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 **«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»**

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Институт:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Факультет:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Кафедра-разработчик:	Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет"
Курс; семестр	3; 5

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	18	0,5
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	63	1,75
Форма аттестации: Экзамен (5 сем)	27	0,75
Всего	180	5

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.Ю. Сенцова

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

У Т В Е Р Ж Д Е Н О

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

1. Цели освоения дисциплины

Целями освоения дисциплины «Программно-аппаратные средства защиты информации» являются:

а) знакомство студентов с современными средствами защиты информации компьютерных систем,

б) овладение методами решения задач защиты информации от несанкционированного доступа с применением программно-аппаратных средств защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Программно-аппаратные средства защиты информации» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Дискретная математика
2. Технологии программирования
3. Электротехника и электроника
4. Языки программирования

Дисциплина «Программно-аппаратные средства защиты информации» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Аппаратные средства телекоммуникационных систем
2. Защита информационных процессов в телекоммуникациях
3. Комплексная система защиты информации
4. Организация и управление службой защиты информации
5. Работа с конфиденциальной информацией

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;

ОПК-9.1. Знает современные достижения науки и техники в области защиты информации, современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты, системный подход к выполнению и организации

ОПК-9.2. Умеет проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ОПК-9.3. Владеет навыками эффективного применения средств криптографической защиты информации, средств технической защиты информации, сетей и систем передачи информации при решении задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен

Знать:

теории информационной безопасности, классификацию и основное содержание нормативных документов в данной области.

Уметь:

выполнять работы по установке, настройке, эксплуатации и обслуживанию программных, программно аппаратных (в том числе крипто- графических) и технических средств и систем защиты информации, проводит контрольные проверки работоспособности применяемых средств

защиты информации

выбирать режимы работы программно-аппаратных средств криптографической и технической защиты информации в операционных системах, настраивает правила фильтрации пакетов в компьютерных сетях

Владеть:

навыками работы с антивирусными пакетами, настройки параметров информационной безопасности в приложениях – браузерах сети Internet

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.	Политика безопасности компьютерных систем. Аудит комплексной системы безопасности	5	2		4	9	12	Лабораторная работа; Реферат; Экзамен
2.	Подсистемы защиты современных операционных систем	5	2		2	9	8	
3.	Программно-аппаратные методы защиты информации	5	2		2	9	12	
4.	Идентификация пользователей компьютерных систем	5	4		4	9	10	
5.	Средства и методы ограничения доступа к файлам и компонентам ЭВМ	5	4		2	9	9	
6.	Вирусы и антивирусные программы	5	4		4	9	12	
	Итого по семестру	**5**	**18**		**18**	**54**	**63**	**Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Политика безопасности компьютерных систем. Аудит комплексной системы безопасности	2	Основные понятия программно–аппаратной защиты информации	ОПК-9.1 ОПК-9.2 ОПК-9.3

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
2.	Подсистемы защиты современных операционных систем	2	Подсистемы защиты операционной системы Windows	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	Программно-аппаратные методы защиты информации	2	Содержание программно-аппаратных методов защиты информации	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	Идентификация пользователей компьютерных систем	4	Идентификация пользователей компьютерных систем – субъектов доступа к данным	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Средства и методы ограничения доступа к файлам и компонентам ЭВМ	2	Методы и средства ограничения доступа к компонентам ЭВМ	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.		2	Защита программ от несанкционированного копирования и исследования	ОПК-9.1 ОПК-9.2 ОПК-9.3
7.	Вирусы и антивирусные программы	2	Вредоносное ПО	ОПК-9.1 ОПК-9.2 ОПК-9.3
8.		2	Методы защиты от вредоносного ПО	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Политика безопасности компьютерных систем. Аудит комплексной системы безопасности	4	Безопасность локальной сети компании	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.	Подсистемы защиты современных операционных систем	2	Межсетевые экраны	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	Программно-аппаратные методы защиты информации	2	SIEM	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	Идентификация пользователей компьютерных систем	4	ПАК "Соболь" и "Secret Net"	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Средства и методы ограничения доступа к файлам и компонентам ЭВМ	2	Настройка доменной среды Windows/расширенное логирование системы	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.	Вирусы и антивирусные программы	4	Тестирование безопасности веб-приложений с Web Security DoJo	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**18**		

8. Самостоятельная работа

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

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Безопасность локальной сети компании	12	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.	Межсетевые экраны	8	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	SIEM	12	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	ПАК "Соболь" и "Secret Net"	10	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Настройка доменной среды Windows/расширенное логирование системы	9	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.	Тестирование безопасности веб-приложений с Web Security DoJo	12	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-9.1 ОПК-9.2 ОПК-9.3
	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.	Безопасность локальной сети компании	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
2.	Межсетевые экраны	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
3.	SIEM	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
4.	ПАК "Соболь" и "Secret Net"	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
5.	Настройка доменной среды Windows/расширенное логирование системы	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
6.	Тестирование безопасности веб-приложений с Web Security DoJo	9	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-9.1 ОПК-9.2 ОПК-9.3
	ВСЕГО	**54**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Программно-аппаратные средства защиты информации» 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			
Лабораторная работа	6	30	48
Реферат	1	6	12

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 «Программно-аппаратные средства защиты информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
Е.К. Баранова, А.В. Бабаш, Информационная безопасность и защита информации [Прочее] Учебное пособие: Москва : Издательский Центр РИОР; Москва : ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=957144 Режим доступа: по подписке КНИТУ
Е. В. Смирнова,, А. В. Пролетарский,, И. В. Баскаков, [и др.], Построение коммутируемых компьютерных сетей [Прочее] учебное пособие: Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89464.html Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
Б. А. Фороузан,, Криптография и безопасность сетей [Прочее] учебное пособие: Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	http://www.iprbookshop.ru/102017.html Режим доступа: по подписке КНИТУ
В. К. Душин, Теоретические основы информационных процессов и систем [Прочее] учебник: Москва : Издательско-торговая корпорация «Дашков и К°», 2016	http://biblioclub.ru/index.php?page=book&id=453880 Режим доступа: по подписке КНИТУ
Н. В. Гришина, Комплексная система защиты информации на предприятии [Прочее] Учебное пособие: Москва : Издательство "ФОРУМ", 2009	http://znanium.com/go.php?id=175658 Режим доступа: по подписке КНИТУ
Е. В. Парфенова, Информационные технологии [Электронный ресурс] Лабораторный практикум: Москва : Издательский Дом МИСиС, 2018	http://www.iprbookshop.ru/78565.html Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Программно-аппаратные средства защиты информации» 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 IPR SMART: 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
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

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 «Программно-аппаратные средства защиты информации»:

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

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
Аудитория 351-А;
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
14. компьютер/ноутбук
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:

Аудитория Г-407, компьютер/ноутбук 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 «Программно-аппаратные средства защиты информации» составляет 9 ч.

В процессе освоения дисциплины «Программно-аппаратные средства защиты информации» используются следующие образовательные технологии:

• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция);