



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

Система менеджмента качества обучения

ПРИНЯТО

решением Ученого совета РТУ МИРЭА
от 28 августа 2019 г.
протокол № 1

УТВЕРЖДАЮ
Ректор РТУ МИРЭА

_____ С.А. Кудж
«__» _____ 2019 г.

**Дополнительная профессиональная программа
повышения квалификации
«Преподавание основ сетевой безопасности в ИТ-классах»**

СМК МИРЭА 8.5.1/03.Пр.130-19



Москва 2020

Раздел 1. «Характеристика программы»

1.1. Цель реализации Программы

Совершенствование профессиональных компетенций обучающихся в области преподавания основ сетевой безопасности в ИТ-классах.

Совершенствуемые компетенции

	Компетенция	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
	Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК – 8

1.2. Планируемые результаты обучения

№	Уметь – знать	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
1.	Уметь: Шифровать информацию методами симметричного и асимметричного шифрования Знать: Основные методы шифрования	ОПК – 8
2.	Уметь: Идентифицировать сетевые угрозы на основе данных мониторинга сети Знать: Принципы построения и функционирования локальных и глобальных компьютерных сетей и их компонентов Виды и признаки сетевых атак. Принципы построения систем защиты информации; Принципы функционирования систем мониторинга сети	
3.	Уметь: Устанавливать аппаратно-программные средства сетевой защиты Знать: 1. Принципы построения систем сетевой защиты;	
4.	Уметь: Проектировать учебные занятия, ориентированные	

№	Уметь – знать	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
	на обучение школьников ИТ- классов основам сетевой безопасности. Знать: Особенности обучения школьников основам сетевой безопасности. Стратегию проектирования учебных занятий, ориентированных на обучение школьников ИТ-классов основам сетевой безопасности.	

3. Категория обучающихся: уровень образования – высшее образование, область профессиональной деятельности – обучение информатике учащихся ИТ-классов в общеобразовательной организации

1.4. Форма обучения: очная с применением ДОТ

1.5. Режим занятий: по согласованию с обучающимися

1.6 Трудоемкость программы: 18 часов, 2 недели.

Раздел 2. «Содержание программы»

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Аудиторные учебные занятия, учебные работы			Формы контроля	Трудоемкость
		Всего ауд., час	Лекции	Практические занятия		
1.	Основные понятия и принципы информационной безопасности	3	2	1		3
2.	Сетевая безопасность	13	8	5		13
3.	Обучение школьников ИТ-классов сетевой безопасности-	2	1	1		2
	Итоговая аттестация					
	Итого:	18	11	7		18

2.2. Учебная программа

№ п/п	Виды учебных занятий, учебных работ	Содержание
Тема 1. Основные понятия и принципы информационной	<i>Лекция, 1 час</i>	Основные понятия и принципы информационной безопасности 1. Принципы обеспечения безопасности информации.

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 3 из 11
-------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------

№ п/п	Виды учебных занятий, учебных работ	Содержание
безопасности		2. Уровни защиты информации. 3. Ключевые термины и определения 4. Идентификация, аутентификация, авторизация 5. Модели информационной безопасности 6. Триада «Конфиденциальность, доступность, целостность». 7. Модель злоумышленника. 8. Способы представления информации.
	<i>Лекция, 1 час</i>	Основы криптографии 1. Основные методы кодирования и декодирования. 2. Основные методы шифрования. 3. Алгоритмы симметричного шифрования 4. Алгоритмы асимметричного шифрования
	<i>Практическое занятие, 1 час.</i>	Практическая работа №1 Работа в группах, индивидуально Задание: Зашифровать сообщение 1. Зашифровать сообщение используя алгоритм симметричного шифрования 2. Зашифровать сообщение используя алгоритм асимметричного шифрования. 3. Проанализировать надежность алгоритмов.
Тема 2. Сетевая безопасность	<i>Лекция, 2 часа</i>	Принципы построения и функционирования локальных и глобальных компьютерных сетей и их компонентов 1. Архитектура компьютерных сетей. 2. стек протоколов TCP/IP и модель OSI/ISO. 3. Основные сетевые протоколы.
	<i>Лекция, 1 час.</i>	Принципы построения и функционирования локальных и глобальных компьютерных сетей. Канальный уровень модели OSI 1. Стандарты IEEE 2. Управление логическим каналом. 3. Управление доступом к передающей среде 4. Функция VLAN
	<i>Лекция, 1 час.</i>	Виды и признаки сетевых атак. Сетевые атаки Broadcast Storm, ARP-Spoofing 1. Виды и признаки сетевых атак.

№ п/п	Виды учебных занятий, учебных работ	Содержание
		2. Сетевые петли. 3. Протоколы STP. 4. Протоколы RSTP, MSTP 5. Атака MITM. 6. Протокол ARP. 7. Работа с утилитой Ettercap 8. Алгоритмы идентификации сетевых угроз на основе данных мониторинга сети.
	<i>Практическое занятие, 1 час.</i>	Практическая работа № 2 Работа в группах, индивидуально Идентифицировать сетевые атаки Задание: 1. Установить утилиту Ettercap 2. Собрать сведения сетевого трафика. 3. Реализовать алгоритм идентификации атаки Storm с использованием утилиты Ettercap Реализовать алгоритм идентификации атаки ARP-Spoofing с использованием утилиты Ettercap
	<i>Лекция, 1 час</i>	Сетевой уровень модели OSI, IP-адресация 1. Общее представление о работе сетей на уровне L3. 2. Статическая маршрутизация. 3. Формат IP-адреса. 4. Заголовок IP-пакета. 5. Заголовки UDP и TCP-сегментов. 6. Протокол ICMP. 7. Утилита ping. 8. Утилита traceroute
	<i>Практическое занятие, 1 час.</i>	Практическая работа № 3 Работа в группах, индивидуально Задание: Определить характеристики процесса передачи данных по сети 1. Реализовать алгоритм расчёта ip-адреса 2. Реализовать алгоритм работы с утилитой ping 3. Реализовать алгоритм работы с утилитой traceroute.
	<i>Лекция, 1 час.</i>	Сканирование и анализ сети на наличие уязвимых узлов 1. Сбор информации о сети. 2. Анализ трафика с помощью Wireshark. 3. Сканирование и зондирование.

№ п/п	Виды учебных занятий, учебных работ	Содержание
		4. Обнаружение потенциальных уязвимостей. 5. Проверка заголовков. 6. Активные зондирующие проверки. 7. Имитация атак.
	<i>Практическое занятие, 1 час.</i>	Практическая работа №4 Работа в группах, индивидуально Задание: Реализовать алгоритмы мониторинга сети <ol style="list-style-type: none"> 1. Установить и настроить программу Wireshark 2. Реализовать алгоритмы мониторинга сетевого трафика с помощью Wireshark: <ul style="list-style-type: none"> № 1 Захвата пакетов в реальном времени из проводного или любого другого типа сетевых интерфейсов; № 2 Настройки фильтров; №3 Захвата трафика; № 4 Отображения времени отправки и получения пакетов.
	<i>Лекция, 1 час</i>	Принципы построения систем сетевой защиты. Межсетевые экраны <ol style="list-style-type: none"> 1. Технологии межсетевых экранов. 2. Стек протоколов. 3. Классификация межсетевых экранов
	<i>Практическое занятие, 1 час.</i>	Практическая работа № 5 Работа в группах, индивидуально Задание: Установить средства сетевой защиты <ol style="list-style-type: none"> 1. Установить утилиту командной строки iptables 2. Установить утилиту управления политиками безопасности межсетевого экрана ufw 3. Настроить межсетевой экран
	<i>Лекция, 1 час. .</i>	Принципы построения систем сетевой защиты. Системы обнаружения и предотвращения проникновений <ol style="list-style-type: none"> 1. Сравнение СОВ и межсетевого экрана. 2. Пассивные и активные системы обнаружения вторжений. 3. Обнаружение атаки, основанное на сигнатурах. 4. Обнаружение атаки по аномальному поведению. 5. Функции и типовые алгоритмы использования SIEM-системы
	<i>Практическое занятие, 1 час.</i>	Практическая работа № 6 Работа в группах, индивидуально

№ п/п	Виды учебных занятий, учебных работ	Содержание
		Задание: Обнаружение вторжений средствами IDS/IPS системы Suricata. Реализовать алгоритмы обнаружения вторжения используя средства IDS/IPS системы Suricata
Тема 3 Обучение школьников основам сетевой безопасности	<i>Лекция, 1 час.</i>	Особенности обучения школьников методам сетевой безопасности. Стратегия проектирования учебных занятий, ориентированных на обучение школьников сетевой безопасности.
	<i>Практическое занятие, 1 час.</i>	Практическая работа № 7 Разработать проект учебного занятия, ориентированного на обучение школьников ИТ- классов сетевой безопасности. (тема по выбору обучающегося)
Итоговая аттестация		Зачет на основании совокупности выполненных работ.

Раздел 3. «Формы аттестации и оценочные материалы»

3.1. Текущий контроль

Практическая работа №1

Зашифровать сообщение используя алгоритмы симметричного (1) и асимметричного (2) шифрования.

Действия:

1. Зашифровать сообщение алгоритмом симметричного шифрования.
2. Зашифровать сообщение алгоритмом асимметричного шифрования.
3. Проанализировать надежность алгоритмов по критерию устойчивости

Требования к работе: работа осуществляется на основании указанных алгоритмов.

Критерии оценивания:

1. Все шаги алгоритма выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 2

Идентифицировать вид атаки Storm, ARP-Spoofing используя утилиту Ettercap

Действия:

1. Установить утилиту Ettercap
2. Собрать сведения сетевого трафика.
3. Реализовать алгоритм идентификации атаки Storm с использованием

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 7 из 11
-------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------

- утилиты Ettercap
4. Реализовать алгоритм идентификации атаки ARP-Spoofing с использованием утилиты Ettercap.

Требования к работе: работа осуществляется на основании выбранных алгоритмов

Критерии оценивания:

1. Все действия выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 3

Определить характеристики процесса передачи данных по сети

Действия:

1. Реализовать алгоритм расчёта ip-адреса
2. Реализовать алгоритм работы с утилитой ping
3. Реализовать алгоритм работы с утилитой traceroute.

Требования к работе: работа осуществляется на основании указанных алгоритмов.

Критерии оценивания:

1. Все действия выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 4

Реализовать алгоритмы мониторинга сети

Действия:

1. Установить и настроить программу Wireshark
2. Реализовать алгоритмы мониторинга сетевого трафика с помощью Wireshark:
 - № 1 Захвата пакетов в реальном времени из проводного или любого другого типа сетевых интерфейсов;
 - № 2 Настройки фильтров;
 - №3 Захвата трафика;
 - № 4 Отображения времени отправки и получения пакетов.

Требования к работе: работа осуществляется на основании заданного алгоритма действий

Критерии оценивания:

1. Все действия выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 5

Установить средства сетевой защиты

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 8 из 11
----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------

Действия:

1. Установить утилиту командной строки iptables
2. Установить утилиту управления политиками безопасности межсетевого экрана ufw
3. Настроить межсетевой экран

Требования к работе: работа осуществляется на основании указанных алгоритмов.

Критерии оценивания:

1. Все действия выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 6

Обнаружение вторжений средствами IDS/IPS системы Suricata

Действия:

1. Установить систему Suricata
2. Реализовать алгоритмы обнаружения вторжения используя средства IDS/IPS системы Suricata

Требования к работе: работа осуществляется на основании заданного алгоритма действий

Критерии оценивания:

1. Все действия выполнены правильно в полном объеме.

Оценивание: зачет/незачет.

Практическая работа № 7

Разработать проект учебного занятия, ориентированного на обучение школьников ИТ- классов сетевой безопасности. (тема по выбору обучающегося).

Требования к работе: работа осуществляется на основании стратегии проектирования учебных занятий, ориентированных на обучение школьников сетевой безопасности.

Критерии оценивания:

1. Все шаги стратегии выполнены правильно в полном объеме.
2. Содержание соответствует возрастным особенностям учащихся.
3. Достижение поставленных целей учебного занятия обеспечено системой заданий, ориентированных на усвоение соответствующих знаний и умений.
4. Запланирована возможность рефлексии относительно поставленных целей.

Оценивание: зачет/незачет

3.2. Итоговая аттестация: зачет на основании совокупности выполненных

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 9 из 11
----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	--------------

работ.

Раздел 4. «Организационно-педагогические условия реализации программы»

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Литература

1. Вычислительные машины, сети и системы телекоммуникаций, Усачев Ю.Е., Чигирёва И.В., ПензГТУ (Пензенский государственный технологический университет), 2014, с. 307
http://e.lanbook.com/books/element.php?pl1_id=62577
2. Новиков С.Н. Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи: электронно-библиотечная система: сайт / С.Н. Новиков. — Москва: Горячая линия-Телеком, 2018. — 128 с. — ISBN 978-5-9912-0410-1 — URL: <https://e.lanbook.com/book/119836> (дата обращения: 04.07.2019). — Режим доступа: для зарегистрир. пользователей. — Текст: электронный.
3. Басыня Е.А. Системное администрирование и информационная безопасность: учебное пособие: электронно-библиотечная система: сайт / Е.А. Басыня. — Новосибирск: НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3484-0 — URL: <https://e.lanbook.com/book/118259> (дата обращения: 05.07.2019). — Режим доступа: для зарегистрир. пользователей. — Текст: электронный.

4.2. Материально-технические условия реализации программы

Техническое обеспечение:

компьютеры;
сервер виртуализации, обеспечивающий работу виртуальных машин;
высокоскоростные каналы связи в локальной вычислительной сети.

Программное обеспечение:

Microsoft Office

Операционная система Microsoft Windows

Операционная система Kali Linux

Утилита командной строки iptables

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 10 из 11
----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---------------

Утилита управления политиками безопасности межсетевого экрана ufw

Программа-анализатор трафика для компьютерных сетей Wireshark

IDS/IPS система Suricata

Перечень современных профессиональных баз данных и информационно справочных систем.

Википедия: <https://ru.wikipedia.com/>. [Дата обращения 01.09.2020]

РТУ МИРЭА Дополнительная профессиональная программа повышения квалификации	Система менеджмента качества обучения Положение СМКО МИРЭА 7.5.1/03.П.08-18	Стр. 11 из 11
----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---------------