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_ 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.10 ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

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) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Разработчики:
Сидлеров С.Д., преподаватель Колледжа информатики и программирования

Рабочая программа учебной дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии
Обеспечения информационной безопасности автоматизированных систем

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

Учебная дисциплина «ОП.10 Основы кибербезопасности» является вариативной 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. 01. ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.	-определять кибератаки и их признаки, процессы и контрмеры информационной безопасности; - по управлению безопасностью, использованию средств контроля, защиты и технологий минимизации последствий; -определять способы защиты конфиденциальности с помощью технологий, продуктов и процедур.	- отличительные черты преступников в сфере кибербезопасности и тех, кто им противостоит; -защита всех компонентов сетевой инфраструктуры; -этические требования, законы в области информационной безопасности и методы разработки политик безопасности; -функции специалистов по кибербезопасности и карьерные возможности.

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы дисциплины	48
Объем работы студентов во взаимодействии с преподавателем	48
в том числе:	
теоретическое обучение	22
практические занятия	24
лабораторные работы	-
контрольные работы	-
самостоятельная работа	-
Промежуточная аттестация в форме дифференцированного зачета	2

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**
Тема 1.1 Концептуальные основы кибербезопасности.	Содержание учебного материала	2	ОК. 01 ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.
	1.Введиние в дисциплину. *2.*Концептуальные основы кибербезопасности. 3. Структура стандарта по киберпезопасности. 4.Базовые меры по кибербезопасности. 5.Национальные стандарты в области киберпезопасности.	2	
	В том числе практических занятий	-	
	Самостоятельная работа студентов	-	
Тема 1.2 Компьютерные сети, информационно-аналитические системы и системы моделирования в технике	Содержание учебного материала	8	
	1.Компьютерные сети, информационно-аналитические системы и системы моделирования в технике. 2.Информационная безопасность. Функциональная безопасность. 3.Уязвимости, угрозы и риски. 4.Вредоносное программное обеспечение. 5.Векторы и поверхности атаки. 6.Последствия кибератак. 7. Нетехнические способы компрометации систем безопасности. 8. Социальная инженерия. 9. Информационная безопасность. 10.Функциональная безопасность. 11.Уязвимости, угрозы и риски. 12.Вредоносное программное обеспечение. 13.Векторы и поверхности атаки. 14.Последствия кибератак.	6	ОК. 01 ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.
	В том числе практических занятий	2	
	1.Практическое занятие «Создание модели локальной сети»	1	

	2.Практическое занятие «Изучение методов кодирования сигналов»	1	
	Самостоятельная работа студентов	-	
Тема 1.3 Киберпространство и основы кибербезопасности, векторы риска.	Содержание учебного материала	18	ОК. 01 ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.
	1.Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации. 2.Проверка подлинности (аутентификация) в Интернете. 3.Меры безопасности для пользователя WiFi. Настройка безопасности. 4.Настройка компьютера для безопасной работы. 5. Ошибки пользователя. 6.Меры личной безопасности при сетевом общении. 7.Настройки приватности в социальных сетях	6	
	В том числе практических и лабораторных занятий	12	
	1.Лабораторная занятие «Парольная защита» 2.Лабораторное занятие «Архивирование с паролем» 3.Лабораторное занятие «Шифр простой замены, таблица Вижинера» 4.Лабораторное занятие «Обмен ключами по Диффи-Хелману» 5.Лабораторное занятие «Шифр RSA» 6.Лабораторное занятие «Циклические коды»	2 2 2 2 2 2	
	Самостоятельная работа студентов	-	
Тема 1.4 Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	Содержание учебного материала	8	ОК. 01 ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.
	1.Понятие безопасности персонального компьютера. 2.Интернет и виды угроз компьютерной безопасности. 3. Проблемы безопасности информационных систем. 4.Методы обеспечения защиты данных в СУБД. 5.Безопасность при удаленном доступе к ресурсам компьютера. 6.Новые технологии и новые угрозы информационной безопасности. 7.Опасная информация в сети. 8.Проблемные сайты.	6	

	9.Риски интернета (контентные, электронные, коммуникационные, потребительские). 10.Проблемы интернет зависимости.		
	В том числе практических и лабораторных занятий	2	
	1.Лабораторное занятие «Расследование, анализ и реагирование на инциденты кибербезопасности в сетевой среде»	2	
	Самостоятельная работа студентов	-	
Тема 1.5 Теоретические основы и практические аспекты защиты киберпространства	Содержание учебного материала	10	ОК. 01 ОК. 02. ОК. 03. ОК. 04. ОК. 09. ОК. 10 ПК. 1.1. ПК. 1.2. ПК. 1.3. ПК. 1.4. ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.6. ПК 3.2.
	1.Задачи и уровни обеспечения защиты киберпространства. 2.Аспекты кибербезопасности. 3.Доктрина информационной безопасности РФ.	2	
	В том числе практических и лабораторных занятий	8	
	1.Лабораторное занятие «Выполнение оценки конфигурации элементов информационной инфраструктуры и определение отклонения данной конфигурация от приемлемой, определенной локальной политикой безопасности»	4	
	2.Лабораторное занятие «Тестирование, внедрение, развертывание, поддерживание и управление аппаратным и программным обеспечением в рамках информационной инфраструктуры организации»	4	
Промежуточная аттестация в форме дифференцированного зачета		2	
Всего:		**48**	

3. Условия реализации дисциплины

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

Кабинет информатики

Оборудование:

-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

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания:

1. Кравченко, В.Б. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении : учебное пособие для студентов учреждений среднего профессионального образования по специальности "Обеспечение информационной безопасности автоматизированных систем" / В.Б. Кравченко .— Москва : Академия, 2019 .— 301 с. + Тираж 1500 экз. — (Профессиональное образование) - 75 экз.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1189327 (дата обращения: 06.06.2022). – Режим доступа: по подписке.

3. Васильева, *И. Н.* Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

4. Внуков, *А. А.* Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 161 с. — (Профессиональное

образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

5.Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика: [16+] / В.Я. Ищейнов. – Москва; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 – ЭБС Университетская библиотека онлайн– Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст: электронный.

4. 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
Уметь: -определять кибератаки и их признаки, процессы и контрмеры информационной безопасности; -приобрести навыки по управлению безопасностью, использованию средств контроля, защиты и технологий минимизации последствий; -определять способы защиты конфиденциальности с помощью технологий, продуктов и процедур. Знать: -знать отличительные черты преступников в сфере кибербезопасности и тех, кто им противостоит; -защиты всех компонентов сетевой инфраструктуры. знать об этических требованиях и законах в области информационной безопасности и методах разработки политик безопасности; -знать о функциях специалистов по кибербезопасности и карьерных возможностях.	«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	Тестирование, Оценка решения практических работ, оценка решения ситуационных задач, Дифференцированный зачет.

	выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки	