Тамбовское государственное автономное профессиональное образовательное учреждение «Тамбовский бизнес-колледж»

Предметная цикловая комиссия информационных дисциплин

Астахова Наталия Вениаминовна Digitally signed by Астахова Наталия Вениаминовна Date: 2023.11.23 22:34:36 +03'00'

Утверждаю
Директор ТОГАПОУ
«Тамбовский бизнес-колледж»
_____ Н.В. Астахова
Приказ №106/1 от 28.08.2023 г.

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.17 КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

среднее профессиональное образование
(программа подготовки специалистов среднего звена)
09.02.07 «Информационные системы и программирование»
(Квалификация: программист)

Тамбов 2023

ОДОБРЕНА

Предметной цикловой комиссией информационных технологий

Разработана на основе Федерального государственного образовательного стандарта по специальности 09.02.07 «Информационные системы и программирование»

Протокол №1

От «28» августа 2023г.

Председатель Предметной цикловой комиссии

_____ Туляков Д.В.

Заместитель директора по НМР

_____ Полубояринова О.В.

Составитель (автор):
Архипова Е.В., преподаватель ТОГАПОУ «Тамбовский бизнес-колледж»

Рецензент:
Указываем рецензента

АННОТАЦИЯ
ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.17 КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цели и задачи учебной дисциплины:

Цель изучения дисциплины заключается в получении обучающимися знаний и умений в области информационной безопасности.

Задачи дисциплины:

формирование у студентов четкого представления о типах каналов утечки информации;

формирование у студентов четкого представления об аппаратных угрозах целостности информации;

формирование у студентов четкого представления о программных угрозах безопасности информации;

получение комплексных знаний о моделях безопасности;

получение комплексных знаний о системах и средствах парольной защиты;

подготовка специалистов, умеющих использовать аппаратные средства защиты информации;

подготовка специалистов, умеющих использовать программные технологии защиты информации.

Основные дидактические единицы (темы):

Тема раздела 1. Понятие информационной безопасности.

Тема раздела 2. Угрозы безопасности.

Тема раздела 3. Антивирусная защита информации.

Тема раздела 4. Законодательный уровень ИБ. Стандарты в области ИБ.

Тема раздела 5. Административный уровень информационной безопасности

Тема раздела 6. Основные программно-технические меры.

Тема раздела 7. Традиционные симметричные криптосистемы.

Тема раздела 8. Современные симметричные криптосистемы.

Тема раздела 9. Асимметричные криптосистемы.

Тема раздела 10. Аутентификация, авторизация и администрирование действий пользователя.

Тема раздела 11. Методы аутентификации, использующие пароли

Тема раздела 12. Электронная цифровая подпись.

В результате освоения дисциплины обучающийся должен **уметь**:

- распознавать отклонения от нормального режима работы информационных систем и принимать меры по конкретному диагностированию причин отклонений;

- использовать средства устранения разрушающих программных воздействий;
- использовать прокси-серверы;
- использовать стандартные средства защиты информации шифрованием, в особенности, встроенные в современные операционные платформы;
- применять эффективные средства администрирования, повышающие защищенность системы;
- выбирать антивирусные программы, соответствующие природе вероятных разрушающих программных воздействий;
- грамотно взаимодействовать с администратором системы и использовать средства программно-аппаратной защиты.

В результате освоения дисциплины обучающийся должен **знать**:

- типы каналов утечки информации;
- аппаратные угрозы целостности информации;
- программные угрозы безопасности информации;
- модели безопасности;
- системы и средства парольной защиты;
- аппаратные средства защиты информации;
- программные технологии защиты информации.

Изучение данной дисциплины направлено на достижение образовательных, воспитательных и практических задач, на дальнейшее развитие личностных способностей и дальнейшего профессионального роста выпускника – будущего специалиста.

Содержание

стр

1. Общая характеристика программы ……..……..6

2. Структура и содержание учебной дисциплины……..…….…..8

3. Условия реализации учебной дисциплины…….14

4. Контроль и оценка результатов освоения учебной дисциплины……..16

1. Общая характеристика программы учебной дисциплины

1.1. Место дисциплины в структуре основной образовательной программы:

Программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.07 «Информационные системы и программирование».

Программа учебной дисциплины может быть использована в профессиональной подготовке работников в области разработки программного обеспечения при наличии среднего (полного) общего образования. Опыт работы не требуется.

Учебная дисциплина входит в общепрофессиональный цикл, имеет связь с дисциплинами ОП.14. Проектирование и техническое сопровождение компьютерных сетей, ОП.11. Компьютерные сети, является дисциплиной, закладывающей базу для последующего изучения профессиональных модулей ПМ 03. Проектирование, разработка и оптимизация веб-приложений

1.2. Цель и планируемые результаты освоения учебной дисциплины:

Цель изучения дисциплины заключается в получении обучающимися знаний и умений в области информационной безопасности.

Задачи:

формирование у студентов четкого представления о типах каналов утечки информации;

формирование у студентов четкого представления об аппаратных угрозах целостности информации;

формирование у студентов четкого представления о программных угрозах безопасности информации;

получение комплексных знаний о моделях безопасности;

получение комплексных знаний о системах и средствах парольной защиты;

подготовка специалистов, умеющих использовать аппаратные средства защиты информации;

подготовка специалистов, умеющих использовать программные технологии защиты информации.

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами,

	руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
	Наименование профессиональных компетенций
ПК 4.4.	Обеспечивать защиту программного обеспечения компьютерных систем программными средствами
ПК 11.6	Защищать информацию в базе данных с использованием технологии защиты информации

Личностные результаты

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Осознающий себя гражданином и защитником великой страны.	ЛР 1
Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.	ЛР 2
Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.	ЛР 3

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**128**
Объем образовательной программы учебной дисциплин (аудиторная нагрузка обучающихся)	**108**
в т.ч.:	
лекционные занятия	52
практические занятия	54
в т.ч. практическая подготовка	28
курсовая работа (проект)	0
Самостоятельная работа	**20**
Итоговая аттестация (диф.зачет, зачет, тест или экзамен)	**2**

2.2. Тематический план и содержание учебной дисциплины «Комплексное обеспечение информационной безопасности»

Наименование модулей, разделов тем программы	Содержание учебного материала, практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся и формы организации деятельности	Объем часах	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
1	2	3	4
Тема 1. Понятие информационной безопасности	**Содержание**	6	ОК 1-11. ПК 11.6 ЛР1-ЛР3
	1.Основные понятия в области информационной безопасности. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность. 2.Методы защиты информации в информационной системе.	2	
	Практическое занятие 1. Проведение анализа информации на предмет целостности, конфиденциальности, доступности	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы	2	
Тема 2. Угрозы безопасности	**Содержание**	10	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1.Угрозы информационной безопасности: классификации, источники возникновения и пути реализации. 2.Санкционированный и несанкционированный доступ к данным. Виды несанкционированного доступа к информации. Средства и механизмы защиты от несанкционированного доступа. 3.Классификация угроз информационной безопасности. 4.Модель нарушителя	6	
	Практическое занятие	4	

	1. Анализ источников, каналов распространения и каналов утечки информации 2. Построение модели потенциального нарушителя ИС		
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной техническо литературы	2	
Тема 3. Антивирусная защита информации	**Содержание**	8	ОК 1-11. ПК 4.4, ПК 11.6 ЛР1-ЛР3
	1. Понятие компьютерного вируса, сущность и возможности проявления. Классификации компьютерных вирусов. Структура современных вирусных программ. 2. Основные методы и средства защиты от воздействия компьютерных вирусов. Современные пакеты антивирусных программ. Характеристики и возможности применения	4	
	Практическое занятие 1.Изучение современных методов антивирусной защиты информации	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы	1	
Тема 4. Законодательный уровень ИБ. Стандарты в области ИБ	**Содержание**	18	ОК 1-11. ПК 11.6 ЛР1-ЛР3
	1.Понятие организационно-правовой защиты информации 2.Основные регламентирующие документы по защите информации 3. Обзор стандартов в области информационной безопасности	4	
	Практическое занятие 1. Анализ Доктрины информационной безопасности Российской Федерации. 2. Анализ Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации». 3. Анализ Федерального закона № 152-ФЗ «О персональных данных». 4. Анализ Федерального закона № 63-ФЗ «Об электронной подписи». 5. Анализ Федерального закона № 5485-1 «О государственной тайне». 6. Анализ Постановление правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».	12	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы	2	

Тема 5. Административный уровень информационной безопасности	**Содержание**	10	ОК 1-11. ПК 4.4, ПК.11.6 ЛР1-ЛР3
	1. Политика безопасности 2. Программа безопасности 3. Синхронизация программы безопасности с жизненным циклом системы 4.Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушение безопасности, планирование восстановительных работ	6	
	Практическое занятие 1. Построение концепции информационной безопасности предприятия 2. Процедурный уровень защиты организации в области информационной безопасности	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	2	
Тема 6. Основные программно-технические меры	**Содержание**	6	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1. Понятие программной, аппаратной и технической защиты информации 2. Методы аппаратной, программной и технической защиты информации	2	
	Практическое занятие 1. Разработка модели защиты 2. Выбор основных механизмов и средств обеспечения безопасности информации	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	1	
Тема 7. Традиционные симметричные криптосистемы.	**Содержание**	10	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1. Понятие шифра. История возникновения и примеры простейших шифров. Отличие шифра от кода, понятие ключа. 2 . Шифры перестановки: шифрующие таблицы, применение магических квадратов. 3.Шифры простой замены: система шифрования Цезаря; аффинная система подстановок Цезаря; система Цезаря с ключевым словом; шифрующие таблицы Трисемуса; биграммный шифр Плейфера; криптосистема Хилла. 4.Шифры сложной замены: система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама	6	
	Практическое занятие 1. Шифр Цезаря 2. Шифр Виженера	4	
	Самостоятельная работа:	2	

	Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.		
Тема 8. Современные симметричные криптосистемы.	**Содержание**	8	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1.Американский стандарт шифрования DES. Режимы работы DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру»; «Обратная связь по выходу». Области применения алгоритма DES. Комбинирование блочных алгоритмов. 2. Отечественный стандарт шифрования данных ГОСТ 28147-89. Режимы работы: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.	4	
	Практическое занятие 1. Шифр DES 2. Шифр ГОСТ Р 28147-89	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	1	
Тема 9. Асимметричные криптосистемы.	**Содержание**	8	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1.Концепция и структура криптосистем с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA: процедуры шифрования и расшифрования, быстродействие и безопасность. 2.Комбинированный метод шифрования 3. Протокол обмена ключами Диффи-Хеллмана	6	
	Практическое занятие 1. Шифр RSA	2	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	2	
Тема 10. Аутентификация, авторизация и администрирование действий пользователя	**Содержание**	8	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1. Понятие идентификации, аутентификации и авторизации. Виды аутентификации. Понятие администрирования действий пользователя. 2. Основные атаки на протоколы аутентификации.	4	
	Практическое занятие 1.Использование программного продукта Dallas Lock, реализующего защиту от НСД, аутентификацию и авторизацию.	4	

	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	1	
Тема 11. Методы аутентификации, использующие пароли	**Содержание**	8	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1. Аутентификации на основе многоразовых паролей 2. Аутентификации на основе одноразовых паролей 3. Аутентификации на основе PIN-кода	4	
	Практическое занятие 1. Администрирование Windows	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	2	
Тема 12. Электронная цифровая подпись.	**Содержание**	8	ОК 1-11. ПК 4.4 ЛР1-ЛР3
	1.Проблемы аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. 2.Алгоритмы электронной цифровой подписи. Алгоритм электронной цифровой подписи RSA. Отечественный стандарт хэш-функции. Отечественный стандарт цифровой подписи	4	
	Практическое занятие 1. Работа с системой PGP 2. Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя	4	
	Самостоятельная работа: Систематическая проработка конспектов занятий, учебной и специальной технической литературы, подготовка к зачету.	2	
	Экзамен	**2**	
Всего		**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение:
Реализация программы дисциплины требует наличия лабораторий системного и прикладного программирования, инфокоммуникационных систем.
Технические средства обучения:
компьютеры, проектор, комплект учебно-методической документации.
Оборудование учебного кабинета:
посадочные места по количеству обучающихся;
рабочее место преподавателя;
учебно-наглядные пособия.
Технические средства обучения:
программное обеспечение общего и профессионального назначения: Notepad, браузеры Internet Explorer, Mozilla Firefox, Google Chrome, Apache HTTP Server, PHP, MySQL, Virtual Box с ОС Ubuntu Linux.

3.2.Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Обязательные печатные издания

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — М. : Издательство Юрайт, 2019. — 321 с.

2. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2018.

Дополнительные печатные издания *(можно указать):*

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ, 2020.-236с.

2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком, 2018. - 544 с.: ил. Допущено УМО ИБ.

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2020.

4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2019.

5. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.

6. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2019.

7. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2020.

8. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. –М.: Академия. 2019.

9. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2018.

10. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2020.

3.2.3. Информационные ресурсы:

1. http://www.intuit.ru
2. http://habrahabr.ru/blogs/programming/
3. http://phpclub.ru/
4. http://www.webscript.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения аудиторных занятий, в т. ч. практических занятий, тестирования и т.д., а также в процессе выполнения обучающимися индивидуальных и самостоятельных заданий.

Результаты обучения	Критерии оценки	Методы оценки
1.Знание типов каналов утечки информации. 2.Знание аппаратных угроз целостности информации. 3.Знание программных угроз безопасности информации. 4.Знание модели безопасности. 5. Знание систем и средств парольной защиты. 6. Знание аппаратных средств защиты информации. 7. Знание программных технологий защиты информации.	Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не	устный опрос тестирование выполнение индивидуальных заданий различной сложности оценка ответов в ходе эвристической беседы, оценка докладов по тематике подготовка презентаций
1.Умение распознавать отклонения от нормального режима работы информационных систем и принимать меры по конкретному диагностированию причин отклонений. 2.Умение использовать средства устранения разрушающих программных воздействий. 3.Умение использовать прокси-серверы. 4.Умение использовать стандартные средства защиты информации шифрованием, в особенности, встроенные в современные операционные платформы. 5. Умение применять эффективные средства администрирования, повышающие защищенность системы. 6.Умение выбирать		

антивирусные программы, соответствующие природе вероятных разрушающих программных воздействий. 7.Умение грамотно взаимодействовать с администратором системы и использовать средства программно-аппаратной защиты.	сформированы, выполненные учебные задания содержат грубые ошибки.	