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

«Защищенные информационные системы и управление информационной безопасностью»

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-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

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

Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения подкомпетенций**
ПК-1.ЗИСиУИБ Способен применять знания способов организации и управления информационными процессами в защищенных информационных системах и методов обеспечения информационной безопасности для решения профессиональных задач	Организация и управление информационными процессами	**Знания** способов организации и управления информационной безопасностью в защищенных информационных системах **Умения** осуществлять информационной безопасностью в защищенных информационных системах **Опыт** управления информационной безопасностью в защищенных информационных системах и управления информационной безопасностью

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 подкомпетенций
ПК-2.ЗИСиУИБ Способен использовать методы управления информационной безопасностью в защищенных информационных системах для решения профессиональных задач	Программная реализация информационных систем и создание программного обеспечения для анализа, распознавания и обработки информации в сфере кибербезопасности	**Знания** методов управления информационной безопасностью и в защищенных информационных системах **Умения** обоснованно выбирать методы управления информационной безопасности **Опыт** оценивать риски информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» образовательной программы, изучается на 2 курсе в 3 семестре.

Входные требования: сформированность компетенций, определяющих готовность использовать современные технологии объектно-ориентированного программирования, применять их в практической деятельности, применять основные концепции, принципы обеспечения кибербезопасности.

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)		
2	3	2	72	16	16	-	40	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции (часы)	Лабораторные работы (часы)	Практические занятия (часы)		
Введение в информационную безопасность	2	-	-	10	Контрольный опрос
Методы и системы защиты информации	6	8	-	10	Контроль выполнения заданий лабораторных работ
					Контрольная работа 1
Ограничения доступа Методы идентификации.	4	8	-	10	Контроль выполнения заданий лабораторных работ
					Контрольная работа 2
Методы и модели управления рисками информационной безопасности.	4		-	10	Контроль выполнения практического задания

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Информационные характеристики объектов защиты. Основные характеристики информационных систем, процессов. Характеристики, влияющие на информационную безопасность. Принципы обеспечения информационной безопасности объектов. Стратегии защиты информации. Факторы, влияющие на формирование стратегий защиты. Классификационная структура множества необходимых стратегий защиты. Общая характеристика основных стратегий.

			Научно-методологический базис для моделирования и исследования объектов защиты. Модели на основе нечётких множеств. Модели на основе марковских случайных процессов. Модели на основе теории игр. Модели, использующие положения нестрогой математики
2	2	2	Защита компьютеров от вредоносных программ. Защита сетей. Некоторые возможные виды атак на порты и службы Методы защиты программ от изучения и разрушающих программных воздействий. Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок; защита от разрушающих программных воздействий; изолированная программная среда
	3	2	Защита информации от несанкционированного доступа (НСД). Каналы утечки информации. Системы анализа защищённости и обнаружения вторжений. Модели и источники каналов утечки информации. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом и физическом уровне от НСД. Методы защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации. Парольные системы опознавания, их сущность, содержание. Способы повышения надежности парольных систем. Средства опознавания аппаратуры, программ, массивов данных.
2	4	2	Компьютерные вирусы как особый класс программных закладок Бинарные вирусы Windows и Linux: структура, порядок инициализации, алгоритмы поиска и заражения жертвы. Сетевые вирусы: онлайн-вирусы, почтовые вирусы, IM-вирусы. Скриптовые вирусы: макровирусы, shell-вирусы, HTML-вирусы. Комбинированные вирусы. Средства и методы маскировки вирусов и противодействия антивирусному программному обеспечению: стелс-технологии, полиморфные преобразования кода
3	5	2	Методы идентификации и проверки подлинности пользователей систем. Идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний; проблема аутентификации данных. Биометрическая идентификация иаутентификация пользователей: основные понятия и механизмы. «Fuzzy extractors». Искусственные нейронные сети в преобразователях биометрия-код. Алгоритм быстрого обучения искусственной нейронной сети. Алгоритм ускоренного тестирования нейросетевого преобразователя биометрия-код (НПБК). Алгоритм полного тестирования НПБК. Базы биометрических образов: назначение, виды, требования к

			формированию. Нейросетевой биометрический контейнер (НБК): назначение, виды. Наиболее вероятные атаки на НБК, защита от них
	6	2	Программные средства разграничения доступа. Модели разграничения доступа. Разграничение доступа по уровням, матрицам полномочий и мандатам. Способы и средства повышения надежности разграничения. Программные средства защиты: регистрации, сигнализации, реагирования
4	7	2	Методы и модели управления рисками информационной безопасности.
	8	2	Модели рисков информационной безопасности. Методы снижения рисков информационной безопасности. Модели риск-ориентированной оценки информационной безопасности бизнеса и деятельности организации

4.2. Практические занятия

Не предусмотрены

4.3. Лабораторные работы

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Наименование работы
2	1	4	Перехват, захват сеанса и способы борьбы с ними
2	2	4	Слабая и сильная идентификация пользователей
3	3	4	Освоение статического и динамического метода
3	4	4	Настройка и использование специализированного антивирусного программного обеспечения

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1-5	20	Самостоятельное изучение материалов по теме модуля.

		Подготовка к лабораторным работам. Формирование отчёта по лабораторным работам.
2	10	Подготовка к контрольным мероприятиям
3	10	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: 02.12.2020)

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: 08.12.2020). -

5. Олифер В.Г. Сетевые операционные системы [Текст] : Учебник для вузов / В.Г. Олифер, Н.А. Олифер. - 2-е изд. - СПб. : Питер, 2009. - 672 с. - (Учебник для вузов). - ISBN 978-5-91180-528-9

Периодические издания

1. Информатика и ее применение : Ежеквартальный журнал / Российская академия наук, Федеральный исследовательский центр «Информатика и управление» Российской академии наук. - М. : ТОРУС ПРЕСС, 2007 - . – URL : http://www.ipiran.ru/journal/issues/ (дата обращения: 19.11.2020)
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)
5. Естественные и технические науки / Издательство "Спутник+". – М. : Спутник+, 2002 -. - URL : http://www.sputnikplus.ru/ (дата обращения: 19.11.2020)
6. Компьютер Пресс / ООО КомпьютерПресс. - М., 1989 -. - URL : **http://www.compress.ru** (дата обращения: 19.11.2020)

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННО-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», в которой 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:** 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=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 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, AllFusion PM, AllFusion DM
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, AllFusion PM, AllFusion DM

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

1. ФОС по подкомпетенции ПК-1.ЗИСиУИБ - «Способен применять знания способов организации и управления информационными процессами в защищенных информационных системах и методов обеспечения информационной безопасности для решения профессиональных задач».

2. ФОС по подкомпетенции ПК-2.ЗИСиУИБ - «Способен использовать методы управления информационной безопасностью в защищенных информационных системах 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 дисциплине предусмотрены следующие виды занятий: лекции, лабораторные работы 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.

Лабораторные работы. Перед выполнением лабораторных работ необходимо изучить материалы лекций и рекомендуемую литературу по каждой теме. На лабораторных работах студенты закрепляют полученные знания и свои навыки, выполняя задание лабораторного практикума.

В процессе изучения курса преподавателем проводятся консультационные занятия. На консультациях студентам даются пояснения по трудноусваиваемым разделам дисциплины.

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 дифференцированного зачета (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.

РАЗРАБОТЧИК:

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

Рабочая программа дисциплины «Защищенные информационные системы и управление информационной безопасностью» по направлению подготовки 09.03.04 «Программная инженерия», направленности (профилю) «Программные средства обеспечения кибербезопасности» 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 /