МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г. Игнатова
«21» 06 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Современное шифрование информации»

Направление подготовки - 09.04.04 «Программная инженерия»
Направленность (профиль) - «Программные средства обеспечения кибербезопасности»

Москва 2020

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

ПК-2 Способен участвовать в программной реализации информационных систем и создании программного обеспечения для анализа, распознавания и обработки информации в сфере кибербезопасности
Сформулирована на основе Профессионального стандарта 06.017 - Руководитель разработки программного обеспечения
Обобщенная трудовая функция - Управление программно-техническими, технологическими и человеческими ресурсами
Трудовые функции: Управление инфраструктурой коллективной среды разработки (C/01.7), Управление процессами оценки сложности, трудоемкости, сроков выполнения работ (C/03.7)

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения компетенций/подкомпетенций**
ПК-2.СШИ Способен использовать современные методы и средства шифрования информации для решения профессиональных задач	Разработка, отладка, модификация и поддержка системного программного обеспечения	**Знания** современных методов и средств шифрования информации **Умения** применять методы, средства и алгоритмы шифрования информации **Опыт** применения средств шифрования для решения практических задач

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы, изучается на 1 курсе во 2 семестре (очная форма обучения).

Входные требования: для изучения дисциплины " Современное шифрование информации " студенты должны обладать знаниями основ программирования, умениями разработки алгоритмов, написания кодов программ, опытом разработки программ на языках высокого уровня.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа			Самостоятельная работа (часы)	Промежуточная аттестация
				Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1	2	4	144		-	32	108	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
Основы модулярной арифметики, проверка простоты и факторизация чисел	-	-	8	22	Тестирование на лекции.
Криптографические системы	-	-	8	22	Тестирование. Выполнение контрольного задания по теме изучаемого модуля. Контроль подготовки реферата по выбранной теме
Криптографические протоколы	-	-	8	22	Тестирование. Контроль подготовки и проведение доклада по выбранной теме
Атака на шифр. Имитостойкость	-	-	8	22	Тестирование Контроль подготовки реферата или доклада по выбранной теме

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

№ модуля дисциплины	№ Практического занятия	Объем занятий (часы)	Наименование занятия
1	1	2	Вводное занятие. Основные понятия. Исторический обзор. Криптография
2	2	2	Преобразования текстов. Математическое определение шифра. Примеры шифров
	3	2	Универсальные методы криптоанализа. Метод полного перебора.
	4	2	Свойства открытых текстов.
	5	2	Аналитический метод. Метод «встреча по середине».
3	6	2	Методы распределения ключей. Симметричные и асимметричные методы шифрования. Достоинство и недостатки того и другого метода.
	7	2	Реализация алгоритмов шифрования. Смесители, программные шифраторы, шифраторы самовосстановления.
	8	2	Статистические методы определения ключей. Многократное использование ключей.
	9	2	Утечка информации по побочным каналам. «Чёрные ходы» в алгоритмах и программах.
4	10	2	Защита от подмены информации. Электронная цифровая подпись.
	11	2	Защита компьютеров от вредоносных программ. Защита сетей. Некоторые возможные виды атак на порты и службы.
	12	2	Однонаправленные функции.
	13	2	Использование законов квантовой механики в криптографии. Обнаружение факта перехвата. Возможность использования квантовых вычислителей.
5	14	2	Перехват, захват сеанса и способы борьбы с ними
	15	2	Слабая и сильная идентификация пользователей
	16	2	Некоторые методы обнаружения и предупреждения хакерских атак.

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	22	Изучение теоретического материала по теме модуля, подготовка к тестированию.
2	22	Изучение теоретического материала по теме модуля, подготовка к тестированию. Подготовка реферата и доклада по выбранной теме.
3	22	Изучение теоретического материала по теме модуля, подготовка к тестированию. Подготовка реферата и доклада по выбранной теме.
4	22	Изучение теоретического материала по теме модуля, подготовка к тестированию. Подготовка реферата и доклада по выбранной теме.
5	20	Изучение теоретического материала по теме модуля, подготовка к тестированию.

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (http://orioks.miet.ru/):

Модуль 1-5

- ✓ Теоретические сведения
- ✓ Задания к рефератам и докладам
- ✓ Задания на самостоятельную работу для изучения теории в рамках подготовки к тестированию и итоговому контролю

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев; Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М. : Радио и связь, 2001. - 376 с. - ISBN 5-256-01518-4

2. Панасенко С.П. Основы криптографии для экономистов : Учеб. пособие / С.П. Панасенко, В.П. Батура; Под ред. Л.Г. Гагариной. - М. : Финансы и статистика, 2005. - 176 с. - ISBN 5-279-02938-6
3. Никифоров С.Н. Методы защиты информации. Пароли, скрытие, шифрование : Учеб. пособие для вузов / С.Н. Никифоров. - 3-е изд., стер. - СПб. : Лань, 2020. - 124 с. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-6352-7 : 182-23,
4.Бутакова Н.Г. Криптографические методы и средства защиты информации : Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6 : 834-20
5. Басалова Г.В. Основы криптографии / Г.В. Басалова. - 2-е изд. - М. : ИНТУИТ.РУ, 2016. - 282 с. - URL: https://e.lanbook.com/book/100302 (дата обращения: 08.12.2020)

Периодические издания

1. Supercomputing Frontiers And Innovations : An International Open Access Journal. / Издательский центр Южно-Уральского государственного университета. - Челябинск : ЮУрГУ, 2014 - . - URL : https://superfri.org/superfri/index (дата обращения: 19.11.2020)
2. Программные системы : теория и приложения : Электронный научный журнал / Ин-т программных систем им. А.К. Айламазяна РАН. - Переславль-Залесский, 2010 - . - URL : http://psta.psiras.ru/archives/archives.html (дата обращения: 19.11.2020)
3. Программирование / Ин-т системного программирования РАН. - М. : Наука, 1975 -. – URL: http://elibrary.ru/contents.asp?titleid=7966 (дата обращения: 19.11.2020)
4. Естественные и технические науки / Издательство "Спутник+". – М. : Спутник+, 2002 -. - URL : http://www.sputnikplus.ru/ (дата обращения: 19.11.2020)
5. Компьютер Пресс / ООО КомпьютерПресс. - М., 1989 -. - URL : **http://www.compress.ru** (дата обращения: 19.11.2020)

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. SWRIT. Профессиональная разработка технической документации: сайт. - URL: https://www.swrit.ru/gost-espd.html (дата обращения: 01.11.2020)
2. Лань : Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: https://e.lanbook.com (дата обращения: 28.10.2020). - Режим доступа: для авторизированных пользователей МИЭТ
3. eLIBRARY.RU : Научная электронная библиотека : сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru/defaultx.asp (дата обращения : 05.11.2020). - Режим доступа: для зарегистрированных пользователей
4. Единое окно доступа к информационным ресурсам: сайт /ФГАУ ГНИИ ИТТ "Информика". – Москва, 2005-2010. - URL: http://window.edu.ru/catalog/ (дата обращения: 01.11.2020)
5. Национальный открытый университет ИНТУИТ: сайт. – Москва, 2003-2021. - URL: http://www.intuit.ru/ (дата обращения: 01.11.2020). - Режим доступа: для зарегистрированных пользователей

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, сочетающее традиционные формы аудиторных занятий и взаимодействие в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС(http://orioks.miet.ru).

В ходе реализации обучения используется смешанное обучение, модель «Перевернутый класс» - учебный процесс начинается с постановки проблемного задания, для выполнения которого студент должен самостоятельно ознакомиться с материалом, размещенным в электронной среде. В аудитории проверяются и дополняются полученные знания с использованием докладов, дискуссий и обсуждений. Работа поводится по следующей схеме: СРС (онлайновая предаудиторная работа с использованием внешнего курса) - аудиторная работа (обсуждение с представлением презентаций с применением на практическом примере изученного материала) - обратная связь с обсуждением и подведением итогов.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: раздел ОРИОКС «Домашние задания», электронная почта, Skype.

В процессе обучения при проведении занятий и для самостоятельной работы используются **внутренние электронные ресурсы:** литература по тематике дисциплины.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Аудитория с комплектом мультимедийного оборудования	ОС Microsoft Windows, Microsoft Office Professional Plus, Google Chrome, Acrobat reader DC
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС	ОС Microsoft Windows, Microsoft Office Professional Plus, Google Chrome, Acrobat reader DC

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-2.СШИ «Способен использовать современные методы и средства шифрования информации для решения профессиональных задач».

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://www.orioks.miet.ru/).

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

В курсе предусмотрены практические занятия и самостоятельная работа. Теоретический материал изучается самостоятельно и затем рассматривается на занятиях с решением практических задач. Текущий контроль проводится на занятиях.

В течение семестра каждый студент готовит реферат или доклад по заданной теме. Презентация доклада проводится аудиторно с обсуждением в общей дискуссии.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется балльная накопительная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме до 70 баллов) и дифференцированный зачет (до 30 баллов). По сумме баллов выставляется итоговая оценка по предмету. Структура и график контрольных мероприятий приведены в ОРИОКС, http://orioks.miet.ru/ .

Мониторинг успеваемости студентов проводится в течение семестра трижды: по итогам 1-8 учебных недель, 9 – 12 учебных недель, 13 – 18 учебных недель.

РАЗРАБОТЧИК:

Доцент института СПИНТех, к.т.н., доцент _____ / В.Г. Дорогов/

Рабочая программа дисциплины «Современное шифрование информации» по направлению подготовки 09.04.04 «Программная инженерия», направленности (профилю) «Программные средства обеспечения кибербезопасности» разработана в институте СПИНТех и утверждена на заседании УС института 24 ноября 2020 года, протокол № 3

Директор института СПИНТех _____/ Л.Г. Гагарина /

ЛИСТ СОГЛАСОВАНИЯ

Программа согласована с Центром подготовки к аккредитации и независимой оценке качества

Начальник АНОК _____ / И.М. Никулина /

Программа согласована с библиотекой МИЭТ
Директор библиотеки _____ / Т.П. Филиппова /