Приложение I.17

к программе СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.10 КИБЕРБЕЗОПАСНОСТЬ

2023

Составитель:

Бокуменко Алекс Витальевич, преподаватель ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Кибербезопасность

наименование дисциплины

1.1. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Корпоративная защита от внутренних угроз информационной безопасности» принадлежит к общепрофессиональному циклу.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК, ЛР	Умения	Знания
ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10; ПК 1.1, ПК 1.2, ЛР 3, 17, 18	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; -выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	- способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; -типовых программных и программно-аппаратных средств защиты информации в ИТКС; -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; -возможных угроз безопасности информации в ИТКС; -способов защиты информации от НСД и специальных воздействий на нее; -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; -организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации; -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации; -возможных угроз безопасности информации в ИТКС; - способов защиты информации НСД и специальных воздействий на нее; -типовых программных и программно-аппаратных средств защиты информации в ИТКС;

	-выявлять и оценивать угрозы безопасности информации в ИТКС; -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; *-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;* *-проводить настройку систем защиты от внутренних угроз информационной безопасности*	-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации *-программные и программно-аппаратные средства защиты информации в ИТКС российского производства;*

1.3. Рекомендуемое количество часов на освоение программы дисциплины

Объем работы обучающихся во взаимодействии с преподавателем 116 часов, в том числе:

- 116 часов вариативной части, направленных на усиление обязательной части программы.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Объем образовательной программы	116
Объем работы обучающихся во взаимодействии с преподавателем	100
в том числе:	
- теоретическое обучение	40
- лабораторные работы (если предусмотрено)	-
- практические занятия (если предусмотрено)	60
- курсовая работа (проект) (если предусмотрено)	-
- самостоятельная работа[1]	12
- промежуточная аттестация (дифференцированный зачет)	4

[1]Самостоятельная работа в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема учебной дисциплины в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

2.2. Тематические план и содержание учебной дисциплины «Корпоративная защита от внутренних угроз информационной безопасности»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах	Коды компетенций, формированию которых способствует элемент программы
7 семестр				
Раздел 1.	**Linux. Виртуализация в ESXI.**		**40**	
Тема 1.1 Изучение серверных и десктопныхверсий ОС Linux. Знакомство с ESXI	**Содержание**		**16**	ОК 1, ОК2, ПК 1.1.
	Введение в Linux. Установка, настройка, администрирование.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Установка, настройка, администрирование Linux		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Kali Linux. Обзор операционной системы и её инструментов.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Bush. Использование команд Linux		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Kali Linux. Обзор операционной системы и её инструментов.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	VMware ESXI Server. Базовая настройка., репозитория.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	VMware ESXI Server. Создание пользователей.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	VMware ESXI Server. Настройка сети.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Практические занятия		32	
	1	Обзор VirtualBox, VMware Workstation, VMware ESXI.		
	2	Установка и конфигурирование ESXI. Развёртывание виртуальных машин в среде виртуализации ESXI.		
	3-4	ESXI. Настройка сети. Создание свичей, групп портов и vlan.		

	5	Установка виртуальных машин (Ubuntu desktop, Kali).		
	6-7	Базовые команды в Linux.		
	8	Инструменты для работы с текстом в Linux.		
	9-10	Файловые подсистемы в Linux.		
	11	Работа в Kali linux		
	12	Серверы Linux. Развёртывание и настройка.		
	13-14	Восстановление данных в Linux.		
	15	Шифрование данных в Linux.		
	16	Криптографическая библиотека OpenSSL		
Раздел 2.	**Настройка оборудования. Создание защищённой сети.**		**56**	ОК 1, ОК2, ПК 1.2.
Тема 2.1 Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP).	**Содержание**		**16**	
	Основы сетей: IPv4, WAN, L Net mask, Gateway.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Модель OSI		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	DNS, DHCP, VLAN		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	AD и Центр сертификации		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Знакомство с RouteOS.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Знакомство с Pfsense и другими Open sense.		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	NGFW. Логика работы правил файрволла.		2	ЛР3, ЛР17, ЛР18.
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			ОК 1, ОК2, ПК 1.2.
	AD и Центр сертификации		2	
	Домашнее задание: Чтение и анализ литературы [1] стр. 10-14			
	Практические занятия		28	
	17	Установка виртуальной машины (Windows Server 2022).		
	18	Развертывание роли DNS в Windows Server.		
	19	Развертывание основного контролера домена Active Directory в Windows Server. Создание пользователей. Настройка групповых политик. Введение машин в домен.		

	20	Установка и базовая настройка Pfsense. Создание интерфейсов, настройка DHCP.		
	21	Установка и базовая настройка RouterOS. Создание интерфейсов, настройка DHCP. Настройка L2TP соединения.		
	22	Установка и базовая настройка NGFW.		
	23	Развертывание роли сервера сертификации в Windows Server.		
	24	Выпуск сертификата. Ldap интеграция NGFW с AD.		
	25-26	Pfsense. Настройка VLAN и Trunk портов.		
	27	RouterOS. Настройка VLAN и Trunk портов		
	28	Основные понятия, принципы разграничения доступа. Создание правил файрволла.		
	29-30	Создание схемы защищённой сети. Построение схемы защищённой сети в ESXI.		
	Самостоятельная работа		12	
	Чтение и разбор литературы по настройке коммутационного оборудования и файровалла.			
		Всего:	**116**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия кабинет информатики.

Кабинет информатики
Оборудование учебного кабинета:

- посадочные места по количеству обучающихся (парты);
- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- рабочее место преподавателя с многофункциональным комплексом (персональный компьютер, периферийное оборудование и оргтехника);
- магнитно-маркерная доска;
- комплект учебно-наглядных пособий и плакатов.

Технические средства обучения:

- мультимедийное оборудование (проектор, экран);
- коммутационное оборудование;
- обучающее программное обеспечение;
- инструментальная среда программирования;
- пакет прикладных программ.

3.2. Информационное обеспечение обучения

Основные источники:

1. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов,. – Спб.: Питер, 2021. – 1008 с. 1 экз

2. Яворски П. "Ловушка для багов"ISBN 978-5-4461-1708-6 Автор Яворски П. 2020 информационные технологии 272 с.

3. Бирюков А А Б59 Информационная безонасность: защита и нанадение. -М.: ДМК Пресс, 2020. - 474 с.: ил

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2020.-272с.:ил.

5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2020.-528с.- (Профессиональное образование)

6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2020. – 616с:ил.

7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2020. – 192с.

8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2020. – 363 с.

9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2020. – 178 с.: ил..

Дополнительные источники:

1. Руководство пользователя MikroTik RouterOS

2. Руководство администратора Cisco NGFW
3. Руководство администратора Pfsense
4. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2020).
2. Сайт ФСТЭК РФ [Электронный ресурс] – режим доступа: http://www.fstec.ru
3. [Электронный ресурс] – режим доступа: http://www.ancad.ru сайт компании АНКАД
4. [Электронный ресурс] – режим доступа: https://mikrotik.wiki сайт MikroTik
5. [Электронный ресурс] – режим доступа: https://www.pfsense.org/ сайт разработчиков pfsense

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
Умения:		
- выявлять и оценивать угрозы безопасности информации в ИТКС;	«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.	Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24. Выполнение индивидуальных заданий различной сложности
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;		Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24.
-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;		Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24.
-проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;		Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24. Выполнение индивидуальных заданий различной сложности
-выявлять и оценивать угрозы безопасности информации в ИТКС;		Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24.
-выявлять и оценивать техническое -настраивать и применять средства защиты		Наблюдение за выполнением практических заданий № 1, 3-24. Оценка выполнения практических заданий № 1, 3-24.

информации в операционных системах, в том числе средства антивирусной защиты;	«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	
Знания:		
- способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;		Оценка отчетов по выполнению практических работ № 1-2
-типовых программных и программно-аппаратных средств защиты информации в ИТКС;		Опрос по теме 2.1
-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;		Оценка отчетов по выполнению практических работ № 3-24 Экзамен
-возможных угроз безопасности информации в ИТКС;		Оценка отчетов по выполнению практических работ № 23-24
-способов защиты информации от НСД и специальных воздействий на нее;		Оценка отчетов по выполнению практических работ № 27-38
-порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;		Опрос по теме 2.15
- способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;		Оценка отчетов по выполнению практических работ № 3-38 Экзамен
-типовых программных и программно-аппаратных		Оценка отчетов по выполнению практических работ № 3-38 Экзамен

средств защиты информации в ИТКС;		
-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;		Опрос по темам 3.1-3.2

Приложение 1

Обязательное

КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ

Личностные результаты	Содержание урока (тема, тип урока, воспитательные задачи)	Способ организации деятельности	Продукт деятельности	Оценка процесса формирования ЛР
ЛР 3 Демонстрирующий приверженность традиционным духовно-нравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовно-нравственных, социокультурных ценностей и норм с учетом осознания последствий поступков. Готовый к деловому взаимодействию и неформальному общению с представителями разных народов, национальностей, вероисповеданий, отличающий их от участников групп с деструктивным и девиантным поведением. Демонстрирующий неприятие социально опасного поведения окружающих и предупреждающий его. Проявляющий уважение к людям старшего поколения, готовность к участию в социальной поддержке нуждающихся в ней **ЛР 17** Способный разрабатывать техническое задание на сопровождение информационной системы, дизайн-концепции веб-приложений в соответствии с корпоративным стилем заказчика, требования к программным модулям на основе анализа проектной и технической документации на предмет взаимодействия компонент **ЛР 18** Способный выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов	**Тема:** NGFW. Логика работы правил файрволла. (2 ч.) **Тип урока:** обобщения и систематизации знаний и способов деятельности. Концерт **Воспитательная задача:** - формирование уважения к своей будущей профессии - формирование культуры потребления информации, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве - формирование представления о возможности карьерного роста при условии непрерывного образования	Просмотр ролика, посвящённого истории появления файрволла. Блиц опрос. Проверка усвоенном материала в формате шарад.	День Файрволла Праздник, посвященный истории появления файрволла. Углубление знаний о своей профессии. Навыки работы с информацией.	- эмоциональное отношение к своей будущей профессии - уровень мотивации проявления стремления работать по своей специальности - навыки анализа и интерпретации информации из различных источников - демонстрация личностного интереса к профессиональному росту