МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 201_ г.

Рабочая программа дисциплины

ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

Направление подготовки	08.03.01
Профиль подготовки	Строительство
Квалификация выпускника	Бакалавр
Форма обучения	очная
Учебный план	2020
Изучается во 2 семестре	

СОГЛАСОВАНО:
Заведующий кафедрой строительства
_____Д.В.Щитов
«__» _____ 201_ г.

Рассмотрено УМК
Протокол №___
от «___»_____201_г.

Председатель УМК института
_____ Нарыжная А.Б.

РАЗРАБОТАНО:
Зав. кафедрой систем управления и информационных технологий
_____ Першин И.М.
«__» _____ 201_г.

_____
Доцент кафедры СУиИТ
_____ Мишин В.В.
«__» _____ 201_ г.

Пятигорск, 2020

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Персональная кибербезопасность» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 38.03.01 Экономика.

Задачи освоения дисциплины: изучение основных понятий кибербезопасности, освоение навыков соблюдения персональной кибербезопасности.

1. Место дисциплины в структуре основной образовательной программы

Дисциплина «Персональная кибербезопасность» является дисциплиной блока ФТД подготовки бакалавра направления 08.03.01 Строительство . Ее освоение происходит во 2 семестре.

2. Связь с предшествующими дисциплинами

Пререквизитом дисциплины является дисциплина .

3. Связь с последующими дисциплинами

Кореквизитов дисциплины является дисциплина .

4. Компетенции обучающегося, формируемые в результате изучения дисциплины

4.1 Наименование компетенции

Код	Формулировка:
ОПК-2	Способен вести обработку, анализ и представление информации в профессиональной деятельности с использованием информационных и компьютерных технологий;

4.2 Знания, умения и навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: методы решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; **Уметь:** осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; **Владеть:** способностью решать стандартные задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**ОПК-2**

5. Объем учебной дисциплины/модуля

Объем занятий: Итого 27ч.1 з.е.
В том числе аудиторных 12 ч.
Из них:
Лекций 12 ч.
Лабораторных работ - ч.
Практических занятий –ч.
Самостоятельной работы12 ч.

Зачет 2 семестр

6. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

6.1 **Тематический план дисциплины**

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
2 семестр							
	Раздел 1. Концепции персональной кибербезопасности						
1	Тема 1. Основные понятия персональной кибербезопасности	ОПК-2,	1,5				7
2	Тема 2. Моделирование угроз персональной кибербезопасности	ОПК-2,	1,5				
3	Тема 3. Криптографические алгоритмы	ОПК-2,	1,5				
4	Тема 4. Методы криптоанализа	ОПК-2,	1,5				
	Раздел 2. Технологии организации персональной кибербезопасности						
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности	ОПК-2,	1,5				8
6	Тема 6. Инструменты организации персональной кибербезопасности	ОПК-2,	1,5				
7	Тема 7. Персональная кибербезопасность в интернет-банкинге	ОПК-2,	1,5				
8	Тема 8. Современные методы защищенной аутентификации	ОПК-2,	1,5				
	Итого за 2 семестр		12				15
	Итого						

6.2 **Наименование и содержание лекций**

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов *	Интерактивная форма проведения
	2 семестр		
	Раздел 1. Концепции персональной кибербезопасности		

1	Тема 1. Основные понятия персональной кибербезопасности Информационная безопасность и кибербезопасность. Свойства оцифрованной информации. Причины киберпреступлений. Проблемы кибербезопасности.	1,5	
2	Тема 2. Моделирование угроз персональной кибербезопасности Анализ рисков как основа управления персональной кибербезопасностью Модель угроз STRIDE. Инструменты анализа и контроля информационных рисков. Сравнительный анализ подходов к распознаванию угроз с использованием различных моделей: CIA, Гексада Паркера, 5A, STRIDE	1,5	
3	Тема 3. Криптографические алгоритмы Обзор алгоритмов шифрования и тенденций развития криптографии. Круг задач, на решение которых ориентированы криптографические методы. Основные понятия и определения криптографии. Рекомендации Microsoft по применению криптографических алгоритмов. Отечественный стандарт шифрования данных ГОСТ 28147-89. Американский стандарт шифрования данных AES. Концепция криптосистемы с открытым ключом. Классификация криптографических алгоритмов. Алгоритмы шифрования с секретным ключом (симметричные). Блочные шифры. Поточные шифры. Алгоритмы шифрования с открытым ключом (асимметричные). Криптоалгоритмы с секретным ключом.	1,5	
4	Тема 4. Методы криптоанализа Обзор современных методов криптоанализа. Классические методы. Новый вид криптоанализа – атаки по побочным каналам. Квантовый криптоанализ. Исходы криптоанализа. Методы криптоанализа и их влияние на развитие криптографии. Предельные возможности по взлому шифров методом полного перебора ключей. Применимость различных типов криптоатак к симметричным и асимметричным криптосистемам и хеш-функциям. Перспективные технологии криптоанализа.	1,5	
	Раздел 2. Технологии организации персональной кибербезопасности		

5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности Оценка средств криптозащиты. Экономическое обоснование расходов на обеспечение персональной кибербезопасности. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности. Преимущества и недостатки существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности. Набор финансово-экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.	1,5	
6	Тема 6. Инструменты организации персональной кибербезопасности Обзор антивирусных средств защиты при организации системы персональной кибербезопасности. Антивирусная защита персональных компьютеров и мобильных устройств. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств персональной	1,5	
7	Тема 7. Персональная кибербезопасность в интернет-банкинге Технологии интернет-банкинга. Технологии биржевой торговли. Правила организации персональной кибербезопасности в интернет-банкинге. Программно-аппаратные средства защиты данных в процессах интернет-банкинга и биржевой торговли.	1,5	
8	Тема 8. Современные методы защищенной аутентификации Методы авторизации пользователя при работе в сети Интернет. Авторизация и аутентификация. Методы создания и хранения паролей. Защищенный личный кабинет интернет-ресурсов.	1,5	
	Итого за 2 семестр	12	
	Итого	12	

6.3 **Наименование лабораторных работ**

Лабораторные работы учебным планом не предусмотрены.

6.4 **Наименование практических занятий не предусмотрены учебным планом**

6.5 **Технологическая карта самостоятельной работы обучающегося**

Технологическая карта

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-2	Подготовка к лекциям	Конспект	Собеседование	11,88	0,12	12
ОПК-2	Самостоятельное	Конспект	Собеседо	2,97	0,03	3

	изучение литературы по темам 1, 5		вание			
			Итого	14,85	0,15	15

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Фонд оценочных средств, позволяющий оценить уровень сформированности компетенций, размещен в УМК дисциплины «Персональная кибербезопасность» на кафедре систем управления и информационных технологий и представлен следующими компонентами:

Код оцениваемой компетенции	**Этап формирования компетенции (№ темы)**	**Средства и технологии оценки**	**Тип контроля (текущий/промежуточный)**	**Вид контроля (текущий/промежуточный)**	**Наименование оценочного средства**
ОПК-2	Темы 1, 5	собеседование	текущий	устный	вопросы для собеседования
ОПК-2	Темы 1,2,5,6,7	отчет письменный	текущий	письменный, с помощью технических средств	темы индивидуальных заданий для письменного отчета

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов*
ОПК-2					
Базовый	**Знать:** методы решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	Минимальные знания о методах решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением	Фрагментарные знания о методах решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информацион	Имеются знания о методах решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением	

	информационной безопасности	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	но-коммуникационных технологий и с учетом основных требований информационной безопасности	информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
	Уметь: осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Минимальные умения осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Демонстрирует умения осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Имеются умения применения осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
	Владеть: способностью	Недостаточно владеет	Испытывает затруднения	Воспроизводит и	

	решать стандартные задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	способностью решать стандартные задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	при решении стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	корректно решать стандартные задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
Повышенный	**Знать:** методы решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				Знает: методы решения стандартных задач профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных

					требований информационной безопасности в рамках основной и дополнительной литературы
	Уметь: осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				Умеет: осуществлять выбор метода решения стандартной задачи профессиональной деятельности на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности в рамках основной и дополнительной литературы
	Владеть: способностью решать стандартные задачи профессиональной деятельности на основе				Владеет: способностью решать стандартные задачи профессиональной деятельнос

	информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				ти на основе информационной библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности в рамках основной и дополнительной литературы

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	2 семестр		
1.	собеседование по теме 1, индивидуальные задания по темам 1, 2	9	25
2.	собеседование по теме 5, индивидуальные задания по темам 5, 6, 7	18	30
	Итого за 2 семестр		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация в форме зачета

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля. Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет (Sзач) при различных рейтинговых баллах
по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	**Количество баллов за зачет ($S_{зач}$)**
$50 \leq R_{сем} \leq 60$	**40**
$39 \leq R_{сем} < 50$	**35**
$33 \leq R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций

Экзамен не предусмотрен учебным планом

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Текущая аттестация студентов проводится преподавателями, ведущими практические занятия по дисциплине, в следующих формах: отчет письменный, собеседование. К практическим занятиям студент должен подготовить ответы на вопросы, выполнить задания по теме занятия.

Допуск к **практическим работам** происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Оценку «отлично» студент получает, если оформление отчета соответсвует установленным требованиям, студент правильно отвечает на предложенные преподавателем контрольные вопросы, студент правильно отвечает на дополнительные вопросы по теме лабораторной работы.

Оценку «хорошо» студент получает, если оформление отчета соответсвует установленным требованиям, студент правильно отвечает на предложенные преподавателем контрольные вопросы.

Оценку «удовлетворительно» студент получает без беседы с преподавателем, если оформление отчета соответсвует установленным требованиям.

Отчет может быть отправлен на доработку в следующих случаях:

- отчет полностью не соответствует установленным требованиям;
- в отчете не раскрыта суть работы.

Критерии оценивания результатов собеседования, индивидуальных заданий к практическим занятиям приведены в Фонде оценочных средств по дисциплине «Персональная кибербезопасность».

8. Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

№ п/п	**Виды самостоятельной**	Рекомендуемые источники информации (№ источника)

	работы	Основная	Дополнительная	Методическая литература	Интернет-ресурсы
	2 семестр				
1	Подготовка к лекциям	1-2	1-2	1-2	1-4
2	Самостоятельное изучение литературы по темам 1, 5	1-2	1-2	1-2	1-4

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

10.1.1. Перечень основной литературы

1. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс]: учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html.

2. Макаров А.М. Организация защиты персональных данных [Электронный ресурс] : лабораторный практикум / А.М. Макаров, И.В. Калиберда, К.О. Бондаренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62971.html

10.1.2. Перечень дополнительной литературы:

1. Скрипник Д.А. Обеспечение безопасности персональных данных [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 121 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52153.html.

2. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [Электронный ресурс] / А.И. Савельев. — Электрон. текстовые данные. — М.: Статут, 2017. — 320 c. — 978-5-8354-1365-2. — Режим доступа: http://www.iprbookshop.ru/65895.html.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению практических занятий по дисциплине по дисциплине «Персональная кибербезопасность».

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Персональная кибербезопасность».

10.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Университетская библиотека online. http://www.biblioclub.ru;

2. ЭБС «IPRbooks». http://www.iprbookshop.ru;

3. Электронная библиотека СКФУ.а. http://catalog.ncstu.ru;

4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Microsoft Windows Professional Russian Upgrade (номер лицензии 61541869); Microsoft Office Russian License (номер лицензии 61541869).

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине обеспечение дисциплины

Специализированная учебная мебель и технические средства обучения, служащие для представления учебной информации: короткофокусный мультимедиа-проектор EPSON EP-X03 переносной; переносной напольный экран SCREEN MEDIA; ноутбук Lenovo G550 подключенный к сети Интернет; доска магнитно-маркерная 1-элементная 120*240

переносная; парта комбинированная 4-х местная со скамьей – 6 шт.; стол компьютерный – 10 шт.; кресло компьютерное регулируемое – 10 шт.; компьютер в сборе Celeron430 – 10 шт.; жалюзи; учебно-наглядные пособия; флипчарт, наборы демонстрационного оборудования и учебно-наглядных пособий.