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 **«КОНТРОЛЬ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ»**

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	5; 9

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	27	0,75
Практическое занятие	9	0,25
Контроль самостоятельной работы	63	1,75
Самостоятельная работа	63	1,75
Форма аттестации: Дифференцированный зачет (9 сем)		
Всего	180	5

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	В.А. Богомолов
Старший преподаватель	В.И. Нурулин

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 «Контроль безопасности в компьютерных сетях» являются:
а) знакомство с основными понятиями в корпоративных информационных системах;
б) получение теоретических знаний по безопасности корпоративных информационных систем;
в) получение навыков защиты корпоративных информационных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Контроль безопасности в компьютерных сетях» 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 «Контроль безопасности в компьютерных сетях» обучающийся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» должен освоить материал предшествующих дисциплин:
1. Информатика
2. Средства и системы технического обеспечения обработки, хранения и передачи информации

Дисциплина «Контроль безопасности в компьютерных сетях» является предшествующей и необходима для успешного освоения последующих дисциплин:
1. Последующих дисциплин нет

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:

способы 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

Уметь:

обеспечивать безопасность компьютерных сетей

Владеть:

методиками обеспечения безопасности компьютерных сетей, в том числе с использованием программно-аппаратных средств защиты информации, обосновать и проконтролировать результаты управленческих решений в области безопасности информации автоматизированных систем

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ 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.	Защита корпоративных сетей.	9	8	5	19	57	57	Лабораторная работа; Практические занятия
2.	Защита корпоративных информационных систем.	9	10	4	8	6	6	
	Итого по семестру	**9**	**18**	**9**	**27**	**63**	**63**	**Дифференцированный зачет**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Защита корпоративных сетей.	2	Мэжсетевые экраны. NAT.	ПК -2.1 ПК -2.2 ПК -2.3
2.		2	Мэжсетевые экраны.Proxy.	ПК -2.1 ПК -2.2 ПК -2.3
3.		2	Мэжсетевые экраны.Фильтры.	ПК -2.1 ПК -2.2 ПК -2.3
4.		2	Мэжсетевые экраны. VPN.	ПК -2.1 ПК -2.2 ПК -2.3
5.	Защита корпоративных информационных систем.	2	Управление доступом.	ПК -2.1 ПК -2.2 ПК -2.3
6.		2	Резервирование.	ПК -2.1 ПК -2.2 ПК -2.3
7.		6	Распределенные информационные системы.	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Защита корпоративных сетей.	5	NAT	ПК -2.1 ПК -2.2 ПК -2.3

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
2.	Защита корпоративных информационных систем.	4	Управление доступом	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**9**		

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Защита корпоративных сетей.	12	NAT	ПК -2.1 ПК -2.2 ПК -2.3
2.		3	Proxy	ПК -2.1 ПК -2.2 ПК -2.3
3.		2	Фильтры	ПК -2.1 ПК -2.2 ПК -2.3
4.		2	VPN	ПК -2.1 ПК -2.2 ПК -2.3
5.	Защита корпоративных информационных систем.	6	Управление доступом	ПК -2.1 ПК -2.2 ПК -2.3
6.		2	Распределенные системы	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**27**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Мэжсетевые экраны. NAT.	2	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
2.	Мэжсетевые экраны.Proxy.	10	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
3.	Мэжсетевые экраны. Фильтры.	12	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
4.	Мэжсетевые экраны. VPN.	33	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
5.	Управление доступом.	2	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
6.	Резервирование.	2	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3
7.	Распределенные системы.	2	подготовка к лабораторной работе, подготовка к практическому занятию	ПК -2.1 ПК -2.2 ПК -2.3

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
	ВСЕГО	**63**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Мэжсетевые экраны. NAT.	4	практические занятия, прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
2.	Мэжсетевые экраны. Proxy.	4	практические занятия, прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
3.	Мэжсетевые экраны. Фильтры.	17	практические занятия, прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
4.	Мэжсетевые экраны. VPN.	32	практические занятия, прием лабораторной работы	ПК -2.1 ПК -2.2 ПК -2.3
5.	Управление доступом.	2	прием лабораторной работы, проверка знаний на практическом занятии	ПК -2.1 ПК -2.2 ПК -2.3
6.	Резервирование.	2	прием лабораторной работы, проверка знаний на практическом занятии	ПК -2.1 ПК -2.2 ПК -2.3
7.	Распределенные информационные системы.	2	прием лабораторной работы, проверка знаний на практическом занятии	ПК -2.1 ПК -2.2 ПК -2.3
	ВСЕГО	**63**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Контроль безопасности в компьютерных сетях» 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
9-й семестр			
Лабораторная работа	7	50	80
Практические занятия	2	10	20
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 «Контроль безопасности в компьютерных сетях» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
С. В. Родин, Г. В. Перминов, А. В. Скрыпников [и др.], Безопасность систем баз данных [Электронный ресурс] Учебное пособие: Воронеж : Воронежский государственный университет инженерных технологий, 2015	http://www.iprbookshop.ru/50628.html Режим доступа: по подписке КНИТУ
В. А. Астапчук, П. В. Терещенко, Корпоративные информационные системы: требования при проектировании [Прочее] Учебное пособие для вузов: Москва : Юрайт, 2020	https://urait.ru/bcode/453261 Режим доступа: по подписке КНИТУ
А. В. Курбесов, Корпоративные информационные системы [Прочее] учебное пособие: Ростов-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2018	http://biblioclub.ru/index.php?page=book&id=567042 Режим доступа: по подписке КНИТУ
А. Ю. Никитаева, Корпоративные информационные системы [Прочее] Учебное пособие: Таганрог : Издательство ТТИ ЮФУ, 2017	http://znanium.com/go.php?id=996036 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
В. Кияев, О. Граничин, Безопасность информационных систем [Прочее] курс: Москва : Национальный Открытый Университет «ИНТУИТ», 2016	http://biblioclub.ru/index.php?page=book&id=429032 Режим доступа: по подписке КНИТУ
А. В. Никулин,, В. В. Артюшенко,, Компьютерные сети и телекоммуникации [Прочее] учебно-методическое пособие по русскому языку как иностранному: Новосибирск : Новосибирский государственный технический университет, 2020	http://www.iprbookshop.ru/99345.html Режим доступа: по подписке КНИТУ
В. В. Артюшенко,, А. В. Никулин,, Компьютерные сети и телекоммуникации [Прочее] учебно-методическое пособие по русскому языку как иностранному: Новосибирск : Новосибирский государственный технический университет, 2020	http://www.iprbookshop.ru/99345.html Режим доступа: по подписке КНИТУ
А. В. Кузин, Д.А. Кузин, Компьютерные сети [Прочее] Учебное пособие: Москва : Издательство "ФОРУМ", 2020	http://znanium.com/go.php?id=1088380 Режим доступа: по подписке КНИТУ
М. В. Дибров, Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 [Прочее] Учебник и практикум Для СПО: Москва : Юрайт, 2020	https://urait.ru/bcode/452574 Режим доступа: по подписке КНИТУ
М. В. Дибров, Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 [Прочее] Учебник и практикум Для СПО: Москва : Юрайт, 2020	https://urait.ru/bcode/453065 Режим доступа: по подписке КНИТУ
Ибе Оливер, Компьютерные сети и службы удаленного доступа [Электронный ресурс] :	http://www.iprbookshop.ru/87999.html Режим доступа: по подписке КНИТУ

Саратов : Профобразование, 2019	

11.3. Электронные источники информации

При изучении дисциплины «Контроль безопасности в компьютерных сетях» 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 «Контроль безопасности в компьютерных сетях»:

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. Виртуальные машины VirtualBOX (GNU GENERAL PUBLIC LICENSE)
2. Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
3. Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
4. RADIUS сервер (GNU GENERAL PUBLIC LICENSE)
5. Sendmail - SMTP сервер (Sendmail License)
6. POP3 сервер (BSD License)
7. IMAP4 сервер (BSD License)
8. NTP сервер (BSD License)
9. Межсетевой экран iptables (GNU GENERAL PUBLIC LICENSE)
10. Межсетевой экран Firewalld (GNU GENERAL PUBLIC LICENSE)
11. Сканер сетевой безопасности nmap (GNU GENERAL PUBLIC LICENSE)
12. Система обнаружения атак snort (GNU GENERAL PUBLIC LICENSE)
13. Система синхронизации данных rsync

Учебные аудитории для проведения учебных занятий оснащены оборудованием:
1. Аудитория П-7;
техническими средствами обучения:
1. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .

Помещения для самостоятельной работы оснащены компьютерной техникой:
1. Аудитория И1-107,
с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

В процессе освоения дисциплины «Контроль безопасности в компьютерных сетях» используются следующие образовательные технологии:
• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• системы дистанционного обучения.