УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «16 » 06 2020 г., протокол №5/20
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16 » 06 2020 г.,

РАБОЧАЯ ПРОГРАММА

Дисциплина	Анализ уязвимостей программного обеспечения
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » 09 2020г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Сутыркина Екатерина Алексеевна	ИБиТУ	доцент, к.ф-м.н

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / Андреев А.С. / *(подпись) (Ф.И.О.)*	_____ / Андреев А.С. / *(подпись) (Ф.И.О.)*
« 10 » 06 2020г.	« 10 » 06 2020г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Анализ уязвимостей программного обеспечения» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию системного и аналитического мышления.

Цели освоения дисциплины:

- изучение студентом основных видов уязвимостей программного обеспечения;
- освоение основных методов и средств анализа и устранения уязвимостей программных реализаций;

Задачи освоения дисциплины:

– развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций;

– формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;

– формирование навыков анализа программных реализаций на предмет наличия уязвимостей;

– развитие навыков организации антивирусной защиты

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к вариативной части дисциплин по выбору Б1.В.ДВ. в рамках профессионального цикла Б1 образовательной программы и читается в 10-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов Основы построения защищенных компьютерных сетей, Основы построения защищенных баз данных, Защита программ и данных, Криптографические методы защиты информации, Основы информационной безопасности, Системный анализ, Теория игр и исследование операций.

Основные положения дисциплины используются в дальнейшем при изучении дисциплин: Криптографические протоколы, Методы верификации, Учебная практика, Производственная практика, Научно-исследовательская работа, Преддипломная практика, ГИА, Подготовка и защита ВКР.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Защита программ и данных» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства	Знать: основные средства и методы анализа программных реализаций на предмет уязвимостей Уметь: разрабатывать программы с защитой от уязвимостей Владеть: навыками выявления и устранения уязвимостей

криптографической защиты информации	
ПК-10 способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: способы, методы и критерии оценки эффективности реализации систем защиты информации Уметь: пользоваться способами, методами и критериями оценки эффективности реализации систем защиты информации Владеть: способами, методами и критериями оценки эффективности реализации систем защиты информации
ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	Знать: основные приёмы и методы создания программных закладок Уметь: противодействовать программным закладкам Владеть: навыками выявления уязвимостей в программных реализациях
ПК-15 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать: способы, методы и критерии оценки эффективности реализации систем защиты информации Уметь: пользоваться способами, методами и критериями оценки эффективности реализации систем защиты информации Владеть: способами, методами и критериями оценки эффективности реализации систем защиты информации
ПК-19 способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать: основные виды и наиболее известные примеры программных уязвимостей Уметь: выявлять и устранять уязвимости программных реализаций и локализовать их последствия Владеть: навыками владения с современными отладчиками
ПСК-2.1 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знать: группы типичных уязвимостей ПО Уметь: использовать СО модель компьютерной системы для создания эффективных алгоритмов безопасности Владеть: навыками работы с современными дизассемблерами и отдатчиками
ПСК-2.2 способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знать: математические методы оценки безопасности программных реализаций Уметь: оценивать опасность обнаруженных уязвимостей программных реализаций Владеть: приёмами анализа программных реализаций на предмет наличия уязвимостей
ПСК-2.3 способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы	Знать: математический аппарат построения адекватных систем оценки безопасности ПО Уметь: проводить экспертизу качества и надежности программных и программно-аппаратных средств

безопасности с использованием современных математических методов	обеспечения информационной безопасности Владеть: основными методами математического аппарата по анализу несанкционированного доступа к ПК
ПСК-2.4 способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знать: специальные средства защиты в современных средах программирования Уметь: строить соответствующие математические модели Владеть: способами оценки и прогнозирования работы моделей безопасности
ПСК-2.5 способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации	Знать: статические и динамические методы анализы программных реализаций Уметь: выбирать адекватный инструмент для оценки эффективности безопасности ПО Владеть: способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 3**.**

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
		10		
Контактная работа обучающихся с преподавателем	30	30		
Аудиторные занятия:				
• Лекции	20	20		
• Практические и семинарские занятия				
• Лабораторные работы (лабораторный практикум)	10	10		
Самостоятельная работа	78	78		
Форма текущего контроля знаний и контроля самостоятельной		Лабораторные работы, тестирование		

работы				
Курсовая работа				
Экзамен				
Всего часов по дисциплине	108	108		
Виды промежуточной аттестации (экзамен, зачет)		зачет		
Общая трудоемкость в зач. ед.	3	3		

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	
Раздел 1. Внедрение программных закладок							
1.Предпосылки внедрения программных закладок	18	5		3*	*	10	лабораторная работа, тестирование
Раздел 2. Обзор уязвимостей, некоторых видов атак и средств защиты							
2.Эволюция угроз.	12	2		0		10	
3.Основные уязвимости.	27	4		3*	*	20	лабораторная работа, тестирование
4.Целевые атаки.	27	4		3*	*	20	лабораторная работа, тестирование
5.Атаки финансовых объектов	24	5		1*	*	18	лабораторная работа, тестирование
Зачеты	1,8						
Итого	108	20		10	(10*)	78	

*-занятия проводятся в интерактивной форме

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Внедрение программных закладок.

Тема 1. Предпосылки внедрения программных закладок. Утверждение о защищенности в рамках субъектно-ориентированной модели компьютерной системы. Условия для внедрения программной закладки. Факторы, мешающие добиться абсолютной защищенности компьютерной системы в реальности. Понятие эксплойта. Пример эксплойта: уязимость сервиса RPC. Группы типичных уязвимостей программного обеспечения. Переполнение буферов. Переполнение буфера в стеке. Простейший пример переполнения буфера. Специальные встроенные средства защиты от переполнения буферов в современных средах программирования. Security cookie. Переполнение буфера в куче. Пример переполнения буфера в куче. Наиболее известные уязвимости, связанные с переполнением буферов. DEP. Недостатки DEP. ASLR. Отсутствие необходимых проверок введенных данных. Эксплойт GetAdmin. Эксплойт %00. Эксплойты Internet Explorer и MSOffice XP. Некорректный контекст безопасности. Эксплойт AdminTrap. Системные окна на рабочем столе пользователя. Устаревшие функции. Эксплойт NetDDE. WMF Exploit (MS06-001). Другие уязвимости. Уязвимость program.exe.

Раздел 2. Обзор уязвимостей, некоторых видов атак и средств защиты.

Тема 2. Эволюция угроз. Вирусы. Черви. Khobe (обход антивирусной защиты). DoS-атаки. MAC-flooding. USB-флэш атака. Phishing. Подмена субдомена DNS. Сокращения названий субдоменов DNS. Троянский конь. SPAM. Scam. Instant Messaging.

Тема 3. Основные уязвимости. Badware. Атака через прокси-серверы. Potentially Unwanted Program (PUP - потенциально нежелательная программа). Атаки через WEB-серверы. Path Traversal (slash-атаки). Spyware. Атаки нулевого дня. Adware (Madware) и Grayware. Взломщик паролей. Dialer. Browser Hijackers. Bot-коды. Ransomware, Scareware и Rouge Security (rogueware). Rootkit. Crimeware. Cross-Site Scripting (CSS). Взлом WEB-приложений с помощью "отравленных" Cookie. Email bombing. Clickjacking и likejecking. Атаки Salami. XML-бомба. Pharming. BHO.

Тема 4. Целевые атаки. Тенденции сетевой безопасности в последние годы. Vishing. Вредоносные программы, сопряженные с Web. Службы новостей RSS/ATOM. XSS Scripting. SQL Injection (SQLi). ARP-spoofing. Фальсификация межсайтовых запросов CSRF. Обход фильтра XSS. Экспоненциальные атаки XSS. Использование фальсификации заголовков запросов. Черные ходы в медиа-файлах. Атаки "Drive-by Download". Человек посередине (Man-In-The-Middle). SideJacking. Атака Man-In-The-Browser.

Тема 5. Атаки финансовых объектов. Crapware. Grayware. Скрытые угрозы безопасности. Фальсификация имен файлов. Атаки APT. RFI-атака. Вставление удаленного файла. Несанкционированный доступ к машинам, отключенным от Интернет.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практические и семинарские занятия не предусмотрены учебным планом.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Цикл лабораторных работ включает в себя 3 объемных лабораторных работы. Задачами цикла являются:

– освоение основных методов анализа уязвимостей программных реализаций на практике;

– освоение принципов работы с современными дизассемблерами и отладчиками;
– получение навыков устранения уязвимостей программных реализаций на компьютерных системах.

Лабораторная 1. Поиск уязвимостей в программной реализации.

Цель: освоение основных приемов и методов поиска уязвимостей в программных реализациях.

Содержание работы: анализ программных реализаций для ОС семейства Windows на предмет наличия наиболее известных уязвимостей методом экспериментов с “черным ящиком”, статическим и динамическим методами анализа программных реализаций.

Результат: подробная демонстрация результатов работы, отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием дизассемблеров, отладчиков, и вспомогательных программных средств, перечисленных в списке п.9 в), отчет должен содержать подробный анализ проделанной работы.

Лабораторная 2. Программные закладки.

Цель: освоение основных приемов и методов создания программных закладок и противодействия программным закладкам.

Содержание работы: методы создания программной закладки, внедрения программной закладки, выявления программной закладки, удаления программной закладки.

Результат: программная закладка и программа для удаления программной закладки, подробная демонстрация результатов работы, отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием дизассемблеров, отладчиков, и вспомогательных программных средств, перечисленных в списке п.9 в), отчет должен содержать подробный анализ проделанной работы.

Лабораторная 3. Атаки на компьютерную систему.

Цель: освоение основных приемов и методов использования уязвимостей в компьютерной системе для атаки и организация противодействия атаке на компьютерную систему.

Содержание работы: основные уязвимости компьютерной системы, использование уязвимостей компьютерной системы для атаки, методы противодействия атаке на компьютерную систему.

Результат: подробная демонстрация результатов работы, отчет о проделанной работе.

Методические указания: выполнение задания должно вестись с использованием дизассемблеров, отладчиков, и вспомогательных программных средств, перечисленных в списке п.9 в), отчет должен содержать подробный анализ проделанной работы.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые работы, контрольные работы, рефераты не предусмотрены учебным планом.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

1. Как эволюционировали вирусы. Какие из зловредов наиболее опасны?
2. Как реализуются атаки переполнения буфера? Как этого избежать? Приведите пример реализации атаки.
3. Как устроены и какие бывают DoS-атаки?
4. Как организована атака MAC-flooding?
5. Что такое Phishingовый сайт?
6. Как происходит подмена субдомена DNS? Сокращения названий субдоменов DNS.

7. Что такое Potentially Unwanted Program (PUP - потенциально нежелательная программа)?
8. Как атакуют WEB-серверы? Какие существуют способы встраивания вредоносного кода на страницу?
9. Что такое «Атаки нулевого дня». Что делают разработчики, узнав о таких атаках? Как узнать, что обнаружена уязвимость и как её закрыть?
10. Что такое Adware (Madware) и Grayware?
11. Как реализуются Hijackers –атаки?
12. Что такое Ransomware, Scareware и Rouge Security (rogueware)?
13. Какие виды Cross-Site Scripting (XSS) вам известны? Как онореализуются и как от них защититься?
14. Как происходит взлом WEB-приложений с помощью "отравленных" Cookie?
15. Email bombing
16. Кликеры Clickjacking и likejecking, что это?
17. Угрозы на стороне сервера. SQL Injection (SQLi).
18. Что такое ARP-spoofing и фальсификация межсайтовых запросов CSRF.
19. Как использовать черные ходы в медиа-файлах?
20. Разновидности атаки «Человек посередине (Man-In-The-Middle).»
21. Какие на данный момент актуальны атаки финансовых объектов?
22. Какие имеются скрытые угрозы безопасности?
23. Что понимают под несанкционированным доступом в машины, отключенные от Интернет?

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

В рамках самостоятельной работы студентам выделяется время на:

– теоретическую подготовку по дисциплине посредством изучения тематической литературы (базовой, дополнительной) и конспектов лекций по дисциплине;

– практическую подготовку по дисциплине посредством выполнения лабораторных работ;

– подготовку к сдаче итогового зачета по дисциплине.

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Предпосылки внедрения программных закладок.	Проработка учебного материала, подготовка к сдаче зачета, лабораторные работы	10	Лабораторная работа, зачет, тест
2. Эволюция угроз	Проработка учебного материала, подготовка к сдаче зачета	10	Зачет , тест
3. Основные уязвимости	Проработка учебного материала, подготовка к сдаче зачета	20	Лабораторная работа, зачет, тест
4. Целевые атаки	Проработка учебного материала, подготовка к сдаче зачета	20	Лабораторная работа, зачет, тест
5. Атаки финансовых объектов	Проработка учебного материала, подготовка к сдаче зачета	18	Лабораторная работа, зачет, тест

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Платонов Владимир Владимирович. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для вузов по спец. 090102 "Компьютерная безопасность", 090105 "Комплекс. обеспечение информ. безопасности автоматизир. систем" / Платонов Владимир Владимирович. - Москва : Академия, 2006
2. Щербаков А.Ю., А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. - М.: Книжный мир, 2009. - 352 с. - ISBN 978-5-8041-0378-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785804103782.html
3. *Внуков, А. А.* Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/444046

дополнительная

1. *Казарин, О. В.* Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/437163

Учебно-методическая

1. Сутыркина Е. А. Методические указания к лабораторным работам по дисциплине «Анализ уязвимостей программного обеспечения» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / Е. А. Сутыркина; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 1,1 МБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4286

Согласовано:

Гл. спец. - ро НБ УлГУ	Полина И. Ю		18.06.2020
должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

МойОфис Стандартный, Альт Рабочая станция 8.

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением :

- RadASM,
- WinAsm Studio,
- MS MASM,
- fasm,
- NASM,
- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- MS WinDbg,
- SysInternals,
- Qt Creator / Qt,
- Eclipse CDT.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: https://www.biblio-online.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: http://znanium.com. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2020].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО

ЦРГОП и ИТ. – URL: http://window.edu.ru/. – Текст : электронный.
6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.
7.2. Образовательный портал УлГУ. – URL: http://edu.ulsu.ru. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

зам нач упр	Ключкова ВВ		18.06.2020
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС,ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус.

Аудитория 24б для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус.

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров.

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- RadASM,
- WinAsm Studio,
- MS MASM,
- fasm,
- NASM,
- Hex-Rays IDA Pro Disassembler,
- OllyDbg.
- MS WinDbg,
- SysInternals,
- Qt Creator / Qt,
- Eclipse CDT.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться некоторые из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент _____ Сутыркина Екатерина Алексеевна
подпись должность ФИО