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

Утверждаю
Декан ФИСТ
_____ Ж.В. Игнатенко
«11» ____10____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки: 09.02.07 Информационные системы и программирование

Квалификация выпускника: Программист

Форма обучения: очная

Год начала подготовки – 2022

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

Согласована
Зав. выпускающей кафедры ПИМ
_____ Ж.В. Игнатенко

Рекомендована
на заседании кафедры ИС
от «17» ____10____ 2022 г.
протокол № 3
Зав. кафедрой _____ А.Ю. Орлова

Одобрена
на заседании учебно-методической
комиссии факультета ФИСТ
от «18» ____10____ 2022 г.
протокол № 3
Председатель УМК _____ Ж.В. Игнатенко

Ставрополь, 2022 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями изучения дисциплины «Информационная безопасность» являются:

– получение теоретических знаний по основам информационной безопасности в сфере профессиональной деятельности обучаемых;

– приобретение умений и навыков по их применению на практике;

– формирование у обучаемых необходимых компетенций.

Задачами изучения дисциплины «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 значимости решения 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 ООП (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)

Требования к входным знаниям, умениям и компетенциям студента формируются на знаниях и умениях, предшествующих дисциплин:

уметь:

– подбирать и настраивать конфигурацию программного обеспечения компьютерных систем;

– проводить инсталляцию программного обеспечения компьютерных систем;

– производить настройку отдельных компонент программного обеспечения компьютерных систем;

– измерять и анализировать эксплуатационные характеристики качества программного обеспечения;

– осуществлять математическую и информационную постановку задач по обработке информации;

– использовать алгоритмы обработки информации для различных приложений;

– использовать языки структурного, объектно-ориентированного программирования и языка сценариев для создания независимых программ;

– разрабатывать графический интерфейс приложения;

– создавать проект по разработке приложения и формулировать его задачи;

– использовать методы тестирования в соответствии с техническим заданием;

– разрабатывать проектную документацию на эксплуатацию информационной системы;

– использовать стандарты при оформлении программной документации;

– использовать методы и критерии оценивания предметной области и методы определения стратегии развития бизнес-процессов организации;

– решать прикладные вопросы интеллектуальных систем с использованием статических экспертных систем, экспертных систем реального времени;

знать:

– основные методы и средства эффективного анализа функционирования программного обеспечения;

– основные виды работ на этапе сопровождения ПО;

– основные принципы контроля конфигурации и поддержки целостности конфигурации ПО.

– основные процессы управления проектом разработки;

– методы и средства проектирования, разработки и тестирования информационных систем;

– основные платформы для создания, исполнения и управления информационной системой;

– национальную и международную систему стандартизации и сертификации и систему обеспечения качества продукции, методы контроля качества;

– сервисно-ориентированные архитектуры;

– важность рассмотрения всех возможных вариантов и получения наилучшего решения на основе анализа и интересов клиента;

– основные понятия системного анализа;

– порядок файлового ввода-вывода;

– порядок создания сетевого сервера и сетевого клиента;

– платформы для создания, исполнения и управления информационной системой;

– особенности программных средств, используемых в разработке ИС;

– реинжиниринг бизнес-процессов;

– системы обеспечения качества продукции;

– методы контроля качества в соответствии со стандартами.

– основные этапы разработки программного обеспечения;

– основные принципы технологии структурного и объектно-ориентированного программирования;

– основные принципы отладки и тестирования программных продуктов;

– инструментарий отладки программных продуктов.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

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

а) общие (ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

б) профессиональные (ПК):

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

В результате освоения дисциплины студент должен:

уметь:

– описывать значимость решения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– анализировать и выделять составные части задач по защите программного обеспечения компьютерных систем;

– осуществлять поиск и использовать актуальные методы защиты программного обеспечения компьютерных систем в соответствии с нормативно-правовой документацией;

– анализировать риски и характеристики качества программного обеспечения;

– выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами;

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

– грамотно излагать свои мысли и оформлять документы по защите компьютерных систем программными и аппаратными средствами на государственном языке, проявлять толерантность в коллективе;

знать:

– значимость решения задач по защите программного обеспечения компьютерных систем в своей профессиональной деятельности;

– как и где осуществлять поиск основных источников информации и ресурсов для решения задач по защите программного обеспечения компьютерных систем;

– основные и актуальные средства защиты компьютерных систем программными и аппаратными средствами в соответствии с нормативно-правовой документацией;

– основные и актуальные методы защиты компьютерных систем программными и аппаратными средствами в соответствии с нормативно-правовой документацией;

– современную научную и профессиональную терминологию и возможные траектории профессионального развития и самообразования по вопросам защиты компьютерных систем программными и аппаратными средствами;

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

– психологические основы деятельности коллектива и особенности личности при решении задач защиты компьютерных систем программными и аппаратными средствами;

Практический опыт ФГОС СПО не предусмотрен

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.	Классификация антивирусных 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 данных.	Персональные данных, их классификация. 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	Проблемы вирусного 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	4	2	2	-	

	безопасности.					
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)	Тема	Количество часов
1	1.1	Актуальность проблемы обеспечения безопасности информации	2
2	1.2	Виды мер обеспечения информационной безопасности (ИБ)	4
3	1.3	Основные принципы построения систем защиты информации	2
4	2.1	Проблемы вирусного заражения. Разновидности и структура современных компьютерных вирусов.	4
5	2.2	Угрозы для мобильных устройств	2
6	2.3	Методы защиты от вредоносных программ.	2
7	2.4	Средства защиты от вредоносных программ.	4
8	2.5	Защита мобильных устройств	2
9	2.6	Оценка потерь от реализации потенциальных угроз и затрат на защиту информации	2
10	3.1	Основы теории правового обеспечения информационной безопасности.	2
11	3.2	Федеральная нормативная база обеспечения информационной безопасности.	2
12	3.3	Защита персональных данных.	2

5.4. Лабораторные работы

Не предусмотрены

5.5. Курсовой проект (курсовая работа, расчетно-графическая работа, реферат, контрольная работа)

Примерный перечень рефератов

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) Административные меры обеспечения ИБ.
6) Законодательные и морально-этические меры обеспечения ИБ.
7) Криптографические методы обеспечения ИБ.
8) Использование простого и динамически изменяющегося пароля.
9) Идентификация и аутентификация пользователей в информационных системах.
10) Защита ПК от несанкционированного доступа.

11) Компьютерный вирус. Понятия и пути распространения вирусов.
12) Основные способы заражения программ.
13) Признаки проявления вредоносных программ.
14) Классификация угроз для мобильных устройств.
15) Характеристика вредоносных программы для мобильных устройств.
16) Программы-вымогатели для мобильных устройств.
17) Вредоносные приложения.
18) Методики оценки рисков в сфере информационной безопасности.
19) Программы-детекторы, программы-ревизоры и фильтры.
20) Программы-полифаги (доктора).
21) Профилактика заражения вирусом.
22) Антивирус Касперского.
23) Основы безопасности мобильных устройств.
24) Методы защиты мобильных устройств от киберугроз.
25) Проверка соответствия уровня защищенности ИС требованиям стандартов в области ИБ.
26) Программное обеспечение для оценки рисков информационной безопасности.
27) Законодательство об информации, информационных технологиях и о защите информации.
28) Государственное регулирование отношений в сфере защиты информации.
29) Основные нормативно-правовые акты и методические документы в области защиты информации.
30) Основные нормативные правовые акты по вопросам безопасности информационных систем персональных данных.
31) Руководящие документы и методические указания в сфере защиты информации.
32) Правовые основы использования персональных данных.
33) Принципы обработки персональных данных.
34) Создание и оценка соответствия информационной системы персональных данных.
35) Права субъектов персональных данных.
36) Обязанности оператора при обработке персональных данных.
37) Электронная цифровая подпись.

5.6. 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

Основные технологии обучения:

– работа с правовой информацией, в том числе с использованием современных компьютерных технологий, ресурсов сети Интернет;
– работа с текстами учебника, дополнительной литературой;
– работа с таблицами, схемами;
– выполнение тестовых заданий по темам;
– участие в дискуссиях;
– работа с документами.

Информационные технологии:

– сбор, хранение, систематизация и выдача учебной информации;

– обработка текстовой и эмпирической информации;

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

– использование электронной информационной образовательной среды на сайте института;

– 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, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей ОПОП созданы комплекты оценочных материалов (фонды оценочных средств). В качестве оценочных материалов контроля знаний применяются: контрольные вопросы для устного опроса; задания для самостоятельной работы, примерные практические и лабораторные работы, образцы тестов, задания для контрольной работы, контрольные вопросы для промежуточной аттестации, позволяющие оценить знания, умения.

Образцы оценочных средств в виде контрольных вопросов, заданий, комплексных заданий, образцов тестов для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины, для контроля самостоятельной работы студента по отдельным разделам дисциплины, а также критерии оценки всех форм контроля, включая

промежуточный контроль по дисциплине, представлены в комплекте оценочных материалов.

Учебно-методическое обеспечение самостоятельной работы:

- методические указания к самостоятельной работе.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Основная литература

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

2. 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, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

8.2. Дополнительная литература

1. Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : Новосибирский государственный технический университет, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91329 . — ЭБС «IPRbooks».

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995 . — ЭБС «IPRbooks».

3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87992 . — ЭБС «IPRbooks».

4. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77317 . — ЭБС «IPRbooks».

5. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89451 . — ЭБС «IPRbooks».

6. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938 . — ЭБС «IPRbooks».

7. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 c. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/74381 . — ЭБС «IPRbooks».

8. Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 c. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/80747 . — ЭБС «IPRbooks».

8.3. Программное обеспечение

- Microsoft Windows;
- Microsoft Office.

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

Базы данных (профессиональные базы данных)

– База данных IT специалиста» [Электронный ресурс] – Режим доступа: http://info-comp.ru/

– База данных «Стратегическое управление и планирование» [Электронный ресурс] – Режим доступа: http://www.stplan.ru/

Информационно-справочные системы

– Информационно-справочная система для программистов [Электронный ресурс] – Режим доступа :http://life-prog.ru

– Справочно-правовая система «КонсультантПлюс» [Электронный ресурс] – Режим доступа http://www.consultant.ru/

Поисковые системы

– https://www.yandex.ru/
– https://www.rambler.ru/
– https://google.ru/

Интернет-ресурсы

– Электронная библиотечная система «IPRbooks» [Электронный ресурс] – Режим доступа :http://www.iprbookshop.ru

– Электронная библиотечная система «Юрайт» [Электронный ресурс] – Режим доступа: http://www.urait.ru

– Бесплатная электронная библиотека онлайн «Единое окно доступа к образовательным ресурсам» [Электронный ресурс] – Режим доступа: http://www.window.edu.ru

– Национальный открытый университет Интуит – интернет университет информационных технологий [Электронный ресурс] – Режим доступа: http://www.intuit.ru/

– Информационный ресурс «Projectimo.ru» [Электронный ресурс] – Режим доступа http://projectimo.ru

– Электронная библиотека «Все учебники» [Электронный ресурс] – Режим доступа http://www.vse-ychebniki.ru/

– Академия ORACLE [Электронный ресурс] – Режим доступа https://academy.oracle.com/ru/

– Русская виртуальная библиотека [Электронный ресурс] – Режим доступа: http://www.rvb.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины необходимо следующее материально-техническое обеспечение:

– для проведения лекций, уроков – аудитория, оборудованная учебной мебелью и средствами обучения: проектором, ПК, экраном, доской;

– для проведения всех видов лабораторных и практических занятий, дисциплинарной, междисциплинарной и модульной подготовки – компьютерный класс с лицензионным программным обеспечением.

– для проведения промежуточной аттестации – компьютерный класс с лицензионным программным обеспечением.

– для 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. Организация обеспечивает печатными и/или электронными образовательными ресурсами в формах адаптированных к ограничениям их здоровья.

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».