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

УТВЕРЖДАЮ
Зам. директора по учебной работе Пятигорского института (филиал) СКФУ
_____М.В. Мартыненко
«__»_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ»

Направление подготовки **09.03.02 Информационные системы и технологии**
Направленность (профиль) **Информационные системы и технологии обработки цифрового контента**
Форма обучения очная
Год начала обучения 2022
Реализуется в 1 семестре

Разработано
Доцент кафедры СУиИТ, кандидат техн. наук, доцент
Мартиросян К.В.

Пятигорск 2022 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Персональная кибербезопасность» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 09.03.02 «Информационные системы и технологии», для решения прикладных задач в рамках бакалаврской программы.

Задачи освоения дисциплины:

- изучение основных понятий кибербезопасности;
- освоение навыков соблюдения персональной кибербезопасности.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Персональная кибербезопасность» является дисциплиной блока ФТД подготовки бакалавра направления 09.03.02 «Информационные системы и технологии». Ее освоение происходит в 1 семестре.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-8 Способность обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы	ИД-1 ПК-8 Понимает способы обеспечения требуемый качественный бесперебойный режим работы инфокоммуникационной системы. ИД-2ПК-8 Обеспечивает требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Находит, анализирует и оценивает нормативные и методические материалы, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной

		безопасности по профилю своей профессиональной деятельности Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Астр. ч.	Из них в форме практической подготовки
Всего:	2	54	
Из них аудиторных:		27	
Лекций			
Лабораторных работ			
Практических занятий		27	
Самостоятельной работы		27	
Формы контроля:			
Зачет с оценкой	1 семестр		

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

5.1. Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
	1 семестр						
	Раздел 1. Концепции персональной кибербезопасности	ИД-1ПК-8, ИД-2 ПК- 8					
1	Тема 1. Основные понятия персональной кибербезопасности	ИД-1ПК-8, ИД-2 ПК- 8		3			6
2	Тема 2. Моделирование угроз персональной кибербезопасности	ИД-1ПК-8, ИД-2 ПК- 8		3			1,5
3	Тема 3. Криптографические алгоритмы	ИД-1ПК-8, ИД-2 ПК- 8		3			1,5
4	Тема 4. Методы криптоанализа	ИД-1ПК-8, ИД-2 ПК- 8		3			3

	Раздел 2. Технологии организации персональной	ИД-1ПК-8, ИД-2 ПК- 8					

	кибербезопасности						
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности	ИД-1ПК-8, ИД-2 ПК- 8		3			3
6	Тема 6. Инструменты организации персональной кибербезопасности	ИД-1ПК-8, ИД-2 ПК- 8		3			3
7	Тема 7. Персональная кибербезопасность в интернет-банкинге	ИД-1ПК-8, ИД-2 ПК- 8		3			3
8	Тема 8. Современные методы защищенной аутентификации	ИД-1ПК-8, ИД-2 ПК- 8		3			3
9	Тема 9. Технологии электронной цифровой подписи	ИД-1ПК-8, ИД-2 ПК- 8		3			3
	Итого за 1 семестр			**27**			**27**
	ИТОГО			**27**			**27**

5.2 Наименование и содержание лекций

Данный вид работы не предусмотрен учебным планом

5.3 Наименование лабораторных работ

Данный вид работы не предусмотрен учебным планом

5.4 Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
	1 семестр		
	Раздел 1. Концепции персональной кибербезопасности		
1	Тема 1. Основные понятия персональной кибербезопасности Практическая работа1 Информационная безопасность и кибербезопасность. Свойства оцифрованной информации. Причины киберпреступлений. Проблемы кибербезопасности.	3	
2	Тема 2. Моделирование угроз персональной кибербезопасности Практическая работа2 Анализ рисков как основа управления персональной кибербезопасностью Модель угроз STRIDE. Инструменты анализа и контроля информационных	3	

	рисков. Сравнительный анализ подходов к распознаванию угроз с использованием		

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

	различных моделей: CIA, Гексада Паркера, 5A, STRIDE		
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.	3	
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.	3	
	Раздел 2. Технологии организации персональной кибербезопасности		
5	Тема 5. Экономическая эффективность средств обеспечения персональной кибербезопасности Практическая работа3 Оценка средств криптозащиты. Экономическое обоснование расходов на обеспечение персональной кибербезопасности. Обоснованный выбор мер и средств обеспечения персональной кибербезопасности. Преимущества и недостатки	3	

	существующих методов обоснования инвестиций в средства обеспечения персональной кибербезопасности. Набор финансово-		

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 12000002A633E3D113AD425FB50002000002A6

Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022

	экономических показателей для оценки эффективности средств обеспечения персональной кибербезопасности с экономических позиций. Методика оценки экономической эффективности средств обеспечения персональной кибербезопасности.		
6	Тема 6. Инструменты организации персональной кибербезопасности Практическая работа4 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.	3	
7	Тема 7. Персональная кибербезопасность в интернет-банкинге Практическая работа5 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.	3	
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.	3	
9	Тема 9. Технологии электронной цифровой подписи Технологии электронной цифровой подписи. Методы создания электронной цифровой подписи. Электронная цифровая подпись. Методы формирования электронной цифровой	3	
	Итого за 1 семестр	**27**	
	Итого	**27**	

5.5 Технологическая карта самостоятельной работы обучающегося

Ко	Вид	Средства и	Объем часов, в том числе

ды реализуемых компетенций,	деятельности студентов	технологии оценки			
			СРС	Контактная работа с	Всего

индикатора(ов)				преподавателем	
1 семестр					
ИД-1ПК-8, ИД-2 ПК-8	Самостоятельное изучение литературы	Собеседование	10,44	1,16	11,6
ИД-1ПК-8, ИД-2 ПК-8	Подготовка к практическим занятиям	Собеседование	4,86	0,54	5,4
ИД-1ПК-8, ИД-2 ПК-8	Подготовка доклада	Доклад	9	1	10
Итого за 1 семестр			24,3	2.7	27
Итого			24,3	2.7	27

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Персональная кибербезопасность» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнения всех видов самостоятельной работы.

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

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для

освоения дисциплины (модуля)

8.1.1. 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

8.1.2. 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.

8.2 Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

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

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

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

1. www.intuit.ru – национальный открытый университет «ИНТУИТ»;
2. www.window.edu.ru –единое окно доступа к образовательным ресурсам;
3. www.citforum.ru – сервер информационных технологий;
4. http://www.iprbookshop.ru – ЭБС «IPRbooks»;
5. www.gpntb.ru – Государственная публичная научно- техническая библиотека России. (ГПНТБ России);
6. http://catalog.ncstu.ru – Электронная библиотека СКФУ;
7. http://www.biblioclub.ru – Университетская библиотека online.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	КонсультантПлюс -

Программное обеспечение:

1 Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор N
2018-01(18). 2018-04(6). 2018-05(6). 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 о
текущий момент окончания поддержки не анонсировано.

2	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 20 09.01.2013г.; набор обновлений Office 2013 Service Pack1 Дата начала жизненного цикла 25.0

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Практические занятия	Учебная аудитория для проведения учебных занятий, оснащена оборудованием и техническими средствами обучения. Переносной ноутбук; переносной проектор; доска.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде.

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

11. 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 также 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.