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
«__» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.06.02 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Направление
подготовки/специальности - 38.04.01 Экономика

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

Программа подготовки – академическая

Форма обучения – очная

Квалификация (степень) выпускника - магистр

Краснодар 2019

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Цели изучения дисциплины соотнесены с общими целями ООП 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 вариативной части Блока 1 "Дисциплины (модули)" учебного плана.

Рассматриваемая дисциплина «Компьютерная безопасность» имеет логическую и содержательно-методическую взаимосвязь с дисциплинами: «Информационные технологии в управлении», «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 общекультурных/профессиональных компетенций (ОК-3, ПК-2, ПК-3)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОК-3	готовностью к саморазвитию, самореализации, использованию творческого потенциала	современные технологии взлома и подходы к защите и обеспечению безопасности компьютерных систем	проводить анализ, выявлять необходимый набор или комбинацию технологий защиты и обеспечения безопасности компьютерных систем	навыками внедрения и настройки инструментов защиты и обеспечения безопасности компьютерных систем
2.	ПК-2	способностью обосновывать актуальность, теоретическую и практическую значимость избранной темы научного исследования	современные методы сбора, обработки и анализа профильной информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности	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	методами сбора, обработки и анализа профильных источников информации для обоснования актуальности и практической значимости реализации предлагаемой системы компьютерной безопасности
3.	ПК-3	способностью проводить самостоятельные исследования в соответствии с разработанной программой	современные методы проведения самостоятельного исследования, источники получения профильной информации, работы технологий в системах компьютерной безопасности, способы их	проводить самостоятельный анализ профильной информации и технологий в области компьютерной безопасности, проводить тестирование и внедрение их в реальной среде	навыками анализа профильной информации и технологий в области компьютерной безопасности, проведения тестирования и внедрения их в реальной среде

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
			внедрения на практике		

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

(для студентов ОФО).

Вид учебной работы		Всего часов	Семестры (часы)			
			С	___		
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**28**	**28**			
Занятия лекционного типа		-	-	-	-	-
Лабораторные занятия		14	14	-	-	-
Занятия семинарского типа (семинары, практические занятия)		14	14	-	-	-
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		-	-			
Промежуточная аттестация (ИКР)		0,3	0,3			
Самостоятельная работа, в том числе:						
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		40	40	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		40	40	-	-	-
Реферат		-	-	-	-	-
Подготовка к текущему контролю		9	9	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**час.**	**144**	**144**	**-**	**-**	**-**
	в том числе контактная работа	**28,3**	**28,3**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Темы дисциплины, изучаемые в С семестре *(очная форма)*

№	Наименование тем	Количество часов				
		Всего	Аудиторная Работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Преступления в сфере компьютерной безопасности, противодействие и законодательная база	10		2		8
2.	Базовые подходы к кодированию и декодированию, системы безопасного кодирования	12		3		9
3.	Использование протоколов кодирования и программирование алгоритмов кодирования	12		3		9
4.	Защита в операционных системах I	12			3	9
5.	Защита в операционных системах II	12			3	9
6.	Проектирование систем безопасной эксплуатации информационных ресурсов	12		3		9
7.	Безопасность сетевых и распределенных систем	12			3	9
8.	Безопасность сетевого администрирования	12			3	9
9.	Безопасность систем хранения данных	11			2	9
10.	Основы защиты экономических данных, обеспечение технической защиты экономических данных	12		3		9
	Контроль	26,7				
	Курсовая работа	-				
	Промежуточная аттестация (ИКР)	0,3				
	Итого по дисциплине:	144	0	14	14	89

2.3 Содержание тем дисциплины:

2.3.1 Занятия лекционного типа

Не предусмотрены.

2.3.2 Занятия семинарского типа

№	Наименование темы	Тематика практических занятий (семинаров)	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, 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.	Коллоквиум 2, 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.	Коллоквиум 3, Кейс 1
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, Групповой проект 2
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, Индивидуальный проект 2

2.3.3 Лабораторные занятия

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
4.	Защита в операционных системах I	Лабораторная работа 1
5.	Защита в операционных системах II	Лабораторная работа 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

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовая работа – не предусмотрена.

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

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

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 текущего контроля

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.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

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.
10. Современные методы кодирования.
11. Современные системы безопасного кодирования.
12. Принятые технологии кодирование в современной компьютерной безопасности.
13. Различие и способы применения протоколов кодирования.
14. Подходы к программированию алгоритмов кодирования.
15. Типовая структура связей между элементами операционной системы и внешними ресурсами.
16. Проектирование безопасной системы эксплуатации информационных ресурсов.
17. Настройка безопасной системы эксплуатации информационных ресурсов.
18. Мониторинг безопасности системы.
19. Безопасная эксплуатации систем Linux, Windows, Виртуальных операционных систем.
20. Модель Белл-Лападула и другие общепринятые модели систем безопасной эксплуатации информационных ресурсов.
21. Протоколы доступа к веб-сайтам, основы защиты данных.
22. Основы обеспечения конфиденциальности передаваемой информации.
23. Слабые места и возможности атаки на сессию пользователя.
24. Основные инструменты гарантирования сохранности и защищенности данных.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

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

Направление 38.04.01 «Экономика»
Программа магистратуры «Экономика и управление»
Кафедра маркетинга и торгового дела
Дисциплина «Компьютерная безопасность»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № __

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)

Критерии оценки теоретических вопросов билета:

- оценка «отлично» выставляется студенту, если были даны полные ответы на два вопроса;
- оценка «хорошо», если были даны ответы на два вопроса с недостаточными полным ответом хотя бы на один из вопросов;
- оценка «удовлетворительно», если были даны неполные ответы на два вопроса;
- оценка «неудовлетворительно» выставляется если были даны неполные ответы на все вопросы или студент затруднился дать ответ;

Критерии оценки практического задания билета:

- оценка «отлично» выставляется студенту, если практическое задание было выполнено полностью, были даны пояснения по каждому пункту задания;
- оценка «хорошо», выставляется студенту, если практическое задание было выполнено полностью, были даны пояснения не по всем пунктам задания;
- оценка «удовлетворительно», выставляется студенту, если практическое задание не было выполнено полностью, были даны пояснения не по всем пунктам задания;
- оценка «неудовлетворительно» выставляется если практическое задание не было выполнено.

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 основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная 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.

1.2 Дополнительная литература:

1. *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.

2. *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.

3. *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.

4. *Schwartz, Randal L.* Learning Perl [Текст] / Randal L. Schwartz. - Sebastopol, Ca: O'Reilly & Associates Inc., 1994. - 246 pp., incl. index. - (UNIX Programming). - ISBN 1565920422.

5. *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.

6. *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.

7. *Wall, Larry* Programming perl [Текст] / Larry Wall, Randal L. Schwartz. - Sebastopol, CA: O'Reilly & Associates Inc., 1991. - 465pp., incl. index. - (UNIX Programming). - ISBN 0937175641.

8. 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.

5.3. Периодические издания:

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.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

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

7. 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 видел 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.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1 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.

8.2 Перечень необходимого программного обеспечения

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

8.3 Перечень информационных справочных систем:

1. *Scopus* http://www.scopus.com
2. *Web of Sciense* http://webofscience.com *ФГБУ «ГПНТБ России»*
3. *Архивы научных журналов на Российской платформе научных журналов НЭИКОН. http://archive.neicon.ru*
4. *Базы данных компании «Ист Вью Информейшн Сервисиз,Инк»* http://dlib.eastview.com
5. *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*
6. *Национальная электронная библиотека http://нэб.рф/*
7. *НЭБ eLIBRARY.RU http://www.elibrary.ru/*
8. *СПС Консультант Плюс ООО «Фактор Плюс»*
9. *ЭБД компании EBSCO Publishing* http://search.ebscohost.com
10. *ЭБС «BOOK.ru» https://www.book.ru*
11. *ЭБС «ZNANIUM.COM» http://www.znanium.com/*
12. *ЭБС «Университетская библиотека онлайн» www.biblioclub.ru*
13. *ЭБС «Юрайт» http://www.biblio-online.ru*
14. *ЭБС Издательства «Лань» http://e.lanbook.com/*
15. *Электронная библиотека grebennikon.ru* www.grebennikon.ru
16. *Электронные издания компании «Ист Вью Информейшн Сервисиз,Инк» http://dlib.eastview.com*

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Занятия семинарского типа	Аудитории А208Н, 202А, 210Н, 216Н, 513А, 514А, 515А, 516А, а также аудитории, укомплектованные презентационной техникой (проектор, экран, ноутбук) и прикладным программным обеспечением (Microsoft Office). Ауд., 2026Л, 2027Л, 4034Л, 4035Л, 4036Л, 5043Л, 201Н, 202Н, 203Н, А203Н
2.	Лабораторные занятия	Лаборатории, укомплектованные специализированной мебелью и техническими средствами обучения. Рабочие места, подключены к локальной сети факультета, имеют доступ к глобальной сети Интернет. Ауд. 201Н, 202Н, 203Н, А203Н, 205А
3.	Групповые и индивидуальные консультации	Кафедра маркетинга и торгового дела (ауд. 223, 224, 230, 236, 206А, 205Н, 218Н), ауд. А208Н
4.	Текущий контроль, промежуточная аттестация	Аудитории, укомплектованные презентационной техникой (проектор, экран, ноутбук) и прикладным программным обеспечением (Microsoft Office).

		Ауд. 520А, 207Н, 208Н, 209Н,212Н, 214Н, 201А,205А, А208Н, 202А, 210Н, 216Н, 513А, 514А, 515А, 516А, 2026Л, 2027Л, 4033Л, 4034Л, 4035Л, 4036Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5043Л, 5045Л, 5046Л, 201Н, 202Н, 203Н, А203Н
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета Ауд. 213А, 218А, 201Н, 202Н, 203Н, А203Н