

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Беспалов Владимир Александрович
Должность: Ректор
Дата подписания: 01.09.2023 12:32:24
Уникальный программный ключ:
ef5a4fe6ed0ffdf3f1a49d6ad1b49464dc1bf7354f736d76c8f8bea882b8d602

МИНОБРАЗОВАНИЯ РОССИИ

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



УТВЕРЖДАЮ

Проректор по учебной работе

И.Г. Игнатова

«11» 06 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации»

Направление подготовки - 09.03.04 «Программная инженерия»

Направленность (профиль) - «Программные технологии распределенной обработки информации», «Инженерия программного обеспечения и компьютерных систем»,
«Программные компоненты информационных систем»

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

ОПК	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения компетенций
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		Знания основных организационных, технических и криптографических методов и средств защиты информации Умения решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Опыт применения криптографических методов и средств защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы, изучается на 4 курсе в 7 семестре (очная форма обучения).

Входные требования: сформированность компетенций, определяющих готовность использовать современные технологии объектно-ориентированного программирования, применять их в практической деятельности, применять современные информационные технологии при решении практических задач.

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)		
4	7	5	180	32	16	16	80	Экз (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1. Основные понятия в курсе «Методы и средства защиты информации»	4	-	2	10	Контрольные опросы 1-2
2. Свойства открытых текстов	4	4	2	25	Контроль выполнения заданий лабораторных работ 1-2
					Контроль выполнения практических заданий
3. Атаки на шифр	8	4	4	25	Контроль выполнения заданий лабораторных работ 3-4
					Контроль выполнения практических заданий
4. Методы распределения ключей	8	4	4	10	Контроль выполнения заданий лабораторных работ 5-6
5. Защита от подмены информации. Имитостойкость	8	4	4	10	Контроль выполнение заданий лабораторных работ 7-8 (итоговое задание)

4.1. Лекционные занятия

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

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Наименование занятия
1, 2	1, 2	4	Программирование простейших шифров
3	3, 4	4	Криптографические способы защиты информации
4	5, 6	4	Защита целостности информации. Электронная цифровая подпись
5	7, 8	4	Защита сетей с применение межсетевых экранов

4.3. Лабораторные работы

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование работы
1,2	1	4	Программирование простейших шифров
3	2	4	Криптографические способы закрытия информации
4	3	4	Защита целостности информации. Электронная цифровая подпись
5	4	4	Защита сетей с применение межсетевых экранов

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1-5	50	Самостоятельное изучение материалов по теме модуля. Подготовка к лабораторным работам. Формирование отчёта по

		лабораторным работам.
2	15	Подготовка к контрольным мероприятиям
3	15	Выполнение итогового задания

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/>):

Модули 1-5

- ✓ Теоретические сведения (лекционные материалы)
- ✓ Методические указания по выполнению практических и лабораторных работ

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 линия-Телеком, 2018. - 248 с. - URL: <https://e.lanbook.com/book/111053> (дата обращения: 12.11.2020). - 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/100448> (дата обращения: 19.11.2020)
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: 08.11.2020). -

Периодические издания

1. SUPERCOMPUTING FRONTIERS AND INNOVATIONS [Электронный ресурс] : AN INTERNATIONAL OPEN ACCESS JOURNAL. – Режим доступа: <https://superfri.org/superfri/index> (дата обращения: 19.11.2020).
2. ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ [Электронный ресурс] : Электронный научный журнал. - На сайте Общероссийского математического портала Math-Net.Ru представлены полные тексты (Пользовательское соглашение) статей журнала с 2010 г
3. ПРОГРАММИРОВАНИЕ / Ин-т системного программирования РАН. - М. : Наука, 1975 -. - Переводная версия PROGRAMMING AND COMPUTER SOFTWARE (составной журнал) <https://link.springer.com/journal/11086> (дата обращения: 19.11.2020).

4. ЕСТЕСТВЕННЫЕ И ТЕХНИЧЕСКИЕ НАУКИ [Электронный ресурс] / Издательство "Спутник+". - Сайт журнала <http://www.etn.sc-site.ru/>. Сайт издательства <http://www.sputnikplus.ru/> (дата обращения: 19.11.2020).

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. Стандарты ЕСПД // Профессиональная разработка технической документации URL: <https://www.swrit.ru/gost-esp.html> (дата обращения: 19.11.2020). ЭБС издательства Лань - <http://e.lanbook.com/>
2. Научная электронная библиотека eLIBRARY.RU URL: <http://elibrary.ru/> (дата обращения: 01.11.2020).
3. Единое окно доступа к информационным ресурсам URL: <http://window.edu.ru/catalog/> (дата обращения: 19.11.2020).
4. Национальный открытый университет ИНТУИТ URL: <http://www.intuit.ru/> (дата обращения: 19.11.2020).

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, «Расширенная виртуальная модель», которая предполагает обязательное присутствие студентов на очных учебных занятиях с последующим самостоятельным выполнением индивидуального задания в мини-группах и индивидуально. Работа поводится по следующей схеме: аудиторная работа (обсуждение с отработкой типового задания с последующим обсуждением) - СРС (онлайновая работа с использованием онлайн-ресурсов, в т.ч. для организации обратной связи с обсуждением, консультированием, рецензированием с последующей доработкой 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 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=oogljMO_5wo&list=PL2jwxGybEFiuQVQtrLPaH7GNB8ak29634&ab_channel=ЛекторийМФТИ (Дата обращения: 19.11.2020)

2. Лекция 13: Нормативно-правовые документы и стандарты в области защиты информации – канал YouTube «НОУ ИНТУИТ» - URL: https://www.youtube.com/watch?v=tGbGhpTsJkg&ab_channel=НОУИНТУИТ (Дата обращения: 19.11.2020)

3. Защита информации, Колыбельников А.И., Лекция 04, 26.09.20 – канал YouTube «Дистанционные занятия МФТИ» - URL: https://www.youtube.com/watch?v=5xzjnS2sx-w&ab_channel=ДистанционныезанятияМФТИ (Дата обращения: 19.11.2020)

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
Компьютерный класс	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, Microsoft Visual Studio
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, Microsoft Visual Studio

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

ФОС по компетенции ОПК-3 «Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности».

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

Освоение дисциплины включает лекции, практические занятия и лабораторные работы в компьютерном классе; практические задания, состоящие из задач по тематике соответствующих модулей.

Лекционные занятия проводятся в традиционной форме с использованием мультимедийных презентаций. На каждой лекции студенты должны составить краткий конспект по теме лекции. При изучении теоретических материалов необходимо обратить внимание на основные моменты и замечания.

Лабораторные работы. Перед выполнением лабораторных и контрольных работ необходимо изучить материалы лекций и рекомендуемую литературу по каждой теме. Лабораторные работы необходимо выполнять в компьютерном классе.

Предполагается последовательное выполнение лабораторных работ, поскольку каждое следующее задание основано на использовании навыков и знаний, полученных при выполнении предыдущих заданий. Результатом выполнения лабораторных работ является документ MS Office, составленный и оформленный в соответствии с требованиями, либо схема алгоритма решения поставленной задачи. Лабораторная работа выполняется по вариантам в соответствии с номером компьютера в зале ВЦ. За лабораторную работу выставляется оценка.

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 80 баллов) и сдача экзамена (до 20 баллов). По сумме баллов выставляется итоговая оценка по предмету. Структура и график контрольных мероприятий доступны в системе 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 СПИНТех, к.т.н., доцент  / В.Г. Дорогов /

Рабочая программа дисциплины «Защита информации» по направлению подготовки 09.03.04 «Программная инженерия», программам «Программные технологии распределенной обработки информации», «Инженерия программного обеспечения и компьютерных систем», «Программные компоненты информационных систем» разработана в институте СПИНТех и утверждена на заседании 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 /