ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8bea882b8d602

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_______________ А.Г. Балашов
«15» 04 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Современные методы контроля, защиты и шифрования информации»

Направление подготовки - 09.04.04 «Программная инженерия»
Направленность (профиль) - «Системное программирование и противодействие киберугрозам»

Москва 2024

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

ПК-1 «Способен осуществлять организацию и управление информационными процессами»

Сформулирована на основе Профессионального стандарта 06.017 Руководитель разработки программного обеспечения

Обобщенная трудовая функция Управление программно-техническими, технологическими и человеческими ресурсами (С)

Трудовые функции: С/01.7 Управление инфраструктурой коллективной среды разработки С/02.7 Управление рисками разработки программного обеспечения

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения компетенций/подкомпетенций**
ПК-1.СМКЗиШИ Способен использовать знания современных методов контроля защиты информации для решения профессиональных задач	Организация и управление информационными процессами	**Знания** современных методов контроля защиты информации, применяемых при организации и управлении информационными процессами **Умения** осуществлять организацию и управление информационными процессами с применением современных методов контроля защиты информации; **Опыт** организации и управления информационными процессами с применением современных методов контроля защиты информации.

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 06.028 - Системный программист

Обобщенная трудовая функция - Организация разработки системного программного обеспечения

Трудовые функции: D/01.7 Планирование разработки системного программного обеспечения, D/04.7 Контроль деятельности рабочей группы программистов по разработке системного программного обеспечения.

Подкомпетенции, формируемые в дисциплине	Задачи профессиональной деятельности	Индикаторы достижения компетенций/подкомпетенций
ПК-2.СМКЗиШИ Способен применять современные методы контроля защиты информации и подходы к программной реализации информационных систем с их применением для решения профессиональных задач	Программная реализация информационных систем и создание программного обеспечения для анализа, распознавания и обработки информации в сфере кибербезопасности	**Знания** современных методов контроля защиты информации и подходов к их программной реализации **Умения** применять методы обеспечения целостности информации **Опыт** оценки стойкости методов защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» образовательной программы.

Входные требования: сформированность компетенций, определяющих готовность использовать современные технологии объектно-ориентированного программирования, применять их в практической деятельности, применять основные концепции, принципы, теории и факты, связанные с информатикой.

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	1	4	144	-	16	32	60	Экз(36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1. Методы контроля и оценки уязвимости	-	4	-	10	Контроль выполнения и защита лабораторных работ
					Контроль выполнения и защита ДЗ 1
2. Оценка стойкости защиты	-	4	-	10	Контроль выполнения и защита лабораторных работ
					Контроль выполнения и защита ДЗ 2
3. Защита и обеспечение целостности	-	8	-	10	Контроль выполнения и защита лабораторных работ
					Контроль выполнения и защита ДЗ 3
4. Современное шифрование информации	-	-	32	30	Контроль выполнения и защита ДЗ 4

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование работы
4	1	2	Вводное занятие. Основные понятия. Исторический обзор. Криптография
	2	2	Преобразования текстов. Математическое определение шифра. Примеры шифров
	3	2	Универсальные методы криптоанализа. Метод полного перебора.
	4	2	Свойства открытых текстов.

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование работы
	5	2	Аналитический метод. Метод «встреча по середине».
	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.
	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.
	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

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование работы
1	1	4	Уязвимости WINDOWS
2	2	4	Количественная оценка стойкости парольной защиты
3	3	4	Защита целостности информации. Электронная цифровая подпись
	4	4	Защита сетей с применение межсетевых экранов

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	6	Самостоятельное изучение материалов по теме модуля. Подготовка к лабораторным работам. Оформление отчетов по лабораторным работам. Подготовка к защите результатов лабораторных работ.
	4	Выполнение ДЗ 1 «Уязвимости WINDOWS»
2	6	Самостоятельное изучение материалов по теме модуля. Подготовка к лабораторным работам. Оформление отчетов по лабораторным работам. Подготовка к защите результатов лабораторных работ.
	4	Выполнение ДЗ 2 «Пароли»
3	6	Самостоятельное изучение материалов по теме модуля. Подготовка к лабораторным работам. Оформление отчетов по лабораторным работам. Подготовка к защите результатов лабораторных работ.
	4	Выполнение ДЗ 3 «ЭЦП»
4	16	Самостоятельное изучение материалов по теме модуля.
	14	Выполнение ДЗ 3 «Метод «встреча по середине»»

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 (ОРИОКС// URL: , http://orioks.miet.ru/):

Общие документы

- ✓ Методические указания студентам по освоению дисциплины
- ✓ Список литературы

Модули 1-4:

- ✓ Теоретические сведения (материалы практических занятий)
- ✓ Методические указания по выполнению лабораторных работ
- ✓ Методические указания по выполнению домашних заданий

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. 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,.

2. Программно-аппаратные средства обеспечения информационной безопасности : Учеб, пособие / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. - М. : Горячая линияТелеком, 2018. - 248 с. - URL: https://e.lanbook.com/book/l 11053 (дата обращения: 20.07.2023). - ISBN 978-5-9912-0470-5.
3. Разработка и защита баз данных в Microsoft SQL Server 2005. - 2-е изд. - М. : ИНТУИТ, 2016. - 147 с. - URL: https://e.lanbook.com/book/l 00448 (дата обращения: 20.07.2023)
4. Скрипник Д.А. Общие вопросы технической защиты информации / Д. А. Скрипник. - 2-е изд. - М. : ИНТУИТ, 2016. - 424 с. - URL: https://e.lanbook.com/book/100275 (дата обращения: 20.07.2023). –

Периодические издания

1. 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: 20.07.2023)
2. Программирование / Ин-т системного программирования РАН. - М. : Наука, 1975 -. - URL: http://elibrarv.ru/contents.asp?titleid=7966 (дата обращения: 20.07.2023)
3. Естественные и технические науки / Издательство "Спутник+". — М. : Спутники-, 2002 -. - URL : http://www.sputnikplus.ru/ (дата обращения: 20.07.2023)

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: 20.07.2023)
2. Лань : Электронно-библиотечная система Издательства Лань. - СПб., 2011-. - URL: https://e.lanbook.com (дата обращения: 20.07.2023). - Режим доступа: для авторизированных пользователей МИЭТ
3. eLIBRARY.RU : Научная электронная библиотека : сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru/defaultx.asp (дата обращения : 20.07.2023). - 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: 20.07.2023)
5. Национальный открытый университет ИНТУИТ: сайт. - Москва, 2003-2021. - URL: http://www.intuit.ru/ (дата обращения: 20.07.2023). - 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.

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 выполнения практических заданий, 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: шаблоны и примеры оформления выполненной работы, разъясняющий суть работы видеоролик, требования к выполнению заданий и оформлению результата.

При проведении занятий и для самостоятельной работы используются внешние электронные ресурсы:

1. Защита информации. Введение в курс "Защита информации" - канал YouTube «Лекторий МФТИ» - URL: https://www.youtube.com/watch?v=oogliMO 5wo&list=PL2iwxGybEFiuQVQtrLPaH7GNB8 ak29634&ab c11аппе1=ЛекторийМФТИ (Дата обращения: 20.07.2023)

2. Лекция 13: Нормативно-правовые документы и стандарты в области защиты информации - канал YouTube «НОУ ИНТУИТ» - URL: https://www.youtube.com/watch?v=tTbGhpTsJkg&ab cЬаппе1=НОУИНТУИТ (Дата обращения: 20.07.2023)

3. Защита информации, Колыбельников А.И., Лекция 04, 26.09.20 - канал YouTube «Дистанционные занятия МФТИ» - URL: https://www.youtube.com/watch?v=5xzinS2sxw&ab c11аппе1=ДистанционныезанятияМФТИ (Дата обращения: 20.07.2023)

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий 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
Компьютерный класс	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	ОС Microsoft Windows, Microsoft Office Professional Plus, Google Chrome, Acrobat reader DC

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
Помещение для самостоятельной работы обучающихся	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду МИЭТ	ОС Microsoft Windows, Microsoft Office Professional Plus, Google Chrome, Acrobat reader DC

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

1. ФОС по подкомпетенции ПК-1.СМКЗиШИ «Способен использовать знания современных методов контроля защиты информации для решения профессиональных задач».

2. ФОС по подкомпетенции ПК-2.СМКЗиШИ «Способен применять современные методы контроля защиты информации и подходы к программной реализации информационных систем с их применением для решения профессиональных задач».

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

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

11.1. Особенности организации процесса обучения

В курсе предусмотрены практические занятия, лабораторные работы 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.

На лабораторных работах студенты закрепляют полученные знания и свои навыки, выполняя задания лабораторного практикума.

В процессе изучения курса преподавателем проводятся консультационные занятия. На консультациях студентам даются пояснения по трудноусваиваемым разделам дисциплины. Допускается задать вопрос преподавателю и по электронной почте.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-балльная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме до 80 баллов) и сдача экзамена (до 20 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.

РАЗРАБОТЧИКИ:

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

Рабочая программа дисциплины «Современные методы контроля, защиты и шифрования информации» по направлению подготовки 09.04.04 «Программная инженерия», направленности (профилю) «Системное программирование и противодействие киберугрозам» разработана в институте СПИНТех и утверждена на заседании Института 15.04 2024 года, протокол № 10

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 /