УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от « 18 » 05 2021 г., протокол № 4/21
Председатель _____М.А. Волков___
(подпись, расшифровка подписи)
« 18 » 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Обнаружение вторжений и защита информационных систем
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	4

Направление бакалавриата**: 09.03.03** «Прикладная информатика»,
профиль «Информационная среда» (Квалификация (степень) - «бакалавр»)
код направления (специальности), полное наименование *полное наименование*

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

Дата введения в учебный процесс УлГУ: « 01 » 09 2021 г.

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
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационные технологии»
/_____/ Андреев А.С. / *(подпись)* *(Ф.И.О.)* « 12 » 05 2021 г.	/_____/ Волков М.А. / *Подпись* *(Ф.И.О.)* « 18 » 05 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

Цель курса – заложить методически правильные основы знаний, необходимые будущим специалистам - практикам в области защиты информации.

Задачи освоения дисциплины:

Основными задачами дисциплины являются:

- ознакомить обучаемых с основным направлениями и методами защиты интрасетей от вторжений;

- научить применять стандартные средства защиты от вторжений (атак).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Обнаружение вторжений и защита информационных систем» изучается в 8 семестре и относится к числу обязательных дисциплин блока Б1.В, предназначенного для студентов, обучающихся по направлению подготовки бакалавриата 09.03.03 «Прикладная информатика».

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов: «Информационные технологии»; «Информационные сети»; «Архитектура вычислительных систем и компьютерных систем»; «Криптографические методы защиты информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области информационных технологий и информационных сетей и основ криптографии;

способность использовать нормативные правовые документы;

способность анализировать социально-значимые проблемы и процессы.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Современные системы автоматизации разработки информационных систем»; «Программирование для Интернет».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ПК-6 - способность принимать участие во внедрении информационных систем	**Знать:** Состав информационных систем и основные требования по их внедрению **Уметь:** Внедрять информационные системы **Владеть:** Навыками внедрения информационных систем
ПК-7 - способность настраивать, эксплуатировать и сопровождать информационные системы и сервисы	**Знать:** Основные современные информационные системы и сервисы в области защиты информации **Уметь:** Настраивать, эксплуатировать и сопровождать типовые средства защиты информации от несанкционированного

	доступа **Владеть:** Навыками администрирования основных подсистем информационной безопасности объекта защиты
ПК-8 - способность проводить тестирование компонентов программного обеспечения ИС	**Знать:** Основные требования информационной безопасности в ходе тестирования программного обеспечения ИС **Уметь:** Проводить тестирование компонентов программного обеспечения ИС учетом основных требований информационной безопасности **Владеть:** Методологией тестирования компонентов программного обеспечения ИС в процессе защиты информации

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 5.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	**Количество часов (форма обучения ___*очная*____)**			
	Всего по плану	**В т.ч. по семестрам**		
		8 семестр		
1	**2**	**3**	**4**	**5**
Контактная работа обучающихся с преподавателем	80	80/80*		
Аудиторные занятия:	80	80/80*		
Лекции	20	20/20*		
Практические и семинарские занятия	20	20/20*		
Лабораторные работы (лабораторный практикум)	40	40/40*		
Самостоятельная работа	64	64		
Форма текущего контроля знаний и контроля самостоятельной работы:		Тестирование на семинарах и лабораторных работах; - вопросы и		

Тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)		тесты перед лекциями; - рефераты на заданные темы		
Курсовая работа				
Виды промежуточной аттестации (экзамен, зачет)	экзамен 36	экзамен 36		
Всего часов по дисциплине:	180 с экзаменом	180 с экзаменом		

* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

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

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	Форма текущего контроля знаний
		лекции	Практич. занятия, семинар	Лабораторные работы			
1	2	3	4	5	6	7	8
Раздел 1. Атаки на интрасети							
1. Введение в курс дисциплины.	3	2				1	Тесты Т1 реферат № 1
2. Классификация вторжений. Типовые удаленные атаки.	6	2	2			2	Тесты Т2, рефераты (№ 1,7,8,9)
3. Интрасети и причины, способствующие атакам.	5	2	2			1	Тесты Т3 рефераты (№ 2,3)
4. Основные методы, используемые нарушителями для проникновения в интрасети.	10	2	4			4	Тесты Т4, рефераты (№ 2,3)
Раздел 2. Основные методы и средства защиты интрасетей от вторжений							
5. Многоуровневая защита интрасетей.	22	2	2	6		12	Тесты Т5, рефераты (№ 10, 11),

							лаб. раб. 1
6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.	24	4	4	6		10	Тесты Т4, рефераты (№ 4,5,12), лаб. раб. 2
7. Системы обнаружения вторжений.	48	4	4	18		22	Тесты Т5, рефераты (№ 2, 13), лаб. раб. № 3, 4
8. Виртуальные частные сети.	26	2	2	10		12	Тесты Т6, рефераты (№ 6,14), лаб. раб. 5
Итого:	144	20	20	40		64	

5. СОДЕРЖАНИЕ КУРСА (МОДУЛЯ)

Раздел 1. Атаки на интрасети

Тема 1. Введение в курс дисциплины.

Во введении рассмотрена актуальность изучаемой дисциплины «Обнаружение вторжений и защита информационных систем». Дана краткая история вторжений (атак) на интрасети и определения основных понятий. Перечислены организации, которые наиболее часто подвержены попыткам осуществления атак: финансовые учреждения и банки; сервис-провайдеры Internet; фармацевтические компании; правительственные и оборонные предприятия; партнеры и заказчики различных правительственных учреждений; международные корпорации.

Тема 2. Классификация вторжений. Типовые удаленные атаки.

Дан вариант классификация вторжений (атак). Рассмотрены типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании). Приведены подходы к защите от типовых удаленных атак.

Тема 3. Интрасети и причины, способствующие атакам.

Понятие интрасети и задачи её защиты. Виды интрасетей. Основные технологии, необходимые для создания интрасетей. Уязвимости интрасетей со стороны всевозможных атак. Роль администрирования интрасетей для защиты их от вторжений.

Тема 4. Основные методы, используемые нарушителями для проникновения в интрасети.

В данной теме рассмотрены основные методы развертывания атак на интрасети, а именно: классические методы (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия); современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы защиты интрасетей от вторжений

Тема 5. Многоуровневая защита интрасетей.

Рассматриваются уровни, обеспечивающие эффективную защиту сети. Она складывается из следующих основных компонентов: политики безопасности интрасети организации; сетевого аудита; защиты на основе межсетевых экранов и систем обнаружения вторжений.

Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Рассмотрена технология межсетевых экранов (МЭ) - одна из самых первых технологий защиты корпоративных сетей от внешних угроз. Показано, что МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты. Функции МЭ. Рассмотрена защита корпоративных сетей на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI (экранирующий маршрутизатор, шлюз сеансового уровня, шлюз прикладного уровня).

Тема 7. Системы обнаружения вторжений.

Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое обнаружение вторжений. Роль хоста-бастиона при обнаружении вторжений.

Тема 8. Виртуальные частные сети.

Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

6.1 Практические занятия не предусмотрены учебным планом дисциплины.

6.2 Темы семинарских занятий:

Раздел 1. Атаки на интрасети

Тема 2. Классификация вторжений. Типовые удаленные атаки (семинар).

1. Обнаружение вторжений. Краткий исторический обзор.
2. Классификация вторжений (атак).
3. Типовые удаленные атаки (анализ сетевого трафика, подмена доверенного субъекта, введение ложного объекта компьютерной сети, отказ в обслуживании).

Тема 3. Интрасети и причины, способствующие атакам (семинар).

1. Понятие интрасети и задачи ее защиты.
2. Сегментирование интрасетей.
3. Проблемы безопасности интрасетей.

Тема 4. Основные методы, используемые нарушителями для проникновения в интрасети (семинар).

1. Классические методы (подбор пароля, метод «грубой силы», метод «зашифровать и сравнить», социальная инженерия).
2. Современные методы (перехват данных, мониторинг в системе X Window, подмена системных утилит, нападения с использованием сетевых протоколов ("Летучая смерть", SYN-бомбардировка, спуффинг).

Раздел 2. Основные методы защиты интрасетей от вторжений

Тема 5. Многоуровневая защита интрасетей (семинар).

1. Политика безопасности интрасети организации.
2. Сетевой аудит.
3. Системы обнаружения вторжений и межсетевые экраны.

Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI (семинар).

1. Классификация межсетевых экранов**.**
2. Функции межсетевых экранов**.**

3. Особенности функционирования межсетевых экранов на различных уровнях модели OSI (экранирующий маршрутизатор, шлюз сеансового уровня, шлюз прикладного уровня).

Тема 7. Системы обнаружения вторжений (семинар).

1. Классификация систем обнаружения вторжений.
2. Интеллектуальное и поведенческое обнаружение вторжений.
3. Роль хоста-бастиона при обнаружении вторжений.

Тема 8. Виртуальные частные сети (VPN) (семинар).

1. Основные понятия и функции VPN.
2. Варианты построения виртуальных защищенных каналов.
3. Средства обеспечения безопасности VPN.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Раздел 2. Основные методы и средства защиты интрасетей от вторжений

Тема 5. Многоуровневая защита интрасетей.

Лабораторная работа № 1. **(6 часов).** «Разработка Политик ИБ предприятия».

Цель: Анализ информационных активов, используемых компанией и выработка концепции основ деятельности по обеспечению корпоративной информационной безопасности. Результат: отчет.

Методические указания: основное внимание должно быть уделено практическому выявлению угроз и базовых уязвимостей конкретных информационных активов предприятия, а также выбору методов и средств противодействия имеющимся угрозам информационной безопасности.

Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Лабораторная работа № **2 (6 часов).** Назначение и возможности встроенных межсетевых экранов (МЭ).

Цель: и зучить возможности и научиться работать с встроенными МЭ (ОС и антивирусные пакеты). Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей встроенных МЭ.

Тема 7. Системы обнаружения вторжений.

Лабораторная работа № 3 **(8 часов).** Назначение и возможности системы обнаружения вторжений «**Dallas Lock**».

Цель: изучить возможности и научиться работать с СОВ «Dallas Lock». Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей СОВ «Dallas Lock».

Лабораторная работа № 4 **(10 часов).** Назначение и возможности Детектора атак АПКШ «Континент».

Тема 8. Виртуальные частные сети (VPN).

Лабораторная работа № 5 **(10 часов)**. Назначение и возможности ПАК «ViPNet».

Цель: Изучить возможности и научиться работать с ПАК «ViPNet». Результат: отчет.

Методические указания: основное внимание должно быть уделено настройке и практическому освоению возможностей ПАК «ViPNet» по построению витрувльныз частных сетей.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

8.1 Курсовые и контрольные работы не предусмотрены учебным планом дисци-

плины.

8.2 Примерная тематика рефератов:

1. Обнаружение вторжений. Краткий исторический обзор.
2. Основные методы обнаружения вторжений.
3. Атаки на сети с использованием сетевых протоколов.
4. Эталонная сетевая модель OSI.
5. Особенности функционирования межсетевых экранов на различных уровнях модели OSI.
6. Виртуальные частные сети (VPN).
7. Типовые удаленные атаки на интрасети.
8. Классификация вторжений (атак).
9. Роль администрирования интрасетей для защиты их от вторжений.
10. Политики безопасности интрасети организации.
11. Сетевой аудит.
12. Технология межсетевых экранов.
13. Классификация систем обнаружения вторжений.
14. Назначение и возможности ПАК «ViPNet».

8.2.1 Правила оформления рефератов

1. Объём реферата 7-10 листов печатного текста. К оформлению рефератов предъявляются такие же требования, как и к курсовым работам для студентов 3 курса, описанные в учебно-методическом пособии: Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Обнаружение вторжений (атак). Краткий исторический обзор.
2. Классификация вторжений (атак).
3. Типовые удаленные атаки. Анализ сетевого трафика.
4. Типовые удаленные атаки. Подмена доверенного субъекта.
5. Типовые удаленные атаки. Введение ложного объекта компьютерной сети.
6. Типовые удаленные атаки. Отказ в обслуживании.
7. Понятие интрасети и задачи ее защиты.
8. Проблемы безопасности интрасетей.
7. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «подбор пароля».
8. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «грубой силы».
9. Классические методы, используемые нарушителями для проникновения в интрасети. Метод «зашифровать и сравнить».
10. Классические методы, используемые нарушителями для проникновения в интрасети. Социальная инженерия.
11. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «перехват данных».
12. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «мониторинг в системе X Window».
13. Современные методы, используемые нарушителями для проникновения в интрасети. Метод «подмена системных утилит».
14. Современные методы, используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов "Летучая смерть".

15. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «SYN-бомбардировка».

16. Современные методы**,** используемые нарушителями для проникновения в интрасети. Метод нападения с использованием сетевых протоколов «спуффинг».

19. Многоуровневая защита интрасетей. Политика безопасности интрасети организации.

20. Многоуровневая защита интрасетей. Сетевой аудит.

17. Классификация межсетевых экранов**.**

18. Функции межсетевых экранов**.**

19. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.

20. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз сеансового уровня.

21. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Экранирующий маршрутизатор.

22. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Шлюз прикладного уровня.

23. Классификация систем обнаружения вторжений.

24. Интеллектуальное и поведенческое обнаружение вторжений.

25. Роль хоста-бастиона при обнаружении вторжений.

26. Виртуальные частные сети (VPN). Основные понятия и функции VPN.

27. Варианты построения виртуальных защищенных каналов.

28. Средства обеспечения безопасности виртуальных частных сетей (VPN).

29. Назначение и возможности ПАК «ViPNet».

29. Назначение и возможности АПКШ «Континент».

30. Назначение и возможности Детектора атак АПКШ «Континент».

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1	2	3	4
Раздел 1. Атаки на интрасети. Тема 1. Введение в курс дисциплины	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 1. Тема 2. Классификация вторжений. Типовые удаленные атаки	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	2	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 1. Тема 3. Интрасети и причины, способствующие атакам	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	1	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 1. Тема 4. Основные методы, используемые нарушителями для проникновения в интрасети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	4	Тесты перед лекцией, вопросы и тесты на семинаре, экзамен
Раздел 2. Основные методы защиты интрасетей от	Подготовка к лекции, семинару, подготовка рефе-	12	Тесты перед лекцией, тесты и

вторжений. Тема 5. Многоуровневая защита интрасетей	ратов, подготовка к лабораторным работам, подготовка к сдаче экзамена		вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 6. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI	Подготовка к лекции, семинару, подготовка рефератов, подготовка к лабораторным работам, подготовка к сдаче экзамена	10	Тесты перед лекцией, тесты и вопросы на семинаре, вопросы на лабораторной работе экзамен
Раздел 2. Тема 7. Системы обнаружения вторжений	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	22	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен
Раздел 2. Тема 8. Виртуальные частные сети	Подготовка к лекции, семинару, подготовка рефератов, подготовка к сдаче экзамена	12	Тесты перед лекцией, тесты и вопросы на семинаре, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы:

основная

1. Шелухин О.И., Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М.: Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203234.html

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469866

дополнительная

1. Бирюков А.А., Информационная безопасность: защита и нападение [Электронный ресурс] / Бирюков А. А. - М. : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785970604359.html.

2. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html.

3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. — Режим доступа: https://gostexpert.ru/gost/gost-27002-2012;

4. Туманов С.А., Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" [Электронный ресурс]: / Туманов С.А. - Новосибирск: Изд-во НГТУ, 2016. - 56 с. - ISBN 978-5-7782-2826-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778228269.html.

учебно-методическая

1. Иванцов А.М. Методические указания для самостоятельной работы студентов по дисциплине «Обнаружение вторжений и защита информации» для студентов бакалавриата по направлению 02.03.03 «Математическое обеспечение и администрирование информационных систем» и 09.03.03 «Прикладная информатика» очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 363 КБ). - Текст : электронный. http://lib.ulsu.ru/MegaPro/Download/MObject/4270

Согласовано:

ДИРЕКТОР НБ / БУРХАНОВА М.М. / / 2021
Должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – 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, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – 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, [2021]. – 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.

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/ 04.05.2021
должность сотрудника УИТиТ	ФИО	подпись дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;
- электронный замок "Соболь" – 3 комплекта;
- система защиты от НСД «Dallas Lock». 4 комплекта;
- программно-аппаратный комплекс средств защиты информации от НСД “Аккорд–АМДЗ” – 1 комплект;
- система защиты конфиденциальной информации и персональных данных «Secret Disk. Базовый комплект с USB-ключом – 4 комплекта;
- персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken – 3 комплекта.

Аудитория 2/246 укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

– для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;

– для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

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 кафедры Иванцов Андрей Михайлович
подпись должность ФИО