ТАМБОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ТАМБОВСКИЙ БИЗНЕС-КОЛЛЕДЖ»

Астахова Наталия Вениаминовна

Подписано цифровой подписью: Астахова Наталия Вениаминовна
Дата: 2024.10.03 13:19:43 +03'00'

УТВЕРЖДАЮ
Директор ТОГАПОУ
«Тамбовский бизнес-колледж»
_____Н.В. Астахова
Приказ № 42 от «30» августа 2024г.

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ)

Наименование программы

Администрирование и эксплуатация аппаратно-программных средств с защитой информации в компьютерных системах

Категория слушателей

Граждане, имеющие среднее профессиональное или высшее образование; граждане, получающие среднее профессиональное или высшее образование

Объем 250 часов

Форма обучения Очно-заочная

Срок обучения 3 месяцев

Тамбов
2024

Разработчик Туляков Денис Валерьевич, преподаватель ТОГАПОУ «Тамбовский бизнес-колледж»

Краткая аннотация

Программа профессиональной переподготовки «**Администрирование и эксплуатация аппаратно-программных средств с защитой информации в компьютерных системах**» позволяет обучающимся освоить проведение работ по документационному и организационно-технологическому обеспечению защиты информации в организациях различных структур и отраслевой направленности.

Специальность «Информационная безопасность» очень престижна и входит в ТОП 50 самых востребованных профессий на сегодняшний день.

В курсе рассматриваются теоретические и практические аспекты программно – аппаратной защита информации. Анализируются возможности различных видов программных и программно-аппаратных средств защиты информации, даются рекомендации по выбору рациональных вариантов и решений по их эффективному применению для противодействия угрозам безопасности автоматизированных систем. Рассматривается техническая сторона защиты информации на ЭВМ и сетей ЭВМ. Конфигурация операционных систем, прикладного программного обеспечения. Вредоносное программное обеспечение, возможности, последствия, борьба с распространением. Уязвимости и способы их эксплуатации, защита от возможных атак с использованием уязвимостей.

В курсе предусмотрены практические работы с рассмотренными средствами программно – аппаратной защиты.

В результате успешного освоения всей программы профессиональной переподготовки слушателям выдаётся диплом о профессиональной переподготовкепо программе«**Администрирование и эксплуатация аппаратно-программных средств с защитой информации в компьютерных системах**», дающий право на ведение новой профессиональной деятельности.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативно-правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

постановление Правительства Российской Федерации от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов»;

приказ Минтруда России от 12 апреля 2013 г. № 148н «О утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов».

Программа разработана на основе профессионального стандарта Российской Федерации по специальностисреднего профессионального образования10.02.01Организация и технология защиты информации и 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Область применения программы

Настоящая программа предназначена для профессиональной переподготовки граждан, желающих изменить вид своей профессиональной деятельности. Реализация программы профессиональной переподготовки направлена на получение компетенций, необходимых для выполнения нового вида профессиональной деятельности, приобретение новой квалификации.

1.3. Требования к слушателям (категории слушателей)

Программа переподготовки рекомендуется лицам, имеющим среднее профессиональное и (или) высшее образование, а также лицам, получающим среднее профессиональное и (или) высшее образование по УГС 09.02.00 «Информатика и вычислительная техника».

1.4. Цель и планируемые результаты освоения программы

Программа направлена на освоение (совершенствование) следующих профессиональных компетенций:

1. Участие в планировании и организации работ по обеспечению защиты объекта.

ПК 1.1. Участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.

ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9. Участвовать в оценке качества защиты объекта.

2. Организация и технология работы с конфиденциальными документами.

ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.

ПК 2.2. Организовывать и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации.

ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации.

ПК 2.4. Организовывать архивное хранение конфиденциальных документов.

ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.

ПК 2.6. Вести учет работ и контроль объектов, подлежащих защите.

ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.

ПК 2.8. Документировать ход и результаты служебного расследования.

ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы и справочную документацию по защите информации.

3. Применение программно-аппаратных и технических средств защиты информации.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Фиксировать отказы в работе средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

4. Участие в организации комплексной системы защиты объекта.

ПК 4.1. Участвовать в разработке организационной структуры комплексной системы защиты информации (далее - КСЗИ).

ПК 4.2. Участвовать в оценке технико-экономического уровня и эффективности организации КСЗИ.

ПК 4.3. участвовать в подготовке заданий на реализацию КСЗИ.

ПК 4.4. Организовывать и планировать работу малых коллективов исполнителей.

Обучающийся в результате освоения программы должен

иметь практический опыт:

участия в эксплуатации систем и средств защиты информации защищаемых объектов;

применения технических средств защиты информации;

выявления возможных угроз информационной безопасности объектов защиты;

уметь:

работать с техническими средствами защиты информации;

работать с защищенными автоматизированными системами;

передавать информацию по защищенным каналам связи;

фиксировать отказы в работе средств вычислительной техники;

знать:

виды, источники и носители защищаемой информации;

источники опасных сигналов;

структуру, классификацию и основные характеристики технических каналов утечки информации;

классификацию технических разведок и методы противодействия им;

методы и средства технической защиты информации;

методы скрытия информации;

программно-аппаратные средства защиты информации;

структуру подсистемы безопасности операционных систем и выполняемые ею функции;

средства защиты в вычислительных сетях;

средства обеспечения защиты информации в системах управления базами данных;

критерии защищенности компьютерных систем;

методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

Форма документа, выдаваемого по результатам освоения программы – диплом о профессиональной переподготовке.

2. УЧЕБНЫЙ ПЛАН

Администрирование и эксплуатация аппаратно-программных средств с защитой информации в компьютерных системах

№	Наименование учебных предметов (модулей)	Работа обучающегося в СДО, в акад. час.		Общая трудоемкость, в акад. час.	Форма промежуточной и итоговой аттестации
		лекции	практические занятия, тестирование		
1.	Модуль 1. Информационная безопасность в компьютерных система. Основные положения	10	10	20	ДЗ
2.	Модуль 2. Методы обеспечения информационной безопасности компьютерных систем	10	10	20	ДЗ
3.	Модуль 3. Средства защиты информации от несанкционированного доступа	10	30	40	ДЗ
4.	Модуль 4. Криптографическая защита информации	8	12	20	ДЗ
5.	Модуль 5. Защитные механизмы в операционных системах Windows.	12	28	40	ДЗ
6.	Модуль 6. Вредоносное ПО. Антивирусная защита.	10	20	30	ДЗ
7.	Модуль 7. Защита информации в компьютерных сетях	10	28	38	ДЗ
8.	Модуль 8. Эксплуатация защищенных автоматизированных систем.	10	28	38	ДЗ
9.	Итоговая аттестация	0	4	4	Экзамен
	Всего:	**80**	**170**	**250**	

3. ПРОГРАММЫ УЧЕБНЫХ МОДУЛЕЙ (ПРЕДМЕТОВ, ДИСЦИПЛИН)

Наименование разделов и тем программы	Содержание учебного материала, практические занятия, самостоятельная учебная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Модуль 1. Информационная безопасность в компьютерных система. Основные положения.		**20**	**3**
Тема 1.1. Понятие информационной безопасности	**Содержание учебного материала**	**2**	
	Лекция Предмет защиты информации, цели и задачи. Примеры нарушения информационной безопасности.Понятия конфиденциальности, целостности, доступности. Роль защиты информации в современном. обществе.	2	*1*
Тема 1.2Основные составляющие ИБ	**Содержание учебного материала**	**4**	
	Лекция Понятия конфиденциальности, целостности, доступности. Роль защиты информации в современном обществе	2	*2*
	Практическая работа (самостоятельно) 1Анализ источников, каналов распространения и каналов утечки информации	2	
Тема 1.3. Классификация угроз ИБ	**Содержание учебного материала**	**8**	
	Лекция Классификация угроз информационной безопасности. Модель нарушителя.	2	*1*
	Практическая работа (самостоятельно) 2 Построение модели нарушителя 3. Требования к безопасности информационных систем. 4Оценка уязвимости информации	6	*2*
Тема 1.4. Законы, стандарты и спецификации в области ИБ	**Содержание учебного материала**		
	Лекция Понятие организационно-правовой защиты информации. Основные регламентирующие документы по защите информации. Обзор наиболее важных стандартов и спецификаций в области информационной безопасности	**4** 2	*1*
	Практическая работа (самостоятельно) 5. Анализ Доктрины информационной безопасности Российской Федерации.	*2*	*2*
Зачет по учебному модулю	**Содержание учебного материала**	**2**	
	Тестирование.		*3*
Модуль 2. Методы обеспечения информационной безопасности компьютерных систем		**20**	*3*
Тема 2.1. Административный уровень информационной безопасности	**Содержание учебного материала**	**4**	*2*
	Лекция Цели, задачи и содержание административного уровня Разработка политики информационной безопасности	2	*1*
	Практическая работа (самостоятельно) 1.Разработать политику и программу безопасности по входным данным предприятия	2	*2*
Тема 2.2. Управление	**Содержание учебного материала**	**4**	*2*

рисками	Лекция Подготовительные этапы управления рисками Основные этапы управления рисками	2	
	Практическая работа (самостоятельно) 2.Оценка рисков информационной безопасности	2	*2*
Тема 2.3. Процедурный уровень информационной безопасности	**Содержание учебного материала**	**6**	*2*
	Лекция Основные классы мер процедурного уровня.Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушение режима безопасности. Планирование восстановительных работ.	2	*1*
	Практическая работа (самостоятельно) 3.Разработать разделение обязанностей персонала и меры физической защиты 4.Оценка безопасности информации на объектах ее обработки	4	*2*
Тема 2.4. Основные программно-технические меры	**Содержание учебного материала**	**4**	*2*
	Лекция Основные понятия программно-технического уровня информационной безопасности Особенности современных информационных систем, существенные с точки зрения безопасности Архитектурная безопасность	2	*1*
	Практическая работа (самостоятельно) 5.Разработать и обосновать механизмы защиты информации	2	*2*
Зачет по учебному модулю	Тестирование.	**2**	*3*
Модуль 3. Средства защиты информации от несанкционированного доступа		**40**	
Тема 3.1. Идентификация и аутентификация	**Содержание учебного материала**	**22**	**2**
	Лекция. Определение понятий "идентификация" и "аутентификация" Механизм идентификация и аутентификация пользователей Аутентификация, авторизация и администрирование действий пользователей Методы аутентификации, использующие пароли и PIN коды	2	
	Практическая работа (самостоятельно) 1.Разработка программного модуля аутентификации на основе одноразового пароля 2.Разработка программы аутентификации пользователя на основе клавиатурного почерка 3.Разработка программы голосовой аутентификации пользователя 4.Разработка и программная реализация модуля авторизации по схеме SSO	20	2
Тема 3.2. Управление доступом	**Содержание учебного материала**	**10**	*2*
	Лекция Основные понятия Ролевое управление доступом Управление доступом в Java-среде Возможный подход к управлению доступом в распределенной объектной среде	4	*2*
	Практическая работа (самостоятельно)	6	

	5.Настройка групп пользователей в Windows 10		
Тема 3.3. Протоколирование и аудит, шифрование, контроль целостности	**Содержание учебного материала**	**6**	*2*
	Лекция Основные понятия. Активный аудит. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.	2	*1*
	Практическая работа (самостоятельно) 6.Шифрующая файловая система EFS и управление сертификатами в Windows 2000/XP/7/10	4	2
Зачет по учебному модулю	Тестирование.	**2**	
Модуль 4. Криптографическая защита информации		**20**	
Тема 4.1 Основы криптографии	**Содержание учебного материала**	**4**	
	Лекция Основные определения и терминология. Из истории криптографии. Маршрутная транспозиция. Таблица Виженера. Модифицированный шифр Цезаря. Одноразовый блокнот.	2	
	Практическая работа (самостоятельно) 1.Шифр простой перестановки	2	
Тема 4.2 Симметричные и ассиметричные криптосистемы шифрования	**Содержание учебного материала**	**8**	
	Лекция Поточные шифры. Блочные шифры. Шифры взбивания и стандарт DES. Сравнение с асимметричными криптосистемами. Асимметричная криптография	2	
	Практическая работа (самостоятельно) 2.Программная реализация шифра Цезаря. 3.Программная реализация шифра Виженера 4.Программная реализация симметричного шифра ГОСТ Р 28147-89	6	
Тема 4.3 Функции хеширования	**Содержание учебного материала**	**6**	
	Лекция Понятие хеш-функции. Использование блочных алгоритмов шифрования для формирования хеш-функции. Электронная цифровая подпись	2	
	Практическая работа (самостоятельно) 5.Программная реализация алгоритма хеширования MD5. 6.Программная реализация алгоритма хеширования SHA-256	4	
Зачет по учебному модулю	Тестирование	**2**	*3*
Модуль 5. Защитные механизмы в операционных системах Windows		**40**	*3*
Тема 5.1. Понятиезащищеннойоперационнойсистемы	**Содержание учебного материала**	**8**	*2*
	Лекция Основные подходы к построению защищенных операционных систем. Административные меры защиты. Адекватная политика безопасности. Стандарты безопасности операционных систем.	2	*1*
	Практическая работа (самостоятельно) 1.Администрирование Windows 10	**6**	*2*

	2.Управление системными службами и процессами Windows		
Тема 5.2. Управлениедоступомв Windows	**Содержание учебного материала**	**8**	*2*
	Лекция Типовые модели управления доступом. Управление доступом в Windows.	2	
	Практическая работа (самостоятельно) 3.Аутентификация в операционных системах при помощи физического объекта 4.Двухфакторная аутентификация в программном обеспечении на основе технологии SSO	**6**	*2*
Тема 5.3. Аутентификацияв Windows	**Содержание учебного материала**	**8**	*2*
	Лекция Задачи идентификации, аутентификации и авторизации пользователей. Аутентификация при удаленном входе в систему. Механизм автоматической блокировки (lock out) пользователя.	2	*1*
	Практическая работа 5. Дискреционный механизм разграничения доступа к файловым объектам 6.Мандатный механизм разграничения доступа к файловым объектам	**6**	*2*
Тема 5.4. Аудитиобнаружениевторжений	**Содержание учебного материала**	**6**	*2*
	Лекция Общие сведения. Системы обнаружения вторжений. Аудит в Windows.	2	*1*
	Практическая работа 7.Аудит событий безопасности операционной системы 8.Анализ и настройка параметров безопасности операционной системы	**4**	*2*
Тема 5.5. Виртуализацияоперационныхсистем	**Содержание учебного материала**	**8**	*2*
	Технологии виртуализации. Виртуализация серверов. Краткий обзор платформ виртуализации. Microsoft	2	
	Практическая работа (самостоятельно) 9.Установка и настройка Hyper-V 10.Установка и настройка VMWare Workstation	**6**	*2*
Зачет по учебному модулю	Тестирование по учебному модулю.	**2**	*3*
Модуль 6. Вредоносное ПО. Антивирусная защита.		**30**	
Тема 6.1История компьютерных вирусов	**Содержание учебного материала**	**2**	
	Лекция Эволюция развития вирусных программ и антивирусной защиты.	2	
Тема 6.2 Классификация вирусов. Признаки присутствия на компьютере вредоносных программ	**Содержание учебного материала**	**8**	
	Лекция Понятие вредоносной программы. Классификация вирусов. Признаки присутствия вредоносных программ.	2	
	Практическая работа (самостоятельно) 1. Основные признаки присутствия на компьютере вредоносных программ -Изучение настроек браузера -Подозрительные процессы - Элементы автозапуска	**6**	

	- Сетевая активность		
Тема 6.3 Методы защиты от вредоносных программ. Основы работы антивирусных программ	**Содержание учебного материала**	**8**	
	Лекция Основные методы защиты от вредоносных программ. Политика безопасности. Встроенный брандмауэр ОС, настройка.	2	
	Практическая работа (самостоятельно) 2.Профилактика заражения вирусами компьютерных систем -знакомство с энциклопедией компьютерных вирусов -Изучение дополнительных возможностей программы Norton AntiVirus	**6**	
Тема 6.4 Классификация антивирусов. Антивирусная защита компьютера и сети.	**Содержание учебного материала**	**10**	
	Лекция Основы работы антивирусных программ. Классификация антивирусных программ. Антивирусная защита компьютера.	2	
	Практическая работа (самостоятельно) 3.Установка и предварительная настройка Антивируса Касперского и Dr. Web Curelt	**8**	
Зачет по учебному модулю	Тестирование по учебному модулю.	**2**	
Модуль 7. Защита информации в компьютерных сетях		**38**	
Тема 7.1. Архитектура и устройство сетей и систем	**Содержание учебного материала**		
	Лекция Иерархическиетопологии. Обеспечениебезопасностисети. Политика безопасности сетей и ее обеспечение Списки управления доступом		
Тема 7.2 Выявление сетевых атак путем анализа трафика	**Содержание учебного материала**		
	Лекция Этапы сетевой атаки.Исследование сетевой топологии. Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы. Реализации атак. Выявление атаки на протокол SMB.		
	Практическая работа (самостоятельно) 1.Выявление сетевых атак путем анализа трафика	**2**	
Тема 7.3Технология межсетевого экранирования	**Содержание учебного материала**		
	Лекция Понятие межсетевого экрана. Компоненты межсетевого экрана. Политика межсетевого экранирования. . Архитектура МЭ.		
	Практическая работа (самостоятельно) 2.Межсетевое экранирование	**2**	
Тема 7.4 Организация виртуальных частных сетей	**Содержание учебного материала**		
	Лекция Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.		
	Практическая работа (самостоятельно) 3.Организация VPN средствами СЗИ VipNet	**24**	

	4.Организация VPN средствами протокола PPTP 5.Использование протокола IPSec для защиты сетей 6.Организация VPN средствами СЗИ StrongNet 7.Организация VPN средствами протокола SSL в Windows Server 2003 8.Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ КриптоПро CSP		
Зачет по учебному модулю	Тестирование по учебному модулю.		
Модуль 8. Эксплуатация защищенных автоматизированных систем		**38**	
Тема 8.1Основы информационных систем как объекта защиты.	**Содержание учебного материала**	**8**	
	Лекция Основные понятия. Предпосылки создания ИС. История развития ИС. Структура ИС. Понятие жизненного цикла АИС. Его структура.Стадии жизненного цикла АИС: начало и уточнение.Стадия конструирования и передачи в эксплуатацию	2	
	Практическая работа (самостоятельно) 1.Разработка технического задания на проектирование автоматизированной системы 2.Категорирование информационных ресурсов	**6**	
Тема 8.2 Содержание и порядок эксплуатации АС в защищенном исполнении.	**Содержание учебного материала**	**4**	
	Лекция Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации	2	
	Практическая работа (самостоятельно) 3.Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	**2**	
Тема 8.3 Особенности эксплуатации и администрирование автоматизированных систем в защищенном исполнении	**Содержание учебного материала**	**14**	
	Лекция	2	
	Практическая работа (самостоятельно) 4.Разграничение доступа к устройствам. Управление доступом. 5.Использование принтеров для печати конфиденциальных документов. Контроль печати 6.Настройка системы для задач аудита 7.Настройка контроля целостности и замкнутой программной среды	**12**	
Тема 8.4 Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание учебного материала**	**10**	
	Лекция	2	
	Практическая работа (самостоятельно) 8.Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем 9.Оформление основных эксплуатационных документов на автоматизированную систему	**8**	
Зачет по учебному модулю	Тестирование по учебному модулю.	**2**	
Итоговая аттестация	**Итоговое тестирование.**	**4**	*3*
Всего:		**250**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Материально-техническое обеспечение

Реализация программы предполагает наличие учебного кабинета

Оборудование учебного кабинета и рабочих мест кабинета:

– 6 маршрутизаторов Cisco 2801 с Base IP IOS, 128 Мбайт DRAM, 32 Мбайта флэш-памяти и модулями HWIC-2A/S;

– 6 коммутаторов Cisco Catalyst 2960;

– набор соединительных кабелей (входят в комплект поставки оборудования для Сетевой академии);

– 6 беспроводных маршрутизаторов класса SOHO;

– 1 компьютер для лабораторных занятий с ОС Microsoft Windows Server 2016;

– 12 компьютеров для лабораторных занятий (Microsoft Windows 10).

Технические средства обучения:

– компьютер с подключением к сети Интернет;

– мультимедийный проектор;

– экран настенный;

– комплект стендов по тематике курса

Набор инструментов для выполнения практических работ

Набор должен содержать следующие инструменты:

- различные кабели Ethernet:
- минимум один прямой кабель на каждого студента.
- минимум один перекрестный кабель на каждого студента.
- обжимные устройства для коннекторов RJ-45.
- сетевые розетки RJ-45.
- коннекторы RJ-45, 8 pin.

4.2. Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Защита информации в компьютерных системах и сетях. Уч. пособие для технических вузов, 5-7695-1796-4, ИЦ ДМК, 2013., 592 стр. Шаньгин В. Ф.
2. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.
3. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.
5. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.
6. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.
7. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.
8. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

Дополнительные источники:

1. Танненбаум Э. Компьютерные сети. 4-е издание, Спб: Издательство "Питер", 2016. ISBN 978-5-318-00492-6;
2. Олифер В., Олифер Н. "Компьютерные сети", Спб: Издательство "Питер", 2015.
3. Зеркина Е. В. Информационная безопасность в системе открытого образования (для специальности 050202 – «Информатика») : учеб. – метод. пособие / Е. В. Зеркина. – Магнитогорск : МаГУ, 2013. – 100 с.
4. Кононов, А. А. Информационное общество: общество тотального риска или общество управляемой безопасности? / А. А. Кононов. – М. : Едиториал УРСС, 2013. – с. 6 -20.
5. Уорли Б. Интернет: реальные и мнимые угрозы / пер. с англ. – М. : КУДИЦОБРАЗ, 2013. -320 с.
6. Джонсон С. как защитить детей от опасностей Интернета : вирусов, программ-шпионов, спама, порносайтов, всплывающих окон / Саймон Джонсон ; пер. с англ. Е. А. Ивановой. – М. : НТ Пресс, 2013. – 304 с. : ил.
7. Андреева Н. В., Асеев Х. М. Обеспечение комплексной безопасности в образовательном учреждении. Безопасность в образовательном учреждении: настольная книга руководителя / Н. В. Андреева, Х. М. Асеев и др. – М. : Айрис-Пресс, 2013. – 247 с.
8. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2008.
9. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2012. – 224 с.
10. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 2-е изд. - СПб.: Питер, 2006 - 703 с.
11. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2009. - 88 с.
12. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2011. – 1024 с.
13. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.
14. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2008
15. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.
16. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008
17. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007.- 531 с.
18. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.
19. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2005.- 147 с.
20. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2013. – 544 с.
21. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2006. – 240 с.

22. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2014. – 672 с.

Северин В. Комплексная защита информации на предприятии. М.: Городец, 2008. – 368 с.

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки IPRbooks (http://www.iprbookshop.ru)
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru

4.3. Организация образовательного процесса

Теоретические и практические занятия проводятся с применением средств дистанционного обучения.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров: первая и высшая категория преподавателей.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КУРСА

Текущий контроль.

Текущий контроль успеваемости осуществляется на основе проверки выполнения практических заданий, а также на основе интерактивных компьютерных тестов, которые содержат контрольные вопросы по каждой изучаемой теме и должны быть сданы студентами (слушателями) в ходе учебного периода.

Рубежный контроль.

Для оценки качества усвоения знаний и уменийпредусмотрены шесть рубежных контролей (зачета по учебному модулю), которые проводятся при завершении изучения учебного модуля в соответствии с тематическим планом.Рубежный контроль проводится в форме компьютерного тестирования. К прохождению рубежного контроля допускаются только те студенты (слушатели), которые успешно сдали все промежуточные тесты и выполнили все текущие задания. Для подготовки к рубежным контролям предусмотрены домашние задания.

Самостоятельный контроль

Студенты (слушатели) имеют возможность при самостоятельном, в том числе и внеаудиторном, изучении интерактивного учебника отвечать на компьютерные тесты и контрольные вопросы, имеющиеся после каждой главы (темы).

Итоговый контроль.

Проверка практических навыков, теоретических знаний и умений должна осуществляться по результатам текущего и рубежного контроля.

В составе учебно-методического обеспечения дисциплины имеются специальные средства для осуществления балльно-рейтингового контроля и расчета предварительных или итоговых оценок.

По умолчанию информационная система, доступная для зарегистрированных преподавателей курса, учитывает результаты сдачи всех компьютерных тестов и итоговой проверочной работы. Преподаватель имеет возможность установить коэффициенты значимости для каждого вида учебной нагрузки, а также добавить новые характеристики (например, посещаемость лекций, активность на практических занятиях, качество выполнения лабораторных и практических занятий и др.).