Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора по
учебной работе

_____ Н.Ю. Долгова
«_10_» _июня_ 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП. 04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Москва 2024 г.

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

Разработчики:

Маринич Анна Леонидовна, преподаватель первой квалификационной категории Колледжа информатики программирования

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии

Протокол от «13» июня 2024 г. №10

Председатель предметной (цикловой) комиссии _____ /А.Л. Маринич/

1. Общая характеристика рабочей программы дисциплины

1.1. Место дисциплины в структуре основной образовательной программы

Дисциплина «ОП. 04 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

1.2.Цель и планируемые результаты освоения дисциплины

В рамках программы дисциплины студентами осваиваются умения и знания

Код общих и профессиональных компетенций	Умения	Знания
ОК 03. ОК 06. ОК 09. ОК 10. ПК 2.4	- классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации - *Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации* - *Формулировать предложения по применению программно-аппаратных средств защиты и других средств защиты информации**	-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 - *организационные меры по защите информации* - *нормативные правовые акты в области защиты информации**

*вариативная часть

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы дисциплины	87
Объем работы студентов во взаимодействии с преподавателем	76
в том числе:	
теоретическое обучение	40
практические занятия	24
самостоятельная работа	11
Промежуточная аттестация в форме экзамена	12

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности студентов	Объем в часах	Коды компетенций формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности		**31**	
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала	10	ОК 03. ОК 06. ОК 09. ПК.2.4
	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». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.	4	
	*Роль специалиста по защите информации**	2	
	*Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства**	4	
	В том числе практических занятий	-	
	Самостоятельная работа студентов	-	
Тема 1.2. Основы защиты информации	Содержание учебного материала	10	ОК 03. ОК 06. ОК 09. ПК.2.4
	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. Цели и задачи защиты информации. Основные понятия в области защиты информации.	4	

	Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.		
	В том числе практических занятий	6	
	1.Практическое занятие «Определение объектов защиты на типовом объекте информатизации.»	4	
	2.Практическое занятие «Классификация защищаемой информации по видам тайны и степеням конфиденциальности.»	2	
	Самостоятельная работа	-	
Тема 1.3. Угрозы безопасности защищаемой информации.	Содержание учебного материала	11	ОК 03. ОК 06. ОК 09. ПК.2.4
	Понятие угрозы безопасности информации Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации Уязвимости. Методы оценки уязвимости информации	2	
	В том числе практических занятий	4	
	1.Практическое занятие «Определение угроз объекта информатизации и их классификация»	4	
	Самостоятельная работа Работа с документами	5	
Раздел 2. Методология защиты информации		44	
Тема 2.1. Методологические подходы к защите информации	**Содержание учебного материала**	2	ОК 03. ОК 06. ОК 09. ПК.2.4
	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.	2	
	В том числе практических занятий	-	
	Самостоятельная работа студентов	-	
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание учебного материала**	6	ОК 03. ОК 06. ОК 09. ПК.2.4 ОК 03. ОК 06. ОК 09. ПК.2.4
	Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и	2	

	документы системы сертификации РФ в области защиты информации		
	В том числе практических занятий	4	
	1.Практическое занятие «Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности»	4	
	Самостоятельная работа	-	
Тема 2.3. *Нормативно правовое регулирование защиты информации**	Содержание учебного материала	20	ОК 03. ОК 06. ОК 09. ПК.2.4
	Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности	4	
	Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения	2	
	Оценка рисков и организация управления процессом защиты информации	4	
	Справочно-правовая система с нормативными и правовыми документами по информационной безопасности международного статуса	4	
	В том числе практических занятий	6	
	1.Практическое занятие *«Создание политики безопасности для коммерческой организации»*	4	
	2.Практическое занятие *«Оценка информационных рисков автоматизированной системы»*	2	
	Самостоятельная работа	-	
Тема 2.4. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	16	ОК 03. ОК 06. ОК 09. ПК.2.4 ОК 03. ОК 06. ОК 09. ПК.2.4
	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы	2	

	построения организационно-распорядительной системы.		
	Уровни и сервисы защиты информации в автоматизированных системах	2	
	Формальные модели безопасности	2	
	Критерии оценки защищенности информационных систем	2	
	В том числе практических занятий	4	
	1.Практическое занятие «Выбор мер защиты информации для автоматизированного рабочего места»	4	
	Самостоятельная работа студентов Работа с документами	6	
Консультации		**4**	
Промежуточная аттестация в форме экзамена		**8**	
Всего:		**87**	

3. Условия реализации дисциплины

3.1. Материально-техническое обеспечение

Для реализации программы дисциплины должны быть предусмотрены специальные помещения: Кабинет нормативного правого обеспечения информационной безопасности

Оборудование учебного кабинета:
-посадочные места по количеству обучающихся;
-рабочее место преподавателя;
-доска меловая;
-место хранения раздаточного и дидактического материала;
-наглядные пособия (комплекты учебных таблиц, плакатов, учебно-наглядных пособий);
-учебно-методические комплекты (УМК) (в т.ч. мультимедийные);
-дидактические материалы (раздаточный материал, ФОС и др.).

Технические средства обучения:
-персональный компьютер с лицензионным программным обеспечением, подключенный к локальной сети и выходом в интернет
-проектор с экраном.
Помещение для самостоятельной работы (Библиотека, читальный зал с выходом в сеть интернет)
-автоматизированные рабочие места обучающихся с выходом в Интернет и доступом в электронную информационно-образовательную среду образовательной организации (процессор Core i5, оперативная память объемом 16 Гб).

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания

1.Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2022

Дополнительные источники:

1.Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 07.11.2023). – Режим доступа: по подписке.
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: 07.11.2023). — Текст : электронный.

Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал Информационная безопасность регионов: Научно-практический журнал
3. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
4. 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

3. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения студентами индивидуальных заданий, проектов, исследований.

Результаты обучения	**Критерии оценки**	**Методы оценки**
Умения: - классифицировать защищаемую информацию по видам тайны и степеням секретности; - классифицировать основные угрозы безопасности информации - *Оформлять техническую документацию в соответствии с нормативными правовыми актами в области защиты информации* - *Формулировать предложения по применению программно-аппаратных средств защиты и других средств защиты информации**;	Оценка умений осуществляется по пятибалльной шкале	Контроль знаний и умений осуществляется в ходе выполнения практических и занятий, промежуточной аттестации в форме экзамена. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы Экспертное заключение преподавателя
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	Оценка знаний осуществляется по пятибалльной шкале	Контроль выполняется по результатам проведения различных форм опроса, выполнения контрольных работ, тестирования, выполнения практических занятий, промежуточной аттестации в форме экзамена. Интерпретация результатов наблюдений преподавателя за деятельностью обучающегося в процессе освоения образовательной программы

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.		Экспертное заключение преподавателя