МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность **07.03.03 Дизайн архитектурной среды**
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения **2021**
Изучается во **2** семестре

г. Пятигорск 2021.

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Персональная кибербезопасность» является формирование набора профессиональных компетенций будущего Бакалавра по направлению подготовки 07.03.03 Дизайн архитектурной среды.

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

2. Место дисциплины в структуре основной образовательной программы

Дисциплина «Персональная кибербезопасность» является дисциплиной блока ФТД подготовки Бакалавра направления 07.03.03 Дизайн архитектурной среды. Ее освоение происходит во 2 семестре.

3. Связь с предшествующими дисциплинами

При изучении данной дисциплины не требуется изучение других дисциплин.

4. Связь с последующими дисциплинами

Знания, полученные во время изучения данной дисциплины, используются при изучении последующих дисциплин учебного плана.

5. Компетенции обучающегося, формируемые в результате изучения дисциплины

5.1 Наименование компетенции

Код	Формулировка:
ОПК-1	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

5.2 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: основные причины выявления киберугроз, методы выявления угроз информационной безопасности **Уметь:** проводить первичный анализ на предмет выявления киберугроз **Владеть:** навыком работы со стандартным набором инструментов пользователя для выявления угроз информационной безопасности	ОПК-1

6. Объем учебной дисциплины/модуля

Объем занятий: Итого 54 ч. 2 з.е.
В том числе аудиторных 24 ч.
Из них:
Лекций 12 ч.
Лабораторных работ - -
Практических занятий – 12 ч.
Самостоятельной работы 30 ч.
Зачет 2 семестр

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

7.1 **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-1	1,5	3			15
2	Тема 2. Моделирование угроз персональной кибербезопасности	ОПК-1	1,5	3			
3	Тема 3. Криптографические алгоритмы	ОПК-1,	1,5				
4	Тема 4. Методы криптоанализа	ОПК-1,	1,5				
	Раздел 2. Технологии организации персональной кибербезопасности						
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности	ОПК-1	1,5	3			12
6	Тема 6. Инструменты организации персональной кибербезопасности	ОПК-1	1,5	1,5			
7	Тема 7. Персональная кибербезопасность в интернет-банкинге	ОПК-1	1,5	1,5			
8	Тема 8. Современные методы защищенной аутентификации	ОПК-1,	1,5				
9	Тема 9. Технологии электронной цифровой подписи	ОПК-1,					
	Итого за 2 семестр		12	12			30
	Итого		12	12			30

7.2 **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 кибербезопасности.	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	
9	Тема 9. Технологии электронной цифровой подписи Технологии электронной цифровой подписи. Методы создания электронной цифровой подписи. Электронная цифровая подпись. Методы формирования электронной цифровой подписи.		
	Итого за 2 семестр	12	
	Итого	12	

7.3 **Наименование лабораторных работ**

Лабораторные занятия учебным планом не предусмотрены.

7.4 **Наименование практических занятий**

№ тем	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма

ы			проведения
	2 семестр		
	Раздел 1. Концепции персональной кибербезопасности		
1	Тема 1. Основные понятия персональной кибербезопасности Лабораторная работа 1 Информационная безопасность и кибербезопасность. Свойства оцифрованной информации. Причины киберпреступлений. Проблемы кибербезопасности.	3	
2	Тема 2. Моделирование угроз персональной кибербезопасности Лабораторная работа 2 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	3	
	Раздел 2. Технологии организации персональной кибербезопасности		
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности Лабораторная работа 3 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.	3	
6	Тема 6. Инструменты организации персональной кибербезопасности Лабораторная работа 4 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 кибербезопасности.	1,5	
7	Тема 7. Персональная кибербезопасность в интернет-банкинге Лабораторная работа 5 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	
	Итого за 2 семестр	12	
	Итого	12	

7.5 **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-1	Подготовка к лекциям	Конспект	Собеседование	1,08	0,12	1,2
ОПК-1	Самостоятельное изучение литературы по темам 1, 5	Конспект	Собеседование	23,76	2,64	26,4
ОПК-1	Подготовка к практическим работам	Индивидуальное задание	Отчет письменный	2,16	0,24	2,4
			Итого	27	3,0	30

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

8.1 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-1	Темы 1, 5	собеседование	текущий	устный	вопросы для собеседования
ОПК-1	Темы 1,2,5,6,7	отчет письменный	текущий	письменный, с помощью технических средств	темы индивидуальных заданий для письменного отчета

8.2 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-1				
Базовый	**Знать:** вероятные угрозы безопасности информации и воз-	Отсутствуют знания вероятных угроз без-	Имеются элементы знаний вероятных	Знания вероятных угроз безопасности инфор-	

	можные пути их реализации	опасности информации и возможных путей их реализации	угроз безопасности информации и возможных путей их реализации	мации и возможных путей их реализации имеются не в полном объеме.	
	Уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Отсутствие умения определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Имеются элементы умения определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Показывает умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты не в полном объеме	
	Владеть: навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Не владеет навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Владеет отдельными навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Владеет навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты не в полном объеме.	

	ОПК-1				
Повышенный	**Знать:** в полном объеме вероятные угрозы безопасности информации и возможные пути их реализации				Знает в полном объеме вероятные угрозы безопасности информации и возможные пути их реализации
	Уметь: в полном объеме определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				Показывает в полном объеме определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
	Владеть: в полном объеме навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				Владеет в полном объеме навыками анализа структуры и содержания информационных про-

					цессов и особенностей функционирования объекта защиты

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**

8.3 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

8.4 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 лабораторным работам студент должен подготовить ответы на вопросы, выполнить задания по теме лабораторной работы.

Допуск к лабораторным 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».

9. 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 лабораторными работами, 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 работы**	Рекомендуемые источники информации (№ источника)			
		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
3	Подготовка к лабораторным работам	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 с. — 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 с. — 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 лабораторных работ 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. 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 Office - №61541869, Microsoft Windows 7 Профессиональная - №61541869

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

Персональный компьютер (12 шт.) в сборе в составе AMD X2 250/4096MB/500Gb/DVDRW/450W, Монитор от компьютера (1 шт.) в сборе в составе Intel Pentium g620/2gb/500gb/dvdRW/hd5550 (стоит на компе 12102), Экран ScreenMedia Goldview 244*183 MW 4/3 (1 шт.), Проектор NEC NP405 (1 шт.)

13. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а так же в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

- индивидуальное равномерное освещение не менее 300 люкс,

- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей)

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента задания могут выполняться в устной форме.