Приложение Б

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

АННОТАЦИИ РАБОЧИХ ПРОГРАММ ДИСЦИПЛИН (МОДУЛЕЙ) ДОПОЛНИТЕЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

профессиональной переподготовки
«Безопасность автоматизированных систем»,

Раздел(предмет) ***Защищенные информационные системы***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Нет*	*140*
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.	*Нет*	
Стандарты информацио	Роль стандартов информационной	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
нной безопасности	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».		
Математические модели защищенных информационных систем	Основные понятия и определения, используемые при описании моделей безопасности информационных систем. Элементы теории защиты информации. Математические основы моделей безопасности.	*Расчетное задание*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	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.		
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	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	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.		
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.	*Нет*	
Тестирование защиты	Модель опасностей. Декомпозиция приложения. Ранжирование интерфейсов по степени уязвимости.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	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.		
Промежуточная аттестация	Зачет	*Нет*	

Раздел(предмет) ***Управление проектами в сфере информационной безопасности***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
Обоснование проекта в сфере информационной безопасности	Основные определения в проектном управлении. Инициация проекта.	*Лабораторная работа*	*119*
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.	*Нет*	
Фазы исполнения и внедрения проекта	Управление проектом на фазе проектирования. Управление проектом на фазе внедрения.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
сфере информационной безопасности			
Промежуточная аттестация	Экзамен	*Нет*	

Раздел(предмет) ***Технологии обеспечения информационной безопасности***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Лабораторная работа*	*119*
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.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Нет*	
Технологии обнаружения вторжений	Анализ защищенности и обнаружение атак. Концепция адаптивного управления безопасностью.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности ОС. Технологии обнаружения атак. Классификация систем обнаружения атак.		
Промежуточная аттестация	Экзамен	*Нет*	

Раздел(предмет) ***Информационно-аналитические системы безопасности***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Лабораторная работа*	*119*
Организация противодействия злоумышленной деятельности	Конкурентная разведка. Противодействие промышленному шпионажу. Защита коммерческой тайны на предприятии.	*Нет*	
Технологии информационно-аналитического обеспечения безопасности	Статистический анализ данных. Инструменты интеллектуального анализа данных. Структура информационно-аналитической системы обеспечения безопасности.	*Нет*	
Промежуточная аттестация	Экзамен	*Нет*	

Раздел(предмет) ***Современные технологии информационных сетей***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
Введение в современные технологии информационных сетей	Особенности организации информационных сетей. Современные технологии в организации информационных сетей.	*Лабораторная работа*	*139*
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.	*Нет*	
Обеспечение защищенности информационных сетей	Использование общедоступных каналов передачи информации. Организация персональных и корпоративных сетей и подсетей. Защита информации в каналах общего использования.	*Нет*	
Вопросы обеспечения эффективности	Администрирование информационных сетей. Системы и средства наблюдения и контроля	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
информационных сетей	информационного обмена и содержимого информации. Технологии обеспечивающие эффективное функционирование информационных сетей.		
Перспективные направления развития информационных сетей	Тенденции развития информационных сетей, перспективные сетевые технологии.	*Нет*	
Промежуточная аттестация	Экзамен	*Нет*	

Раздел(предмет) ***Технологии и методы защиты информации в сети Интернет***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
Основы безопасной работы в сети Интернет	Угрозы информационной безопасности в сети Интернет. Принципы безопасного использования Интернет-ресурсов. Технологии безопасной передачи информации в сети Интернет.	*Расчетное задание*	*140*
Средства защиты информации в компьютерных сетях	Защита от вредоносного программ и спама. Межсетевое экранирование. Организация виртуальных защищенных VPN-сетей.	*Нет*	
Обнаружение и предотвращение вторжений	Понятие и классификация атак на компьютерные сети. Методы обнаружения атак. Системы обнаружения вторжений.	*Нет*	
Промежуточная аттестация	Зачет	*Нет*	

Раздел(предмет) ***Информационная безопасность компьютерных сетей***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Лабораторная работа*	*139*
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.	*Нет*	
Технологии виртуальных защищенных сетей	Виртуальные локальные сети. Конфигурирование виртуальных локальных сетей. Виртуальные защищенные сети VPN. Технологии и протоколы VPN. Построение VPN на основе маршрутизаторов.	*Нет*	
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.	*Нет*	
Защита беспроводных сетей передачи информации	Защищенные системы беспроводной связи. Беспроводные виртуальные сети.	*Нет*	
Промежуточная	Зачет	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
аттестация			

Раздел(предмет) ***Криптографические методы и средства защиты информации***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
Введение в криптографию	Введение в криптографию. Основные определения. История криптографии. Классификация криптоалгоритмов.	*Лабораторная работа*	*161*
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.	*Нет*	
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.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	Шифр RC4. Шифрование, использующее современные шифры с симметричным ключом. Применение современных блочных шифров. Использование шифров потока. Методы повышения криптостойкости симметричных криптосистем.		
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.	*Нет*	
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.	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	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 поведенческие методы биометрии.		
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.	*Нет*	
Основы современной стеганографии	Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.		
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.	*Нет*	
Промежуточная аттестация	Экзамен	*Нет*	

Раздел(предмет) ***Криптографические методы и средства защиты автоматизированных систем***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
Криптографические методы и средства защиты автоматизированных систем	Проектирование программного обеспечения в соответствии с вариантом задания и подходом к проектированию	*Решение задач*	*0*
Промежуточная аттестация	Защита курсовой работы	*Нет*	

Раздел(предмет) ***Программно-аппаратные средства защиты информации***

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
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.	*Лабораторная работа*	*139*
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.	*Нет*	
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	*Нет*	

Наименование дисциплин (модулей)	Содержание дисциплин (модулей)	Форма ТК	Количество часов
	использования. Гарантированное удаление данных.		
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.	*Нет*	
Промежуточная аттестация	Экзамен	*Нет*	

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

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