестирование защиты	1 2	8	8				4					
1.8.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7					
2	Управление проектами в сфере информационной безопасности	1 1 9. 0	56 3	56			0.3	62. 7			Экзамен		
2.1.	Обоснование проекта в сфере информационной безопасности	2 1	8	8				13		Лабораторная работа			
2.2.	Планирование проекта в сфере информационной	6 4	34	34				30					

	безопасности											
2.3.	Фазы исполнения и внедрения проекта сфере информационной безопасности	3 2	14	14				18				
2.4.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
3	Технологии обеспечения информационной безопасности	1 1 9. 0	56 .3	56			0.3	62. 7			Экзамен	
3.1.	Общие проблемы информационной безопасности	2 0	8	8				12		Лабораторн ая работ а		
3.2.	Технологии защиты данных	3 0	12	12				18				
3.3.	Технологии защиты межсетевого обмена данными	4 2	24	24				18				
3.4.	Технологии обнаружения вторжений	2 5	12	12				13				
3.5.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
4	Информационно-аналитические системы безопасности	1 1 9. 0	56 .3	56			0.3	62. 7			Экзамен	
4.1.	Информационно-аналитическая деятельность в системе безопасности	3 8	18	18				20		Лабораторн ая работ а		
4.2.	Организация противодействия злоумышленной деятельности	3 8	18	18				20				
4.3.	Технологии информационно-аналитического обеспечения безопасности	4 1	20	20				21				
4.4.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
5	Современные технологии информационных сетей	1 3 9. 0	74 .3	74			0.3	64. 7			Экзамен	
5.1.	Введение в современные технологии	1 3	8	8				5		Лабораторн ая		

	информационных сетей									работа		
5.2.	Организация информационных сетей	60	34	34				26				
5.3.	Обеспечение защищенности информационных сетей	28	14	14				14				
5.4.	Вопросы обеспечения эффективности информационных сетей	28	14	14				14				
5.5.	Перспективные направления развития информационных сетей	8	4	4				4				
5.6.	Промежуточная аттестация	20	0.3				0.3	1.7				
6	Технологии и методы защиты информации в сети Интернет	140.0	74.3	74			0.3	65.7			Зачет с оценкой	
6.1.	Основы безопасной работы в сети Интернет	42	22	22				20		Расчетное задание		
6.2.	Средства защиты информации в компьютерных сетях	48	26	26				22				
6.3.	Обнаружение и предотвращение вторжений	48	26	26				22				
6.4.	Промежуточная аттестация	20	0.3				0.3	1.7				
7	Информационная безопасность компьютерных сетей	139.0	74.3	74			0.3	64.7			Зачет с оценкой	
7.1.	Общие вопросы информационной безопасности компьютерных сетей	20	10	10				10		Лабораторная работа		
7.2.	Информационная безопасность IP-сетей	32	18	18				14				
7.3.	Технологии виртуальных защищенных сетей	37	22	22				15				
7.4.	Информационная	2	14	14				12				

	безопасность промышленных сетей	6										
7.5.	Защита беспроводных сетей передачи информации	2 2	10	10				12				
7.6.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
8	Криптографические методы и средства защиты информации	1 6 1. 0	74 3	74			0.3	86. 7		Экзамен		
8.1.	Введение в криптографию	1 7	8	8				9		Лабораторная работа		
8.2.	Математические основы криптографии	1 8	8	8				10				
8.3.	Симметричная криптография	3 2	16	16				16				
8.4.	Асимметричная криптография	1 8	8	8				10				
8.5.	Целостность и установление подлинности	2 2	12	12				10				
8.6.	Управление криптографическим и ключами	1 8	8	8				10				
8.7.	Основы современной стеганографии	1 6	6	6				10				
8.8.	Основы криptoанализа	1 8	8	8				10				
8.9.	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
9	Криптографические методы и средства защиты автоматизированных систем	0	0							Защита курсово й работы		
9.1.	Криптографические методы и средства защиты автоматизированных систем	0	0							Решен ие задач		
9.2.	Промежуточная аттестация	0	0									
10	Программно-аппаратные средства защиты информации	1 3 9. 0	74 .3	74			0.3	64. 7		Экзамен		

10.1	Общие вопросы обеспечения безопасности	1 2	8	8				4		Лабораторная работа		
10.2	Средства для контроля и управления доступом	3 3	18	18				15				
10.3	Средства для предотвращения несанкционированного доступа к программам компьютера	4 6	24	24				22				
10.4	Средства обнаружения и организация защиты от утечек информации	4 6	24	24				22				
10.5	Промежуточная аттестация	2. 0	0. 3				0.3	1.7				
11	Итоговая аттестация	3. 6. 0	2. 5	2			0.5	33. 5				Итоговый аттестационный экзамен
	<b>ИТОГО:</b>	<b>1 2 5 1. 0</b>	<b>61 7. 2</b>	<b>61 4</b>	<b>0</b>	<b>0</b>	<b>32</b>	<b>63 38</b>	<b>0</b>			

### 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.
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

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		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.
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

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		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.
1.8.	Промежуточная аттестация	Зачет
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 коммуникаций и управления конфигурацией в проекте.
2.3.	Фазы исполнения и внедрения проекта сфере	Управление проектом на фазе проектирования. Управление проектом на фазе внедрения.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
	информационной безопасности	
2.4.	Промежуточная аттестация	Экзамен
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 защищенности ОС. Технологии обнаружения атак.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		Классификация систем обнаружения атак.
3.5.	Промежуточная аттестация	Экзамен
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.
4.4.	Промежуточная аттестация	Экзамен
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

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		обеспечивающие эффективное функционирование информационных сетей.
5.5.	Перспективные направления развития информационных сетей	Тенденции развития информационных сетей, перспективные сетевые технологии.
5.6.	Промежуточная аттестация	Экзамен
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.
6.4.	Промежуточная аттестация	Зачет
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.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
7.6.	Промежуточная аттестация	Зачет
8.	Криптографические методы и средства защиты информации	
8.1.	Введение в криптографию	Введение в криптографию. Основные определения. История криптографии. Классификация криptoалгоритмов.
8.2.	Математические основы криптографии	Модульная арифметика и алгебраические структуры. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические 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 Кузнецик). 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 крипtosистем.
8.4.	Асимметричная криптография	Крипtosистема RSA. Принцип работы современных асимметричных крипtosистем. Крипtosистема RSA. Крипtosистема Эль-Гамаля. Крипtosистема Рабина. Крипtosистемы на основе метода эллиптических кривых. Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая крипtosистему 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

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		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 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 РКИ. 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 криptoанализа	Обзор методов криptoанализа. Методы криptoанализа. Криptoанализ блочных шифров. Частотный криptoанализ. Современные методы криptoанализа. Дифференциальный криptoанализ. Линейный криptoанализ. Интерполяционный криptoанализ. Методы криptoанализа, основанные на слабости ключевых разверток.
8.9.	Промежуточная аттестация	Экзамен
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.

№	Наименование дисциплин (модулей)	Содержание дисциплин (модулей)
		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. 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.
9.5.	Промежуточная аттестация	Экзамен
10.	Криптографические методы и средства защиты автоматизированных систем	
10. 1.	Криптографические методы и средства защиты автоматизированных систем	Проектирование программного обеспечения в соответствии с вариантом задания и подходом к проектированию
10. 2.	Промежуточная аттестация	Защита курсовой работы

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
Решение задач	Решение задач по теме дисциплины
Лабораторная работа	Выполнение лабораторной работы по теме дисциплины
Расчетное задание	Выполнение расчетного задания по теме дисциплины

## 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. Девягин, 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. Девягин. – М. : Горячая Линия-Телеком, 2011. – 320 с. – ISBN 978-5-9912-0147-6.;

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапонина. – 2-е изд., испр. – М. : Интернет-Ун-т информ. технологий : БИНОМ. Лаборатория знаний, 2009. – 531 с. – (Основы информационных технологий). – ISBN 978-5-9556-0102-1.;

3. Новиков, В. К. Средства, технологии, системы и технические каналы утечки информации для осуществления киберслежки за человеком и его деятельностью : [монография] / В. К. Новиков, М. Г. Краснов, И. С. Рекунов. – Москва : Горячая Линия-Телеком, 2021. – 160 с. – ISBN 978-5-9912-0928-1.;

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. ;

5. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В. А. Сердюк, Гос. ун-т - Высшая школа экономики. – М. : Высшая школа экономики, 2011. – 572 с. – ISBN 978-5-7598-0698-1.;

6. Технические системы защиты информации : учебник для образовательных организаций, реализующих программы высшего образования по направлению "Информационная безопасность" / В. И. Аверченков, М. Ю. Рытов, М. Л. Гулак, [и др.]. – Старый Оскол : ТНТ, 2021. – 264 с. – Авторы указаны на обороте тит. л. – ISBN 978-5-94178-708-1..

б) литература ЭБС и БД:

1. А. В. Артемов- "Информационная безопасность: курс лекций", Издательство: "Межрегиональная академия безопасности и выживания", Орел, 2014 - (257 с.)  
<https://biblioclub.ru/index.php?page=book&id=428605>;

2. А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов, М. О. Таныгин, Е. А. Кулешова- "Технологии обеспечения безопасности информационных систем", Издательство: "Директ-Медиа", Москва, Берлин, 2021 - (210 с.)  
<https://biblioclub.ru/index.php?page=book&id=598988>;

3. А. М. Голиков- "Защита информации от утечки по техническим каналам", Издательство: "Томский государственный университет систем управления и радиоэлектроники", Томск, 2015 - (256 с.)  
<https://biblioclub.ru/index.php?page=book&id=480636>;

4. А. П. Кирпичников, З. М. Хайбуллина- "Криптографические методы защиты компьютерной информации", Издательство: "Казанский научно-исследовательский технологический университет (КНИТУ)", Казань, 2016 - (100 с.)  
<https://biblioclub.ru/index.php?page=book&id=560536>;

5. В. В. Креопалов- "Технические средства и методы защиты информации: учебно-практическое пособие", Издательство: "Евразийский открытый институт", Москва, 2011 - (278 с.)

<https://biblioclub.ru/index.php?page=book&id=90753>;

6. В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев- "Основы информационной безопасности", Издательство: "Юнити-Дана|Закон и право", Москва, 2018 - (287 с.)

<https://biblioclub.ru/index.php?page=book&id=562348>;

7. Голиков А. М.- "Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика", Издательство: "Лань", Санкт-Петербург, 2018 - (452 с.)

<https://e.lanbook.com/book/101847>;

8. Ю. В. Косолапов- "Криптографические протоколы на основе линейных кодов", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2020 - (100 с.)

<https://biblioclub.ru/index.php?page=book&id=598671>;

9. Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков- "Программно-аппаратные средства защиты информационных систем", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов, 2017 - (194 с.)

<https://biblioclub.ru/index.php?page=book&id=499013>;

10. Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако, О. Г. Иванова, В. Г. Однолько- "Организация безопасной работы информационных систем", Издательство: "Тамбовский государственный технический университет (ТГТУ)", Тамбов, 2014 - (132 с.)

<https://biblioclub.ru/index.php?page=book&id=277794>.

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](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 3.

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