



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



**АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН (МОДУЛЕЙ)
ДОПОЛНИТЕЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

повышения квалификации

«Организация и технологии защиты информации: новое в отрасли»,

Раздел(предмет) *Актуальное правовое и нормативное регулирование
информационной безопасности*

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Актуальное правовое и нормативное регулирование информационной безопасности</i>	Тема № 1. Правовое обеспечение ИБ Основы правового обеспечения ИБ в РФ. Система правового регулирования отношений в информационной области. Правовое регулирование отношений в области: - служебной и профессиональной тайн; - персональных данных; - информационной безопасности объектов критической информационной инфраструктуры энергетики; - интеллектуальной собственности; - технического регулирования; - массовой информации, телекоммуникаций и связи. Тема № 2. Организационное обеспечение ИБ Основы организационного обеспечения ИБ предприятия. Конфиденциальная	<i>Нет</i>	<i>3</i>

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	информация (КИ). Допуск персонала к КИ и работа с этим персоналом. Пропускной и внутренний режим предприятия. Охрана и физическая защита предприятия. Защита информации при: - проведении совещаний; - в рекламной и публикационной деятельности. Контроль защиты КИ на предприятии. Организация и проведение служебных расследований по фактам разглашения КИ и утраты носителей КИ.		

Раздел(предмет) *Управление информационной безопасностью*

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Управление информационной безопасностью</i>	Тема № 1. Национальные стандарты в области ИБ. Управление ИБ предприятия на основе стандартов ГОСТ Р ИСО/МЭК 27000 в области менеджмента ИБ Требования национальных стандартов по управлению ИБ: комплекс стандартов СТО БР ИББС-1.0-2014; ГОСТ Р ИСО/МЭК 27001:2006; ГОСТ Р ИСО/МЭК 27002:2021; ГОСТ Р ИСО/МЭК 27005:2010. Тема № 2. Управление физической защитой информационных активов предприятия и контроль доступа к ним Реализация политик «чистого стола» и «чистого экрана». Хранение носителей информации.	<i>Нет</i>	<i>6</i>

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	<p>Обеспечение сохранности компьютерной и оргтехники. Прием и отправка корреспонденции. Доступ к копирующим устройствам. Тема № 3. Управление программно-аппаратной защитой активов предприятия</p> <p>Защита программного обеспечения и массивов информации от внедрения вредоносного кода. Реализация политик резервного копирования, журнальной регистрации событий информационной системы и ошибочных действий пользователей.</p> <p>Защита от неавторизованного доступа. Обеспечение безопасности информационных активов при использовании облачных сервисов.</p> <p>Безопасность сменных носителей. Утилизация носителей информации. Тема №4. Управление безопасностью процедур обработки и обмена информацией между организациями</p> <p>Организация процедур обработки и хранения информации. Обеспечение безопасного обмена информацией, программным обеспечением и носителями информации между организациями.</p> <p>Безопасность электронной почты. Тема № 5. Разработка, внедрение и совершенствование системы менеджмента ИБ на предприятии</p> <p>Определение</p>		

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	<p>области действия СМИБ на предприятии и разработка политики СМИБ: концепция, предъявляемые к СМИБ требования, управление рисками и критерии их оценки. Организация мониторинга и анализа СМИБ. Совершенствование СМИБ на основе полученных результатов. Тема №6. Оценка эффективности СМИБ предприятия с помощью программных средств Связь СМИБ с жизненным циклом информационных технологий предприятия. Общая характеристика программного комплекса.</p>		

Раздел(предмет) *Менеджмент рисков информационной безопасности*

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Менеджмент рисков информационной безопасности</i>	<p>Тема № 1. Термины и определения. Моделирование угроз информационной безопасности Термины и определения: угроза, риск, моделирование угроз, оценка, оценивание и анализ рисков. Цели и задачи моделирования угроз информационной безопасности. Базовая модель угроз. Тема № 2. Управление рисками в концепциях отечественных и зарубежных стандартов Управление рисками в концепции ГОСТ ИСО/МЭК 27005: Управление рисками</p>	<i>Нет</i>	<i>6</i>

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	в концепции стандарта США NIST 800-30, COBIT 5,0.		

Раздел(предмет) **Компьютерная безопасность**

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Компьютерная безопасность</i>	Тема № 1. Классификация угроз безопасности информации при обработке и хранении на ПК Виды и источники угроз ИБ. Виды сетевых атак. Снижение вероятности угрозы sniffing пакетов. Меры по ликвидации угрозы IP-spoofing. Тема № 2. Технические аспекты безопасности компьютерных данных Борьба с атаками на уровне приложений. Безопасность локальных вычислительных сетей. Распределенное хранение файлов. УровниЗИ. Аутентификация пользователя. Тема № 3. Атаки снаружи и изнутри Что включает ЗИ от НСД. Атаки снаружи и изнутри Достоинства и недостатки программно-аппаратных средств ЗИ. Механизмы защиты при идентификации и аутентификации пользователя. Система управления доступом. Система протоколирования аудита. Виды механизмов защиты для обеспечения конфиденциальности данных и сообщений. Контроль участников взаимодействия. Служба	<i>Нет</i>	6

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	<p>регистрации и наблюдения. Программа «Логическая бомба». Тема №4. Направления работ по защите информационной системы объекта Требования к автоматизированным системам защиты 3-й, 2-й и 1-й групп. Классы ЗИ от НСД для вычислительной техники. Выбор класса защищенности. Межсетевые экраны: требования и показатели защищенности. Программы-вирусы, пути их распространения, методы их обнаружения и противодействия им.</p>		

Раздел(предмет) *Современные аспекты безопасности информационных технологий*

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Современные аспекты безопасности и информационных технологий</i>	<p>Тема № 1. Безопасность персональных данных. Новый взгляд на старые проблемы Новое в законодательстве РФ и нормативном регулировании защиты персональных данных. Угрозы персональным данным в современном информационном пространстве. Оценка рисков, связанных с утечкой персональных данных. Тема № 2. Безопасность критической информационной инфраструктуры и проблема импортозамещения Организация защиты</p>	<i>Нет</i>	<i>6</i>

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	<p>значимых объектов ключевой информационной инфраструктуры (ЗО КИИ) на основе современных требований законодательства РФ. Подключение субъектов КИИ к ГосСОПКА. Перечень используемых программно-аппаратных и программных средств защиты информации для обеспечения безопасности ЗОО КИИ с учетом требований импортозамещения</p>		

Раздел(предмет) *Образовательные и профессиональные стандарты по защите информации*

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Образовательные и профессиональные стандарты по защите информации</i>	<p>Тема № 1. Общие положения Основы безопасности ИТ. Угрозы безопасности ИТ. Тема № 2. Основные принципы и меры по обеспечению безопасности ИТ. Правовые основы обеспечения безопасности ИТ Тема № 3. Обеспечение безопасности информационных технологий</p> <p>Организационная структура системы обеспечения безопасности ИТ. Обязанности конечных пользователей и ответственных за обеспечение безопасности ИТ в подразделениях. Документы, регламентирующие правила парольной и антивирусной</p>	<i>Нет</i>	<i>3</i>

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	защиты. Тема № 4. Обеспечение безопасности компьютерных систем и сетей		

Раздел(предмет) **Методика практической подготовки специалистов в сфере информационной безопасности**

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
<i>Методика практической подготовки специалистов в сфере информационной безопасности</i>	Тема № 1. Круглый стол: Концептуальные основы подготовки специалистов по информационной безопасности Поколение стандартов ФГОС ВО 3++. Профессиональные стандарты. Практическая реализация в информационной системе «Электронный МЭИ». Актуальные знания, необходимые специалисту по информационной безопасности (программа «Эталон») Тема № 2. Аналитический обзор существующих подходов к построению процесса подготовки специалистов в области защиты информации Тема № 3. Краткосрочные формы обучения специалистов в области информационной безопасности	<i>Нет</i>	<i>4</i>

Руководитель
кафедры БИТ, ЦПП
ИИЭБП

(должность, ученая степень,
ученое звание)

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Кунбутаев Л.М.
Идентификатор	R7a759843-KunbutayevLM-28fc24a

(подпись)

Л.М.
Кунбутаев

(расшифровка
подписи)

Начальник ОДПО

Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
Сведения о владельце ЦЭП МЭИ	
Владелец	Крохин А.Г.
Идентификатор	R6d4610d5-KrokhinAG-aa301f84

А.Г. Крохин

(должность, ученая степень,
ученое звание)

(подпись)

(расшифровка
подписи)