АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ СОЦИАЛЬНЫЙ ИНСТИТУТ»

Утверждаю
Декан ФИСТ
_____ Ж.В. Игнатенко
«20» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки: 09.02.07 Информационные системы и программирование

Квалификация выпускника: Разработчик веб и мультимедийных приложений

Форма обучения: очная

Год начала подготовки – 2024

Разработана
Канд. техн. наук, доцент, доцент
_____С.В. Аникуев

Согласована
Зав. кафедрой ПИМ
_____ Д.Г. Ловянников

Рекомендована
на заседании кафедры ИС
от «17» мая 2024 г.
протокол № 9
Зав. кафедрой _____ А.Ю. Орлова

Одобрена
на заседании учебно-методической
комиссии факультета ФИСТ
от «20» мая 2024 г.
протокол № 9
Председатель УМК _____ Ж.В. Игнатенко

Ставрополь, 2024 г.

Федоровский Александр Петрович
2024.05.29 22:39:47+03'00'

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями изучения дисциплины «Информационная безопасность» являются:

–получение теоретических знаний поосновам информационной безопасностив сфере профессиональной деятельности обучаемых;

– приобретение умений и навыков по их применению на практике;

– формирование у обучаемых необходимых компетенций.

Задачами изучениядисциплины «Информационная безопасность» являются:

– умение анализировать, выделять составные части и описывать значимость решения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– умение анализировать риски и применять актуальные методы защиты программного обеспечения компьютерных систем в соответствии с нормативно-правовой документацией;

– умение оценивать результат и последствия своих действий по защите компьютерных систем программными и аппаратными средствами;

– умение грамотно излагать свои мысли при оформлении документов по защите компьютерных систем программными и аппаратными средствами;

– усвоение значимостирешения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– усвоение основных актуальных средств и методов защиты компьютерных систем программными и аппаратными средствами в соответствии с нормативно-правовой документацией;

– усвоение современной научной и профессиональной терминологии и возможных траекторий профессионального развития и самообразования по вопросам защиты компьютерных систем программными и аппаратными средствами;

– усвоение правил оформления документов и построения устных сообщений по вопросам защиты компьютерных систем программными и аппаратными средствами;

– усвоение психологических основ деятельности коллектива и особенностей личности при решении задач защиты компьютерных систем программными и аппаратными средствами;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность»относится к вариативной части общепрофессионального цикла ОПОП (ОП.В.4) и находится в логической и содержательно-методической связи с другими дисциплинами.

Предшествующие дисциплины (курсы, модули, практики)	Последующие дисциплины (курсы, модули, практики)
Компьютерные сети Информатика Информационные технологии	Стандартизация, сертификация и техническое документоведение Администрирование информационных систем Производственная практика (преддипломная)

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций по данной специальности:

Код и наименование компетенции	Результаты обучения

ОК01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности ОК03. Планировать и реализовывать собственное профессиональное и личностное развитие. ОК04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. ОК05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. ОК06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. ДПК 1.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами. ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием. ПК 9.8. Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности.	**знать:** – Назначение и виды информационных технологий, технологии сбора, накопления, обработки, передачи и распространения информации. – Состав, структуру, принципы реализации и функционирования информационных технологий. – Базовые и прикладные информационные технологии – Инструментальные средства информационных технологий. **уметь:** – Обрабатывать текстовую и числовую информацию. – Применять мультимедийные технологии обработки и представления информации. – Обрабатывать экономическую и статистическую информацию, используя средства пакета прикладных программ.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общий объем дисциплины составляет 82 часа.

Вид учебной работы	Всего часов	Семестр
		4*(6**)
Аудиторные занятия (работа обучающихся во взаимодействии с преподавателем) (всего)	**62**	**62**
в том числе:		
Лекции (Л)	30	30
Практические занятия (ПЗ)	30	30
Семинары (С)		
Лабораторные работы (ЛР)		
Консультация	2	2

Самостоятельная работа (всего) (СР)	**4**	**4**
в том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Контрольная работа		
Реферат	4	4
Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям)		
Промежуточная аттестация	**16**	**16**
Вид промежуточной аттестации (экзамен)	экзамен	экзамен
Общий объем, час	**82**	**82**

* на базе среднего общего образования

** на базе основного общего образования

5. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

5.1. Содержание дисциплины

№ раздела (темы)	Наименование раздела (темы)	Содержание раздела (темы)
1.	Борьба с угрозами несанкционированного доступа к информации	
1.1	Актуальность проблемы обеспечения безопасности информации	История возникновения проблемы защиты информации. Причины утечки и искажения информации. Требования, предъявляемые к уровню обеспечения информационной безопасности. Надёжность и уязвимость информации в информационных системах.
1.2	Виды мер обеспечения информационной безопасности (ИБ)	Технические меры обеспечения ИБ. Программно-математические меры обеспечения ИБ. Разграничение доступа к защищаемой информации. Административные меры обеспечения ИБ. Законодательные и морально-этические меры обеспечения ИБ. Криптографические методы обеспечения ИБ. Контроль доступа к аппаратуре.
1.3	Основные принципы построения систем защиты информации	Использование простого и динамически изменяющегося пароля. Особенности защиты информации в персональных компьютерах(ПК). Идентификация и аутентификация пользователей в информационных системах. Защита ПК от несанкционированного доступа. Регистрация всех обращений к защищаемой информации.
2.	Борьба с вирусным заражением информации	
2.1	Проблемы вирусного заражения. Разновидности и структура современных компьютерных вирусов.	Компьютерный вирус. Понятия и пути распространения вирусов. Основные способы заражения программ. Основные классы вирусов. Программные и аппаратные закладки. Классификация закладок и их общие характеристики.

		Саморазмножающиеся и другие разновидности закладок. Троянский конь. Структура и способы распространения. Временная и логическая бомба. Структура и способы распространения. Винлокер. Структура и способы распространения. Червь. Структура и способы распространения. Признаки проявления вредоносных программ.
2.2	Угрозы для мобильных устройств	Классификация угроз для мобильных устройств. Характеристика вредоносных программы для мобильных устройств. Программы-вымогатели для мобильных устройств. Вредоносные приложения.
2.3	Методы защиты от вредоносных программ.	Методики оценки рисков в сфере информационной безопасности. Своевременная компьютерная профилактика. Обязательное использование антивирусной защиты. Физическое отключение внутренней сети организации от Интернета и использование для выхода в Интернет выделенных компьютеров.
2.4	Средства защиты от вредоносных программ.	Классификацияантивирусных программ. Программы-детекторы, программы-ревизоры и фильтры. Программы-полифаги (доктора). Профилактика заражения вирусом. Антивирус Касперского.
2.5	Защита мобильных устройств	Основы безопасности мобильных устройств. Методы защиты мобильных устройств от киберугроз. Специальная программа – «сканер». Проверка в режиме «налету».
2.6	Оценка потерь от реализации потенциальных угроз и затрат на защиту информации	Проверка соответствия уровня защищенности ИС требованиям стандартов в области ИБ. Программное обеспечение для оценки рисков информационной безопасности. Оценка рисков по графику соотношения – «затраты на защиту — ожидаемые потери».Идентификация риска. Модель безопасности с полным перекрытием.
3.	Организационно-правовое обеспечение информационной безопасности	
3.1	Основы теории правового обеспечения информационной безопасности.	Содержание и структура правового обеспечения. Законодательство об информации, информационных технологиях и о защите информации. Правовой режим информации. Правовой статус обладателя информации. Правовой режим информационных технологий. Государственное регулирование отношений в сфере защиты информации.
3.2	Федеральная нормативная база обеспечения информационной безопасности.	Основные нормативно-правовые акты и методические документы в области защиты информации. Основные общие нормативные правовые акты. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных. Руководящие документы и методические указания в сфере защиты информации.
3.3	Защита персональных	Персональные данных, их классификация.

	данных.	Правовые основы использования персональных данных. Принципы обработки персональных данных. Создание и оценка соответствия информационной системы персональных данных. Права субъектов персональных данных. Обязанности оператора при обработке персональных данных. Электронная цифровая подпись.

5.2. Структура дисциплины

№ раздела (темы)	Наименование раздела (темы)	Количество часов				
		Всего	Л	ПЗ (С)	ЛР	СР
1.1	Актуальность проблемы обеспечения безопасности информации	4	2	2	-	-
1.2	Виды мер обеспечения информационной безопасности (ИБ)	8	4	4	-	-
1.3	Основные принципы построения систем защиты информации	4	2	2	-	-
2.1	Проблемывирусного заражения. Разновидности и структура современных компьютерных вирусов.	8	4	4	-	-
2.2	Угрозы для мобильных устройств	4	2	2	-	-
2.3	Методы защиты от вредоносных программ.	4	2	2	-	-
2.4	Средства защиты от вредоносных программ.	6	2	4	-	-
2.5	Защита мобильных устройств	4	2	2	-	-
2.6	Оценка потерь от реализации потенциальных угроз и затрат на защиту информации	6	4	2	-	-
3.1	Основы теории правового обеспечения информационной безопасности.	6	2	2	-	2
3.2	Федеральная нормативная база обеспечения информационной безопасности.	4	2	2	-	
3.3	Защита персональных данных.	6	2	2	-	2
	Консультация	2	-	-	-	
	Промежуточная аттестация	16	-	-	-	
	Общий объем, час	**82**	**30**	**30**	-	**4**

5.3. Практические занятия и семинары

№ п/п	№ раздела (темы)	Вид (ПЗ, С)	Тема	Количество часов
1	1.1	ПЗ	Актуальность проблемы обеспечения безопасности информации	2
2	1.2	ПЗ	Виды мер обеспечения информационной безопасности (ИБ)	4
3	1.3	ПЗ	Основные принципы построения систем защиты информации	2

4	2.1	ПЗ	Проблемывирусного заражения. Разновидности и структура современных компьютерных вирусов.	4
5	2.2	ПЗ	Угрозы для мобильных устройств	2
6	2.3	ПЗ	Методы защиты от вредоносных программ.	2
7	2.4	ПЗ	Средства защиты от вредоносных программ.	4
8	2.5	ПЗ	Защита мобильных устройств	2
9	2.6	ПЗ	Оценка потерь от реализации потенциальных угроз и затрат на защиту информации	2
10	3.1	ПЗ	Основы теории правового обеспечения информационной безопасности.	2
11	3.2	ПЗ	Федеральная нормативная база обеспечения информационной безопасности.	2
12	3.3	ПЗ	Защита персональных данных.	2

5.4. Лабораторные работы

Не предусмотрены

5.5. Самостоятельное изучение разделов (тем) дисциплины

№ раздела (темы)	Вопросы, выносимые на самостоятельное изучение	Количество часов
3.1	Основы теории правового обеспечения информационной безопасности.	2
3.3	Защита персональных данных.	2
	Промежуточная аттестация	16

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Информационные технологии, используемые при осуществлении образовательного Основные технологии обучения:

– работа с информацией, в том числе с использованием ресурсов сети Интернет;

– подготовка и реализация проектов (мультимедийных презентаций и пр.) по заранее заданной теме;

– исследование конкретной темы и оформление результатов в виде доклада с презентацией;

– работа с текстами учебника, дополнительной литературой;

– выполнение индивидуальных заданий.

Информационные технологии:

– сбор, хранение, систематизация, обработка и представление учебной и научной информации;

– обработка различного рода информации с применением современных информационных технологий;

– самостоятельный поиск дополнительного учебного и научного материала, с использованием поисковых систем и сайтов сети Интернет, электронных энциклопедий и баз данных;

– использование электронной почты преподавателей и обучающихся для рассылки, переписки и обсуждения возникших учебных проблем;

– использование дистанционных образовательных технологий (при необходимости)

Активные и интерактивные образовательные технологии, используемые в аудиторных занятиях

№ раздела (темы)	Вид занятия (Л, ПЗ, С, ЛР)	Используемые активные и интерактивные образовательные технологии	Количество часов
1.2	Л	Лекция-визуализация	2
2.1	ПЗ	Анализ конкретных ситуаций	4
2.4	Л	Проблемное обучение	2
2.6	Л	Проблемное обучение	4
2.4	ПЗ	Анализ конкретных ситуаций	4
2.6	ПЗ	Анализ конкретных ситуаций	2
3.3	Л	Проблемное обучение	2

Практическая подготовка обучающихся

№ раздела (темы)	Вид занятия (ЛК, ПР, ЛР)	Виды работ	Количество часов
-	-	-	-

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Типовые задания для текущего контроля.

Перечень типовых контрольных вопросов для устного опроса

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности.
4. Надёжность и уязвимость информации в информационных системах.
5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).
14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус. Понятия и пути распространения вирусов.

18. Основные способы заражения программ.
19. Основные классы вирусов.
20. Программные и аппаратные закладки.
21. Классификация закладок и их общие характеристики.
22. Саморазмножающиеся и другие разновидности закладок.
23. Троянский конь.
24. Структура и способы распространения.
25. Временная и логическая бомба. Структура и способы распространения.
26. Винлокер. Структура и способы распространения.
27. Червь. Структура и способы распространения.
28. Признаки проявления вредоносных программ.
29. Классификация угроз для мобильных устройств.
30. Характеристика вредоносных программы для мобильных устройств.
31. Программы-вымогатели для мобильных устройств.
32. Вредоносные приложения.
33. Методики оценки рисков в сфере информационной безопасности.
34. Своевременная компьютерная профилактика.
35. Обязательное использование антивирусной защиты.
36. Физическое отключение внутренней сети организации от Интернета и использование для выхода в Интернет выделенных компьютеров.
37. Классификация антивирусных программ.
38. Программы-детекторы, программы-ревизоры и фильтры.
39. Программы-полифаги (доктора).
40. Профилактика заражения вирусом.
41. Антивирус Касперского.
42. Основы безопасности мобильных устройств.
43. Методы защиты мобильных устройств от киберугроз.
44. Специальная программа – «сканер».
45. Проверка в режиме «налету».
46. Проверка соответствия уровня защищенности ИС требованиям стандартов в области ИБ.
47. Программное обеспечение для оценки рисков информационной безопасности.
48. Оценка рисков по графику соотношения – «затраты на защиту — ожидаемые потери». Идентификация риска.
49. Модель безопасности с полным перекрытием.
50. Содержание и структура правового обеспечения.
51. Законодательство об информации, информационных технологиях и о защите информации.
52. Правовой режим информации.
53. Правовой статус обладателя информации.
54. Правовой режим информационных технологий.
55. Государственное регулирование отношений в сфере защиты информации.
56. Основные нормативно-правовые акты и методические документы в области защиты информации.
57. Основные общие нормативные правовые акты.
58. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
59. Руководящие документы и методические указания в сфере защиты информации.
60. Персональные данных, их классификация.
61. Правовые основы использования персональных данных.
62. Принципы обработки персональных данных.

63. Создание и оценка соответствия информационной системы персональных данных.

64. Права субъектов персональных данных.

65. Обязанности оператора при обработке персональных данных.

66. Электронная цифровая подпись.

Типовые тестовые задания

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

В) нет правильного ответа

2.Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

1. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

2. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

3. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

4. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации
В) все ответы правильные

5. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

6. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

7. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

8. Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

9. Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

10. Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

11. Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

12. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

13. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

14. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

15. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

20. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

21. Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

22. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

23. Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

24. Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

25. Конфиденциальную информацию можно разделить:

А) предметную
Б) служебную
В) глобальную

26. Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

27. Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

28. К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

29. Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

30. Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

31. Ошибка – это…
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

32. Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

33. Побочное влияние – это…
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

34. СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

35. Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация
В) программное обеспечение

36. По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

37. По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

38. Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

39. Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные
40. Информацию с ограниченным доступом делят:
А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

41. Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

42. Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

43. Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

44. К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

45. Что относится к организационным мероприятиям:
А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

46. Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) аппаратные
Б) криптографические
В) физические

47. Программные средства – это…
А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

48.. Криптографические средства – это…
А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

7.2 Контрольно-оценочные материалы для итоговой аттестации по дисциплине

1. История возникновения проблемы защиты информации.
2. Причины утечки и искажения информации.
3. Требования, предъявляемые к уровню обеспечения информационной безопасности (ИБ).
4. Надёжность и уязвимость информации в информационных системах.
5. Технические меры обеспечения ИБ.
6. Программно-математические меры обеспечения ИБ.
7. Разграничение доступа к защищаемой информации.
8. Административные меры обеспечения ИБ.
9. Законодательные и морально-этические меры обеспечения ИБ.
10. Криптографические методы обеспечения ИБ.
11. Контроль доступа к аппаратуре.
12. Использование простого и динамически изменяющегося пароля.
13. Особенности защиты информации в персональных компьютерах (ПК).

14. Идентификация и аутентификация пользователей в информационных системах.
15. Защита ПК от несанкционированного доступа.
16. Регистрация всех обращений к защищаемой информации.
17. Компьютерный вирус. Понятия и пути распространения вирусов.
18. Основные способы заражения программ.
19. Основные классы вирусов.
20. Классификация закладок и их общие характеристики.
21. Саморазмножающиеся и другие разновидности закладок.
22. Троянский конь. Структура и способы распространения.
23. Временная и логическая бомба. Структура и способы распространения.
24. Винлокер. Структура и способы распространения.
25. Червь. Структура и способы распространения.
26. Признаки проявления вредоносных программ.
27. Классификация угроз для мобильных устройств.
28. Характеристика вредоносных программы для мобильных устройств.
29. Программы-вымогатели для мобильных устройств.
30. Методики оценки рисков в сфере информационной безопасности.
31. Своевременная компьютерная профилактика от вирусов.
32. Использование антивирусной защиты.
33. Классификация антивирусных программ.
34. Основы безопасности мобильных устройств.
35. Методы защиты мобильных устройств от киберугроз.
36. Программное обеспечение для оценки рисков информационной безопасности.
37. Содержание и структура правового обеспечения информационной безопасности.
38. Государственное регулирование отношений в сфере защиты информации.
39. Основные нормативно-правовые акты и методические документы в области защиты информации.
40. Основные общие нормативные правовые акты по вопросам информационной безопасности.
41. Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
42. Персональные данных, их классификация.
43. Принципы обработки персональных данных.
44. Создание и оценка соответствия информационной системы персональных данных.
45. Права субъектов персональных данных.
46. Обязанности оператора при обработке персональных данных.
47. Электронная цифровая подпись.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература

1. Баранова, Е. К. Основы информационной безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860126
2. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873

3. *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, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

8.2. Дополнительная литература

1. Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2024. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2138953. Режим доступа: по подписке.
2. *Богатырев, В. А.* Информационные системы и технологии. Теория надежности : учебное пособие для вузов / *В. А. Богатырев. — 2-е изд. — Москва :* Издательство Юрайт, 2024. — 366 с. — (Высшее образование). — ISBN 978-5-534-15951-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510320
3. *Богатырев, В. А.* Надежность информационных систем : учебное пособие для среднего профессионального образования / В. А. Богатырев. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 366 с. — (Профессиональное образование). — ISBN 978-5-534-18930-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/555113
4. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543631

8.3. Программноеобеспечение

Microsoft Office Professional Plus 2019

8.4. Базы данных, информационно-справочные и поисковые системы, Интернет-ресурсы

Базы данных (профессиональные базы данных)

–База данных IT специалиста – http://info-comp.ru/

Информационно-справочные системы

–Справочно-правовая система «КонсультантПлюс» –http://www.consultant.ru/

Поисковые системы

- Яндекс–https://www.yandex.ru/
- Rambler– https://www.rambler.ru/
- Google–https://google.com/

Электронные образовательные ресурсы

–Корпорация Майкрософт в сфере образования – https://www.microsoft.com/ru-ru/education/default.aspx

- Цифровой образовательный ресурс IPR SMART – https://www.iprbookshop.ru/

9.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины необходимо следующее материально-техническое обеспечение:

– для проведения лекций, уроков – аудитория, укомплектованная оборудованием и техническими средствами обучения: учебная мебель, экран, проектор, компьютер, расходный материал;

– для проведения всех видов практических занятий – компьютерный класс с лицензионным программным обеспечением, укомплектованный оборудованием и техническими средствами обучения: учебная мебель, экран, проектор, компьютеры (с лицензионным программным обеспечением), расходный материал;

– для текущего контроля и промежуточной аттестации – компьютерный класс с лицензионным программным обеспечением, укомплектованный оборудованием и техническими средствами обучения: учебная мебель, экран, проектор, компьютеры (с лицензионным программным обеспечением), расходный материал;

– для проведения индивидуальных и групповых консультаций – компьютерный класс с лицензионным программным обеспечением, укомплектованный оборудованием и техническими средствами обучения: учебная мебель, экран, проектор, компьютеры (с лицензионным программным обеспечением), расходный материал;

– для организации самостоятельной работы – помещение, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Института.

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (тьютора), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков..

В целях доступности получения среднего профессионального образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

– присутствие тьютора, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

– специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

– индивидуальное равномерное освещение не менее 300 люкс,

– при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

– присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

– обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

– обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются тьютору;

– по желанию студента задания могут выполняться в устной форме.

Программа составлена в соответствии с требованиями ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование».