Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Экономический факультет

УТВЕРЖДАЮ
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т. А. Хагуров
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.06.02 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Направление
подготовки/специальности - 38.04.01 Экономика

Направленность (профиль) /
специализация - магистерская программа «Экономика и менеджмент»

Форма обучения – очная

Квалификация - магистр

Краснодар 2024

Рабочая программа дисциплины *Компьютерная безопасность* составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.04.01 «Экономика»

Программу составил(и):
А. В. Троцик, доцент, к. э. н.

Рабочая программа дисциплины *Компьютерная безопасность* утверждена на заседании кафедры маркетинга и торгового дела

протокол № 7 «21» 03 2024 г.
Заведующий кафедрой А. Н. Костецкий


подпись

Утверждена на заседании учебно-методической комиссии экономического факультета
протокол № 9 «14» мая 2024 г.
Председатель УМК факультета/института Л. Н. Дробышевская


подпись

Рецензенты:
А. А. Полиди, руководитель направления стратегического консалтинга, старший партнер, ООО «Арка-групп»
И. В. Раюшкина, заместитель директора Департамента международных связей КубГУ

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цели изучения дисциплины соотнесены с общими целями ОПОП ВО по направлению 38.04.01 «Экономика», в рамках которой преподается дисциплина «Компьютерная безопасность»: обучение студентов теоретическим основам и прикладным аспектам дизайна, выбора модели, внедрения и контроля эффективности систем безопасности, современными технологиями и подходами в реализации безопасности информационных систем, информационных ресурсов и систем автоматизации современного бизнеса.

1.2 Задачи дисциплины

1. Ознакомить с современными технологиями взлома и подходами к защите и обеспечению безопасности компьютерных систем.
2. Научить проводить анализ, выявлять необходимый набор или комбинацию технологий защиты и обеспечения безопасности компьютерных систем.
3. Обучить навыкам внедрения и настройки инструментов защиты и обеспечения безопасности компьютерных систем.
4. Ознакомить с современными методами сбора, обработки и анализа профильной информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности.
5. Научить пользоваться профильными источниками информации для выбора и проектирования наиболее подходящей системы компьютерной безопасности компании, учитывая предполагаемый объем работ, потребности в трудовых, финансовых и материально-технических ресурсах
6. Обучить методами сбора, обработки и анализа профильных источников информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности.
7. Ознакомить с современными методиками проведения самостоятельного исследования, источниками получения профильной информации, работы технологий в системах компьютерной безопасности, способам их внедрения на практике.
8. Научить проводить самостоятельный анализ профильной информации и технологий в области компьютерной безопасности, проводить тестирование и внедрение их в реальной среде.
9. Обучить навыкам анализа профильной информации и технологий в области компьютерной безопасности, проведения тестирования и внедрения их в реальной среде.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерная безопасность» относится к элективной части учебного плана.

Рассматриваемая дисциплина «Компьютерная безопасность» имеет логическую и содержательно-методическую взаимосвязь с дисциплинами: «Управление информационными технологиями», «Менеджмент», «Экономика предприятий», «Современные методы алгоритмизации и программирования» и соответствующие требования к «выходным» знаниям, умениям, опыту деятельности обучающегося, необходимым для освоения данной дисциплины.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ПК-3 Способен разрабатывать стратегии поведения экономических агентов на различных рынках	
ИПК-3.1 Анализирует стратегии поведения экономических агентов на различных рынках	*Знает* современные технологии взлома и подходы к защите и обеспечению безопасности компьютерных систем; современные методы сбора, обработки и анализа профильной информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности
	Умеет проводить анализ, выявлять необходимый набор или комбинацию технологий защиты и обеспечения безопасности компьютерных систем; пользоваться про-

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	фильными источниками информации для выбора и проектирования наиболее подходящей системы компьютерной безопасности компании, учитывая предполагаемый объем работ, потребности в трудовых, финансовых и материально-технических ресурсах
	Владеет навыками внедрения и настройки инструментов защиты и обеспечения безопасности компьютерных систем; методами сбора, обработки и анализа профильных источников информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности
ИПК-3.2 Разрабатывает предложения о совершенствованию стратегии поведения экономических агентов на различных рынках	*Знает* современные методы проведения самостоятельного исследования, источники получения профильной информации, работы технологий в системах компьютерной безопасности, способы их внедрения на практике
	Умеет проводить самостоятельный анализ профильной информации и технологий в области компьютерной безопасности, проводить тестирование и внедрение их в реальной среде
	Владеет навыками анализа профильной информации и технологий в области компьютерной безопасности, проведения тестирования и внедрения их в реальной среде

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часов), их распределение по видам работ представлено в таблице.

Виды работ	Всего часов	Форма обучения			
		очная		очно-заочная	заочная
		4-ый семестр (часы)	X семестр (часы)	X семестр (часы)	X курс (часы)
Контактная работа, в том числе:	**34**	**34**			
Аудиторные занятия (всего):	**34**	**34**			
занятия лекционного типа	12	12			
лабораторные занятия	22	22			
практические занятия					
семинарские занятия					
Иная контактная работа:	**27**	**27**			
Контроль самостоятельной работы (КСР)	26,7	26,7			
Промежуточная аттестация (ИКР)	0,3	0,3			
Самостоятельная работа, в том числе:	**83**	**83**			
Курсовая работа/проект (КР/КП) (подготовка)					
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)	83	83			
Контроль:					
Подготовка к экзамену					
час.	**144**	**144**			

Общая трудоемкость	**в том числе контактная работа**	**34**	**34**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:
Распределение видов учебной работы и их трудоемкости по темам дисциплины.
Темы дисциплины, изучаемые в 4-ом семестре *(очная форма обучения)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Преступления в сфере компьютерной безопасности, противодействие и законодательная база	11	1		2	8
2.	Базовые подходы к кодированию и декодированию, системы безопасного кодирования	11	1		2	8
3.	Использование протоколов кодирования и программирование алгоритмов кодирования	11	1		2	8
4.	Защита в операционных системах I	11	1		2	8
5.	Защита в операционных системах II	11	1		2	8
6.	Проектирование систем безопасной эксплуатации информационных ресурсов	11	1		2	8
7.	Безопасность сетевых и распределенных систем	11	1		2	8
8.	Безопасность сетевого администрирования	11	1		2	9
9.	Безопасность систем хранения данных	13	2		2	9
10.	Основы защиты экономических данных, обеспечение технической защиты экономических данных	15	2		4	9
	ИТОГО по разделам дисциплины	117	12		22	83
	Контроль самостоятельной работы (КСР)	26,7				26,7
	Курсовая работа					
	Промежуточная аттестация (ИКР)	0,3				0,3
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	144	12		22	110

2.3 Содержание тем дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1.	Преступления в сфере компьютерной безопасности, противодействие и законодательная база	Компьютерная безопасность определение и значимость в современном мире. Основные виды преступлений в сфере компьютерной безопасности. Меры противодействия киберпреступности. Основные инициативы противодействия преступлениям в сфере компьютерной безопасности.	Коллоквиум 1
2.	Базовые подходы к кодированию и декодированию. Системы безопасного кодирования	Основы процесса кодирования и декодирования. Современные методы кодирования. Современные системы безопасного кодирования.	Коллоквиум 2
3.	Использование протоколов кодирования и программирование алгоритмов кодирования	Принятые технологии кодирования в современной компьютерной безопасности. Различие и способы применения протоколов кодирования. Подходы к программированию алгоритмов кодирования.	Коллоквиум 3
4.	Защита в операционных системах I		Лабораторная работа 1

5.	Защита в операционных системах II		Лабораторная работа 2
6.	Проектирование систем безопасной эксплуатации информационных ресурсов	Типовая структура связей между элементами операционной системы и внешними ресурсами. Проектирование безопасной системы эксплуатации информационных ресурсов. Настройка безопасной системы эксплуатации информационных ресурсов. Мониторинг безопасности системы. Безопасная эксплуатации систем Linux, Windows, Виртуальных операционных систем. Модель Белл-Лападула и другие общепринятые модели систем безопасной эксплуатации информационных ресурсов.	Коллоквиум 4
7.	Безопасность сетевых и распределенных систем		Лабораторная работа 3
8.	Безопасность сетевого администрирования		Лабораторная работа 4
9.	Безопасность систем хранения данных		Лабораторная работа 5
10.	Основы защиты экономических данных, обеспечение технической защиты экономических данных	Протоколы доступа к веб-сайтам, основы защиты данных. Основы обеспечения конфиденциальности передаваемой экономической информации. Слабые места и возможности атаки на сессию пользователя. Основные инструменты гарантирования сохранности и защищенности экономических данных.	Коллоквиум 5

2.3.2 Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

№	Наименование темы	Тематика практических темы	Форма текущего контроля
1	2	3	4
1.	Преступления в сфере компьютерной безопасности, противодействие и законодательная база	Компьютерная безопасность определение и значимость в современном мире. Основные виды преступлений в сфере компьютерной безопасности. Меры противодействия киберпреступности. Основные инициативы противодействия преступлениям в сфере компьютерной безопасности.	Индивидуальный проект 1
2.	Базовые подходы к кодированию и декодированию. Системы безопасного кодирования	Основы процесса кодирования и декодирования. Современные методы кодирования. Современные системы безопасного кодирования.	Групповой проект 1
3.	Использование протоколов кодирования и программирование алгоритмов кодирования	Принятые технологии кодирования в современной компьютерной безопасности. Различие и способы применения протоколов кодирования. Подходы к программированию алгоритмов кодирования.	Кейс 1
4.	Защита в операционных системах I		Лабораторная работа 1
5.	Защита в операционных системах II		Лабораторная работа 2
6.	Проектирование систем безопасной эксплуатации информационных ресурсов	Типовая структура связей между элементами операционной системы и внешними ресурсами. Проектирование безопасной системы эксплуатации информационных ресурсов. Настройка безопасной системы эксплуатации информационных ресурсов. Мониторинг безопасности системы. Безопасная эксплуатации систем Linux, Windows, Виртуальных операционных систем. Модель Белл-Лападула и другие общепринятые модели систем безопасной эксплуатации информационных ресурсов.	Групповой проект 2

7.	Безопасность сетевых и распределенных систем		Лабораторная работа 3
8.	Безопасность сетевого администрирования		Лабораторная работа 4
9.	Безопасность систем хранения данных		Лабораторная работа 5
10.	Основы защиты экономических данных, обеспечение технической защиты экономических данных	Протоколы доступа к веб-сайтам, основы защиты данных. Основы обеспечения конфиденциальности передаваемой экономической информации. Слабые места и возможности атаки на сессию пользователя. Основные инструменты гарантирования сохранности и защищенности экономических данных.	Индивидуальный проект 2

2.3.3 Примерная тематика курсовых работ (проектов)

Курсовая работа – не предусмотрена.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Занятия лекционного и семинарского типа	Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
2	Выполнение самостоятельной работы обучающихся	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
3	Выполнение лабораторных работ	Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) 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,
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,

3. Образовательные технологии

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового штурма, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

1. *Практические занятия* - разбор конкретных ситуаций (кейсов) с заданиями, способствующими развитию профессиональных компетенций.
2. *Индивидуальные проекты* – задания, выполняемы студентом лично по заданной теме.
3. *Групповые проекты* – задания, выполняются всей группой или малыми группами по 2-3 человека. Групповая работа направлена на совместное взаимодействие, использования сильных и слабых сторон каждого члена группы и коллективной ответственностью за результат.
4. *Кейс* - это ситуация, взятая из практики, реальный случай, анализируя который студенты получают реальный опыт решения бизнес задач, а также возможность применить инструменты и знания, полученные в теории на практике, получить навык применения этих инструментов.
5. *Лабораторные работы* - направлены на применение полученных знаний на практике и фиксацию результата в виде письменного отчета или презентации.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения для проведения текущего контроля

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИПК-3.1 Анализирует стратегии поведения экономических агентов на различных рынках	*Знает* современные технологии взлома и подходы к защите и обеспечению безопасности компьютерных систем; современные методы сбора, обработки и анализа профильной информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности	Коллоквиум 1-3	Вопрос на экзамене 1-24
		Умеет проводить анализ, выявлять необходимый набор или комбинацию технологий защиты и обеспечения безопасности компьютерных систем; пользоваться профильными источниками информации для выбора и проектирования наиболее подходящей системы компьютерной безопасности компании, учитывая предполагаемый объем работ, потребности в трудовых, финансовых и материально-технических ресурсах	Кейс 1, Групповой проект 1	
		Владеет навыками внедрения и настройки инструментов защиты и обеспечения безопасности компьютерных систем; методами сбора, обработки и анализа профильных источников информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности	Лабораторная работа 1, 2, Индивидуальный проект 1	
2	ИПК-3.2 Разрабатывает предложения о совершенствованию стратегии поведения	*Знает* современные методы проведения самостоятельного исследования, источники получения профильной информации, работы технологий в системах компьютерной безопасности, способы их внедрения на практике	Кейс 1-3, Тест 4	Вопрос на экзамене 25-50

	экономических агентов на различных рынках	*Умеет* проводить самостоятельный анализ профильной информации и технологий в области компьютерной безопасности, проводить тестирование и внедрение их в реальной среде	Групповой проект 2	
		Владеет навыками анализа профильной информации и технологий в области компьютерной безопасности, проведения тестирования и внедрения их в реальной среде	Лабораторная работа 5-9, Индивидуальный проект 2	

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

Фонд оценочных средств дисциплины состоит из средств текущего контроля (практические задания) и промежуточной аттестации (экзамен).

В качестве оценочных средств, используемых для текущего контроля успеваемости, предлагается перечень вопросов, которые прорабатываются в процессе освоения курса. Данный перечень охватывает все основные разделы курса, включая знания, получаемые во время самостоятельной работы. Кроме того, важным элементом технологии является самостоятельное решение и сдача студентами заданий. Это полностью индивидуальная форма обучения. Студент рассказывает свое решение преподавателю, отвечает на дополнительные вопросы.

Коллоквиумы

Методические указания:

В данном виде проверки знаний студенту задаётся вопрос в аудитории или он размещается в системе электронного обучения Кубанского государственного университета, на который студент отвечает письменно; в случае устных ответов, письменные ответ так же дублируется в электронном виде.

Коллоквиум 1

1. Компьютерная безопасность определение и значимость в современном мире.
2. Основные виды преступлений в сфере компьютерной безопасности.
3. Меры противодействия киберпреступности.
4. Основные инициативы противодействия преступлениям в сфере компьютерной безопасности.

Критерии оценки коллоквиумов:

- оценка «отлично» выставляется студенту, если были даны полные ответы на 90-100% вопросов;
- оценка «хорошо», если были даны полные ответы на 70-89% вопросов;
- оценка «удовлетворительно», если были даны полные ответы на 40-69% вопросов;
- оценка «неудовлетворительно» выставляется если полные ответы были даны менее чем на 39% вопросов.

Индивидуальный проект

Методические указания:

Индивидуальные проекты выполняются студентом лично на заданную тематику. Проекты тесно связаны с проведением своего собственного исследования и получения профессиональных навыков по заданной теме. Результаты работы оформляются в письменном виде, а также в виде презентации для всей группы.

Индивидуальный проект 1

Исходя из таблицы анализа наиболее встречающихся видов преступлений в сфере компьютерной безопасности в 2014 году (Таблица 1) ниже:

1. Проведите анализ и перечислите наиболее вероятный тренды (направления) в развития компьютерной безопасности (5-6 трендов).

2. По каждому направлению проведите исследование о текущих инструментах, применяемых современными специалистами в сфере компьютерной безопасности.

3. Создайте презентацию своего исследования, по 1-2 слайда на каждый выявленный тренд.

4. Дайте свои рекомендации по совершенствованию подходов в компьютерной безопасности на основании представленного анализа.

5. Проведите презентацию исследования и защиту своих выводов перед группой.

Таблица 1 - Исследование причин и доли совершенных преступлений в области компьютерной безопасности

Тип преступления в области информационной безопасности	Всего совершенных от числа попыток, %	Совершенных сотрудником, %	Совершенных не сотрудником, %	Источник преступления не определен, %
Вирус, черви или другой вредоносный код	74	18	46	26
Несанкционированный доступ к информации	55	25	30	10
Нелегальное рассылка спама по электронной почте	53	6	38	17
Шпионская программа	52	13	33	18
Атака DOS	49	9	32	14
Фрод, подделка платежного носителя (карточка и тп…)	46	19	28	5
Фишинг (подделка сайта с целью сбора персональных данных пользователей)	46	5	35	12
Кража персональных данных, включая финансовую информацию	40	23	16	6
Кража интеллектуальной собственности	35	24	12	6
Намеренное раскрытие персональной или личной информации	35	17	12	9
Кража паспортных и других данных идентификации	33	13	19	6
Саботаж: намеренная порча, удаление или уничтожение информации, систем или сетей	30	14	14	6
Использование сети ботами и зомби машинами	30	6	19	10
Порча сайта	24	4	14	7
Вымогательство	16	5	9	4
Другие виды	17	6	8	7

Источник: *William Stalling, Lawrie Brown. Computer Security Principles and Practice, Third Edition, Global Edition, Pearson Education Limited, Harlow, Essex CM20 2JE, England, 2015, p 634*

Критерии оценки индивидуальных проектов:

- оценка «отлично» выставляется студенту, если были выполнены все пункты индивидуального проекта в полном объеме, подготовлена презентация и проведена защита своей работы;
- оценка «хорошо» выставляется студенту, если была выполнена большая часть пунктов индивидуального проекта, подготовлена презентация и проведена защита своей работы;
- оценка «удовлетворительно» выставляется студенту, если была выполнена меньшая часть пунктов индивидуального проекта, подготовлена презентация и проведена защита своей работы;
- оценка «неудовлетворительно» выставляется если индивидуальный проект не выполнялся.

Групповой проект

Методические указания:

Групповые проекты выполняются студентами всей группой или малыми группами по несколько человек. Проекты тесно связаны с проведением своего собственного исследования и получения профессиональных навыков по заданной теме проекта. Важен вклад каждого участника группы. Результаты работы оформляются в письменном виде, а также в виде презентации для всей группы. В процессе взаимодействия студенты

не только получают необходимые знания и навыки, но и учатся работать в команде, эффективно распределять ответственность и полномочия, учитывать мнение каждого участника.

Групповой проект 1

1. Выберите одного партнера в группе студентов курса.
2. Скачайте PGP по следующей ссылке http://ppgp.sourceforge.net/usb.html или разархивируйте приложенный к заданию архив с программой.
3. Запустите файл PortableBGP.exe
4. ВАЖНО! На этом этапе все последующие пункты должны быть подтверждены «Скрин-шотами» экрана.
5. Заполните ФИО, е-мейл и ключевую фразу для шифрования.
6. Обменяйтесь публичными ключами (так как сервера обмена публичными ключами не поддерживаются в данном ПО, вам необходимо экспортировать и переслать друг другу свои публичные ключи).
7. Импортируйте в программе публичные ключи друг друга, теперь есть возможность обмениваться шифрованными сообщениями!
8. Для шифровки сообщения нажмите кнопку Encrypt, введите текст, в поле Target выберите публичный ключ получателя сообщения.
9. Отправьте партнеру письмо с зашифрованном сообщением.
10. Партнер получает письмо, нажимает Decrypt и вводит ключевую фразу своего персонального ключа.
11. Программа дешифрует сообщение!
12. Скомпонуйте в одном файле и выложите «скрин-шоты» проведенной работы и полученного сообщения как результат выполнения своей части группового проекта.

Критерии оценки групповых проектов:

- оценка «отлично» выставляется всем студентам в группе, если были выполнены все пункты проекта в полном объеме, подготовлена презентация и проведена защита своей работы;
- оценка «хорошо» выставляется всем студентам в группе, если была выполнена большая часть пунктов проекта, подготовлена презентация и проведена защита своей работы;
- оценка «удовлетворительно» выставляется всем студентам в группе, если была выполнена меньшая часть пунктов проекта, подготовлена презентация и проведена защита своей работы;
- оценка «неудовлетворительно» выставляется всем студентам в группе если проект не выполнялся.

Лабораторные работы

Методические указания:

Работа, направленная на применение полученных знаний на практике и фиксацию результата в виде письменного отчета или презентации. Все задания в лабораторной работе структурированы по этапам и тесно связаны с практической работой студентов в классе, на предприятии или реальной рыночной среде.

Лабораторная работа 1

Проверьте насколько быстро Вы сможете взломать пароль для учетной записи операционной системы Windows:

1. Скачайте Программы подбора паролей типа HashSuiteFree, John the Ripper, Ophcrack или используйте приложенный к заданию архив с программой.
2. Скачайте Программы сбора зашифрованных паролей учетных записей (Хэш) тип Powerdump, используйте приложенный к заданию архив с программой или приложенный тестовый файл со скачанными паролями.
3. Используйте программу для сбора паролей учетных записей Вашей операционной системы или используйте приложенный файл с выгрузкой паролей в виде ХЭШ строки.
4. ВАЖНО! На этом этапе все последующие пункты должны быть подтверждены «Скрин-шотами» экрана.
5. При наличии паролей в любом виде в виде ХЭШ строки, запустите программу подбора паролей.
6. Следуйте инструкциям к выбранной программе по загрузке ХЭШ паролей.
7. Запустите функцию подбора паролей.
8. Приложите результат дешифровки из программы в виде стандартного отчета программы или «Скрин-шота».

Критерии оценки лабораторных работ:

- оценка «отлично» выставляется студенту, если были выполнены все пункты лабораторной работы в полном объеме, подготовлены соответствующие заключения, которые были изложены на презентации, получены ответы на все уточняющие вопросы в полном объеме с обоснованием и ссылками на результаты, показанные в лабораторной работе;
- оценка «хорошо», если были выполнены не все пункты лабораторной работы в полном объеме, некоторые заключения не соответствовали полученным результатам, не получены ответы на все уточняющие вопросы в полном объеме с обоснованием и ссылками на результаты, показанные в лабораторной работе;
- оценка «удовлетворительно», если были выполнены не все пункты лабораторной работы в полном объеме, большая часть заключений не соответствовала полученным результатам, не получены ответы на большую часть уточняющих вопросов в полном объеме с обоснованием и ссылками на результаты показанные в лабораторной работе;
- оценка «неудовлетворительно» выставляется если лабораторная работа не делалась.

Кейсы

Методические указания:

В данном задании студентам выдается описание конкретных ситуаций (кейсов) в бизнесе, после изучения которых студент дает свое видение решений по заданным вопросам или свои рекомендации по решению ситуативных вопросов по кейсу.

Кейс 1

по теме «Выбор корпоративного решения шифрования коммерческой информации»

Алиса ответственна за выбор корпоративного решения шифрования информации в компании. Компания продает страховые продукты. Информация, пересылаемая в компании, конфиденциальная, но не является государственной тайной. Алиса рассматривает различные виды методов шифрования и соответствующих продуктов. В итоге выбирает коммерческий продукт на основе криптографического алгоритма с открытым ключом (RSA - Rivest, Shamir и Adleman).

Вопросы и задания по кейсу:

1. Является ли выбор Алисы, наилучшим решением для компании?
2. Почему или почему нет?

Критерии оценки кейсов:

- оценка «отлично» выставляется студенту, если были даны обоснованные ответы на 90-100% вопросов, с аргументацией и выводами, подкрепленными ссылками на условия кейса, позволившие сделать данные заключения при ответе на вопросы;
- оценка «хорошо», если были даны обоснованные ответы на 70-89% вопросов, с аргументацией и выводами, подкрепленными ссылками на условия кейса, позволившие сделать данные заключения при ответе на вопросы;
- оценка «удовлетворительно», если были даны обоснованные ответы на 40-69% вопросов, с аргументацией и выводами, подкрепленными ссылками на условия кейса, позволившие сделать данные заключения при ответе на вопросы;
- оценка «неудовлетворительно» выставляется если были даны обоснованные ответы менее чем на 39% вопросов, с аргументацией и выводами, подкрепленными ссылками на условия кейса, позволившие сделать данные заключения при ответе на вопросы.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

Оценивание компетенций осуществляется в форме экзамена. Критерием оценки является правильность ответов на поставленные вопросы.

Вопросы к экзамену

1. Компьютерная безопасность определение и значимость в современном мире.
2. Основные виды преступлений в сфере компьютерной безопасности.
3. Меры противодействия киберпреступности.
4. Основные инициативы противодействия преступлениям в сфере компьютерной безопасности.
5. Компьютерная безопасность определение и значимость в современном мире.
6. Основные виды преступлений в сфере компьютерной безопасности.
7. Меры противодействия киберпреступности.

8. Основные инициативы противодействия преступлениям в сфере компьютерной безопасности.
9. Основы процесса кодирования и декодирования. Современные методы кодирования.
10. Современные системы безопасного кодирования.
11. Принятые технологии кодирование в современной компьютерной безопасности.
12. Различие и способы применения протоколов кодирования.
13. Подходы к программированию алгоритмов кодирования.
14. Типовая структура связей между элементами операционной системы и внешними ресурсами.
15. Проектирование безопасной системы эксплуатации информационных ресурсов.
16. Настройка безопасной системы эксплуатации информационных ресурсов.
17. Мониторинг безопасности системы.
18. Безопасная эксплуатации систем Linux, Windows, виртуальных операционных систем.
19. Модель Белл-Лападула и другие общепринятые модели систем безопасной эксплуатации информационных ресурсов.
20. Протоколы доступа к веб-сайтам, основы защиты данных.
21. Основы обеспечения конфиденциальности передаваемой информации.
22. Слабые места и возможности атаки на сессию пользователя.
23. Основные инструменты гарантирования сохранности и защищенности данных.
24. Типы вредоносных уязвимостей веб ресурсов.
25. Механика инициирования и противодействия DDOS-атакам.
26. Содержание и схема работы атаки CSRF (cross site forgery).
27. Технологии снифинга и спуфинга пакетов и предпосылки успешной реализации.
28. Типы и содержание атак по протоколу TCP. Работа TLS (transport layer security).
29. Основные различия в архитектуре двух популярных сетевых протоколов TCP и UDP и примеры их применения.
30. Типы брандмауэров и их распространенное использование в корпоративной сети.
31. PKI (инфраструктура открытых ключей) в предотвращении атаки MITM (man-in-the-middle).
32. Наиболее распространенные типы атак на PKI (инфраструктуру открытых ключей).
33. Примеры и типы цифровых сертификатов, используемых при современных безопасных процедурах обмена данными.
34. Основные сценарии реализации VPN-туннелирования.
35. Общий сценарий работы TLS/SSL VPN.
36. Причины создания структуры DNS (сервер доменных имен) и известные в ней уязвимости безопасности.
37. Методы обеспечения безопасности СУБД (системы управления реляционными базами данных).
38. Защита системы баз данных с помощью контроля доступа, аутентификация и авторизация.
39. Дискреционная безопасность в SQL и способы ее реализации.
40. Содержание механики атаки SQL-инъекций.
41. Основные факторы успешности атаки SQL-инъекции.
42. Наиболее распространенные контрмеры при атаке SQL-инъекций.
43. Основные этапы плана обеспечения безопасности СУБД.
44. Содержание семи принципов защиты данных.
45. Понятие и значение GDPR (general data protection regulation).
46. Термин «персональные данные» и содержание этой категории.
47. Мероприятия в плане управления данными.
48. Пределы ответственности Главного риск-офицера (CRO).
49. Виды конфиденциальных персональных данных.
50. Защита персональных данных при передаче за границу.

Образцы билетов к экзамену

Федеральное государственное бюджетное образовательное учреждение высшего образования «Кубанский государственный университет»

Направление 38.04.01 «Экономика»
Программа магистратуры «Экономика и менеджмент»
Кафедра маркетинга и торгового дела
Дисциплина «Компьютерная безопасность»
Образец билета к экзамену

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Компьютерная безопасность определение и значимость в современном мире.
2. Основные инструменты гарантирования сохранности и защищенности данных.
3. Практическое задание: На своем компьютере создайте две виртуальных машины: веб-сервер и злоумышленник. На веб-сервер, установите программный пакет (например, Apache) и данное веб-приложение, которое уязвим к SQL-инъекции атаки. Веб-приложение необходимо так же использовать базу данных, для этого установите необходимое программное обеспечение базы данных, например, MySQL. **ВАЖНО! На этом этапе все последующие пункты должны быть подтверждены «Скрин-шотами» экрана.** Проведите со стороны компьютера злоумышленника различные стратегии атака SQL-инъекции на веб-сервер. Сообщите, какие стратегии работают для этого конкретного веб-приложения. Некоторые программы баз данных имеют защиту для смягчения атак с использованием SQL-инъекций. Пронаблюдайте как срабатывают эти защитные механизмы.

Заведующий кафедрой, к. э. н., доцент _____А. Н. Костецкий
(подпись)

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– 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;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
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.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

1. Computer security [Текст]: principles and practice / William Stallings, Lawrie Brown. - 4th ed. Global ed. - Harlow (Essex, England): Pearson, 2018. - 800 p., incl. appendices, index. - References: p.764-776. - ISBN 978-0-292-220061-1: 5992 p. 89 к.
2. *Williams, H. Paul* Model building in mathematical programming [Текст] / H. Paul Williams. - 4th edition. - Chichester., et al.: John Wiley & Sons, 2003. - 350 pp., incl. index. - (Management Science). - ISBN 0471997889: 400 p.
3. *Jamsa, Kris* Internet Programming [Текст] / Kris Jamsa, Ken Cope. - Las Vegas, NV: Jamsa Press a division of Kris Jamsa Software Inc., 1995. - 588 pp.: ill. - ISBN 1884133126.
4. *Schmidt, Friedhelm* The SCSI Bus and IDE Interface [Текст]: Protocols, Applications and Programming / Friedhelm Schmidt; translated by J. Michael Schultz,TransTech Translations. - Workingham, England: Addison-Wesley Publishing Company, 1995. - 301 pp., incl. index; Disk included: ill. - ISBN 0201422840.
5. *Schwartz, Randal L.* Learning Perl [Текст] / Randal L. Schwartz. - Sebastopol, Ca: O'Reilly & Associates Inc., 1994. - 246 pp., incl. index. - (UNIX Programming). - ISBN 1565920422.
6. *Lowell, Jay* Arthur Unix Shell Programming [Текст] / Jay Arthur Lowell, Ted Burns. - 3rd ed. - New York [a. o.]: John Wiley & Sons Inc., 1994. - 462 pp.: ill. - ISBN 0471599417.
7. *Barkakati, Nabajyoti* X Window System Programming [Текст] / Nabajyoti Barkakati. - Second Edition. First printing 1994; Disk applicated. - Indianapolis, Indiana: Sams Publishing, 1994. - 980 pp.: ill. - (UNIX Library). - ISBN 0672305429.
8. *Wall, Larry* Programming perl [Текст] / Larry Wall, Randal L. Schwartz. - Sebastopol, CA: O'Reilly & Associates Inc., 1991. - 465pp., incl. index. - (UNIX Programming). - ISBN 0937175641.
9. Research Topics in Functional Programming [Текст] / Edited by Turner D. A. - Menlo Park: Addison-Wesley Publishing Company, 1990. - 373 p. - Includes bibliogr. ref. - ISBN 0201172364.

5.2. Периодическая литература

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

1) Computers & Security. The International Source of Innovation for the Information Security and IT Audit Professional Editor: Eugene H. Spafford. https://www.journals.elsevier.com/computers-and-security ежемесячный научно-популярный журнал.
2) Cybersecurity Journal, https://cybersecurity-journal.com/ - ежемесячный научно-популярный журнал.
3) International Journal of Information and Computer Security http://www.inderscience.com/jhome.php?jcode=ijics ежемесячный научно-популярный Журнал.
4) Information and Computer Security (http://systems.enpress-publisher.com/index.php/ICS) - ежемесячный научно-популярный журнал.
5) Journal of Computer Security (http://ores.su/en/journals/journal-of-computer-security/) - ежемесячный научно-популярный журнал.
6) Proceedings of the Computer Security Foundations Workshop (https://techtrendnews.com/proceedings-of-the-computer-security-foundations-workshop-iii/) - ежемесячный научно-популярный журнал.
7) IEEE Security and Privacy (http://www.ieee-security.org/) - ежемесячный научно-популярный журнал.
8) Computers and Security - ежемесячный научно-популярный журнал.
9) Proceedings of the ACM Conference on Computer and Communications Security (https://publons.com/journal/1774/proceedings-of-the-acm-conference-on-computer-and-) - ежемесячный научно-популярный журнал.
10) Information and Computer Security – ежемесячный научно-популярный журнал.
11) Journal of Supply Chain Management – ежемесячный научно-популярный журнал.
12) Big Data Research – ежемесячный научно-популярный журнал.
13) International Journal of Agile Systems and Management – ежемесячный научно-популярный журнал.
14) Harvard Business Review – ежемесячный научно-популярный журнал.

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

1) https://www.scimagoir.com/ - Scimago Institution Rankings, Глобальный рейтинг научных изданий и статей.
2) https://www.hacking-lab.com/index.html - набор инструмента повышения грамотности в области компьютерной безопасности Hacking Lab
3) https://www.handsonsecurity.net/ - информация по компьютерной безопасности, практически работы в области компьютерной безопасности.
4) https://www.infosecinstitute.com/ - сайт института Infosec Institute
5) https://developer.microsoft.com/ru-ru/ - сайт для разработчиков Microsoft
6) https://www.kali.org/ - сайт Kali Linux
7) https://www.tenable.com/ - сайт безопасности Nessus

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки).
2. *Scopus* http://www.scopus.com
3. *Web of Sciense* http://webofscience.com *ФГБУ «ГПНТБ России»*
4. *Архивы научных журналов на Российской платформе научных журналов НЭИКОН. http://archive.neicon.ru*
5. *Базы данных компании «Ист Вью Информейшн Сервисиз,Инк»* http://dlib.eastview.com
6. *БД издательства SpringerNature http://npg.com, http://link.springer.com, http://www.springerprotocols.com,http://materials.springer.com, http://link.springer.com/search?facet-content-type=%22ReferenceWork%22, http://zbmath.org*
7. *Национальная электронная библиотека http://нэб.рф/*
8. *НЭБ eLIBRARY.RU http://www.elibrary.ru/*

9. *СПС Консультант Плюс ООО «Фактор Плюс»*
10. *ЭБД компании EBSCO Publishing* http://search.ebscohost.com
11. *ЭБС «BOOK.ru» https://www.book.ru*
12. *ЭБС «ZNANIUM.COM» http://www.znanium.com/*
13. *ЭБС «Университетская библиотека онлайн» www.biblioclub.ru*
14. *ЭБС «Юрайт» http://www.biblio-online.ru*
15. *ЭБС Издательства «Лань» http://e.lanbook.com/*
16. *Электронная библиотека grebennikon.ru* www.grebennikon.ru
17. *Электронные издания компании «Ист Вью Информейшн Сервисиз,Инк» http://dlib.eastview.com*

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

5.4 Перечень информационных технологий

1. Мультимедийные технологии, применяемые в кабинетах и аудиториях оборудованных экраном, видеопроектором, персональными компьютерами.
2. Компьютерные технологии и программные продукты, необходимые для сбора и систематизации информации, проведения требуемых программой расчетов.
3. Microsoft Windows 8, 10.
4. Microsoft Office Professional Plus.

5.5 Перечень необходимого программного обеспечения

1. MS Power Point.
2. MS Word.
3. MS Excel.

6. Методические указания для обучающихся по освоению дисциплины (модуля)

Каждый модуль курса представлен в электронной базе университета moodle.kubsu.ru. По темам курса студенту предоставляется для самостоятельного изучения и проработки: теоретический блок; практические задания в виде кейсов, лабораторных работ, групповых или индивидуальных проектов.

Теоретический блок – студент использует материалы теоретического блока, рекомендованные преподавателем в каждом модуле электронного курса, а также списком дополнительной литературы.

Самостоятельное изучение и текущий контроль качества решения заданий позволяет решить 2 задачи: студенту наиболее полно ознакомится с темой курса и расширить свои знания и навыки по теме; преподавателю оценивать успеваемость студента по курсу.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине (модулю)

Для реализации дисциплины в учебном процессе применяются специализированные аудитории; оборудование для лабораторных работ, практических занятий или других занятий (проектор (для лекций или семинаров), компьютеры и программное обеспечение для расчетов).

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Учебные аудитории для проведения лабораторных работ Лаборатория информационных и управляющих систем 201Н Лаборатория экономической информатики 202Н	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютеры, ноутбуки Оборудование: ПК, Терминальные станции, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus 1С: Предприятие 8 SPSS Statistics
Лаборатория экономики и управления 212Н	Презентации и плакаты, Многофункциональный профессиональный видео детектор банкнот и ценных бумаг, Счетчики банкнот, Инфракрасный детектор банкнот и ценных бумаг, Универсальный детектор банкнот и ценных бумаг, Детектор подлинности банкнот, Ящик денежный, Планшетный импринтер, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ	Microsoft Windows 8, 10, Microsoft Office Professional Plus

	к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд. 213 А, 218 А)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10, Microsoft Office Professional Plus