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.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации»

Специальность - 40.05.01 «Правовое обеспечение национальной безопасности»
Специализация «Уголовно-правовая»

2020 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

ПК-2 Способен защищать права и свободы человека в киберпространстве **Сформулирована на основе профессионального стандарта:** 09.001 «Следователь-криминалист». **Обобщенная трудовая функция:** Организация и осуществление криминалистической деятельности, связанной с проведением следственных и иных процессуальных действий с целью предварительного расследования преступлений. **Трудовые функции:** Криминалистическое сопровождение производства предварительного расследования (производство предварительного расследования) преступлений A/01.7		
Подкомпетенции, формируемые в дисциплине	**Задачи профессиональной деятельности**	**Индикаторы достижения компетенций/подкомпетенций**
ПК-2.ЗИ - Способен применять базовые знания по обеспечению информационной безопасности при решении профессиональных задач	Защита прав и свобод человека, в том числе в киберпространстве.	**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.

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)		
3	6	4	144	32	24	8	80	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ и наименование модуля	Контактная работа			Самостоятельная работа	Формы текущего контроля
	Лекции	Практические занятия	Лабораторные занятия		
1. Методы и средства защиты информации	16	4	12	40	Контроль выполнения Лабораторных работ 1-2 и ДЗ 1-4. Контрольная работа 1
2. Криптографическая защита информации	16	4	12	40	Контроль выполнения Лабораторных работ 3-4 и ДЗ 5-8. Контрольная работа 2

4.1. Лекционные занятия

№ модуля дисциплины	№ лекции	Объем занятий (часы)	Краткое содержание
1	1	2	Вводная лекция. Основные понятия. Исторический обзор. Криптография. Имитостойкость.
1	2	2	Преобразования текстов. Математическое определение шифра.
1	3	2	Свойства открытых текстов.
1	4	2	Атаки на шифр. Стойкость шифра. Совершенно стойкие шифры по Шеннону.
1	5	2	Универсальные методы криптоанализа. Метод полного перебора.
1	6	2	Аналитический метод. Метод «встреча по середине».

1	7	2	Статистические методы определения ключей. Многократное использование ключей.
1	8	2	Методы распределения ключей. Симметричные и асимметричные методы шифрования. Достоинство и недостатки того и другого метода.
2	9	2	Реализация алгоритмов шифрования. Смесители, программные шифраторы, шифраторы самовосстановления.
2	10	2	Утечка информации по побочным каналам. «Чёрные ходы» в алгоритмах и программах.
2	11	2	Однонаправленные функции.
2	12	2	Защита от подмены информации. Электронная цифровая подпись.
2	13	2	Использование законов квантовой механики в криптографии. Обнаружение факта перехвата. Возможность использования квантовых вычислителей.
2	14	2	Слабая и сильная идентификация пользователей
2	15	2	Защита компьютеров от вредоносных программ. Защита сетей. Некоторые возможные виды атак на порты и службы.
2	16	2	Перехват, захват сеанса и способы борьбы с ними. Методы обнаружения и предупреждения хакерских атак. Заключение.

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1	2	Защита целостности информации. Электронная цифровая подпись
1	2	2	Защита сетей с применением межсетевых экранов
2	3	2	Программирование простейших шифров
2	4	2	Криптографические способы закрытия информации

4.3. Лабораторные занятия

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Краткое содержание
1	1	6	Защита целостности информации. Электронная цифровая подпись
1	2	6	Защита сетей с применением межсетевых экранов
2	3	6	Программирование простейших шифров
2	4	6	Криптографические способы закрытия информации

4.4. Самостоятельная работа студентов

№ модуля дисциплины	Объем занятий (часы)	Вид СРС
1	10	Выполнение домашнего задания ДЗ-1: Определение количества информации. Изучение рекомендованной литературы по теме «Выявление угроз несанкционированного доступа к конфиденциальной информации». Подготовка к практическому занятию №1
1	10	Подготовка к практическому занятию №2. Выполнение домашнего задания ДЗ-2: Определить мощность алфавита, с помощью которого передано сообщение, содержащее 4096 символов, если информационный объем сообщения составляет 2 Кбайт. Изучение рекомендованной литературы по теме «Управление доступом в ОС WINDOWS и LINUX».
1	10	Подготовка к выполнению лабораторного задания №1. Подготовка к практическому занятию №3. Выполнение домашнего задания ДЗ-3: Зашифровать и расшифровать сообщения шифрами замены, перестановки и их сочетанием. Изучение рекомендованной литературы по теме «Разработка политики SELinux».
1	10	Подготовка к тесту №1. Подготовка к практическому занятию №4. Выполнение домашнего задания ДЗ-4: Определить информационною энтропию.
2	10	Подготовка к выполнению лабораторного задания №2. Подготовка к тесту №2. Подготовка к практическому занятию №5. Выполнение домашнего задания ДЗ-5: Зашифровать и расшифровать сообщение с открытым /закрытым ключом. Изучение рекомендованной литературы по теме «Настройка списков доступа в вычислительных сетях».
2	10	Подготовка к тесту №3. Подготовка к выполнению лабораторного задания №3. Подготовка к практическому занятию №6. Выполнение домашнего задания ДЗ-6: подготовка перечня производителей межсетевых экранов и их продуктов с их отличительными особенностями. Изучение рекомендованной литературы по теме «Межсетевое экранирование».
2	10	Подготовка к практическому занятию №7. Выполнение домашнего задания ДЗ-7: подготовка презентации на тему «Архитектура и реализация DMZ сегмента сети». Изучение рекомендованной литературы по теме «Построение DMZ сегмента сети».
2	10	Подготовка к выполнению лабораторного задания №4. Подготовка к БДЗ №1 на тему «Программирование простейших шифров.

		Электронная подпись»: Подготовка к практическому занятию №8. Выполнение домашнего задания ДЗ-8: подготовка перечня актуальных VPN-сервисов с их отличительными особенностями. Изучение рекомендованной литературы по теме «Исследование технологии VPN». Подготовка к контрольной работе №1

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-espd.html (дата обращения: 19.11.2020).
2. ЭБС издательства Лань - http://e.lanbook.com/ (дата обращения: 19.11.2020).
3. Научная электронная библиотека eLIBRARY.RU URL: http://elibrary.ru/ (дата обращения: 01.11.2020).
4. Единое окно доступа к информационным ресурсам URL: http://window.edu.ru/catalog/ (дата обращения: 19.11.2020).
5. 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=tTbGhpTsJkg&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
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.ЗИ - Способен применять базовые знания по обеспечению информационной безопасности при решении профессиональных задач

Фонд оценочных средств представлен отдельным документом и размещен 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

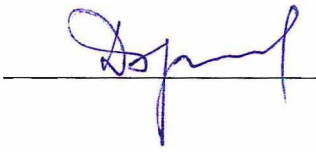
Для оценки успеваемости студентов по дисциплине используется накопительная балльная система.

Баллами оцениваются: выполнение каждого контрольного мероприятия в семестре (в сумме до 70 баллов) и сдача дифференцированного зачёта (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.



/Дорогов В.Г./

Рабочая программа дисциплины «Защита информации» по специальности 40.05.01 «Правовое обеспечение национальной безопасности» специализации «Уголовно-правовая» разработана СПИНТех и утверждена на заседании УС Института 24.11 202 0 года, протокол № 3.

Директор института СПИНТех,
д.т.н., профессор

_____/Л.Г. Гагарина/

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с кафедрой Права.

Заведующий кафедрой

_____/Л.В. Бертовский/

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

Начальник АНОК _____/Никулина И.М./

Рабочая программа согласована с библиотекой МИЭТ

Директор библиотеки _____/Филиппова Т.П./