Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пономарева Светлана Викторовна
Должность: Проректор по УР и НО
Дата подписания: 20.09.2023 20:28:09
Уникальный программный ключ:
bb52f959411e64617366ef2977b97e87139a1a2b

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)

УТВЕРЖДАЮ
Директор АТК

_____ В.А. Зибров

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за	**Авиационно-технологический колледж**
Учебный план	09.02.07-2022-2-ИСП9.plx Информационные системы и программирование Профиль получаемого профессионального образования при реализации программы среднего общего образования: Технологический
Квалификация	**Программист**
Форма обучения	**очная**
Общая трудоемкость	**0 ЗЕТ**

Часов по учебному плану	70	Формы контроля в семестрах:
в том числе:		зачеты с оценкой 3
аудиторные занятия	64	
самостоятельная работа	6	

2022 г.

Распределение часов дисциплины по семестрам

Семестр	3		Итого	
Недель	16 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	44	44	44	44
Практические	20	20	20	20
Итого ауд.	64	64	64	64
Сам. работа	6	6	6	6
Итого	70	70	70	70

2022 г.

Программу составил(и):

Меркулов Владимир Анатольевич _____

Рецензент(ы):

_____

Рабочая программа дисциплины (модуля)

Информационная безопасность

разработана в соответствии с ФГОС СПО:

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.07 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОГРАММИРОВАНИЕ (приказ Минобрнауки России от 09.12.2016 г. № 1547)

составлена на основании учебного плана:

Информационные системы и программирование
Профиль получаемого профессионального образования при реализации программы среднего общего образования: Технологический

утвержденного Учёным советом университета от

Рабочая программа одобрена на заседании ЦК

Авиационно-технологический колледж

Протокол от №
Срок действия программы: уч.г.

личная подпись инициалы, фамилия

1. ОБЛАСТЬ ПРИМЕНЕНИЯ РАБОЧЕЙ ПРОГРАММЫ	
1.1	Является прочное и сознательное овладение студентами знаниями и умениями работы с прикладными программами, применением информационных технологий, которые необходимы современному специалисту для осуществления профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	ОП.13
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Операционные системы и среды
2.1.2	Основы алгоритмизации и программирования
2.1.3	Информационные технологии / Адаптивные информационные и коммуникационные технологии
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Внедрение и поддержка компьютерных систем
2.2.2	Обеспечение качества функционирования компьютерных систем
2.2.3	Веб-программирование
2.2.4	Разработка программных модулей
2.2.5	Поддержка и тестирование программных модулей
2.2.6	Разработка мобильных приложений
2.2.7	Системное программирование
2.2.8	Экзамен по модулю
2.2.9	Учебная практика

3. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ) - ТРЕБОВАНИЯ К РЕЗУЛЬТАТУ ОСВОЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
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 05.: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09.: Использовать информационные технологии в профессиональной деятельности.
ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 11.6.: Защищать информацию в базе данных с использованием технологии защиты информации.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	источники возникновения информационных угроз;
3.1.2	контроль выполнения практических заданий,
3.1.3	устный опрос, контроль самостоятельной работы, тестирование;
3.1.4	модели и принципы защиты информации от несанкционированного доступа;
3.1.5	методы антивирусной защиты информации
3.2	**Уметь:**
3.2.1	применять правовые, организационные, технические и программные средства защиты информации;
3.2.2	устный опрос, контроль выполнения практических заданий, контроль самостоятельной работы, тестирование;
3.2.3	создавать программные средства защиты информации
3.2.4	

4 . ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Актив и Интеракт.	Примечание
	Раздел 1. Концепция информационной безопасности						

1.1	Национальные интересы РФ в информационной сфере /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
1.2	Законодательство в области лицензирования и сертификации /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
1.3	Информационные стандарты информационного обмена /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 2. Угрозы безопасности информационных систем						
2.1	Характеристика составляющих и основные термины и определения информационной безопасности. Основные понятия информационной безопасности в локальных сетях /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
2.2	Защита информации передаваемой по локальным сетям /Пр/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
2.3	Основные подходы к классификации угроз информационной безопасности. Информационные, программно-математические, физические и организационные угрозы /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации						
3.1	Модели и основные принципы защиты информации от несанкционированного доступа /Лек/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
3.2	Защита информации от копирования: задание некопируемых меток /Пр/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
3.3	Защита информации в глобальной сети /Ср/	3	1	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
3.4	Проблемы идентификации и аутентификации пользователей. Методы аутентификации и их основные характеристики /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
3.5	Программно-аппаратная защита информации от локального несанкционированного доступа. Защита информации от несанкционированного доступа в операционных системах /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 4. Проблема вирусного заражения программ						
4.1	Структуры современных антивирусных программ. Классификация антивирусных программ /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
4.2	Инсталляция и настройка антивирусных программ /Пр/	3	4	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
4.3	Структура и классификация современных вредоносных программ. Методы обнаружения и удаления вирусов /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		

4.4	Обнаружение современных вредоносных программ /Пр/	3	6	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
4.5	Настройка и обновление баз антивирусных программ /Ср/	3	1	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 5. Защита от утечки информации по техническим каналам						
5.1	Прямые и косвенные каналы утечки информации. Каналы и методы несанкционированного доступа к конфиденциальной информации /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
5.2	Понятие канала несанкционированного доступа к защищаемой информации. Классификацию типов каналов несанкционированного доступа к защищаемой информации /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
5.3	Каналы несанкционированного доступа к защищаемой информации с доступом злоумышленника и без доступа злоумышленника. Каналы несанкционированного доступа к защищаемой информации с изменением информации и без изменения информации /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
5.4	Криптографические средства, обеспечивающие шифрование конфиденциальных данных. Организация доступа к конфиденциальной информации через промежуточные терминальные серверы. Системы активного мониторинга /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
5.5	Методы шифрование конфиденциальных данных /Пр/	3	6	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
5.6	Спецпрограммные комплексы, предназначенные для выявления несанкционированных действий пользователей /Ср/	3	1	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 6. Организационно-правовое обеспечение информационной безопасности						
6.1	Служба безопасности объекта. Права и обязанности сотрудников службы безопасности /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
6.2	Защита коммерческой тайны и интеллектуальной собственности /Лек/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
6.3	Методы защиты конфиденциальной информации /Ср/	3	1	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		
	Раздел 7. Промежуточная аттестация						
7.1	Промежуточная аттестация /ЗачётСОц/	3	2	ПК 11.6.	Л1.1 Л1.2Л2.1 Л2.2		

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Государственное регулирование информационной безопасности.
22. Деятельность международных организаций в сфере информационной безопасности.
23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
24. Доктрина информационной безопасности России.
25. Уголовно-правовой контроль над компьютерной преступностью в России.
26. Федеральные законы по ИБ в РФ.
27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.
29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.
31. Организация конфиденциального делопроизводства.
32. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Организационно-правовой статус службы безопасности.
35. Защита информации в Интернете.
36. Электронная почта и ее защита.
37. Защита от компьютерных вирусов.
38. «Больные» мобильники и их «лечение».
39. Популярные антивирусные программы и их классификация.
40. Организация системы защиты информации экономических объектов.
41. Криптографические методы защиты информации.
42. Этапы построения системы защиты информации.
43. Оценка эффективности инвестиций в информационную безопасность.
44. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
45. Управление информационной безопасности на государственном уровне.
46. Аудит ИБ автоматизированных банковских систем.
47. Электронная коммерция и ее защита.
48. Менеджмент и аудит информационной безопасности на уровне предприятия.
49. Информационная безопасность предпринимательской деятельности.
50. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

5.2. Темы письменных работ

5.3. Перечень видов оценочных средств

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Озерский Сергей Владимирович, Попов Игорь Владимирович, Самарский юридический институт Федеральной службы исполнения наказаний; Владимирский юридический институт Федеральной службы исполнения наказаний; Сибирский юридический университет	Информационная безопасность: Учебное пособие	Самара: Самарский юридический институт ФСИН России, 2019
Л1.2	Партыка Татьяна Леонидовна, Попов Игорь Иванович, Российский государственный гуманитарный университет; Российский экономический университет им. Г.В. Плеханова	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2021

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Баранова Елена Константиновна, Бабаш Александр Владимирович	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИОР, 2019
Л2.2	Нестеров Сергей Александрович, С. А. Нестеров	Информационная безопасность: Учебник и практикум	Москва: Издательство Юрайт, 2019

6.3.1 Перечень программного обеспечения

6.3.1.1	Mathworks (в составе: MATLAB (MathWorks SMS- Software Maintenance Service), Simulink, Control System Toolbox, Neural Network Toolbox, Fuzzy Logic Toolbox, Optimization Toolbox, Partial Differential Equation Toolbox, Signal Processing Toolbox, Simscape Multibody, Simscape, Symbolic Math Toolbox, Statistics and Machine Learning Toolbox, System Identification Toolbox

6.3.2 Перечень информационных справочных систем

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Реализация программы дисциплины требует наличия лаборатории «Программного обеспечения и сопровождения компьютерных систем»:
7.2	- Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;) или аналоги;
7.3	- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;)или аналоги;
7.4	- Проектор и экран;
7.5	- Маркерная доска;
7.6	- Программное обеспечение общего и профессионального назначения

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
(См.Приложение)