УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.Е. Федоров
«_25_» _____06_____ 2021 г.

Рабочая программа дисциплины (модуля)*
Тестирование компьютерных систем на проникновения

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация № 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)
специалист по защите информации

Форма обучения
очная

Год(ы) набора 2021

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2021 г.

Рабочая программа дисциплины (модуля) принята:
Ученым советом математического факультета

Протокол заседания № 13 от «24» 06 2021 г.

Председатель Ученого совета
математического факультета _____ Е.А. Сбродова

Секретарь Ученого совета
математического факультета _____ С.А. Никитина

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой компьютерной безопасности и прикладной алгебры.

Протокол заседания № 10 от «04» 06 2021 г.

Заведующий кафедрой _____ А.Н. Ручай

Автор (составитель):
Зав.кафедрой, канд.физ.-мат. наук, доцент _____ А.Н. Ручай

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель преподавания дисциплины – формирование у студентов компетенций, необходимых для проведения тестирования компьютерных систем на проникновение.

Задачей дисциплины является формирование у студентов знаний о принципах и алгоритмах проведения тестирования компьютерных систем на проникновение, формирования практических навыков исследования защищенности информационно-коммуникационных систем, выявления угроз информационной безопасности и выработке рекомендаций по их локализации.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации.

ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.

ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.02

2.1 Требования к предварительной подготовке обучающегося:

Информатика

Модели безопасности компьютерных систем

Алгебра

Аппаратные средства вычислительной техники

Методы программирования

Компьютерные сети

Защита программ и данных

Защита в операционных системах

Беспроводные сети

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-2: Способен проводить мониторинг защищенности компьютерных систем

Знать:

– этапы проведения тестирования компьютерных систем на проникновение;
- теоретические основы компьютерных атак, моделируемых в рамках проведения экспериментов по проникновению в компьютерные системы;
- принципы работы сканеров безопасности и методику проверки получаемых ими сведений;
- правила документирования и построения отчетов по результатам проводимых тестов на проникновение.

Уметь:

- использовать сканеры информационной безопасности и проводить оценку, получаемых ими сведений;
- моделировать современные компьютерные атаки, представляющие актуальные угрозы информационной безопасности для компьютерных систем;
- детектировать средства обнаружения компьютерных вторжений и предотвращения утечек информации;
- использовать приемы обхода IDS, IPS, DLP-систем, антивирусного программного обеспечения и криптографических протоколов, применяемых для защиты компьютерных систем;

- проводить оценку конфигурации средств защиты информации и давать рекомендации по ее корректировке.
Владеть:
– практическими навыками проведения тестирования компьютерных систем на проникновение и подготовки по их результатам соответствующих отчетов.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– современные российские и международные стандарты в области информационной безопасности;
3.1.2	– этапы проведения тестирования компьютерных систем на проникновение.
3.2	**Уметь:**
3.2.1	– применять методы выявления уязвимостей информационных систем и проводить оценку информационной защищенности;
3.2.2	- моделировать современные компьютерные атаки, представляющие актуальные угрозы информационной безопасности для компьютерных систем;
3.2.3	- детектировать средства обнаружения компьютерных вторжений и предотвращения утечек информации.
3.3	**Владеть:**
3.3.1	– практическими навыками проведения тестирования компьютерных систем на проникновение и подготовки по их результатам соответствующих отчетов.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Общая трудоемкость	**4 ЗЕТ**
Часов по учебному плану : 144 в том числе : аудиторные занятия : 72 самостоятельная работа : 72 :	Виды контроля в семестрах: экзамены 9

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. 1. Методика проведения тестирования компьютерных систем			
1.1	Общие понятия тестирования компьютерных систем на проникновение /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.2	Правовое регулирование тестирования компьютерных систем на проникновение /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.3	Основы проведения тестирования компьютерных систем. Проработка лекционного материала. /Ср/	9	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 2. 2. Сбор информации			
2.1	Понятие и назначение «Open source intelligence». /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.2	Метаданные /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.3	Сбор информации в открытых телекоммуникационных сетях /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.4	Сканирование компьютерных систем /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.5	Сбор информации. OSINT. Конкурентная разведка. Проработка лекционного материала. Закрепление практического материала. /Ср/	9	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 3. 3. Сканирование компьютерных систем			

3.1	Методы сканирования сетевых портов /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.2	Обход средств обнаружения вторжений при сканировании сетевых портов /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.3	Использование библиотеки "scapy" для проведения различных видов сканирования сетевых портов. /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.4	Сканирование компьютерных систем. NMAP. OpenVAS. Проработка лекционного материала. Закрепление практического материала. /Ср/	9	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 4. 4. Эксплуатация уязвимостей программного обеспечения			
4.1	Общедоступные базы эксплойтов /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.2	Metasploit Framework /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.3	Обход и тестирование средств антивирусной защиты /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.4	Использование программного обеспечения «Metasploit Framework» /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.5	Использование дополнительных модулей «Metasploit Framework» /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.6	Эксплуатация уязвимостей программного обеспечения. Metasploit Framework. Проработка лекционного материала. Закрепление практического материала. /Ср/	9	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 5. 5. Проведение экспериментов по оценке защищенности вычислительных систем.			
5.1	Классификация сетевых компьютерных атак. /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.2	Уязвимости сетевых протоколов. /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.3	ARP-спуфинг. IP-спуфинг. /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.4	Подавление DHCP-сервера. /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.5	DNS-спуфинг. Strip SSL. /Лек/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.6	Прослушивание и модификация сетевого трафика. /Лаб/	9	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.7	Подавление в сети DHCP-сервера. /Лаб/	9	3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.8	Атака на клиентское приложение /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

5.9	Атака «stripssl» на протокол HTTPS /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.10	Анализ сетевого трафика программой Intercepter-NG /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.11	Атака на беспроводную сеть /Лаб/	9	2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.12	Тестирование средств антивирусной защиты. Проработка лекционного материала. Закрепление практического материала. /Ср/	9	12	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 6. 6. Оценка защищенности компьютерных систем, выработка рекомендаций			
6.1	Оценка защищенности компьютерных систем, выработка рекомендаций. /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.2	Отчет о проведении тестирования компьютерной системы на проникновение /Лаб/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.3	Сетевые компьютерные атаки. /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
6.4	Оценка защищенности компьютерных систем, выработка рекомендаций /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Устный опрос.
Лабораторная работа.
Самостоятельная работа.
Экзамен.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Вопросы для устного опроса для текущей аттестации
1. Этапы тестирования компьютерных систем на проникновение.
2. Виды и классификации тестирований компьютерных систем на проникновение.
3. Black box, White box, Black hat, White hat.
4. Понятие этичного взлома.
5. Правовые основы проведения теста на проникновение.
6. Понятие и назначение «Open source intelligence».
7. Lo-tech OSINT.
8. Hi-tech OSINT.
9. Общее понятие футпринтинга.
10. Принципы технологии «google hacking database».
11. Методы анализа метаданных.
12. Методы сканирования портов.
13. SYN-сканирование.
14. ACK-сканирование.
15. XMAS-сканирование.
16. FIN-сканирование.
17. UDP-сканирование.
18. Window-сканирование.
19. Способы идентификации приложений, детектирование уязвимостей.
20. Алгоритмы функционирования антивирусных средств.
21. Проактивная защита.
22. Реактивная защита.
23. Виртуализация окружения.
24. Эмуляция кода.
25. Полиморфный программный код.
26. Метаморфный программный код.

27. Шифрование программного кода.
28. Методы обхода средств антивирусной защиты, сетевых экранов, систем обнаружений вторжений.
29. Эксплойт.
30. Классификация компьютерных атак.
31. Сетевые атаки на канальный уровень стека протоколов TCP/IP.
32. Сетевые атаки на сетевой уровень стека протоколов TCP/IP.
33. Сетевые атаки на транспортный уровень стека протоколов TCP/IP.
34. Атаки на протоколы маршрутизации.
35. Протокол DHCP.
36. Истощение DHCP-сервера.
37. DNS.
38. DNS-спуфинг.
39. Шторм ложных DNS-запросов.
40. Методы целевого внедрения специального программного обеспечения.
41. Атака Strip-SSL.
42. Механизм защиты HSTS.
43. HSTS спуфинг.
44. Алгоритм работы WPA2.
45. Атака деаутентификации WPA2.
46. Документальное оформление теста на проникновение

Перечень самостоятельных работ
1. Разработка сетевого сканера.
2. Использование технологии OSINT в открытых телекоммуникационных сетях.

Перечень лабораторных работ
1. Сбор информации в открытых телекоммуникационных сетях.
2. Использование библиотеки "scapy" для проведения различных видов сканирования сетевых портов.
3. Использование программного обеспечения «Metasploit Framework».
4. Использование дополнительных модулей «Metasploit Framework».
5. Прослушивание и модификация сетевого трафика.
6. Подавление в сети DHCP-сервера.
7. Атака на клиентское приложение.
8. Атака «stripssl» на протокол HTTPS.
9. Анализ сетевого трафика программой Intercepter-NG.
10. Атака на беспроводную сеть.
11. Отчет о проведении тестирования компьютерной системы на проникновение.

Полные тексты лабораторных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Перечень вопросов к экзамену
1. Этапы тестирования компьютерных систем на проникновение.
2. Виды и классификации тестирований компьютерных систем на проникновение.
3. Black box, White box, Black hat, White hat.
4. Понятие этичного взлома.
5. Правовые основы проведения теста на проникновение.
6. Понятие и назначение «Open source intelligence».
7. Общее понятие футпринтинга.
8. Принципы технологии «google hacking database».
9. Методы анализа метаданных.
10. Методы сканирования портов.
11. Способы идентификации приложений, детектирование уязвимостей.
12. Алгоритмы функционирования антивирусных средств.
13. Методы обхода средств антивирусной защиты, сетевых экранов, систем обнаружений вторжений.
14. Общая схема применения эксплойта.
15. Классификация компьютерных атак.
16. Сетевые атаки на канальный уровень стека протоколов TCP/IP.
17. Сетевые атаки на сетевой уровень стека протоколов TCP/IP.
18. Сетевые атаки на транспортный уровень стека протоколов TCP/IP.
19. Атаки на протоколы маршрутизации.
20. Уязвимости DHCP-протокола.
21. Атаки на службу DNS.
22. Методы целевого внедрения специального программного обеспечения.

23. Атака Strip-SSL.
24. Документальное оформление теста на проникновение.

6.4. Критерии оценивания

Порядок проведения промежуточной аттестации
В течение семестра студент должен выполнить одиннадцать лабораторных работ, каждая из которых оценивается в 5 баллов.
Максимальный балл за лабораторную работу – 5 баллов.
Максимальный балл за лабораторные работы в семестре – 55 баллов.
Также необходимо выполнить две самостоятельные работы.
Максимальный балл за самостоятельную работу – 5 баллов.
Допуском до проведения экзамена являются сданные студентом лабораторные и самостоятельные работы в течение семестра.
Экзамен проводится в один этап, на котором студент отвечает на два теоретических вопроса. Продолжительность – 30 минут.
Максимальный балл за ответ на теоретический вопрос – 15 баллов.

Сводная таблица рейтинга успеваемости (8 семестр)

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа №1-11	11x5=55
2	Самостоятельная работа № 1,2	2x5=10
3	Посещаемость (все занятия)	5
4	Экзамен (теоретический вопрос)	2x15=30
Итого		100

Критерии оценивания теоретического вопроса
Максимальный баллы за ответы на теоретические вопросы — 30 баллов.
Отлично/зачтено/12-15 баллов - Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.
Хорошо/зачтено/8-11 баллов - Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует логичность и последовательность. Однако допускается неточность в ответе.
Удовлетворительно/зачтено/4-7 баллов - Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа.
Неудовлетворительно/не зачтено/0-4 балла - Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

Критерии оценки лабораторной работы
Максимальный балл за лабораторные работы за семестр – 55 баллов.
5 баллов - лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
4 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
3 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
2 балла – лабораторная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
1 балл – при выполнении лабораторной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.
0 баллов – не выполнена лабораторная работа.

Критерии оценки самостоятельной работы
Максимальный балл за самостоятельные работы за семестр –10 баллов.
5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;
3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
2 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;
1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.
0 баллов – не выполнена самостоятельная работа.

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.
Для экзамена:
0-59 баллов – неудовлетворительно (2);
60-74 баллов – удовлетворительно (3);
75-90 баллов – хорошо (4);
91-100 баллов – отлично (5).

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Баранова Е.К., Бабаш А.В.	Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие (http://znanium.com/catalog/document?id=326176)	Москва : Издательский Центр РИОР, 2019	ЭБС
Л1.2	Клименко И.С.	Информационная безопасность и защита информации: модели и методы управления: монография (http://znanium.com/catalog/document?id=347076)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2020	ЭБС
Л1.3	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие (https://biblioclub.ru/index.php?page=book&id=571485)	Москва, Берлин : Директ-Медиа, 2020	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (http://znanium.com/catalog/document?id=327912)	Москва : Издательство "ФОРУМ", 2019	ЭБС
Л2.2	Глинская Е.В., Чичварин Н.В.	Информационная безопасность конструкций ЭВМ и систем: учебное пособие (http://znanium.com/catalog/document?id=327864)	Москва : ООО "Научно-издательский центр ИНФРА-М", 2019	ЭБС
Л2.3	Шаньгин В. Ф.	Защита информации в компьютерных системах и сетях (http://e.lanbook.com/books/element.php? pl1_cid=25&pl1_id=3032)	Москва : ДМК Пресс, 2012	ЭБС
Л2.4	Баранова Е.К., Бабаш А.В.	Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие (http://znanium.com/catalog/document?id=359654)	Москва : Издательский Центр РИОР, 2020	ЭБС

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

MS Office365

NetBeans

Notepad++

VirtualBox

Ubuntu Linux

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Электронный каталог научной библиотеки ЧелГУ [Электронный ресурс] : база данных / Челяб. гос. ун-т. – Челябинск, 1992.

2. Консультант Плюс [Электронный ресурс] : справочно-правовая система : база данных / Регион. центр правовой информ. Информправо.

3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека [научной периодики на русском языке]. — Москва, [1999-]. - Доступ к полным текстам после регистрации из сети ЧелГУ. – URL: http://elibrary.ru/defaultx.asp.

4. Moodle [Электронный ресурс]: система дистанционного обучения : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.uio.csu.ru/login/index.php.

5. Научная библиотека Челябинского государственного университета [Электронный ресурс] : [сайт] / Челяб. гос. ун-т. – Челябинск, [2001-]. – Режим доступа: http://www.lib.csu.ru/ , свободный. – Загл. с экрана.

6. Интернет университет информационных технологий [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://www.intuit.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения: проектором, экраном, магнитно-маркерной доской, маркером; с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения занятий лекционного типа имеется демонстрационное оборудование: проектор, экран.

Лабораторные занятия проходят в учебных лабораториях технических средств защиты информации и "Сетевой полигон" (ауд. 421, 423, учебный корпус №1). Материально-техническое обеспечение приведено в паспортах лабораторий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении данной дисциплины используются лекционные, лабораторные занятия и самостоятельная работа студента. На лекционных занятиях преподаватель излагает основное содержание тем программы. Проработку лекционного материала студенту желательно проводить как после каждого занятия, так и по завершению темы. Это позволит связать воедино полученные сведения и составить цельную картину.

На лабораторных занятиях рассматриваются методы проведения тестирования компьютерных систем на проникновение. Рекомендуется перед каждым лабораторным занятием выполнить домашнее задание, что позволить лучше усвоить предыдущий материал, и изучить лекционный материал по предстоящей теме. Студенту желательно проявлять активное участие на лабораторных и лекционных занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни.

Важным моментом при изучении любой дисциплины является организация самостоятельной работы. При освоении материала не следует стремиться к механическому запоминанию приведенных определений, формулировок и положений, если требования прямо не указывают на это. Вполне эффективной может оказаться попытка понять суть явления, выработать свое отношение к нему, опираясь на материал, содержащийся в рекомендованной литературе. Сказанное особенно эффективно, когда речь идет о таких требованиях, как «понимает» или «имеет представление». Напротив, если студент имеете дело с требованием к деятельности «должен уметь», то рекомендуется поупражняться в соответствующем виде деятельности. Все это имеет непосредственное отношение к подготовке к практическим занятиям.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (онлайн-лекции

(вебинары), чаты, видео-конференции и др.) или отложенного времени (система дистанционного обучения Moodle, видеохостинг YouYube, форумы, электронная почта и др.).
Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством электронной почты, мессенджеров, социальных сетей и т.п.
Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе.

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.
Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно-образовательной среды.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.
1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).
Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:
Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.
Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.