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

УТВЕРЖДАЮ
Проректор по УР и КО
_____Ю.Е. Леденева
«_19_»_____10_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Дополнительная профессиональная программа «Информационные системы и прикладная информатика»

Форма обучения: заочная

Разработана
к.т.н., доцент
_____С.В. Аникуев

Согласована
зав. кафедрой ИС
_____А.Ю. Орлова

Рекомендована
на заседании кафедры
от «_19_»_____10_____2022г.
протокол №_2_
Зав. кафедрой ИС
_____А.Ю. Орлова
Одобрена
на заседании учебно-методической
комиссии факультета
от «_19_»_____10_____2022 г.
протокол №_2_
Председатель УМК
_____Ж .В. Игнатенко

Ставрополь, 2022 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Информационная безопасность и защита информации» являются:

- формирование у обучающихся теоретических знаний и практических навыков по обеспечению информационной безопасности;

-ознакомление обучающихся с разновидностями современных подходов, принципов и методов создания информационных систем защиты данных, технического и программного обеспечения информационных систем безопасности, включая системное, функциональное и прикладное программное обеспечение и аппаратные средства защиты информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Процесс изучения курса направлен на совершенствование и (или) формирование следующих компетенций:

1) Способность гарантировать качество, надежность и информационную безопасность ИС.

Знать:

- Виды угроз ИС и методы обеспечения информационной безопасности
- Методики оценки качества, надежности и информационной безопасности ИС.

Уметь:

- Выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.

Владеть:

- Навыками оценки качества, надежности и информационной безопасности ИС.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часов.

Вид учебной работы	Всего часов	Периоды обучения
		54 календ. дня
Аудиторные занятия (всего)	**38**	**38**
в том числе:		
Лекции (Л)		14
Практические занятия (ПЗ)		24
Семинары (С)		
Лабораторные работы (ЛР)		
Внеаудиторные занятия (самостоятельная работа) (СР)	**70**	**70**
в том числе:		
Курсовой проект (работа)		
Расчетно-графические работы		
Контрольная работа		
Реферат		
Самоподготовка (самостоятельное изучение разделов, проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)		68

Вид промежуточной аттестации (зачет)		2
Общая трудоемкость, час	**108**	**108**

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

4.1. Содержание дисциплины

№ раздела (темы)	Наименование раздела (темы)	Содержание раздела (темы)
1	Информационная безопасность: понятия и определения	Роль информационной безопасности и ее место в системе национальной безопасности, информационная безопасность, её основные составляющие и аспекты. Понятие защиты информации. Нормативно-правовые основы обеспечения ИБ в Российской Федерации. Нормативно-правовые акты Российской Федерации в области ИБ. Стандарты информационной безопасности. Реализация комплексной системы защиты информации. Виды контроля нарушений ИБ. Риски безопасности мобильных устройств.
2	Угрозы информационной безопасности	Понятие угрозы информационной безопасности. Классификация угроз по различным признакам.
3	Вредоносные программы	Понятие вредоносных программ. Классификация вредоносных программ. Способы распространения вредоносных программ
4	Методы и средства защиты компьютерной информации	Программно-технические методы обнаружения вирусов. Административно-технологические методы защиты. Особенности защиты информации в персональных компьютерах. Методы и средства защиты компьютерной информации. Методы обеспечения информационной безопасности. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта)
5	Криптографические методы защиты информации	Наука криптография. Криптографические методы защиты информации. Криптосистемы, управление ключами, электронная цифровая подпись. Требования к криптосистемам. Симметричные криптосистемы. Системы с открытым ключом. Реализация криптографических методов.
6	Лицензирование и сертификация в области защиты информации	Понятия лицензирования и сертификации в области защиты информации. Нормативная правовая база системы сертификации средств защиты информации. Порядок проведения лицензирования.
7	Критерии безопасности компьютерных систем	Классы безопасности компьютерных систем. Категории требований безопасности компьютерных систем. Требования в отношении политики безопасности. Группы безопасности компьютерных систем.

4.2. Структура дисциплины

№ раздела (темы)	Наименование раздела (темы)	Количество часов				
		Всего	Л	ПЗ (С)	ЛР	СР
1.	Информационная безопасность: понятия и определения	12	2	2	-	8
2.	Угрозы информационной безопасности	14	2	2	-	10
3.	Вредоносные программы	16	2	4	-	10
4.	Методы и средства защиты компьютерной информации	16	2	4	-	10
5.	Криптографические методы защиты информации	16	2	4	-	10
6.	Лицензирование и сертификация в области защиты информации	16	2	4	-	10
7.	Критерии безопасности компьютерных систем	16	2	4	-	10
	Зачет	2	-	-	-	-
	Общая объем, час.	**108**	**14**	**24**	**-**	**68**

4.3. Практические занятия и семинары

№ п/п	**№ раздела (темы)**	**Тема**	Кол-во часов
1	1	Установка и настройка сервера DNS	2
2	2	Настройка параметров безопасности домена	2
3	3	Работа с Active Directory	4
4	4	Настройка параметров безопасности домена	4
5	5	Работа с серверами HTTP и FTP	4
6	6	Мониторинг состояния элементов сети	4
7	7	Настройка параметров безопасности Интернет браузера	4

4.4. Лабораторные работы

не предусмотрены

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

не предусмотрен

4.6. Внеаудиторная (самостоятельная) работа

Виды самостоятельной работы	Количество часов
Выполнение практического задания	38
Изучение специальной методической литературы и анализ научных источников	20
Подготовка конспектов и презентаций по теме	10

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Информационные технологии, используемые при осуществлении

образовательного процесса по дисциплине

При чтении лекций используется компьютерная техника для демонстрации слайдов с помощью программного приложения Microsoft Power Point. На практических занятиях студенты представляют результаты выполнения самостоятельной работы, подготовленные с помощью программного приложения Microsoft Power Point. При выполнении практических заданий на практических занятиях, студентами используется программное обеспечение: Windows 7, MSOffice, Visual Basic 6.0 Enterprise Edition (Installation Notes) (English).

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация проводится в форме зачета.

1. Типовые вопросы к устному опросу

Тема 1. Информационная безопасность: понятия и определения

- Роль информационной безопасности и ее место в системе национальной безопасности, информационная безопасность, её основные составляющие и аспекты.
- Понятие защиты информации.
- Нормативно-правовые основы обеспечения ИБ в Российской Федерации.
- Нормативно-правовые акты Российской Федерации в области ИБ.
- Стандарты информационной безопасности.
- Реализация комплексной системы защиты информации.
- Виды контроля нарушений ИБ.
- Риски безопасности мобильных устройств.

Тема 2. Угрозы информационной безопасности

- Понятие угрозы информационной безопасности.
- Классификация угроз по различным признакам.

Тема 3. Вредоносные программы

- Понятие вредоносных программ.
- Классификация вредоносных программ.
- Способы распространения вредоносных программ

Тема 4. Методы и средства защиты компьютерной информации

- Программно-технические методы обнаружения вирусов.
- Административно-технологические методы защиты.
- Особенности защиты информации в персональных компьютерах.
- Методы и средства защиты компьютерной информации.
- Методы обеспечения информационной безопасности.
- Ограничение доступа.
- Контроль доступа к аппаратуре.
- Разграничение и контроль доступа к информации.
- Предоставление привилегий на доступ.
- Идентификация и установление подлинности объекта (субъекта)

Тема 5. Криптографические методы защиты информации

- Наука криптография.

– Криптографические методы защиты информации.
– Криптосистемы, управление ключами, электронная цифровая подпись.
– Требования к криптосистемам.
– Симметричные криптосистемы.
– Системы с открытым ключом.
– Реализация криптографических методов.

Тема 6. Лицензирование и сертификация в области защиты информации
– Понятия лицензирования и сертификации в области защиты информации.
– Нормативная правовая база системы сертификации средств защиты информации.
– Порядок проведения лицензирования.

Тема 7. Критерии безопасности компьютерных систем
– Классы безопасности компьютерных систем.
– Категории требований безопасности компьютерных систем.
– Требования в отношении политики безопасности.
– Группы безопасности компьютерных систем.

2. Перечень типовых заданий к практическим занятиям

Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС.

Задача 1.

Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата – с целью продажи этой информации конкурирующей организации.

Задача 2.

П. П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей.

Задача 3.

Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю.

Задача 4.

Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем фирмы «Электронная галерея» И. С. Дубцовым судебного иска к продавцу этой же фирмы, если по вине последнего произошло электрическое замыкание и было повреждено значительное количество компьютерной техники?

Задача 5.

Будет ли привлечена к уголовной ответственности главный бухгалтер торговой сети «Оптпром» С. Н. Вульф, если ее действия повлекли уничтожение компьютерной информации в базах данных вышеуказанной торговой сети и после ревизии предприятие было оштрафовано на 350 ООО рублей?

Задача 6.

Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации,

если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки различным организациям на общую сумму 670 ООО рублей.

Задача 7.

За несанкционированный доступ и копирование компьютерной информации суд приговорил гражданина РФ В. А. Лютикова к 5 годам лишения свободы.

Задача 8.

По вине оператора по набору данных М. Л. Плехановой, работавшей с компьютерной системой бухгалтерских платежей, торговая сеть «Антиквар» понесла денежные убытки в размере 1 850 000 рублей. М. Е. Плехановой было предъявлено обвинение по ст. 273 УК РФ.

Задача 9.

Студентам технического университета за доступ к компьютерной системе службы внутренних дел и копирование части файлов данной системы было предъявлено обвинение по ст. 272, п. 1 УК РФ.

Задача 10.

Н. А. Симонова, сотрудница отдела продаж косметической компании «Макияж», за распитие кофейного напитка в непосредственной близости от ЭВМ была наказана исправительными работами сроком на 15 суток.

Задача 11.

Оператор ПК торговой сети «Вернисаж» Д. С. Ермилов был обвинен по ст. 272, п. 1 УК РФ за изменение данных в поле «Адрес» в базе данных клиентских платежей. Эту модификацию он произвел по просьбе самой клиентки в связи с изменением ее места жительства.

Задача 12.

За распространение программы, действие которой заключается в уничтожении текстовых файлов в какой-либо компьютерной сети, студент III курса авиационного техникума был наказан судом штрафом в размере 100 минимальных размеров оплаты труда.

Задача 13.

За несанкционированный доступ к компьютерной информации в файлах химико-биологического исследовательского центра «New Life» и ее модификацию гражданку РФ А. С. Иванову суд приговорил к 8 месяцам исправительных работ.

Задача 14.

За нарушение работы с компьютерной системой бухгалтерских платежей авиакомпании «Небеса» сотруднице вышеупомянутой организации Т. В. Бариновой. действия которой привели к модификации компьютерных данных и принесли авиакомпании «Сибирь» денежные убытки в размере 150 000 рублей, было предъявлено обвинение по ст. 274 УК РФ.

3. Перечень заданий к самостоятельной работе слушателя

1. Опишите виды угроз, с которыми вам приходилось сталкиваться в трудовой деятельности.
2. Разработайте план мероприятий по ликвидации угрозы информационной безопасности.
3. Подготовьте презентацию «Криптографические методы защиты информации».
4. Разработайте архитектуру надежной и качественной АИС.

4. Типовые вопросы и задания к зачету (промежуточная аттестация)

Промежуточная аттестация проводится в форме зачёта. Зачет проводится после выполнения учебного плана программы в части установленного объема различных видов учебной деятельности.

Зачет по дисциплине проводится за счет часов, отведённых на изучение дисциплины.

Зачет по дисциплине включает в себя: собеседование преподавателя со студентами по контрольным вопросам (не более 5) и 1 ситуационную задачу.

При оценке знаний, полученных обучающимся при изучении дисциплины, должно быть учтено, что для получения зачета по изученной дисциплине необходимо показать знание и понимание основных вопросов рассмотренного материала, а также способность найти и применить необходимые знания для разрешения конкретной ситуации:

оценка «зачтено» выставляется обучающемуся, если он дал четкий, не позволяющий двойного толкования ответ, а также за способность решать задачу и применять ее в конкретном случае на практике, убедительно аргументируя свои выводы, либо если первоначально ответ не позволяет однозначно трактовать изложенный обучающимся материал, но при помощи дополнительных вопросов он показывает способность ориентироваться в нормах и применять их к соответствующим обстоятельствам.

оценка «не зачтено» выставляется обучающемуся, если в знании основного материала по программе имеются существенные пробелы, а также, если он допустил принципиальные ошибки при изложении материала либо не смог правильно ответить на вопросы преподавателя.

Вопросы:

1. Программа информационной безопасности России и пути ее реализации.
2. Роль и место информационной безопасности экономических систем в системе национальной безопасности РФ.
3. Концепция информационной безопасности.
4. Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.
5. Основные положения теории информационной безопасности информационных систем.
6. Основные принципы защиты информации в компьютерных системах.
7. Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности.
8. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
10. Компьютерные преступления.
11. Организационное обеспечение информационной безопасности.
12. Три вида возможных нарушений информационной системы.
13. Понятие угрозы. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
14. Виды противников или «нарушителей». Причины, виды, каналы утечки и искажения информации.
15. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации.
16. Анализ способов нарушений информационной безопасности.
17. Информационная безопасность в условиях функционирования в России глобальных сетей.
18. Общая проблема информационной безопасности информационных систем.

19. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).
20. Основные технологии построения защищенных экономических информационных систем (ЭИС).
21. Защита информации от несанкционированного доступа. Математические и методические средства защиты.
22. Политика безопасности. Модели безопасности и их применение.
23. Защита. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.
24. Использование защищенных компьютерных систем.
25. Стандарты по оценке защищенных систем. Примеры практической реализации.
26. Понятие разрушающего программного воздействия.
27. Методы перехвата и навязывания информации.
28. Компьютерные вирусы. Понятия о видах вирусов. Современные антивирусные программы.
29. Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Передача пароля по сети.
30. Особенности криптографического и стеганографического преобразования информации.
31. Стойкость алгоритмов шифрования. Типы алгоритмов шифрования. Примеры криптографических алгоритмов. Особенности применения криптографических методов.
32. Особенности реализации систем с симметричными и несимметричными ключами. Электронная подпись.
33. Защита офисных документов. Способы распространения программного обеспечения.
34. Техническая защита от несанкционированного копирования.
35. Базовые методы нейтрализации систем защиты от несанкционированного копирования.
36. Идентификация параметров персонального компьютера.
37. Идентификация жестких дисков. Идентификация гибких дисков.
38. Оценка уникальности конфигурации компьютера.
39. Подходы к построению защищенной операционной системы. Административные меры защиты.
40. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС.
41. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.

Ситуационные задачи:

1. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата – с целью продажи этой информации конкурирующей организации».

2. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «П. П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe). В результате внедрения этого вируса было уничтожено 40 % банковских

программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей».

3. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю».

4. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Решение в пользу какой стороны и почему вынесет суд при предъявлении владельцем фирмы «Электронная галерея» И. С. Дубцовым судебного иска к продавцу этой же фирмы, если по вине последнего произошло электрическое замыкание и было повреждено значительное количество компьютерной техники?»

5. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Будет ли привлечена к уголовной ответственности главный бухгалтер торговой сети «Оптпром» С. Н. Вульф, если ее действия повлекли уничтожение компьютерной информации в базах данных вышеуказанной торговой сети и после ревизии предприятие было оштрафовано на 350 ООО рублей?»

6. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки различным организациям на общую сумму 670 ООО рублей».

7. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «За несанкционированный доступ и копирование компьютерной информации суд приговорил гражданина РФ В. А. Лютикова к 5 годам лишения свободы».

8. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «По вине оператора по набору данных М. Л. Плехановой, работавшей с компьютерной системой бухгалтерских платежей, торговая сеть «Антиквар» понесла денежные убытки в размере 1 850 000 рублей. М. Е. Плехановой было предъявлено обвинение по ст. 273 УК РФ».

9. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Студентам технического университета за доступ к компьютерной системе службы внутренних дел и копирование части файлов данной системы было предъявлено обвинение по ст. 272, п. 1 УК РФ».

10. Выявите и опишите уровень угрозы информационной безопасности. Обоснуйте набор оптимальных организационно-технических мероприятий по защите информации в ИС. Оцените качество и надежность существующей ИС для проблемы: «Н.

А. Симонова, сотрудница отдела продаж косметической компании «Макияж», за распитие кофейного напитка в непосредственной близости от ЭВМ была наказана исправительными работами сроком на 15 суток».

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

7.2. Дополнительная литература

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

3. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

7.3. Программное обеспечение

Антивирусное ПО

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

http://www.intuit.ru/
http://www.edu.ru/
http://www.i-exam.ru/

7.5. Методические указания по освоению дисциплины.

При изучении каждой из тем курса дисциплины рекомендуется, прежде всего, ознакомиться с материалом соответствующей лекции, в которой изложены основные теоретические вопросы. Для более подробного ознакомления с темой необходимо изучить рекомендуемую литературу, Интернет-ресурсы и материалы курса.

Освоение большинства тем невозможно без выполнения практических заданий и упражнений. Для самопроверки и в качестве подготовки к текущему и итоговому контролю большое значение имеет выполнение тестовых заданий.

При выполнении практических работ необходимо выполнить всю работу согласно тексту задания. Результаты работы сохранить в файлах. После выполнения задания необходимо преподавателю продемонстрировать результаты работы и быть готовым ответить на вопросы и продемонстрировать выполнение отдельных пунктов задания. Защита практических работ осуществляется в дни и часы, устанавливаемые преподавателем.

Самостоятельная работа по данной дисциплине предусматривает подготовку к лекциям и практическим занятиям, изучение источников информации по дисциплине, подготовку творческих заданий, подготовку к текущему и итоговому контролю.

8.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины требуется следующее материально-техническое обеспечение:

- для проведения занятий лекционного типа - аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: учебная мебель, экран, проектор, ноутбук.

- для проведения занятий семинарского типа - аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: учебная мебель, экран, проектор, ноутбук.

- для проведения текущего контроля и промежуточной аттестации - аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: учебная мебель, экран, проектор, ноутбук.

- для самостоятельной работы обучающихся - аудитория оснащенная компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среде организации.