МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Юридический институт
Кафедра информационного права и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы обеспечения информационной безопасности

Кафедра информационного права и информатики юридического института

Образовательная программа

40.05.02 Правоохранительная деятельность

Направление(профиль) подготовки:

Оперативно-розыскная деятельность

Уровень высшего образования
специалитет

Форма обучения
дистанционная

Статус дисциплины: **входит в обязательную часть ОПОП(дисциплина по выбору)**

Дисциплина «Основы обеспечения информационной безопасности» рекомендована в 2021 году в соответствии с требованиями ФГОС ВО – специалитет по специальности 40.05.02 Правоохранительная деятельность от 28 августа 2020 года №1131.

Разработчик(и): московский государственный технический университет имени Н.Э. Баумана (Основы обеспечения информационной безопасности | Открытый МГТУ (bmstu.ru))

Дисциплина одобрена:

на заседании кафедры информационного права и информатики

от «28» 05 2021г., протокол № 10

Зав. кафедрой _____ Абдусаламов Р.А.

На заседании методической комиссии юридического института

От «29» 06 2021 г., протокол № 10.

Председатель _____ Арсланбекова А.З.

Согласовано:

С учебно-методическим управлением «09» 07 2021г.

Начальник УМУ _____ Гасангаджиева А.Г.

О курсе

Курс включает в себя разделы по теоретическому и практическому изучению основ информационной безопасности. Курс рассчитан на 17 недель. Общий объем дисциплины составляет 2 зачетные единицы (з.е.), 72 часа.

Предусмотрено промежуточное контрольное тестирование по каждой лекции курса, которое состоит из 10 вопросов, проводится в первые 10 минут каждой лекции и представляет собой эффективную меру повторения и усвоения студентами материала предыдущей лекции.

Требования

Курс рассчитан на иностранных учащихся, имеющих начальные знания по фонетике и графике русского языка

Программа курса

Модуль 1.

Современные угрозы и модели каналов утечки информации

1. 1. Информационная безопасность и уровни ее обеспечения – 2 ч.

Общие понятия о защищаемой информации, виды и направления её добывания. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Составляющие информационной безопасности.

2. Понятие и структура угроз безопасности информации– 4 ч.

Источники, виды и способы дестабилизирующего воздействия на информацию. Характеристики источников, среды распространения и приемников информации. Классификация угроз безопасности информации: угрозы утечки информации по техническим каналам; угрозы несанкционированного доступа к информации. Вирусы как угроза информационной безопасности. Типовые удаленные атаки и их характеристика. Анализ уязвимостей технологий автоматизации умного дома. Модель угроз. Модель нарушителя информационной безопасности.

3. Классификация и характеристика технических каналов утечки информации. Каналы утечки информации, обрабатываемой средствами вычислительной техники – 2 ч.

Виды электромагнитных излучений, электромагнитные и электрические каналы утечки информации. Методы и средства съема информации по радиоканалу.

Электромагнитные излучения и съем информации, обрабатываемой средствами вычислительной техники. Параметрические каналы утечки информации.

4. Каналы утечки информации при её передаче по каналам связи – 2 ч.

Перехват информации, передаваемой по каналам радиосвязи. Съем информации с проводных (кабельных линий связи). Съем информации с помощью технологи Bluetooth и в Wi-Fi-сетях. Методы и средства съема информации в высокочастотных и волоконно-оптических кабелях.

5. Классификация и характеристика каналов утечки речевой информации – 2 ч.

Технические каналы утечки речевой информации и методы ее съема. Методы дистанционного проникновения в помещение для скрытого съема аудиоинформации. Технические средства съема аудиоинформации: малогабаритные проводные, радио- и стетоскопные микрофоны, направленные, лазерные и ИК микрофоны.

Технические средства съема аудиоинформации: эндовибраторы, аудиотранспондеры и вторичные микрофоны, устройства ВЧ навязывания, устройства с перемодуляцией радиоизлучений на нелинейных элементах, устройства с двойной модуляцией, устройства с питанием и передачей информации по сети, диктофоны.

6. Технические каналы утечки видовой информации – 2 ч.

Технические средства съема видеоинформации и их общая характеристика. Методы дистанционного проникновения в помещение для скрытого съема аудио- и видеоинформации.

Самостоятельная работа:

1. Просмотр тематических видео-лекций – 2 ч.
2. Просмотр тематической видео-инструкции по моделированиюугроз безопасности информации на примере конкретного объекта информатизации – 0,5 ч.
3. Выполнение домашнего задания по моделированиюугроз безопасности информации на примере конкретного объекта информатизации – 6 ч.
4. Другие виды самостоятельной работы – 1 ч.

Модуль 2.

Методы и средства обеспечения информационной безопасности

1. 1. Общие сведения о методах и средствах выявления каналов утечки информации – 2 ч.

Индикаторы электромагнитных излучений, радиочастотомеры. Радиоприемные устройства, нелинейные локаторы, досмотровая техника, рентгеновские установки, металлодетекторы.

2. Основы проектирования системы защиты объектов информатизации – 2 ч.

Принципы построения системы. Основы комплексного обеспечения информационной безопасности.

1. 3. Организация защиты речевой информации – 2 ч.

Активные и пассивные способы защиты речевой (акустической) информации. Подавление диктофонов. Нейтрализация микрофонов. Организационные мероприятия по защите речевой информации.

4. Защита информации, обрабатываемой средствами вычислительной техники – 2 ч.

Пассивные и активные методы подавления технических каналов утечки информации. Программные и аппаратно-программные методы защиты информации в персональных компьютерах.

5. Защита информации в телекоммуникационных сетях – 2 ч.

Средства и методы защиты от сетевых компьютерных угроз: средства межсетевого экранирования, обнаружения вторжений, анализа защищенности, антивирусные средства.

6. Криптографические методы защиты информации – 2 ч.

Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.

7. Организационное обеспечение информационной безопасности – 2 ч.

Организация работы с документами и носителями информации. Способы уничтожения информации. Организация внутриобъектового и пропускного режимов. Регламентация действий при осуществлении информационных процессов.

8.Оценка эффективности мероприятий по защите информации в организации – 2 ч.

Аттестация объекта информатизации по требованиям безопасности информации. Методы проверок и испытаний, применяемые при проведении аттестационных испытаний.

Самостоятельная работа:

1. Просмотр тематических видео-лекций – 3 ч.
2. Просмотр тематических видео-инструкций:

- Установка и настройка средства защиты информации от несанкционированного доступа – 0,5 ч.

- Реализация операций контрольного суммирования на основе средств контроля целостности – 0,5 ч.

- Реализация способов гарантированного уничтожения информации – 0,5 ч.

- Реализация криптографических методов защиты информации посредством использования программы шифрования – 0,5 ч.

- Комплексирование системы защиты от несанкционированного доступа на примере конкретного объекта информатизации – 0,5 ч.

1. Выполнение домашнего задания по реализации операций контрольного суммирования на основе средств контроля целостности – 6 ч.
2. Другие виды самостоятельной работы – 1 ч.

Модуль 3.

Государственная политика в области информационной безопасности

1. 1. Законодательные основы технической защиты информации в Российской Федерации – 2 ч.

Законодательные меры защиты информации. Основные стандарты в области обеспечения информационной безопасности. Государственные органы обеспечения информационной безопасности. Обзор нормативной документации по технической защите информации. Ответственность за нарушения в сфере информационной безопасности

2. Основы государственной политики Российской Федерации в области информационной безопасности – 2 ч.

Национальные интересы личности, общества и государства в информационной сфере. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства.

Самостоятельная работа:

1. Просмотр тематических видео-лекций – 1 ч.

Другие виды самостоятельной работы – 1 ч.

Результаты обучения

В результате освоения курса «Основы информационной безопасности» студент будет способен:

- способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

- понимать физическую природу возникновения технических каналов утечки информации;

- знать физические принципы построения и функционирования технических средств защиты информации;

- проводить классификацию технических каналов утечки информации и организовывать работы по ТЗИ;

- знать законодательные основы проведения работ в области технической защиты информации;

- знать требования нормативной документации в части технической защиты информации;

- проводить анализ законодательной базы и нормативной документации с целью формирования требований по ТЗИ объектов обрабатывающих защищаемую информацию;

- формировать требования по технической защите информации на конкретных объектах

- понимать основные проблемы и направления совершенствования методологии оценки защищенности информации; перспективные процедуры и методики обнаружения каналов съема и утечки информации, поиска закладных устройств и измерения сигналов в побочных каналах утечки информации;

- уметь анализировать возможности съема информации за счет побочных электромагнитных излучений и наводок, а также за счет использования закладных устройств;

- понимать структуру и задачи федеральных органов, ответственных за обеспечение и организацию работ в области технической защиты информации;

- основные понятия в области защищаемой информации и направлений её добывания;

- производить информационный поиск в международной сети Интернет и правовых базах типа Консультант плюс, Гарант и др. в данной предметной области;

- владеть способами оформления и представления результатов информационной работы в области защиты информации в виде аналитических обзоров и презентаций.

Компетенции

СОПК-1 – способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

СОПК-7 - способностью владеть методами решения задач анализа и расчета характе-ристик радиотехнических цепей;

СОПК-9 - способностью собирать, обрабатывать, анализировать и систематизировать научно-техническую информацию по тематике исследования, использовать достижения оте-чественной и зарубежной науки, техники и технологии;

СОК- 4 – способностью использовать основы правовых знаний в различных сферах проф. деятельности.