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

«_30_» _июня_ 2021г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.08 Кибербезопасность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2021г.

Рабочая программа учебный дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчики:
Поколодина Е.В., к.э.н., преподаватель 1 КК Колледжа информатики и программирования
Дьяков А.И., преподаватель Колледжа информатики и программирования

Рецензент: Эдгулова Елизавета Каральбиевна., председатель Цикловой комиссии информационных технологий и программирования колледжа информационных технологий и экономики КБГУ, кандидат физико-математических наук

Рабочая программа учебной дисциплины рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии
Основы информационной безопасности
(наименование ПЦК)

Протокол от «13» 05 2020 г. № 10

Председатель ПЦК _____ Е.В.Поколодина
(подпись)

РЕЦЕНЗИЯ
НА РАБОЧУЮ ПРОГРАММУ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.08 Кибербезопасность

по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем,
составленную преподавателями Колледжа информатики и программирования ФГОБУ ВО «Финансовый университет при Правительстве РФ»
Поколодиной Е.В., Дьяковым А.И.

Рабочая программа разработана в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа дисциплины «Кибербезопасность» состоит из четырёх разделов:

1. Общая характеристика программы учебной дисциплины
2. Структура и содержание учебной дисциплины
3. Условия реализации учебной дисциплины
4. Контроль и оценка результатов освоения учебной дисциплины.

Структура, содержание, тематический план, учебная нагрузка - 88 часов, указанной рабочей программы, из них 48 часов теоретических и 32 часа практических занятий, достаточны для изучения представленных тем.

В целом рецензируемая рабочая программа дисциплины соответствует ФГОС СПО, обеспечивает формирование общих компетенций ОК2, ОК05, ПК 1.1, -1.4, ПК 2.1,2.2,2.3,2.6 ПК 3.2. и заслуживает высокой оценки.

Планируемые затраты времени на теоретические и практические работы гармонично распределены в зависимости от сложности тем и позволяют студентам использовать, получаемые при реализации данной программы, современные знания, как по экономике, так и по управлению, в своей будущей специальности.

Рабочая программа учебной дисциплины ОП.08 Кибербезопасность может быть рекомендована для использования в учебном подразделении СПО ФГОБУ ВО «Финансовый университет при Правительстве РФ» для подготовки студентов по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рецензент: Эдгулова Елизавета Каральбиевна., председатель Цикловой комиссии информационных технологий и программирования колледжа информационных технологий и экономики КБГУ, кандидат физико-математических наук

Подпись

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «ОП.08 Кибербезопасность» является вариативной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Учебная дисциплина «ОП.08 Кибербезопасность» обеспечивает формирование профессиональных и общих компетенций по всем видам деятельности ФГОС специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в

защищенном исполнении

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	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 УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	88
Объем работы обучающихся во взаимодействии с преподавателем	88
в том числе:	
теоретическое обучение	46
практические занятия	32
лабораторные работы	-
контрольные работы	-
курсовая работа (проект) *(если предусмотрено)*	-
самостоятельная работа	8
Промежуточная аттестация в форме дифференцированного зачета	2

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1.1 Концептуальные основы кибербезопасности.	**Содержание учебного материала**	**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**	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.
Тема 1.2 Компьютерные сети, информационно-аналитические системы и системы моделирования в технике	**Содержание учебного материала**	**18**	
	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.	**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.
	В том числе практических занятий и лабораторных работ:	**6**	
	Практическое занятие №1	**6**	
	Самостоятельная работа обучающихся	**2**	
	Оформление отчета по выполнению практической работы		

Тема 1.3 Киберпространство и основы кибербезопасности, векторы риска.	**Содержание учебного материала**	**30**	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	**16**	
	В том числе практических занятий и лабораторных работ:	**12**	
	Лабораторная работа № 1 Парольная защита **Лабораторная работа №2** Архивирование с паролем **Лабораторная работа № 3** Шифр простой замены, таблица Вижинера **Лабораторная работа № 4** Обмен ключами по Диффи-Хелману **Лабораторная работа №5** Шифр RSA **Лабораторная работа №6** Циклические коды	**2** **2** **2** **2** **2** **2**	
	Самостоятельная работа обучающихся	**2**	
	Оформление отчета по выполнению лабораторных работ		
Тема 1.4 Общие сведения о безопасности ПК и интернета, проблема интернет-зависимости	**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.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. 9.Риски интернета (контентные, электронные, коммуникационные,	**12**	

	потребительские). 10.Проблемы интернет зависимости.		
	В том числе практических занятий и лабораторных работ:	**4**	
	Лабораторная работа №7 «Расследование, анализ и реагирование на инциденты кибербезопасности в сетевой среде»	**4**	
	Самостоятельная работа обучающихся	**2**	
	Оформление отчета по выполнению лабораторной работы		
Тема 1.5 Теоретические основы и практические аспекты защиты киберпространства	**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.Задачи и уровни обеспечения защиты киберпространства. 2.Аспекты кибербезопасности. 3.Доктрина информационной безопасности РФ.	**6**	
	В том числе практических занятий и лабораторных работ:	**10**	
	Лабораторная работа №8 «Выполнение оценки конфигурации элементов информационной инфраструктуры и определение отклонения данной конфигурация от приемлемой, определенной локальной политикой безопасности»	**6**	
	Лабораторная работа №9 «Тестирование, внедрение, развертывание, поддерживание и управление аппаратным и программным обеспечением в рамках информационной инфраструктуры организации»	**4**	
	Самостоятельная работа обучающихся	**2**	
	Оформление отчета по выполнению лабораторных работ		
Промежуточная аттестация в форме дифференцированного зачета		**2**	
Всего:		**88**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения (в соответствии с ФГОС и ПООП):
Лаборатория сетей и систем передачи информации
Специализированная мебель:
Стол студенческий двухместный – 22 шт.
Стол студенческий одноместный – 25 шт.
Стулья студенческие –67 шт.
Стол (учительский) – 1 шт.
Стул (учительский) – 1 шт.
Доска меловая – 1 шт.
Технические средства обучения:
Компьютер студенческий – 15 шт.
Компьютер преподавателя – 1 шт.
Мультимедиа-проектор - 1 шт.
Экран с электроприводом – 1 шт.
Колонки для воспроизведения аудио – 1 шт.
Компьютеры подключены к локальной вычислительной сети, информационно-образовательной среде Финуниверситета и сети Интернет
Перечень лицензионного программного обеспечения:
1) Антивирусная защита: ESET NOD32
2) Windows, Microsoft Office
3) Microsoft Visio, Microsoft Project, Microsoft SQL Server, Microsoft Visual Studio, 1С Предприятие (учебная версия), эмуляторы активного сетевого оборудования, программное обеспечение сетевого оборудования

3.2. Информационное обеспечение реализации программы

3.2.1. Печатные 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, 2018 .— 301 с. + Тираж 1500 экз. — (Профессиональное образование) - 75 экз.

3.2.2 Электронные издания (электронные ресурсы)

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093657 – Режим доступа: по подписке.

2.Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469758.

3.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, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475890.

4.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 УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования.

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	«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	Тестирование Дифференцированный зачет, экспертное наблюдение выполнения лабораторных работ, наблюдение за выполнением практических работ, оценка решения ситуационных задач

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.	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	