МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 65A182AF55E85519218FE36C1C7FB48A
Владелец: Евсина Татьяна Алексеевна
Действителен: с 16.11.2022 до 09.02.2024

УТВЕРЖДАЮ
Директор филиала КузГТУ
_____ Т.А. Евсина
«29» мая 2023 г.

Рабочая программа дисциплины
Программные и программно-аппаратные средства защиты информации

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

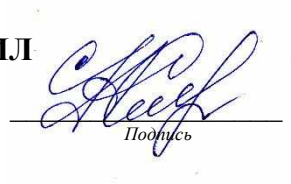
Форма обучения
очная

Год набора 2023

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2023 г.

РАБОЧУЮ ПРОГРАММУ СОСТАВИЛ

Преподаватель отделения СПО  С.А. Строкин

Подпись

СОГЛАСОВАНО

заведующий отделением СПО  Е.В. Севостьянова

Подпись

СОГЛАСОВАНО

Зам. директора по УР  Т.А. Евсина

Подпись

Рабочая программа обсуждена на заседании

учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол №6 от 29мая 2023 года

1. Общая характеристика рабочей программы дисциплины

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Программные и программно-аппаратные средства защиты информации» является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Учебная дисциплина «Программные и программно-аппаратные средства защиты информации» обеспечивает формирование профессиональных и общих компетенций в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2 Цель и планируемые результаты освоения дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общих компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
Знать: номенклатуру информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации;
Уметь: определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
Знать: возможные траектории профессионального развития и самообразования;
Уметь: выстраивать траектории профессионального и личностного развития;

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
Знать: психологию коллектива; психологию личности;
Уметь: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;

ОК 09. Использовать информационные технологии в профессиональной деятельности.
Знать: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности;
Уметь: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.
Знать: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности;
Уметь: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы;

профессиональных компетенций:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; Иметь практический опыт: установки, настройки программных средств защиты информации в автоматизированной системе;

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации в операционных системах; особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных; Уметь: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; Иметь практический опыт: обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использования программных и программно-аппаратных средств для защиты информации в сети;

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
Знать: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; Уметь: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; Иметь практический опыт: тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи; применения симметричных и асимметричных криптографических алгоритмов; использования средств шифрования данных;

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
Знать: особенности и способы применения программных средств и гарантированного уничтожения информации; особенности и способы применения аппаратных средств гарантированного уничтожения информации; Уметь: применять средства гарантированного уничтожения информации; выбирать средства гарантированного уничтожения информации; Иметь практический опыт: учёта, обработки, информации, для которой установлен режим конфиденциальности; хранения и передачи информации, для которой установлен режим конфиденциальности;

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Знать: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; Иметь практический опыт: работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе;

В результате освоения дисциплины обучающийся в общем по дисциплине должен
Знать:
- актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;
- номенклатуру информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации;
- возможные траектории профессионального развития и самообразования;
- психологию коллектива; психологию личности;
- современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности;
- правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности;
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- особенности и способы применения программных и программно-аппаратных средств защиты информации в операционных системах; особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных;

- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
- особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации;
- особенности и способы применения программных средств и гарантированного уничтожения информации; особенности и способы применения аппаратных средств гарантированного уничтожения информации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

Уметь:
- распознавать задачу и/или проблему в профессиональном и/или социальном контексте;
- определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска;
- выстраивать траектории профессионального и личностного развития;
- организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;
- применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение;
- понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;
- применять средства гарантированного уничтожения информации; выбирать средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

Иметь практический опыт:
- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использования программных и программно-аппаратных средств для защиты информации в сети;
- тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи; применения симметричных и асимметричных криптографических алгоритмов; использования средств шифрования данных;
- учёта, обработки, информации, для которой установлен режим конфиденциальности; хранения и передачи информации, для которой установлен режим конфиденциальности;
- работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе;

2. Структура и содержание дисциплины

2.1 Объем дисциплины и виды учебной работы

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 2 / Семестр 4			
Объем дисциплины	114		
в том числе:			
лекции, уроки	46		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
лабораторные работы			
практические занятия	54		
Консультации			
Самостоятельная работа	14		
Промежуточная аттестация			
Индивидуальное проектирование			
Форма промежуточной аттестации			
Курс 3 / Семестр 5			
Объем дисциплины	162		
в том числе:			
лекции, уроки	38		
лабораторные работы			
практические занятия	60		
курсовое проектирование	30		
Консультации	10		
Самостоятельная работа	24		
Промежуточная аттестация			
Индивидуальное проектирование			
Форма промежуточной аттестации	КП		

2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
4 семестр		
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации		
Лекции		
	Лекция 1.1.1 Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации.Классификация методов и средств программно-аппаратной защиты информации	1
Тема 1.2. Стандарты безопасности		
Лекции		
	Лекция 1.2.1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2
	Лекция 1.2.2. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
Практические занятия		
	Практическое занятие 1.2.1. Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.	4
	Практическое занятие 1.2.2. Обзор стандартов. Работа с содержанием стандартов	4
Тема 1.3. Защищенная автоматизированная система		

Лекции		
	Лекция 1.3.1. Автоматизация процесса обработки информации , Понятие автоматизированной системы. , Особенности автоматизированных систем в защищенном исполнении., Основные виды АС в защищенном исполнении., Методы создания безопасных систем, Методология проектирования гарантированно защищенных КС, Дискреционные модели, Мандатные модели	1
Практические занятия		
	Практическое занятие 1.3.1. Учет, обработка, хранение и передача информации в АИС, Ограничение доступа на вход в систему., Идентификация и аутентификация пользователей, Разграничение доступа.	4
	Практическое занятие 1.3.2. Регистрация событий (аудит)., Контроль целостности данных, Уничтожение остаточной информации.	2
	Практическое занятие 1.3.3. Управление политикой безопасности. Шаблоны безопасности, Криптографическая защита. Обзор программ шифрования данных, Управление политикой безопасности. Шаблоны безопасности	2
Тема 1.4. Дестабилизирующее воздействие на объекты защиты		
Лекции		
	Лекция 1.4.1. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию	1
Практические занятия		
	Практическое занятие 1.4.1.Распределение каналов в соответствии с источниками воздействия на информацию	2
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа		
Лекции		
	Лекция 1.5.1. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД	1
	Лекция 1.5.2. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	1
	Лекция 1.5.3. Особенности защиты данных от изменения. Шифрование.	1
Практические занятия		
	Практическое занятие 1.5.1. Организация доступа к файлам	2
	Практическое занятие 1.5.2. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2
Самостоятельная работа		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	8
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем		
Лекции		
	Лекция 2.1.1. Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	1
Тема 2.2.Защита программ от изучения		
Лекции		

	Лекция 2.2.1. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям.	1
Тема 2.3. Вредоносное программное обеспечение		
Лекции		
	Лекция 2.3.1 Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.Бот-неты. Принцип функционирования. Методы обнаружения. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии.	2
Практические занятия		
	Практическое занятие 2.3.1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
Тема 2.4. Защита программ и данных от несанкционированного копирования		
Лекции		
	Лекция 2.4.1. Несанкционированное копирование программ как тип НСД.Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям.Защитные механизмы в современном программном обеспечении на примере MS Office.	1
Практические занятия		
	Практическое занятие 2.4.1. Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	2
Тема 2.5. Защита информации на машинных носителях		
Лекции		
	Лекция 2.5.1. Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов. Безвозвратное удаление данных. Принципы и алгоритмы.	1
Практические занятия		
	Практическое занятие 2.5.1. Применение средства восстановления остаточной информации на примере Foremost или аналога	2
	Практическое занятие 2.5.2. Применение специализированного программно средства для восстановления удаленных файлов	2
	Практическое занятие 2.5.3. Применение программ для безвозвратного удаления данных	2
	Практическое занятие 2.5.4. Применение программ для шифрования данных на съемных носителях	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей		
Лекции		
	Лекция 2.6.1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ. Устройства Touch Memory.	1
Тема 2.7. Системы обнаружения атак и вторжений		
Лекции		
	Лекция 2.7.1. СОВ и СОА, отличия в функциях. Основные архитектуры	1

	СОВ.Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ.Программный компонент СОВ.Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
Практические занятия		
	Практическое занятие 2.7.1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2
Самостоятельная работа		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	6
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей		
Лекции		
	Лекция 3.1.1. Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	8
Тема 3.2. Средства организации VPN		
Лекции		
	Лекция 3.2.1. Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	10
Практические занятия		
	Практическое занятие 3.2.1 Развертывание VPN	10
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия		
Лекции		
	Лекция 4.1.1. Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня. Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.	10
Практические занятия		
	Практическое занятие 4.1.1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия "опасных" портов	8
5 семестр		
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных		
Лекции		
	Лекция 5.1.1. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны.	10

	Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
Практические занятия		
	Практическое занятие 5.1.1. Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server	12
Самостоятельная работа		10
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты		
Лекции		
	Лекция 6.1.1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2
	Лекция 6.1.2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2
	Лекция 6.1.3. Классификация отслеживаемых событий. Особенности построения систем мониторинга	4
	Лекция 6.1.4. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	2
	Лекция 6.1.5. Классификация сетевых мониторов.	2
	Лекция 6.1.6. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2
Практические занятия		
	Практическое занятие 6.1.1. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов.	10
	Практическое занятие 6.1.2. Проведение аудита ЛВС сетевым сканером	10
Тема 6.2. Изучение мер защиты информации в информационных системах		
Лекции		
	Лекция 6.2.1. Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	4
Практические занятия		
	Практическое занятие 6.2.1. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	28
Тема 6.3. Изучение современных программно-аппаратных комплексов.		
Лекции		
	Лекция 6.3.1. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов. Изучение типовых решений для построения VPN на примере VipNet или других аналогов. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	10
Самостоятельная работа		14
Консультации		10
Курсовая работа(проект), в том числе:		30
Курсовая работа(проект) - выполнение		28
Промежуточная аттестация в форме защиты курсовой работы(проекта)		2

3 Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)

3.1 Специальные помещения для реализации программы

Наличия учебного кабинета «информационной безопасности, лаборатории информационных технологий».

Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий «Информационная безопасность»;
- электронное учебное пособие.

Технические средства обучения:
- компьютер с лицензионным программным обеспечением, мультимедийный диапроектор, интерактивная доска.

.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475890 .

3.2.2. Дополнительная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. защита программного обеспечения.: учебник и практикум для СПО / Казарин О. В., Забабурин А. С.. – Москва : Юрайт, 2021. – 312 с. – ISBN 978-5-534-13221-2. – URL:https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-476997. – Текст : электронный.

3.2.3 Методическая литература

Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL:http://library.kuzstu.ru/meto.php?n=9964. – Текст : электронный

3.2.4 Интернет ресурсы

1. ЭИОС КузГТУ:
a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.
b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.
c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.
2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.
3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.
4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.
5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.
6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.
7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.
9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.
10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Организация самостоятельной работы обучающихся

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля).

Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

6. Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных, так и современных интерактивных технологий. При контактной работе педагогического работника с обучающимися применяются следующие элементы интерактивных технологий:

- совместный разбор проблемных ситуаций;
- совместное выявление причинно-следственных связей вещей и событий, происходящих в повседневной жизни, и их сопоставление с учебным материалом.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.