Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета

_____ О.Н. Левчегов
«*24*» *апреля* 20*24* г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Липецк - 2024

Рабочая программа дисциплины «Основы информационной безопасности» разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:
Якушов Ю.А. старший преподаватель кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.
Протокол от 23.04.2024 г. №10

Заведующий кафедрой
Учет и информационные технологии в бизнесе _____ Н.С. Морозова

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1 Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Изучению данной дисциплины предшествует освоение дисциплин: Информатика Учебная дисциплина должна изучаться перед рассмотрением материала по профессиональным модулям: является базовой при изучении профессиональных модулей ПМ.01 и ПМ.02.

Рабочая программа дисциплины обеспечивает формирование ключевых компетенций цифровой экономики: коммуникация и кооперация в цифровой среде, саморазвитие в условиях неопределенности, креативное мышление, управление информацией и данными, критическое мышление в цифровой среде.

Она обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС квалификации «Техник по защите информации» с применением сквозных информационных технологий в области информационной безопасности в телекоммуникационных, компьютерных, автоматизированных системах и сетях организаций и предприятий в эпоху цифровой экономики 4.0. Особое значение дисциплина имеет при формировании и развитии ОК 09. Использовать информационные технологии в профессиональной деятельности.

Рабочая программа составлена для очной формы обучения, в том числе с применением элементов дистанционных образовательных технологий и электронного обучения. При обучении инвалидов и лиц с ограниченными возможностями здоровья дистанционные образовательные технологии и электронное обучение предусматривают возможность приема-передачи информации в доступных для них формах.

1.2 Цель и планируемые результаты освоения дисциплины:

В рамках программы дисциплины обучающимися осваиваются умения и знания:

Общие компетенции

Код компетенции	Формулировка компетенции	Знания, умения
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие. (Ключевые компетенции цифровой экономики Саморазвитие в условиях неопределенности)	Умения: определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования. –- ставить себе образовательные цели под возникающие жизненные задачи; –находить информацию в целях самообразования и обучения,

	(Ключевые компетенции цифровой экономики Саморазвитие в условиях неопределенности)	- создавать электронные конспекты при помощи онлайн платформ для создания, представления и анализа презентаций; – самостоятельно определять пробелы в своих знаниях и компетенциях с использованием инструментов самооценки и цифровых оценочных средств LMS, – выбирать цифровые средства в целях саморазвития, использовать цифровые тренажеры для обучения - адаптироваться к появлению новых цифровых средств, приложений, программного обеспечения
		Знания: - содержание актуальной нормативно-правовой документации; - современная научная и профессиональная терминология; - возможные траектории профессионального развития. -основных образовательных Интернет-ресурсов, типов цифрового образовательного контента; - возможностей и ограничений образовательного процесса при использовании цифровых технологий. - возможности, область применения и интерфейс цифровых инструментов для обучения
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	Умения: описывать значимость своей профессии; Презентовать структуру профессиональной деятельности по профессии (специальности)
		Знания: - сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности
ОК 09	Использовать информационные	Умения:

	технологии в профессиональной деятельности (Ключевые компетенции цифровой экономики Элемент цифровой грамотности в профессиональной деятельности)	– применять средства информационных технологий для решения профессиональных задач; – использовать современное программное обеспечение.
		Знания: – современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.	Умения: – понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), – понимать тексты на базовые профессиональные темы; – участвовать в диалогах на знакомые общие и профессиональные темы; – строить простые высказывания о себе и о своей профессиональной деятельности; – кратко обосновывать и объяснить свои действия (текущие и планируемые); – писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции

Основные виды деятельности	Код и формулировка компетенции	Показатели освоения компетенции

Защита информации в информационно – телекоммуникационных , компьютерных, автоматизированных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Умения: классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации
		Знания: сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности.

В соответствии с Профессиональным стандартом «Специалист по защите информации в автоматизированных системах» для выполнения трудовой функции 3.1.1 Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем с целью овладения профессиональной деятельности умениями для выполнения трудовых функций и соответствующими компетенциями обучающийся в ходе освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен:

уметь:

- конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией;
- обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации;
- производить монтаж и диагностику компьютерных сетей;
- использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи

знать:

- типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;
- базовую конфигурацию системы защиты информации автоматизированной системы;
- особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- нормативные правовые акты в области защиты информации;
- организационные меры по защите информации,

Для выполнения трудовой функции 3.1.2 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем, обучающийся должен:

уметь:

- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации.

знать:

- нормативные правовые акты в области защиты информации;
- основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации;
- эксплуатационная и проектная документация на автоматизированную систему;
- основные методы организации и проведения технического обслуживания технических средств информатизации;
- организационные меры по защите информации.

Для выполнения трудовой функции 3.1.3 Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем, обучающийся должен:

уметь:

- использовать программные средства для архивирования информации;
- использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации;
- использовать типовые криптографические средства защиты информации, в том числе электронную подпись

знать:

- процедуры по архивированию информации, обрабатываемой автоматизированной системой;
- назначение и принципы работы основных узлов современных технических средств информатизации;
- организацию ремонтного обслуживания компонентов автоматизированной системы;
- регламент автоматизированной системы по уничтожению информации и машинных носителей информации.
- нормативные правовые акты в области защиты информации;
- основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации.

В соответствии с Профессиональным стандартом «Специалист по защите информации в телекоммуникационных системах и сетях» для выполнения трудовой функции 3.1.1 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД с целью овладения профессиональной

деятельности умениями для выполнения трудовых функций и соответствующими компетенциями обучающийся в ходе освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен:

уметь:

- проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НСД
- проводить монтаж (для программных средств - установку) СССЭ, средств и систем защиты СССЭ от НСД
- проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД

знать:

- номенклатуру, функциональное назначение и основные характеристики СССЭ
- номенклатуру, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НСД
- нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НСД
- нормативные правовые акты в области связи, информатизации и защиты информации

Для выполнения трудовой функции 3.1.2 Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД, обучающийся должен:

уметь:

- проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД, предусмотренный регламентом их эксплуатации
- выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
- проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

знать:

- типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД
- последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования
- последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД
- организационные меры по защите информации
- нормативные правовые акты в области связи, информатизации и защиты информации.

Для выполнения трудовой функции 3.1.2 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД, обучающийся должен:

уметь:

- организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД
- правила ведения эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
- методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НС.

В соответствии с Профессиональным стандартом «Специалист по безопасности компьютерных систем и сетей» для выполнения трудовой функции 3.1.1 Обслуживание программно-аппаратных средств защиты информации в операционных системах с целью овладения профессиональной деятельности умениями для выполнения трудовых функций и соответствующими компетенциями обучающийся в ходе освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен:

уметь:

- настраивать компоненты подсистем защиты информации операционных систем;
- управлять учетными записями пользователей, в том числе генерацией, сменой и восстановлением паролей;
- применять программно-аппаратные средства защиты информации в операционных системах;
- применять антивирусные средства защиты информации в операционных системах;
- работать в операционных системах с соблюдением действующих требований по защите информации;
- проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;
- устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;
- выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации;
- контролировать целостность подсистем защиты информации операционных систем;
- устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации;
- оформлять эксплуатационную документацию программно-аппаратных средств защиты информации.

знать:

- архитектуру и пользовательские интерфейсы операционных систем
- порядок обеспечения безопасности информации при эксплуатации операционных систем
- источники угроз информационной безопасности и меры по их предотвращению
- сущность и содержание понятия информационной безопасности, характеристики ее составляющих
- типовые средства защиты информации в операционных системах
- программно-аппаратные средства и методы защиты информации
- порядок эксплуатации средств антивирусной защиты в операционных системах
- формы и методы инструктажа пользователей по порядку работы в операционных системах
- общие принципы функционирования программно-аппаратных средств криптографической защиты информации
- порядок оформления эксплуатационной документации
- нормативные правовые акты в области защиты информации
- основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- организационные меры по защите информации

Для выполнения трудовой функции 3.1.2 Обслуживание программно-аппаратных средств защиты информации в компьютерных сетях, обучающийся должен:

уметь

- применять программно-аппаратные средства защиты информации в компьютерных сетях;
- устанавливать межсетевые экраны в компьютерных сетях;
- конфигурировать межсетевые экраны в соответствии с заданными правилами;
- контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами;
- работать в компьютерных сетях с соблюдением действующих требований по защите информации;
- проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях;
- устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации;
- формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях,

знать:

- топологии и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях;
- состав и основные характеристики оборудования, применяемого при построении компьютерных сетей;
- типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях;
- типовые сетевые атаки и способы защиты от них;
- сущность и содержание понятия информационной безопасности, характеристики ее составляющих;
- основные источники угроз информационной безопасности и меры по их предотвращению;
- программно-аппаратные средства и методы защиты информации;
- основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей;
- порядок оформления эксплуатационной документации;
- общие принципы функционирования средств криптографической защиты информации в компьютерных сетях;
- порядок обеспечения безопасности информации при эксплуатации компьютерных сетей;
- формы и методы инструктажа пользователей по порядку работы в компьютерных сетях;
- нормативные правовые акты в области защиты информации;
- основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- организационные меры по защите информации.

В соответствии с Профессиональным стандартом «Специалист по технической защите информации» для выполнения трудовой функции 3.1.1 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок с целью овладения профессиональной деятельности умениями для выполнения трудовых функций и соответствующими компетенциями обучающийся в ходе освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен:

уметь:

- производить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить настройку и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов;
- проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок и при необходимости организовывать их ремонт с привлечением производителей технических средств защиты информации;

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации;
- технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;
- способы защиты информации от утечки по техническим каналам;
- технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- методы и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- технические описания и инструкции (руководства) по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок);
- техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
- порядок устранения неисправностей и организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.

Для выполнения трудовой функции 3.1.2 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам, обучающийся должен:

уметь:

- производить установку и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить настройку и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с технической документацией, инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить устранение выявленных неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и при необходимости организовывать их ремонт с привлечением производителей технических средств защиты информации,

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации;
- технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные);
- возможности средств акустической речевой разведки;
- технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных электронных устройств перехвата информации в технические средства и (или) помещения;
- основные характеристики электронных устройств перехвата информации;
- способы защиты акустической речевой информации от утечки по техническим каналам;
- технические средства защиты акустической речевой информации от утечки по техническим каналам;
- методы и методики контроля эффективности защиты акустической речевой информации от утечки по техническим каналам;
- средства контроля эффективности защиты акустической речевой информации от утечки техническим каналам;
- технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам;
- проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам);
- порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам;
- порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта.

Для выполнения трудовой функции 3.1.2 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа, обучающийся должен:

уметь:

- производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;

- проводить испытания программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;
- проводить устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организовывать их ремонт с привлечением производителей этих средств;

знать:

- нормативные правовые акты, методические документы, национальные стандарты в области защиты информации от несанкционированного доступа и аттестации автоматизированных систем на соответствие требованиям по защите информации;
- способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах;
- методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее;
- методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий;
- средства контроля защищенности информации от несанкционированного доступа;
- методики контроля защищенности информации от несанкционированного доступа;
- технические описания и инструкции по эксплуатации программно-технических средств защиты информации от несанкционированного доступа;
- техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий;
- порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины, в том числе:	**62**
3.1.Объем работы обучающихся во взаимодействии с преподавателем	**36**
Теоретическое обучение	18
Практические занятия	18
б) промежуточная аттестация (дифференцированный зачет)	-
3.2.Самостоятельная работа обучающихся	**26**

2.2. Тематический план и содержание дисциплины.

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Основы информационной безопасности		**62**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**4**	ОК 03, ОК 06, ОК 09, ОК 10
	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности».		
	Самостоятельная работа	**12**	
	Внеаудиторная работа с ЭБС. Создание презентаций в приложении Prezi, подготовка публичных выступлений по темам: Примеры преступлений в сфере информации и информационных технологий. Защита человека от опасной информации и от неинформированности в области информационной безопасности для проведение информационных бесед со студентами учебного заведения		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	**6**	ОК 03, ОК 06, ОК 09, ОК 10
	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки,		

	передачи. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	Практические занятия	**2**	
	Практическое занятие №1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
	Самостоятельная работа	**4**	
	Внеаудиторная работа с ЭБС. Ответы на вопросы. Сообщения по теме		
Тема 1.3. Угрозы безопасности защищаемой информации	**Содержание учебного материала**	**2**	ОК 03, ОК 06, ОК 09, ОК 10
	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации.		
	Практические занятия	**8**	
	Практическое занятие №2 Определение объектов защиты на типовом объекте информатизации. Практическое занятие №3 Определение угроз объекта информатизации и их классификация Практическое занятие №4 Уязвимости. Методы оценки уязвимости информации Практическое занятие №5 Исследование каналов и методов несанкционированного доступа к информации		
	Самостоятельная работа	**2**	
	Внеаудиторная работа с ЭБС. Ответы на вопросы. Сообщения по теме		
Тема1.4. Методологические подходы к защите информации	**Содержание учебного материала**	**4**	ОК 03, ОК 06, ОК 09, ОК 10
	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.		
	Практические занятия	**6**	
	Практическое занятие №6 Исследование методик определения требований к защите информации. Практическое занятие №7 Исследование параметров защищаемой информации и оценка факторов, влияющих на		

	требуемый уровень защиты информации. Практическое занятие №8 Анализ основных принципов защиты информации.		
	Самостоятельная работа	**2**	
	Внеаудиторная работа с ЭБС. Ответы на вопросы. Сообщения по теме		
Тема1.5 Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	**2**	ОК 03, ОК 06, ОК 09, ОК 10
	Организационная структура системы защиты информации Законодательные акты в области защиты информации Российские и международные стандарты, определяющие требования к защите информации.		
	Практические занятия	**2**	
	Практическое занятие №9 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности (часть 1)		
	Самостоятельная работа	**6**	
	Практическое занятие №10 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности (часть 2) Практическое занятие №11 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности (часть 3) Практическое занятие №12 Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности (часть 4)		
	Зачет	**2**	
			Всего: 62 часа

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Для реализации программы дисциплины предусмотрены следующие специальные помещения (в соответствии с ФГОС и ПООП):

1. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
(Кабинет информатики)

Специализированная мебель:
Лекционные парты – 13 шт.
Стулья – 37 шт.
Стол компьютерный – 1 шт.
Учебная доска – 1 шт.
Экран настенный – 1шт.

Технические средства обучения:
Компьютер преподавателя – 1 шт.
Компьютер обучающегося (ноутбук) – 12 шт.
Многофункциональное устройство/принтер – 1 шт.
Мультимедиа проектор – 1 шт.
Аудиоколонки – 1шт.

2. Лаборатория программных и программно-аппаратных средств защиты информации

Специализированная мебель:
Лекционные парты – 26 шт.
Стулья – 53 шт.
Стол компьютерный – 1 шт.
Учебная доска – 1 шт.
Экран настенный– 1 шт.

Технические средства обучения:
Компьютер преподавателя – 1 шт
Мультимедиа проектор – 1 шт.
Аудиоколонки – 1шт
Сервер – 2 шт.
Источники бесперебойного питания – 2 шт.
Многофункциональное устройство -1 шт.

Антивирусные программные комплексы; аппаратные средства аутентификации пользователя; программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации; средства защиты информации от несанкционированного доступа, блокирования доступа и нарушения целостности; программные средства криптографической защиты информации; программные средства выявления уязвимостей и оценки защищенности информационно-телекоммуникационной системы, анализа сетевого трафика.

Перечень лицензионного программного обеспечения:
1) Антивирусная защита Kaspersky Endpoint Security
2) Astra Linux, Libre Office
3) Программные средства криптографической защиты информации
4) Программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации, средствами защиты информации от НСД, блокирования доступа и нарушения целостности;

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

3. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
(Методический кабинет)

Специализированная мебель:
Компьютерные столы – 20 шт.
Стол письменный – 13 шт.
Кресло компьютерное – 20 шт.
Стулья – 26 шт.
Шкаф для учебно-методических материалов – 6 шт.

Технические средства обучения:
Персональные компьютеры – 18 шт.
Мультимедиа проектор – 1 шт.
Экран настенный – 1 шт.
Аудиоколонки – 1шт.

4. Помещения для самостоятельной работы: Библиотека и читальный зал с выходом в сеть Интернет

Специализированная мебель:
Стол кафедра – 3 шт.
Каталожный ящик – 1 шт.
Шкаф для читательских формуляров – 3 шт.
Витрина для книг – 3 шт.
Стол ученический – 24 шт.
Кресло компьютерное – 2 шт.
Стул - 48 шт.
Стол эргономичный с тумбой – 1 шт.
Шкаф для документов – 3 шт.

Технические средства обучения:
Персональные компьютеры– 18 шт.

Перечень профессиональных баз данных и информационно-справочных систем

Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» [Электронный ресурс]. URL: http://window.edu.ru/catalog/?p_rubr=2.2.75.6

Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: http://www.iprbookshop.ru/

Электронно-библиотечная система Юрайт: https://urait.ru

Электронно-библиотечная система Znanium: https://znanium.com/

Электронно-библиотечная система Book.ru: https://book.ru/

Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional
Microsoft Windows
Astra Linux , Libre Office

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Основные издания

Основные источники:

1. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860126 (дата обращения: 29.03.2024)

Дополнительные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 222 с. — ISBN 978-5-406-11653-1. — URL: https://book.ru/book/950118 (дата обращения: 29.03.2024)

2. Бабаш, А. В., Информационная безопасность. Лабораторный практикум + еПриложение : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2023. — 131 с. — ISBN 978-5-406-11731-6. — URL: https://book.ru/book/949452 (дата обращения: 29.03.2024).

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290 (дата обращения: 29.03.2024)

4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/542339 (дата обращения: 29.03.2024).

5. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва : Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный

6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536225 (дата обращения: 29.03.2024).

7. Елин, В. М., Организационное и правовое обеспечение информационной безопасности : учебное пособие / В. М. Елин, А. К. Жарова, ; под общ. ред. А. В. Царегородцева. — Москва : КноРус, 2024. — 177 с. — ISBN 978-5-406-12576-2. — URL: https://book.ru/book/952750 (дата обращения: 29.03.2024).

8. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543873 (дата обращения: 29.03.2024).

9. 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.com/catalog/product/2118689 (дата обращения: 29.03.2024).

10. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности : учебное пособие / Ю. А. Родичев. - Санкт-Петербург : Питер, 2021. - 256 с. - (Серия «Учебник для вузов»). - ISBN 978-5-4461-0861-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1766376 (дата обращения: 29.03.2024)

11. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178 (дата обращения: 29.03.2024).

Периодические издания:

12. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

13. Журналы Защита информации. Инсайд: Информационно-методический журнал Информационная безопасность регионов: Научно-практический журнал

14. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

15. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

В соответствии со ст. 43 Конституции Российской Федерации, 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012, приказом Минобрнауки России от 09.11.2015 N 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», ГОСТ Р 57723-2017 «Информационно-коммуникационные технологии в образовании. Системы электронно-библиотечные. Общие положения», ГОСТ Р 52872-2019 «Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности», все предлагаемые электронные ресурсы максимально комфортны для

чтения слабовидящими людьми. Масштабирование текста достигает 300 процентов. При изменении масштаба сохраняется возможность видеть всю страницу текста, не обрезая его.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Умения: классифицировать защищаемую информацию по видам тайны и степеням секретности; –классифицировать основные угрозы безопасности информации; **Знания:** сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Контроль выполняется по результатам проведения различных форм опроса, выполнения контрольных работ, тестирования, выполнения практических работ, промежуточной аттестации. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя