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
_____ И.Г. Игнатова
«21» 06 2021 г.
М.П.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Теоретические основы кибербезопасности»

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 06.028 Системный программист

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

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

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-2.ТОКБ Способен использовать знания теоретических основ кибербезопасности для решения профессиональных задач	Программная реализация информационных систем и создание программного обеспечения для анализа, распознавания и обработки информации в сфере кибербезопасности	**Знания** теоретических основ кибербезопасности при реализации информационных систем **Умения** разрабатывать компоненты информационных систем и программное обеспечения в сфере кибербезопасности **Опыт** применения средств разработки компонентов информационных систем и программного в сфере кибербезопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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

Входные требования к дисциплине – знание основных особенностей современных программных средств, операционных систем, информационных систем и технологий,

основных принципов программирования на языке высокого уровня, умение применять современные средства и языки программирования 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	1	2	72	32	-	-	40	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
1.Введение в кибербезопасность	16	-	-	12	Контроль выполнения домашних заданий Тестирование
2. Теория и практика обеспечения информационной безопасности	16	-	-	12	Контроль выполнения домашних зданий Контрольная работа

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Понятия о видах вирусов.

	2	2	Понятие информационной безопасности. Факторы конфиденциальности, доступности, целостности, учета и неотрекаемости. Механизмы информационной безопасности. Политика. Идентификация. Аутентификация. Контроль доступа. Авторизация. Аудит и мониторинг. Реагирование на инциденты. Управление конфигурациями, пользователями, рисками. Инструментарий информационной безопасности. Обученный персонал. Нормативное обеспечение. Стратегии и модели безопасности. Криптография и стеганография. Антивирусное обеспечение, межсетевые экраны, средства обнаружения атак. Резервное копирование, дублирование (резервирование). Аварийный план
	3	2	История развития проблем защиты информации и информационной безопасности. Роль информации в современном постиндустриальном и будущем информационном обществе. Проблемы информационного взрыва. Проблемы и особенности информационного общества. Информатизация, информационные процессы и отношения. Социальные цели информатизации. Проблемы информатизации
	4	2	Роль государства в формировании информационного общества. Национальные интересы Российской Федерации в информационной сфере. Информационная безопасность в открытом демократическом обществе. Нормативное обеспечение работы службы информационной безопасности. Основные положения документа «Доктрина информационной безопасности РФ». Основные положения ФЗ РФ «Об информации, информатизации и защите информации». Основные положения ФЗ РФ «О правовой охране программ для электронных вычислительных машин и баз данных». Международные конвенции об охране авторских прав. Основные положения ФЗ РФ «Об электронной цифровой подписи». Основные положения ФЗ РФ «О государственной тайне»
	5	2	Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
2	6	2	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.
	7-8	4	Понятие защищенности информации в информационной системе. Комплексный системный подход к защите информации. Модели оценки ценности информации. Угрозы безопасности информации (нарушение секретности, конфиденциальности, целостности, доступности). Причины и источники угроз безопасности информации. Системная классификация и общий анализ угроз безопасности информации. Угрозы секретности

			(конфиденциальности) информации: разглашение, утечка, несанкционированный доступ. Возможности несанкционированного получения информации с помощью технических средств. Защита информации от утечки по техническим каналам. Противодействие несанкционированному доступу к источникам конфиденциальной информации
	9	2	Криптография. Криптоанализ. Стеганография. Тайнопись. Шифр с ключом. Методы шифрования заменой, гаммированием, вставкой, перестановкой. Обзор систем шифрования DES, ГОСТ 28147-89. Конкурс AES и его итоги. Частотный статистический анализ текста как основной метод криптоанализа. Шифры с симметричным и несимметричным ключом. Шифрование с открытым ключом. Технологии реализации неотрекаемости и электронной цифровой подписи. Символьная и цифровая стеганография. Метод Грибоедова. Симпатические чернила. Современные методы стеганографии. Практические выводы.
	10	2	Тайнопись. Шифры с ключом (симметричным и асимметричным). Шифр Цезаря — Цицерона. Шифр Массонов. Метод шифрования заменой. Компьютерная реализация шифра Цезаря — Цицерона. Шифр Ришелье. Методы шифрования заменой и гаммированием. Компьютерная реализация шифра Ришелье. Шифр с использованием обратного порядка букв. Классический шифр замены (ключ — перестановка первых цифр). Методы шифрования перестановкой и гаммированием. Компьютерная реализация классического шифра замены (ключ — перестановка первых цифр). Шифры Петра I. Комбинирование методов шифрования. Компьютерная реализация шифров Петра I. Тюремный шифр. Книжный шифр (2 вида). Методы шифрования заменой. Понятие о криптографической стойкости шифра, ключа, ее измерение, практические выводы. Русская тарабарщина. Методы шифрования вставкой пустышек. Символьный криптоанализ, частотный анализ текста, биграммы, триграммы. Понятие о совершенном шифре
	11-12	4	Цифровая криптография. Поточное и блочное шифрование. Краткая характеристика шифров DES, ГОСТ 28147-89. Конкурс AES и его результаты. Понятие о битовой криптографической стойкости шифра, ключа, ее измерение, практические выводы. Поточное цифровое шифрование. Обратимые битовые операции. Формула поточного шифрования текущего бита и ее сущность. Линейные регистры сдвига. Генераторы последовательностей наибольшей длины. Нелинейные поточные шифры. Фильтрующие, комбинационные и динамические схемы. Блочное цифровое шифрование. Основные примитивы блочного шифрования: сложение и умножение особого типа, исключающее «или», циклические сдвиги, перестановка бит, табличная подстановка. Классическая сеть Файштеля. Сеть Файштеля с 4 ветвями (типы 1, 2,

			3). Слои, циклы и раунды
	13-14	4	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Контрольная работа.
	15-16	4	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности

4.2. Практические занятия

Не предусмотрены

4.3. Лабораторные работы

Не предусмотрены

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	12	Изучение теоретического материала и рекомендованной литературы по темам модуля. Выполнение домашних заданий Подготовка к тестированию
2	8	Изучение теоретического материала и рекомендованной литературы по темам модуля. Выполнение домашних заданий
	4	Подготовка к контрольной работе.

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/):

Модули 1 -2

- ✓ Материалы для выполнения домашних заданий
- ✓ Теоретические материалы по темам модулей

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. 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.

2. 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: 08.12.2020). -

Периодические издания

1. Современные научные исследования и инновации: Научно-практический журнал. – М.: Международный научно-инновационный центр, 2011 - . - URL: http://web.snauka.ru/archive (дата обращения: 22.11.2020).

2. 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)

3. 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)

4. Программирование / Ин-т системного программирования РАН. - М. : Наука, 1975 -. – URL: http://elibrary.ru/contents.asp?titleid=7966 (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 «расширенная виртуальная модель», которая предполагает обязательное присутствие студентов на очных учебных занятиях с последующим самостоятельным выполнением индивидуального задания. Работа поводится по следующей схеме: аудиторная работа (семинар 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: разделы ОРИОКС «Новости», «Домашние задания»; электронная почта, социальные сети (vk.com), мессенджеры (Telegram), Zoom.

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=tTbGhpTsJkg&ab_channel=НОУИНТУИТ (Дата обращения: 28.11.2020)

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 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	ОС Microsoft Windows, Microsoft Office Professional

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	к сети «Интернет» и обеспечением доступа в ОРИОКС	Plus, Google Chrome, Acrobat reader DC, Jet Brains Pycharm, Python
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. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-2.ТОКБ «Способен использовать знания теоретических основ кибербезопасности 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 дисциплине предусмотрены следующие виды занятий: лекции и самостоятельная работа. Форма промежуточного контроля – зачет с оценкой.

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.

Защита домашних заданий происходит аудиторно. Предусмотрены консультации преподавателя.

11.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме до 50 баллов), активность в семестре (в сумме до 8 бонусных баллов) и сдача дифференцированного зачета (50 баллов).

По сумме баллов выставляется итоговая оценка по предмету. Структура и график контрольных мероприятий доступен в ОРИОКС// URL: 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:

Ассистент Института СПИНТех _____ / А.И. Капитанов /

Доцент Института СПИНТех, к.т.н. _____ / Р.А. Касимов /

Рабочая программа дисциплины «Теоретические основы кибербезопасности» 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

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества

Начальник АНОК _____/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ

Директор библиотеки _____/ Т.П.Филиппова /