МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

РАБОЧАЯ ПРОГРАММА
по дисциплине **«УЯЗВИМОСТЬ И БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ»**

Специальность:	10.05.05 Безопасность информационных технологий в правоохранительной сфере
Специализация:	Технологии защиты информации в правоохранительной сфере
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	Очная
Институт:	Инженерный химико-технологический институт
Факультет:	Факультет экологической, технологической и информационной безопасности
Кафедра-разработчик:	Кафедра «Информационная безопасность»
Курс; семестр	3; 5

Вид нагрузки	Часы	Зачётные единицы
Лекция	27	0,75
Практическое занятие	36	1
Контроль самостоятельной работы	27	0,75
Самостоятельная работа	27	0,75
Форма аттестации: Экзамен (5 сем)	27	0,75
Всего	144	4

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1461 от 22.11.2020) по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере для специализации «Технологии защиты информации в правоохранительной сфере» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент Л.Х. Сафиуллина

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании кафедры «Информационная безопасность», протокол от 26.05.2021 г. № 10.

Заведующий кафедрой ***Согласовано*** В.А. Богомолов

У Т В Е Р Ж Д Е Н О

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Уязвимость и безопасность вычислительных сетей» являются:

формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Уязвимость и безопасность вычислительных сетей» относится к формируемой участниками образовательных отношений части ООП и формирует у обучающихся по специализации «Технологии защиты информации в правоохранительной сфере» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Уязвимость и безопасность вычислительных сетей» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:

1. Аппаратные средства вычислительной техники
2. Средства и системы технического обеспечения обработки, хранения и передачи информации

Дисциплина «Уязвимость и безопасность вычислительных сетей» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Безопасность корпоративных информационных систем
2. Контроль безопасности в компьютерных сетях

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ПК -2 Способен обеспечить безопасность компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

ПК -2.1. Знает принципы построения компьютерных сетей, порядок реализации методов и средств межсетевого экранирования, источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению, принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

ПК -2.2. Умеет оценивать угрозы безопасности информации в компьютерных сетях, настраивать правила фильтрации пакетов в компьютерных сетях, оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях, обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях

ПК -2.3. Владеет навыками применения программно-аппаратных средств защиты информации в компьютерных сетях и управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях

В результате освоения дисциплины обучающийся должен

Знать:

принципы функционирования и создания безопасных компьютерных сетей.

Уметь:

оценивать уязвимости и угрозы информации в компьютерных сетях;

проектировать системы безопасности в компьютерных системах и сетях.

Владеть:

навыками применения средств безопасности компьютерных систем и сетей.

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Безопасность компьютерных сетей	5	9	18		11	15	Практические занятия; Экзамен
2.	Защита от сетевых атак. Контроль трафика	5	8	8		8	4	
3.	Средства и методы защиты информации в компьютерных сетях	5	8	6		4	6	
4.	Защита информации в виртуальных частных сетях (VPN)	5	2	4		4	2	
	Итого по семестру	**5**	**27**	**36**		**27**	**27**	**Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Безопасность компьютерных сетей	2	Компьютерные сети как объект защиты. Подходы к обеспечению информационной безопасности компьютерных сетей	ПК -2.1
2.		2	Уязвимость информации, обрабатываемой в компьютерных сетях	ПК -2.1
3.		2	Нормативно-правовые основы обеспечения защиты информации в компьютерных сетях	ПК -2.1
4.		3	Разработка регламентов информационной безопасности компьютерных сетей предприятия	ПК -2.1
5.	Защита от сетевых атак. Контроль трафика	2	Основы захвата и анализа сетевого трафика	ПК -2.1
6.		2	Выявление сетевых атак путем анализа трафика	ПК -2.1
7.		4	Системы обнаружения атак. Сетевые решения	ПК -2.1
8.	Средства и методы защиты информации в компьютерных сетях	2	Идентификация в компьютерных сетях	ПК -2.1
9.		2	Антивирусная защита компьютерных сетей	ПК -2.1

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
10.		2	Криптографические методы защиты информации в сетях	ПК -2.1
11.		1	Защита компьютерной сети с использованием межсетевых экранов	ПК -2.1
12.		1	Протоколирование и аудит в компьютерных сетях	ПК -2.1
13.	Защита информации в виртуальных частных сетях (VPN)	1	Технология виртуальных частных сетей (VPN)	ПК -2.1
14.		1	Организация защиты виртуальных частных сетей (VPN)	ПК -2.1
	ВСЕГО	**27**		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Безопасность компьютерных сетей	2	Изучение интерфейса программы анализатора «Ethereal»	ПК -2.3
2.		2	Фильтрация пакетов и захват трафика	ПК -2.3
3.		4	Анализ протоколов Ethernet и ARP	ПК -2.2
4.		4	Анализ протоколов IP и ICMP	ПК -2.3
5.		4	Анализ протокола TCP	ПК -2.2
6.		2	Выявление сетевых атак путем анализа трафика	ПК -2.3
7.	Защита от сетевых атак. Контроль трафика	4	Выбор схемы аутентификации и настройка параметров аутентификации компьютерной сети	ПК -2.3
8.		4	Настройка политики межсетевого экранирования с использованием протокола IPSec. Разработка и реализация алгоритма анализа данных протоколирования в компьютерной сети	ПК -2.3
9.	Средства и методы защиты информации в компьютерных сетях	4	Антивирусные программные комплексы	ПК -2.2
10.		2	Анализ сетевого трафика путем TCP–сканирования	ПК -2.2
11.	Защита информации в виртуальных частных сетях (VPN)	4	Организация VPN средствами протокола PPTP	ПК -2.2
	ВСЕГО	**36**		

7. Содержание лабораторных занятий

Проведение лабораторных занятий не предусмотрено учебным планом

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Изучение интерфейса программы анализатора «Ethereal»	3	подготовка к практическому занятию	ПК -2.3
2.	Фильтрация пакетов и захват трафика	3	подготовка к практическому занятию	ПК -2.3
3.	Анализ протоколов Ethernet и ARP	3	подготовка к практическому занятию	ПК -2.2
4.	Анализ протоколов IP и ICMP	2	подготовка к практическому занятию	ПК -2.3
5.	Анализ протокола TCP	3	подготовка к практическому занятию	ПК -2.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
6.	Выявление сетевых атак путем анализа трафика	1	подготовка к практическому занятию	ПК -2.3
7.	Выбор схемы аутентификации и настройка параметров аутентификации компьютерной сети	2	подготовка к практическому занятию	ПК -2.3
8.	Настройка политики межсетевого экранирования с использованием протокола IPSec. Разработка и реализация алгоритма анализа данных протоколирования в компьютерной сети	2	подготовка к практическому занятию	ПК -2.3
9.	Антивирусные программные комплексы	3	подготовка к практическому занятию	ПК -2.2
10.	Анализ сетевого трафика путем TCP–сканирования	3	подготовка к практическому занятию	ПК -2.2
11.	Организация VPN средствами протокола PPTP	2	подготовка к практическому занятию	ПК -2.2
	ВСЕГО	**27**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Изучение интерфейса программы анализатора «Ethereal»	2	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
2.	Фильтрация пакетов и захват трафика	1	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
3.	Анализ протоколов Ethernet и ARP	2	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.2
4.	Анализ протоколов IP и ICMP	2	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
5.	Анализ протокола TCP	2	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.2
6.	Выявление сетевых атак путем анализа трафика	2	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
7.	Выбор схемы аутентификации и настройка параметров аутентификации компьютерной сети	4	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
8.	Настройка политики межсетевого экранирования с использованием протокола IPSec. Разработка и реализация алгоритма анализа данных протоколирования в компьютерной сети	4	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.3
9.	Антивирусные программные комплексы	2	проверка знаний на практическом занятии	ПК -2.2
10.	Анализ сетевого трафика путем TCP–сканирования	2	проверка знаний на практическом занятии	ПК -2.2
11.	Организация VPN средствами протокола PPTP	4	подготовка к практическому занятию, проверка знаний на практическом занятии	ПК -2.2
	ВСЕГО	**27**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Уязвимость и безопасность вычислительных сетей» используется рейтинговая система. Максимальное и

минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
5-й семестр			
Практические занятия	11	36	60
Экзамен	1	24	40
Итого		**60**	**100**

10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

11. Информационно-методическое обеспечение дисциплины

11.1. Основная литература

При изучении дисциплины «Уязвимость и безопасность вычислительных сетей» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В.Ф. Шаньгин, Информационная безопасность компьютерных систем и сетей [Прочее] Учебное пособие: Москва : Издательский Дом "ФОРУМ", 2020	http://znanium.com/go.php?id=1093657 Режим доступа: по подписке КНИТУ
Г. М. Суворова, Информационная безопасность [Прочее] Учебное пособие для вузов: Москва : Юрайт, 2021	https://urait.ru/bcode/467370 Режим доступа: по подписке КНИТУ
Т. Л. Партыка, И.И. Попов, Информационная безопасность [Прочее] Среднее профессиональное образование: Москва : Издательство "ФОРУМ", 2020	http://new.znanium.com/go.php?id=1081318 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов [и др.], Информационная безопасность. Практические аспекты [Прочее] учеб. пособие для студ. вузов спец. "Информ. безопасность": СПб. : ИЦ "Интермедия", 2021	5 экз. УНИЦ ФГБОУ ВО «КНИТУ»
И. А. Малашкевич, Е. С. Кубашева, Е. Н. Чекулаева, Информатика и вычислительная техника. Информационная безопасность автоматизированных систем [Прочее] учебно-методическое пособие: Йошкар-Ола : ПГТУ, 2019	http://biblioclub.ru/index.php?page=book&id=562246 Режим доступа: по подписке КНИТУ
А. А. Петров, Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] : Саратов : Профобразование, 2019	http://www.iprbookshop.ru/87998.html Режим доступа: по подписке КНИТУ
С. П. Панасенко, К. Я. Мытник, Смарт-карты и	https://e.lanbook.com/book/116128

информационная безопасность [Электронный ресурс] : Москва : ДМК Пресс, 2018	Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Уязвимость и безопасность вычислительных сетей» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPRbooks: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

УНИЦ
Согласовано

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных

Scopus Доступ свободный: www.scopus.com
Web of Science Доступ свободный: apps.webofknowledge.com

Информационные справочные системы

Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

12. Материально-техническое обеспечение дисциплины

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Уязвимость и безопасность вычислительных сетей»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

1. Лекционные занятия:

a. комплект электронных презентаций/слайдов,
b. аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук, …)

2. Лабораторные работы

a. лаборатория кафедры «ИБ»,
b. шаблоны отчетов по лабораторным работам.

3. Прочее

a. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет,
b. рабочие места для студентов в количестве не менее 15-ти.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Уязвимость и безопасность вычислительных сетей» составляет 18 ч.

В процессе освоения дисциплины «Уязвимость и безопасность вычислительных сетей» используются следующие образовательные технологии:

• системы дистанционного обучения.