Рабочая программа дисциплины (модуля)*

Анализ уязвимостей программного обеспечения

Направление подготовки (специальность)

10.05.01 Компьютерная безопасность

Направленность (профиль)

специализация N 1 "Анализ безопасности компьютерных систем"

Присваиваемая квалификация (степень)

специалист по защите информации

Форма обучения

очная

Год(ы) набора 2023

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

Челябинск 2023 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Знать современные методы эксплуатации бинарных уязвимостей программного обеспечения и уметь их эксплуатировать с учётом специфики современных защитных механизмов.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ОПК 1.2.1 Знает основные средства и методы защиты программного обеспечения от анализа и нарушения целостности; основные программные методы защиты данных от несанкционированного доступа.

ОПК 1.2.2 Умеет проводить анализ программных средств, применяемых для контроля и защиты информации; проводить анализ программ и алгоритмов на предмет соответствия требованиям защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.О.32.03

2.1 Требования к предварительной подготовке обучающегося:

Обучающиеся должны владеть знаниями и навыками в области системного и низкоуровневого программирования, операционных систем, программных методов защиты, получаемыми в рамках следующих дисциплин:

Языки программирования

Языки Ассемблера

Системное программирование

Защита программ и данных

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

Знания и практические навыки, полученные при изучении дисциплины, расширяет профессиональный кругозор и используются обучающимися при разработке дипломных работ. Данная дисциплина является предшествующей для следующих дисциплин:

Исследование вредоносного программного обеспечения

Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

ОПК-1.2: Способен оценивать корректность программных реализаций алгоритмов защиты информации;

Знать:

– методы эксплуатации современных уязвимостей бинарного программного обеспечения;
– методы поиска уязвимостей бинарного программного обеспечения;
– требования и рекомендации по обеспечению безопасности бинарного программного обеспечения;
– современные уязвимости аппаратного обеспечения;
– современные защитные механизмы, противодействующие эксплуатации уязвимостей бинарного программного обеспечения.

Уметь:

– эксплуатировать классические и современные уязвимости бинарного программного обеспечения;
– использовать базы данных уязвимостей при проведении анализа безопасности;
– использовать лучшие практики по предотвращению появления уязвимостей в бинарном программном обеспечении;
– эксплуатировать уязвимости аппаратного обеспечения;
– использовать методы противодействия защитным механизмам.

Владеть:

– навыками создания эксплоитов для бинарного программного обеспечения;
– навыками использования инструментальных средств поиска и эксплуатации уязвимостей;
– навыками создания бинарного программного обеспечения с учётом требований безопасности;
– навыками создания эксплоитов для уязвимостей аппаратного обеспечения и прошивок;
– навыками создания эксплоитов с учётом защитных механизмов.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	– классические и современные уязвимости в бинарном коде, методы их эксплуатации, защитные механизмы.
3.2	**Уметь:**
3.2.1	– эксплуатировать уязвимости в бинарном коде с учетом противодействия защитных механизмов.
3.3	**Владеть:**
3.3.1	– навыки создания эксплоитов.
3.3.2	– навыки поиска уязвимостей в бинарном коде.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**7 ЗЕТ**
Часов по учебному плану : 252 в том числе : аудиторные занятия : 136 самостоятельная работа : 71,1 часов на контроль : 27 контактная работа: 153,9 ИКР: 0	Виды контроля в семестрах: экзамены 9 зачеты 8

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Раздел 1. Уязвимости ПО в UNIX-подобных системах			
1.1	Уязвимости прикладных программ /Лек/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.2	Уязвимости прикладных программ /Лаб/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.3	Уязвимости прикладных программ /Ср/	8	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.4	Защитные механизмы /Лек/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.5	Защитные механизмы /Лаб/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.6	Защитные механизмы /Ср/	8	8	Л1.1 Л1.3Л2.1 Л2.3 Э1 Э2
1.7	Уязвимости кода режима ядра /Лек/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.8	Уязвимости кода режима ядра /Лаб/	8	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
1.9	Уязвимости кода режима ядра /Ср/	8	6,1	Л1.1 Л1.3Л2.1 Л2.3 Э1 Э2
	Раздел 2. Раздел 2. Уязвимости ПО в Windows NT			

2.1	Уязвимости прикладных программ. /Лек/	8	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.2	Уязвимости прикладных программ /Лаб/	8	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.3	Уязвимости прикладных программ /Ср/	8	6	Л1.1 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.4	Защитные механизмы /Лек/	8	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.5	Защитные механизмы /Лаб/	8	8	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.6	Защитные механизмы /Ср/	8	5	Л1.1 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.7	Уязвимости кода режима ядра /Лек/	9	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.8	Уязвимости кода режима ядра /Лаб/	9	10	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
2.9	Уязвимости кода режима ядра /Ср/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 3. Зачёт			
3.1	Иная контактная работа: индивидуальные консультации, текущий контроль. /КонтАт/	8	6,9	
	Раздел 4. Раздел 3. Уязвимости в аппаратном обеспечении			
4.1	Уязвимости процессоров и оперативной памяти /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.2	Уязвимости процессоров и оперативной памяти /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.3	Уязвимости процессоров и оперативной памяти /Ср/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
4.4	Уязвимости во встраиваемых системах и IoT-устройствах /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
4.5	Уязвимости во встраиваемых системах и IoT-устройствах /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2

4.6	Уязвимости во встраиваемых системах и IoT-устройствах /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
4.7	Уязвимости коммуникационных протоколов /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
4.8	Уязвимости коммуникационных протоколов /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
4.9	Уязвимости коммуникационных протоколов /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.3 Э1 Э2
	Раздел 5. Раздел 4. Уязвимости специализированного ПО			
5.1	Уязвимости браузеров /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.2	Уязвимости браузеров /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.3	Уязвимости браузеров /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.4	Уязвимости виртуальных машин /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.5	Уязвимости виртуальных машин /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.6	Уязвимости виртуальных машин /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.7	Уязвимости офисных приложений /Лек/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.8	Уязвимости офисных приложений /Лаб/	9	4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
5.9	Уязвимости офисных приложений /Ср/	9	6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 6. Экзамен			
6.1	Экзамен /Экзамен/	9	27	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2
6.2	Иная контактная работа: индивидуальные консультации, текущий контроль. /КонтАт/	9	11	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Зачетные задания.
Домашние задания.
Аудиторные задания.
Вопросы на зачёте.
Задания на зачёте.
Вопросы на экзамене.
Задания на экзамене.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Темы для домашних, аудиторных и зачетных заданий:
1. Шеллкоды для эксплоитов.
2. Уязвимости переполнения буфера в стеке.
3. Уязвимости переполнения буфера в кучу.
4. Уязвимости целочисленного переполнения.
5. Уязвимости переполнения кучи.
6. Защитные механизмы компиляторов и операционных систем.
7. Уязвимости аппаратного обеспечения и прошивок.

Примеры домашних, аудиторных и зачетных заданий:
1. Реализовать шеллкоды без нулевых байт.
2. Исследовать бинарное программное обеспечение, найти уязвимость и проэксплуатировать её.
3. Проэксплуатировать уязвимости и выполнить шеллкод.
4. Переполнить буфер и исполнить шеллкод.
5. Проэксплуатировать уязвимости сетевых приложений.
6. Проэксплуатировать уязвимости форматных строк.
7. Проэксплуатировать уязвимости переполнения в куче.
8. Проэксплуатировать уязвимости и обойти защиту стека.
9. Проэксплуатировать уязвимости и обойти DEP.
10. Проэксплуатировать уязвимости и обойти ASLR.
11. Проэксплуатировать уязвимость с использованием методов противодействия защитным механизмам.
12. Реализовать эксплоит с использованием ROP.
13. Обойти DEP с помощью ROP и выполнить шеллкод.
14. Проэксплуатировать уязвимости в плагинах для браузеров.
15. Написать шеллкоды для ядра Windows NT.
16. Проэксплуатировать уязвимости в драйверах под Windows NT.
17. Написать шеллкоды для ядра Linux.
18. Проэксплуатировать уязвимости в драйверах под Linux.
19. Проэксплуатировать уязвимость в аппаратном обеспечении.
20. Проэксплуатировать уязвимость в прошивке.

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Темы заданий на зачёте:
1. Шеллкоды для эксплоитов.
2. Уязвимости переполнения буфера в стеке.
3. Уязвимости переполнения буфера в кучу.
4. Уязвимости целочисленного переполнения.
5. Уязвимости переполнения кучи.
6. Защитные механизмы компиляторов и операционных систем.

Примеры заданий на зачёте:
1. Реализовать шеллкоды без нулевых байт.
2. Исследовать бинарное программное обеспечение, найти уязвимость и проэксплуатировать её.
3. Проэксплуатировать уязвимости и выполнить шеллкод.
4. Переполнить буфер и исполнить шеллкод.
5. Проэксплуатировать уязвимости сетевых приложений.
6. Проэксплуатировать уязвимости форматных строк.
7. Проэксплуатировать уязвимости переполнения в куче.

8. Проэксплуатировать уязвимости и обойти защиту стека.
9. Проэксплуатировать уязвимости и обойти DEP.
10. Проэксплуатировать уязвимости и обойти ASLR.
11. Проэксплуатировать уязвимость с использованием методов противодействия защитным механизмам.
12. Реализовать эксплоит с использованием ROP.
13. Обойти DEP с помощью ROP и выполнить шеллкод.
14. Проэксплуатировать уязвимости в плагинах для браузеров.

Примеры вопросов на зачёте:
1. Шеллкоды для эксплоитов.
2. Техника создания эксплоитов.
3. Уязвимости переполнения буфера в стеке.
4. Уязвимости переполнения буфера в кучу.
5. Уязвимости целочисленного переполнения.
6. Уязвимости переполнения кучи.
7. Защитные механизмы компиляторов.
8. Защитные механизмы операционных систем.
9. Защитные механизмы аппаратного обеспечения.
10. Методы противодействия защитным механизмам.
11. Методы поиска уязвимостей.
12. Методы безопасного программирования.

Темы заданий на экзамене:
1. Шеллкоды для эксплоитов.
2. Уязвимости переполнения буфера в стеке.
3. Уязвимости переполнения буфера в кучу.
4. Уязвимости целочисленного переполнения.
5. Уязвимости переполнения кучи.
6. Защитные механизмы компиляторов и операционных систем.
7. Уязвимости аппаратного обеспечения и прошивок.

Примеры заданий на экзамене:
1. Реализовать шеллкоды без нулевых байт.
2. Исследовать бинарное программное обеспечение, найти уязвимость и проэксплуатировать её.
3. Проэксплуатировать уязвимости и выполнить шеллкод.
4. Переполнить буфер и исполнить шеллкод.
5. Проэксплуатировать уязвимости сетевых приложений.
6. Проэксплуатировать уязвимости форматных строк.
7. Проэксплуатировать уязвимости переполнения в куче.
8. Проэксплуатировать уязвимости и обойти защиту стека.
9. Проэксплуатировать уязвимости и обойти DEP.
10. Проэксплуатировать уязвимости и обойти ASLR.
11. Проэксплуатировать уязвимость с использованием методов противодействия защитным механизмам.
12. Реализовать эксплоит с использованием ROP.
13. Обойти DEP с помощью ROP и выполнить шеллкод.
14. Проэксплуатировать уязвимости в плагинах для браузеров.
15. Написать шеллкоды для ядра Windows NT.
16. Проэксплуатировать уязвимости в драйверах под Windows NT.
17. Написать шеллкоды для ядра Linux.
18. Проэксплуатировать уязвимости в драйверах под Linux.
19. Проэксплуатировать уязвимость в аппаратном обеспечении.
20. Проэксплуатировать уязвимость в прошивке.

Примеры вопросов на экзамене:
1. Шеллкоды для эксплоитов.
2. Техника создания эксплоитов.
3. Уязвимости переполнения буфера в стеке.
4. Уязвимости переполнения буфера в кучу.
5. Уязвимости целочисленного переполнения.
6. Уязвимости переполнения кучи.

7. Защитные механизмы компиляторов.
8. Защитные механизмы операционных систем.
9. Защитные механизмы аппаратного обеспечения.
10. Методы противодействия защитным механизмам.
11. Уязвимости аппаратного обеспечения
12. Уязвимости прошивок.
13. Методы поиска уязвимостей.
14. Методы безопасного программирования.

Пример билета
1. Проэксплуатировать уязвимость с использованием методов противодействия защитным механизмам..
2. Уязвимости переполнения кучи.

6.4. Критерии оценивания

За своевременное и самостоятельное выполнение учебных работ в течение семестра студент получает рейтинговые баллы. Сумма за выполнение основных заданий в полном объёме - 100. Сверх этой суммы могут начисляться баллы за выполнение дополнительных заданий.
Пропуск по неуважительной причине одной пары влечет вычет 1 балла из итоговой суммы за семестр.
При нехватке баллов преподавателем может быть предоставлено дополнительное задание или возможность доделать задание, в котором была оценена не вся функциональность.

Основные баллы выставляются за выполнение объемных зачётных заданий, которые выполняются дома и сдаются в течение семестра. Сумма в 100 баллов делится между зачётными заданиями (не обязательно равномерно). При выдаче зачётного задания определено сколько баллов выставляется за реализацию определённой функциональности. Для зачётных заданий может быть определена функциональность повышенной сложности, за выполнение которой выставляются дополнительные баллы. Также дополнительные баллы могут быть выставлены по усмотрению преподавателя за особо примечательную реализацию.
При сдаче зачётного задания производится опрос по техническим деталям реализации и по теории, используемой при выполнении заданий. Неудовлетворительный ответ будет означать несамостоятельность выполнения задания, что влечёт выставление 0 баллов за соответствующую функциональность. Если для одного задания это повторяется более 2 раз, то за всё задание выставляется 0 баллов без возможности повторной сдачи.
Выполнение заданий предполагает некоторую программную реализацию, к которой будут предъявляться обычные требования по качеству кода. Код должен быть удобочитаемым, хорошо структурированным, написанным в едином стиле. Иначе возможна сбавка до 5 баллов. За программные ошибки, приводящие к работоспособности кода не для всех возможных случаев, возможна сбавка до 10 баллов (в зависимости от критичности ошибки). За программные ошибки, приводящие к аварийному некорректному завершению программы, возможна сбавка до 10 баллов (в зависимости от критичности ошибки).
По пройденному материалу выдаются небольшие задания для выполнения дома и/или во время семинарских занятий. За эти задания выставляются небольшие дополнительные баллы. Сдавать их можно либо в день выдачи либо на следующем занятии. Домашние и аудиторные задания – это небольшие задания, за которые обычно выставляется 1-2 балла. Они оцениваются атомарно: либо задание выполнено (выставляется указанное при выдаче задания количество баллов), либо не выполнено (0 баллов).

Итоговая оценка за дисциплину выставляется по результатам выполнения заданий текущего контроля. При необходимости во время зачёта и экзамена может быть предоставлена возможность получить дополнительные баллы (не более 20), выполнив дополнительные задания и ответив (в устной форме) на вопросы.
Дополнительные задания, выдаваемые на зачёте и экзамене, являются относительно объемными, за них выставляется до 10-15 баллов. Поэтому к ним применимы описанные выше критерии оценивания зачётных заданий с соответствующей корректировкой баллов: сбавка за некорректную работу до 5 баллов, за аварийное завершение – до 5 баллов.

Ответ на зачёте и экзамене оценивается по трём параметрам.
1. Построение ответа (структура ответа, грамотность речи, последовательность и т.д.).
Студент самостоятельно правильно выстраивает структуру ответа, изложение последовательное, речь грамотная без оговорок. 2 балла
Изложение студента непоследовательное и обрывочное, взаимосвязи частей ответа не всегда прослеживаются. Раскрытие сути ответа невозможно без уточняющих вопросов. 1 балл.
Студент испытывает существенные трудности при самостоятельном построении ответа, способен только давать краткие ответы на конкретные вопросы. 0 баллов.
2. Фактическая полнота ответа.

Студент правильно ответил на теоретический вопрос билета. Показал отличные знания в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы. 4 балла.
Студент ответил на теоретический вопрос билета с небольшими неточностями. Показал хорошие знания в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов. 3 балла.
Студент ответил на теоретический вопрос билета с существенными неточностями. Показал удовлетворительные знания в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей. 2 балла.
При ответе на теоретический вопрос билета студент продемонстрировал недостаточный уровень знаний. При ответах на дополнительные вопросы было допущено множество неправильных ответов. 1 балл.
Студент не ответил на вопрос. 0 баллов.
3. Собственный анализ излагаемого материала его оценка в контексте взаимодействия с другими областями, умение применять на практике.
Студент ясно осознаёт место излагаемого материала в общей структуре профессионального знания, знает стандартные примеры использования и предлагает свои, даёт собственные компетентные оценки. 4 балла.
Студент осознаёт взаимосвязи и знает стандартные примеры использования. Допускает неточности при самостоятельном анализе. 3 балла.
Студент в общих чертах осознаёт взаимосвязи и знает стандартные примеры использования. При проведении самостоятельного анализа нуждается в уточняющих вопросах, при этом допускает существенные неточности. 2 балла.
Студент знает основные стандартные примеры использования. Не осознаёт взаимосвязей с другими областями. 1 балл.
Студент не осознаёт взаимосвязей и практическое приложение излагаемого материала. 0 баллов.

Баллы, полученные за выполнение заданий текущего контроля и промежуточной аттестации, переводятся в оценки за экзамен и зачет следующим образом.
Перевод рейтинговых баллов в оценки за зачет:
61 и более баллов – зачтено;
60 и менее баллов – не зачтено.
Перевод рейтинговых баллов в оценки за экзамен:
91 и более баллов – отлично;
76 - 90 баллов – хорошо;
61 - 75 баллов – удовлетворительно;
60 и менее баллов – неудовлетворительно.

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	Зубков С. В.	Assembler. Для DOS, Windows и Unix (https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1243)	Москва : ДМК Пресс, 2008	ЭБС
Л1.2	Кузнецов А.С., Якимов И.А., Пересунько П.В.	Системное программирование: учебное пособие (https://znanium.com/catalog/document?id=342172)	Красноярск : Сибирский федеральный университет, 2018	ЭБС
Л1.3	Монаппа К. А.	Анализ вредоносных программ (https://e.lanbook.com/book/123709)	Москва : ДМК Пресс, 2019	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Рудаков П. И., Финогенов К. Г.	Язык ассемблера: уроки программирования: практическое пособие (https://biblioclub.ru/index.php?page=book&id=89393)	Москва : Диалог-МИФИ, 2001	ЭБС

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.2	Котельников Е.	Введение во внутреннее устройство Windows: курс лекций (https://biblioclub.ru/index.php?page=book&id=429084)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л2.3	Аблязов Р. З.	Программирование на ассемблере на платформе x86-64 (http://e.lanbook.com/books/element.php? pl1_cid=25&pl1_id=1273)	Москва : ДМК Пресс, 2011	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Лань [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Лань. – URL: http://e.lanbook.com/. http://e.lanbook.com/
Э2	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. – URL: http://biblioclub.ru/. http://biblioclub.ru/

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Visual Studio

VirtualBox

Adobe Reader

Notepad++

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. MSDN Library [Электронный ресурс]. URL: https://msdn.microsoft.com/.

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, персональными компьютерами.

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)

Для изучения дисциплины предусмотрены проведение лекционных и лабораторных занятий, а также

самостоятельная работа студентов.
Лекционные занятия обеспечивают теоретическое изучение дисциплины. Основными методами обучения являются информационно-объяснительный и проблемный. На лекциях излагается основное содержание тем программы, проводится анализ основных понятий и методов, разбираются примеры программного кода, демонстрируются особенности функционирования эксплоитов и защитных механизмов, обсуждаются возможные приложения изложенных методов.
Лабораторные занятия служат для закрепления теоретических основ, излагаемых в лекциях, и получения практического опыта реализации методов эксплуатации программного обеспечения. Основные методы: репродуктивный и частично-поисковый. Для проведения текущего промежуточного контроля на каждом лабораторном занятии выдаются небольшие практические задания, рассчитанные на выполнение в течение занятия, и домашние задания.
Для самостоятельной работы студентам следует использовать методические материалы, имеющиеся в Научной библиотеке ЧелГУ, а также выложенные на сайте математического факультета ЧелГУ и на сайте кафедры компьютерной безопасности и прикладной алгебры. Для студентов проводятся индивидуальные консультации, каждому студенту при необходимости могут быть выданы индивидуальные задания для самостоятельной работы, позволяющие углубленно изучить отдельные темы дисциплины.
Стоит особо подчеркнуть, что курс носит практический характер. Основным результатом освоения курса является умение применять изученные методы на практике. Поэтому для успешного освоения курса обязательно полное выполнение всех практических заданий.

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.

10.05.01, специализация N 1 "Анализ безопасности компьютерных систем", Компьютерная безопасность, Анализ уязвимостей программного обеспечения, 2023, очная

Проректор по учебной работе утверждено 24.04.2023 В.Е. Федоров

Ученым советом математического факультета

Протокол заседания № 8 от 13.04.2023

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 10 от 31.03.2023

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) И. А. Маткин

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1