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
«28» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки/специальность 10.03.01 Информационная безопасность
Направленность (профиль)/специализация **Безопасность компьютерных систем**
Форма обучения очная
Год начала обучения 2022
Реализуется в 8 семестре

Разработано
Доцент кафедры СУиИТ, кандидат ист. наук, доцент
Русак С.Н.

Пятигорск 2022 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Основы управления информационной безопасностью» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

В соответствии с указанной целью при изучении данной дисциплины ставятся следующие задачи:

- анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- разработка предложений по совершенствованию системы управления информационной безопасностью;
- формирование комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относятся к части, **Коммуникативные аспекты профессиональной деятельности**. Ее освоение происходит в 8 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
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ИД-1 ОПК-5 Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации. ИД-2 ОПК-5. Понимает определять необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации. ИД-3 ОПК-5 Наделен навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по	Умеет использовать комплексный подход в организации политики информационной безопасность в вопросах защиты конфиденциальных документов Определяет информационные ресурсы подлежащих защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	**ИД1 ОПК-1.1** Разрабатывает и умеет реализовать политики управления доступом в компьютерных системах	
ОПК-1.2.Способен администрировать средства защиты информации в компьютерных системах и сетях	**ИД1 ОПК-1.2** Применяет на практике методы администрирования средств защиты информации в компьютерных системах и сетях	
ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты	ИД-1 ПК-3 Понимает угрозы безопасности, режимы противодействия. ИД-2 ПК-3 Способен определять состав и порядок администрирования подсистемы информационной безопасности. ИД-3 ПК-3 Обладает навыками мониторинга функционирования подсистемы ИБ.	

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Астр. ч.	Из них в форме практической подготовки
Всего:	5	135	
Из них аудиторных:		36	
Лекций		18	
Лабораторных работ			
Практических занятий		18	
Самостоятельной работы		99	
Формы контроля:			
Экзамен			
Зачет с оценкой	8		
Зачет			
Курсовая работа (проект)			
РГР			
Контрольная работа			
Эссе			
Реферат			

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	Самостоятельна

			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	я работа, часов
8 семестр							
1	Тема 1. Основные положения и терминология. Введение в понятие основы управления информационной безопасностью	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
2	Тема 2. Документация по комплексной правовой защите информации на предприятии	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
3	Тема 3. Мотивация к обеспечению информационной безопасности на предприятии.	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	3	3			
4	Тема 4. Процесс управления информационной безопасностью.	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
5	Тема 5. Этапы создания системы управления ИБ.	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
6	Тема 6. Оценка информационных рисков. Управление рисками. Основные понятия	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	3	3			
7	Тема 7. Протоколирование и аудит. Активный аудит	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
8	Тема 8. Современные методы и средства анализа и управление рисками информационных систем компаний	ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	1,5	1,5			
	Тема 9. Организационно-правовые формы управления безопасностью		3	3			
	Итого за 8 семестр		**12**		**12**		**99**

5.2 Наименование и содержание лекций

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Обьем часов	Из них практическая подготовка, часов
8 семестр			

1	**Тема:** Основные положения и терминология. Введение в понятие основы управления информационной безопасностью *Основные понятия и определения по теме. Управление. Циклическая модель улучшения процессов Основные определения и критерии классификации угроз*	1,5	
2	**Тема:** Документация по комплексной правовой защите информации на предприятии . *- «Оранжевая книга» как оценочный стандарт.* *- Критерии оценки безопасности информационных систем* *- Стандарты управления информационной безопасностью.*	1,5	
3	**Тема:** Мотивация к обеспечению информационной безопасности на предприятии. *- Процесс оценки риска информационной безопасности.* *- Идентификация уязвимостей и построение модели нарушителя.* *- Предварительный анализ информационной безопасности предприятия.*	3	
4	**Тема:** Процесс управления информационной безопасностью.. *- Существующие и планируемые средства контроля.* *- Программные средства защиты информации на предприятии.* *- Аппаратные средства защиты информации на предприятии.*	1,5	
5	**Тема:** Этапы создания системы управления ИБ.. – *Принятие решения о создании СУИБ.* – *Подготовка к созданию СУИБ.* – *Анализ рисков.* – *Разработка политик и процедур СУИБ.* – *Внедрение СУИБ в эксплуатацию.*	1,5	
6	**Тема:** Оценка информационных рисков. Управление рисками. Основные понятия. – *идентификация всех активов в рамках выбранной области деятельности;* – *определение ценности*	3	

	идентифицированных активов; – *идентификация угроз и уязвимостей для идентифицированных активов;* – *оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;* – *выбор критериев принятия рисков;* *подготовка плана обработки рисков.*		
7	**Тема:** Протоколирование и аудит. Активный аудит. *Характерная особенность протоколирования и аудита. Задача активного аудита. Средства активного аудита.*	1,5	
8	**Тема:** Современные методы и средства анализа и управление рисками информационных систем компаний. *Актуальность задачи обеспечения информационной безопасности для бизнеса. Обоснование необходимости инвестиций в информационную безопасность компании. Программные комплексы анализа и контроля информационных рисков: британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания Digital Security).*	1,5	
	Тема: Организационно-правовые формы управления безопасностью. *В целях непосредственного выполнения функций по обеспечению безопасности государством образуются специальные органы обеспечения безопасности.*	3	
	Итого за 8 семестр	18	

5.3 Наименование лабораторных работ не предусмотрено учебным планом

5.4 Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
	8 семестр		

1	**Практическая работа №1 «Основополагающие документы в области информационной безопасности»** *изучить основополагающие документы в области информационной безопасности и российские и международные, которые используются в России*	1,5	1,5
2	Практическая работа №2 **Обеспечение информационной безопасности в ведущих зарубежных странах** *ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах*	1,5	1,5
3	Практическая работа № 3 **«Требования и показатели защищенности автоматизированных средств обработки информации»** *ознакомиться с требованиями и показателями защищенности автоматизированных средств обработки информации*	3	3
4	Практическая работа № 4 **«Алгоритмы поведения вирусных и других вредоносных программ»** *Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.*	1,5	1,5
5	Практическая работа № 5 ***Тема: «Процедура аутентификации пользователя на основе пароля»*** *изучение технологии аутентификации пользователя на основе пароля.*	1,5	1,5
6	Практическая работа № 6 **«Анализ рисков информационной безопасности»** *ознакомиться с алгоритмами оценки риска информационной безопасности*	3	3
7	Практическая работа № 7 **«Типовые» каналы утечки информации объектов информатизации ОВД. Условия и факторы, способствующие утечке информации ограниченного доступа. Модели возможных нарушителей»** *ознакомиться с условиями и факторами, способствующими утечке информации ограниченного доступа*	1,5	1,5
8	Практическая работа №8 **«Разработка политики информационной безопасности предприятия»** *Изучить деятельность определенной*	1,5	1,5

	организации и провести предварительный анализ ее информационной безопасности		
	Практическая работа № 9 **«Построение концепции информационной безопасности предприятия»** *знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры*	3	3
	Итого за 8семестр	18	
	Итого	18	

5.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
8 семестр					
ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	Самостоятельное изучение литературы и источников	Собеседование	76,86	8,54	85,4
ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	Подготовка к практическим занятиям	Опрос	3,24	0,36	3,6
ОПК-5, ОПК-1.1, ОПК-1.2, ПК-3	Написание реферата/доклада	Доклад	9	1	10
Итого за 8 семестр			**89,1**	**9,9**	**99**

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 «Основы управления информационной безопасностью» 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 (модуль) построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

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

Практические работы направлены на приобретение опыта 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. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

8.1.2. Перечень дополнительной литературы:

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.

2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

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

1. Методические рекомендации по выполнению лабораторных работ по дисциплине «Основы управления информационной безопасностью».

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине " Основы управления информационной безопасностью».

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

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Основы управления информационной безопасностью»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

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 занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

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

1	КонсультантПлюс - http://www.consultant.ru/

Программное обеспечение:

1	Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013. Окончание бесплатной поддержки – 2023-01 ИЛИ Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент окончания поддержки не анонсировано.
2	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674 Дата начала жизненного цикла 09.01.2013г.; набор обновлений Office 2013 Service Pack1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04.2018; Дополнительная дата окончания поддержки 11.04.2023г.

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

Практические занятия	Учебная аудитория для проведения занятий семинарского типа (практических работ) – – компьютерная аудитория	Количество рабочих мест – 12 Оборудование: Персональные компьютеры, объединенные в локальную сеть и имеющие выход в интернет
Самостоятельная работа	Помещения для самостоятельной работы	Компьютеры с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду ИСУ СКФУ.

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

Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

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 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.