МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Основы информационной безопасности»

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	1

Разработано
Лапина М.А. - доцент кафедры вычислительной математики и кибернетики.

Ставрополь 2026 г.

Цель и задачи освоения дисциплины

Цель дисциплины: Целью освоения дисциплины «Основы информационной безопасности» является формирование у будущего специалиста по специальности 10.05.03 «Информационная безопасность автоматизированных систем» профессиональных компетенций в области организационных и правовых аспектов защиты информации, а также умения применять нормативно-правовые и управленческие механизмы для обеспечения информационной безопасности.

Задачи дисциплины:

1. изучение нормативно-правовой базы в области информационной безопасности, включая международные и национальные стандарты;
2. формирование навыков разработки и внедрения организационных мер защиты информации в соответствии с законодательством;
3. освоение методов управления рисками и обеспечения соответствия требованиям регуляторов в сфере ИБ;
4. развитие умений анализа правовых последствий нарушений информационной безопасности и защиты данных;
5. изучение основ лицензирования, сертификации и аудита систем информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к дисциплинам обязательной части, специальности 10.05.03 Информационная безопасность автоматизированных систем. Ее освоение происходит в 1 семестре.

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

Код, формулировка компетенции	**Код, формулировка индикатора**	**Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов**
ОПК-1 Способен оценивать роль информации, информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	ИД-1ОПК-1 Понимает основные методологические принципы теории информационной безопасности; проблемы государственной и региональной информационной безопасности	Предоставляет отчёт с детальным анализом роли информации и информационных технологий информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства.
	ИД-2ОПК-1 Применяет основные методологические принципы теории информационной безопасности	Предоставляет детальный отчёт по результатам обеспечения информационной безопасности с использованием основных методологических принципов теории информационной безопасности.
	ИД-3ОПК-1 Определяет роль информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства	Предоставляет детальный отчёт с детальным анализом роли информации, информационной безопасности в современном обществе, их значение обеспечения объективных потребностей личности, общества и государства
	ИД-1ОПК-5 Знаком с действующим	Предоставляет детально

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	законодательством Российской Федерации в области информационной безопасности и защиты информации; системами защиты государственной тайны; определяет перечень сведений, относящихся к конфиденциальной информации и способы ее защиты; знаком с понятием и принципами электронной подписи (ЭП); определяет виды компьютерных вирусов; классифицирует компьютерные преступления; использует понятие и способы защиты интеллектуальной собственности; Знаком с действующим законодательством в области международного и российского права в области защиты информации; знаком со способами совершения преступлений в сфере компьютерной информации; знаком с правовыми режимами защиты информации.	проработанный план по использованию Законодательства Российской Федерации в области информационной безопасности и защиты информации; систем защиты государственной тайны с перечнем сведений относящихся к конфиденциально й информации и способы ее защиты; принципов электронной подписи (ЭП); различных видов компьютерных вирусов; классификаций компьютерных преступлений; понятий и способов защиты интеллектуальной собственности; международного и российского права в области защиты информации; способов совершения преступлений в сфере компьютерной информации; правовых режимов защиты информации.
	ИД-2ОПК-5 Определяет рациональные меры по обеспечению организационной защите на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов	Предоставляет детально проработанный план по организации защиты на объекте; организации работы персонала с конфиденциальной информацией; разработке проектов нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов
	ИД-3ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	Предоставляет детальный отчет с демонстрацией способности применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 3 з.е. 108 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	18/0
Лабораторных работ/из них практическая подготовка	0
Практических занятий/из них практическая подготовка	36/0
Самостоятельная работа	18
Формы контроля	
Экзамен **1 семестр**	36

Зачет	-
Зачет с оценкой	-
Курсовая работа	нет

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий

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

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
	1 СЕМЕСТР						
1.	**Анализ источников, каналов распространения и каналов утечки информации** Выявление, как информация создаётся, передаётся и может быть утрачена, анализ рисков и способов защиты. В данной теме студентам предстоит изучить, как информация создается, передается и где возникают риски её утечки. Особое внимание будет уделено источникам, каналам распространения и потенциальным каналам утраты информации. В конце изучения темы студент будет уметь анализировать информационные потоки и выявлять риски нарушения безопасности.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование

2.	**Проведение анализа информации на предмет целостности** Оценка сохранности данных в процессе хранения и передачи, проверка на отсутствие несанкционированных изменений, методы контроля целостности, использование хеш-функций и цифровых подписей. В данной теме студентам предстоит освоить методы анализа информации на предмет целостности. Особое внимание будет уделено проверке неизменности данных при передаче и хранении, использованию хеш-функций и цифровых подписей. В конце изучения темы студент будет знать способы контроля целостности информации и сможет их применять на практике.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
3.	**Оценка уязвимости информации** Анализ потенциальных угроз и слабых мест в системе защиты информации, выявление точек возможного вторжения, использование инструментов сканирования и тестирования на проникновение. В данной теме студентам предстоит провести оценку уязвимости информационных систем. Особое внимание будет уделено методам анализа угроз, выявлению слабых мест в защите и инструментам тестирования на проникновение. В конце изучения темы студент будет уметь оценивать потенциальные риски и предлагать меры по их снижению.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
4.	**Требования к безопасности информационных систем** Определение минимальных и рекомендуемых требований для защиты данных и систем, подходы к обеспечению конфиденциальности, целостности и доступности информации. В данной теме студентам предстоит изучить требования к безопасности информационных систем, направленные на защиту данных. Особое внимание будет уделено принципам обеспечения конфиденциальности, целостности и доступности информации. В конце изучения темы студент будет уметь формулировать базовые требования к защите ИС.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование

5.	**Требования к безопасности информационных систем в России** Изучение нормативных документов, таких как ФЗ-152, ГОСТ Р 57580, постановления правительства, требования ФСТЭК и ФСБ, регламентирующих защиту ИС в РФ. В данной теме студентам предстоит изучить нормативно-правовые акты, регулирующие безопасность информационных систем в России. Особое внимание будет уделено таким документам, как ФЗ-152, ГОСТ Р 57580, требованиям ФСТЭК и ФСБ. В конце изучения темы студент будет знать основные положения законодательства РФ в области ИБ.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
6.	**Оценка состояния безопасности ИС США** Обзор стандартов США в сфере ИБ (например, NIST), принципов построения систем безопасности, подходов к управлению рисками и реагированию на инциденты. В данной теме студентам предстоит ознакомиться с подходами США к обеспечению безопасности ИС. Особое внимание будет уделено стандартам NIST, процедурам управления инцидентами и оценки рисков. В конце изучения темы студент будет знать ключевые принципы построения систем ИБ в США.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
7.	**Определение классов защищенности средств вычислительной техники от несанкционированного доступа** Классификация СВТ по уровням защиты, определение требований к каждому классу, методы оценки соответствия, примеры сертифицированных устройств. В данной теме студентам предстоит изучить классификацию средств вычислительной техники по уровням защищенности от НСД. Особое внимание будет уделено требованиям к различным классам защиты, методам оценки и сертификации. В конце изучения темы студент будет знать классы защищенности и критерии их соответствия.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование

8.	**Определение требований к защите информации** Разработка политики безопасности в зависимости от вида обрабатываемой информации, категории данных и угроз, установление процедур доступа и контроля. В данной теме студентам предстоит научиться определять требования к защите информации в зависимости от её категории и уровня угроз. Особое внимание будет уделено политике безопасности, контролю доступа и разработке защитных мер. В конце изучения темы студент будет уметь формулировать требования к защите данных.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
9.	**Анализ терминов и определений информационной безопасности** Изучение базовой терминологии в области ИБ: конфиденциальность, угроза, уязвимость, инцидент, криптография и других ключевых понятий. В данной теме студентам предстоит изучить ключевые термины в области информационной безопасности. Особое внимание будет уделено понятиям конфиденциальности, угроз, уязвимостей, инцидентов и криптографических методов. В конце изучения темы студент будет понимать и правильно использовать терминологию ИБ.	ОПК-1 ИД-1ОПК-1 ИД-2ОПК-1 ИД-3ОПК-1 ОПК-5 ИД-1ОПК-5 ИД-2ОПК-5 ИД-3ОПК-5	2	4	-	2	Собеседование
	ИТОГО за 1 семестр		**18**	**36**	**-**	**18**	
	ИТОГО		**18**	**36**	**-**	**18**	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине базируется на перечне осваиваемых компетенций с указанием индикаторов. 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 (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины.

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина «Основы информационной безопасности» 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 практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным 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

8.1.1. Перечень основной литературы:

1. Сычев Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : ИНФРА-М, 2024. — 337 с. — (Среднее профессиональное образование). - ISBN 978-5-16-019432-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2118689
2. Башмакова Е. И. Информатика и информационные технологии. Умный Excel: библиотека функций : учебное пособие / Е. И. Башмакова. — 2-е изд. — Москва : Ай Пи Ар Медиа, 2024. — 109 с. — ISBN 978-5-4497-3416-7. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/142075

8.1.2. Перечень дополнительной литературы:

1. Мандра А.Г. Информатика и информационные технологии: лабораторный практикум / А.Г. Мандра, А.В. Попов, А.И. Дьяконов. - 2-е изд. - Самара: Самар. гос.техн. ун-т, 2020. - 64 с.
2. Гвоздева В. А. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. — Москва : ФОРУМ : ИНФРА-М, 2026. — 542 с.

— (Среднее профессиональное образование). - ISBN 978-5-8199-0856-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169724

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

1. Методические указания по выполнению лабораторных работ по дисциплине "Основы информационной безопасности" (электронный ресурс)

2. Методические указания по организации и проведению самостоятельной работы по дисциплине "Основы информационной безопасности" (электронный ресурс)

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

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Основы информационной безопасности»
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, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

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

1	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция К
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

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

Практические занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины 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 обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины 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 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.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-

телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются:

способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование);

ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»;

для синхронного обучения - время проведения онлайн-занятий и преподаватели;

для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.