МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Учебно-методическое объединение по образованию
в области информатики и радиоэлектроники

УТВЕРЖДАЮ
Первый заместитель Министра образования
Республики Беларусь
_____ А.Г. Баханович
_____

Регистрационный № _____

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАДИОСИСТЕМАХ

Примерная учебная программа по учебной дисциплине
для специальности
7-06-0713-03 Радиосистемы и радиотехнологии

СОГЛАСОВАНО
Председатель Учебно-методического объединения по образованию в области информатики и радиоэлектроники
_____В.А. Богуш
_____

СОГЛАСОВАНО
Начальник Главного управления профессионального образования Министерства образования Республики Беларусь
_____С.Н. Пищов
_____

СОГЛАСОВАНО
Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ И.В. Титович
_____

Эксперт-нормоконтролер
_____
_____

Минск 2024

СОСТАВИТЕЛЬ:
Н.И.Листопад, заведующий кафедрой информационных радиотехнологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор

РЕЦЕНЗЕНТЫ:
Кафедра телекоммуникаций и информационных технологий Белорусского государственного университета (протокол № 3 от 24.10.2024);
И.А.Король, начальник лаборатории – заместитель директора по информационной безопасности Научно-инженерного республиканского унитарного предприятия «Межотраслевой научно-практический центр систем идентификации и электронных деловых операций» Национальной академии наук Беларуси, кандидат физико-математических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ПРИМЕРНОЙ:
Кафедрой информационных радиотехнологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 2 от 16.09.2024);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 4 от 20.12.2024);
Научно-методическим советом по радиосистемам и радиотехнологиям Учебно-методического объединения по образованию в области информатики и радиоэлектроники (протокол № 2 от 21.10.2024)

Ответственный за редакцию: С.С. Шишпаронок

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Примерная учебная программа по учебной дисциплине «Технологии обеспечения информационной безопасности в радиосистемах» разработана для магистрантов учреждений высшего образования, обучающихся по специальности 7-06-0713-03 «Радиосистемы и радиотехнологии» в соответствии с требованиями образовательного стандарта углубленного высшего образования и примерного учебного плана вышеуказанной специальности.

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств ее обработки. В связи с возрастающей ролью информации в современном обществе проблема информационной безопасности становится все более важной и актуальной.

Технологии информационной безопасности определяются как целостная система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знаний, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

При анализе проблематики, связанной с технологиями информационной безопасности в радиосистемах, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Такими же примерно темпами происходит развитие и радиосистем. В этой связи важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

Воспитательное значение учебной дисциплины «Технологии обеспечения информационной безопасности в радиосистемах» заключается в формировании у обучающихся математической культуры и научного мировоззрения; развитии исследовательских умений, аналитических способностей, креативности, необходимых для решения научных и практических задач; развитии познавательных способностей и активности: творческой инициативы, самостоятельности, ответственности и организованности; формировании способностей к саморазвитию, самосовершенствованию и самореализации.

Изучение данной учебной дисциплины способствует созданию условий для формирования интеллектуально развитой личности обучающегося, которой присущи стремление к профессиональному совершенствованию, активному участию в экономической и социально-культурной жизни страны, гражданская ответственность и патриотизм.

ЦЕЛЬ, ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель учебной дисциплины: приобретение и закрепление структурированных фундаментальных и прикладных знаний и компетенций в области обеспечения информационной безопасности в радиосистемах.

Задачи учебной дисциплины:

систематизация теоретических и практических сведений в области методов и способов обеспечения информационной безопасности в компьютерных сетях и радиосистемах в целом;

приобретение фундаментальных и прикладных знаний и умений в области безопасности информации в радиосистемах;

освоение базовых умений и навыков для осуществления деятельности в сфере обеспечения информационной безопасности при разработке и эксплуатации программно-аппаратных комплексов.

Базовыми учебными дисциплинами для учебной дисциплины «Технологии обеспечения информационной безопасности в радиосистемах» являются учебные дисциплины общего высшего образования: «Линейная алгебра и аналитическая геометрия», «Математический анализ», «Теория вероятностей и математическая статистика».

В свою очередь учебная дисциплина «Технологии обеспечения информационной безопасности в радиосистемах» содержательно связана с такими учебными дисциплинами, как «Моделирование процессов и систем», «Прикладные аспекты радиосистем и радиотехнологий» и является базой для таких учебных дисциплин как, «Прикладные методы криптографии и кодирования информации в радиосистемах», «Проектирование программных систем», «Технологии распределенных реестров»

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения учебной дисциплины «Технологии обеспечения информационной безопасности в радиосистемах» формируется следующая углубленная профессиональная компетенция: владеть современными методами обеспечения эффективного и безопасного обмена информацией в радиосистемах.

В результате изучения учебной дисциплины обучающийся должен:

знать:

основные понятия информационной безопасности;

нормативно-правовую базу информационной безопасности;

основные принципы проектирования систем защиты информации;

уязвимости беспроводных радиосистем и радиотехнологий;

технологии защиты локальных и глобальных сетей, а также радиосистем в целом;

уметь:

использовать стандарты и нормативно-правовые документы информационной безопасности в профессиональной деятельности;

применять математические методы, физические законы и вычислительную технику для решения практических задач;

применять методы проектирования систем защиты информации;

оформлять результаты экспериментов и формулировать соответствующие выводы;

иметь навык:

решения научно-исследовательских, проектных и технологических задач с использованием информационных технологий;

проектирования и моделирования широкополосных беспроводных сетей для коммерческих и прикладных систем широкого назначения;

разработки моделей и политик безопасности.

Примерная учебная программа рассчитана на 90 учебных часов, из них – 44 аудиторных. Примерное распределение аудиторных часов по видам занятий: лекции – 28 часов, лабораторные занятия – 16 часов.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

Наименование раздела, темы	Всего аудиторных часов	Лекции	Лабораторные занятия
Раздел 1. Информация. Основные понятия и принципы безопасности	**4**	**4**	
Тема 1. Понятие информации. Информация в материальном мире	2	2	
Тема 2. Информационная система контролируемого доступа к ресурсам	2	2	
Раздел 2. Основные положения информационной безопасности в компьютерных сетях	**4**	**4**	
Тема 3. Модели информационной безопасности	2	2	
Тема 4. Киберпреступность	2	2	
Раздел 3. Методология обеспечения информационной безопасности в компьютерных сетях	**4**	**4**	
Тема 5. Нормативно-правовая база информационной безопасности	2	2	
Тема 6. Требования к обеспечению информационной безопасности в радиосистемах	2	2	
Раздел 4. Базовые технологии компьютерной безопасности	**10**	**6**	**4**
Тема 7. Модель эшелонированной системы защиты информации	2	2	
Тема 8. Криптографические методы обеспечения конфиденциальности информации	6	2	4
Тема 9. Защита транспортной инфрастуктуры компьютерных сетей и систем	2	2	
Раздел 5. Системы защиты информации	**12**	**4**	**8**
Тема 10. Технологии анализа трафика и состояния сетей передачи данных	6	2	4
Тема 11. Электронные цифровые подписи	6	2	4
Раздел 6. Системы защиты информации от угроз доступности	**4**	**4**	
Тема 12. Требования к каналам связи и серверам	2	2	

Наименование раздела, темы	Всего аудиторных часов	Лекции	Лабораторные занятия
Тема 13. Организация хранения информации. Технология защищенного канала	2	2	
Раздел 7. Основы формальной теории защиты информации в компьютерных сетях	**6**	**2**	**4**
Тема 14. Технологии управления доступом. Основные модели	6	2	4
Итого:	**44**	**28**	**16**

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. ИНФОРМАЦИЯ. ОСНОВНЫЕ ПОНЯТИЯ И ПРИНЦИПЫ БЕЗОПАСНОСТИ

Тема 1. ПОНЯТИЕ ИНФОРМАЦИИ. ИНФОРМАЦИЯ В МАТЕРИАЛЬНОМ МИРЕ

Введение. Определения информации. Закон Республики Беларусь «Об информации, информатизации и защите информации»: основные определения. Основные понятия и принципы безопасности. Меры информации: подходы к определению ее количества. Общая схема структуры связи в радиосистемах.

Тема 2. ИНФОРМАЦИОННАЯ СИСТЕМА КОНТРОЛИРУЕМОГО ДОСТУПА К РЕСУРСАМ

Концепция совместного использования ресурсов. Идентификация. Аутентификация. Авторизация. Уязвимость, угроза, атака, ущерб.

Раздел 2. ОСНОВНЫЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Тема 3. МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Триада «Конфиденциальность, доступность, целостность». Гексада Паркера и модель STRIDE. Конфиденциальность, целостность, доступность информации. Понятие сохранности информации. Основные методы обеспечения информационной безопасности.

Тема 4. КИБЕРПРЕСТУПНОСТЬ

Современные тренды в сфере киберпреступлений. Типы и примеры атак: пассивные и активные атаки. Отказ в обслуживании. Внедрение вредоносных программ. Кража личности, фишинг. Сетевая разведка. Методы веб-атак. Ответственность за противоправные действия в сфере информационных технологий.

Раздел 3. МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Тема 5. НОРМАТИВНО-ПРАВОВАЯ БАЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международное законодательство и международные стандарты в сфере информационной безопасности. Национальное законодательство Республики Беларусь и национальные стандарты в сфере информационной безопасности. Критически важные объекты информатизации. Лицензирование и сертификация в Республике Беларусь. Технический регламент ТР 2013/027/BY. Классификация стандартов.

Тема 6. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАДИОСИСТЕМАХ

Модель нарушителя. Понятие риска и его оценки. Управление рисками. Стандартные методики оценки рисков. Рекомендации NIST. Методика RiskWatch. Методика CRAMM. Методика OCTAVE. Аудит информационной безопасности.

Раздел 4. БАЗОВЫЕ ТЕХНОЛОГИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Тема 7. МОДЕЛЬ ЭШЕЛОНИРОВАННОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Организационные меры и меры обеспечения физической безопасности. Технические каналы утечки информации. Идентификация и аутентификация. Авторизация и разграничение доступа. Базовая схема идентификации и аутентификации. Классификация методов аутентификации. Факторы идентификации человека. Многоразовые пароли. Одноразовые пароли. Аутентификация на основе сертификатов. Технология единого логического входа.

Тема 8. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

Основы криптографии. Симметричные криптосистемы. Асимметричные криптосистемы. Физические неклонируемые функции. Квантовая криптография. Алгоритм DES. Алгоритм RSA. Атаки на криптосистемы.

Тема 9. ЗАЩИТА ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ КОМПЬЮТЕРНЫХ СЕТЕЙ И СИСТЕМ

Протоколы и их уязвимость. Атаки на транспортную инфраструктуру. TCP-атаки. ICMP-атаки. UDP-атаки. IP-атаки. DNS-атаки. Сетевая разведка.

Раздел 5. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 10. ТЕХНОЛОГИИ АНАЛИЗА ТРАФИКА И СОСТОЯНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Аудит. Файерволы. Системы обнаружения вторжений. Криптографические методы обеспечения целостности информации: криптографические хэш-функции, коды проверки подлинности.

Тема 11. ЭЛЕКТРОННЫЕ ЦИФРОВЫЕ ПОДПИСИ

Требования к электронной цифровой подписи. Инфраструктура открытых ключей. Электронная цифровая подпись и электронный документооборот в Республике Беларусь. Аутентификация программных кодов.

Раздел 6. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УГРОЗ ДОСТУПНОСТИ

Тема 12. ТРЕБОВАНИЯ К КАНАЛАМ СВЯЗИ И СЕРВЕРАМ

Дублирование, резервирование и избыточность каналов связи, балансировка нагрузки. Статическая и динамическая маршрутизация. Дублирование и виртуализация серверов, использование кластеров, управление надежностью оборудования.

Тема 13. ОРГАНИЗАЦИЯ ХРАНЕНИЯ ИНФОРМАЦИИ. ТЕХНОЛОГИЯ ЗАЩИЩЕННОГО КАНАЛА

Общие сведения. Резервное копирование. Зеркалирование. Использование RAID-массивов. Технологии распределенных реестров. Способы образования защищенного канала. Иерархия технологий защищенного канала. Туннелирование. Протокол IPSec.

Раздел 7. ОСНОВЫ ФОРМАЛЬНОЙ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Тема 14. ТЕХНОЛОГИИ УПРАВЛЕНИЯ ДОСТУПОМ. ОСНОВНЫЕ МОДЕЛИ

Формы представления ограничений на доступ. Способы назначений прав. Дискреционный метод управления доступом. Мандатный метод управления доступом. Ролевая модель доступа. Формальные модели управления доступом. Модель дискреционного доступа Харризона-Руззо-Ульмана. Модель мандатного доступа Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

ОСНОВНАЯ

1. Таненбаум, Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – Санкт-Петербург : Питер, 2020. – 960 с.
2. Теоретические основы цифровой радиосвязи : учебное пособие / Н. И. Листопад [и др.]. – Минск : БГУИР, 2012. – 330 с.
3. Закон Республики Беларусь «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: http://pravo.by/document/?guid=3871&p0=H10800455. – Дата доступа: 24.10.2024.
4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах / В. Ф. Шаньгин. – Москва : Форум ; Инфра-М, 2024. – 592 с.

ДОПОЛНИТЕЛЬНАЯ

5. От хранения данных к управлению информацией : учебник / пер. с англ. Н. Вильчинского. – 2-е изд. – Санкт-Петербург : Питер, 2016. – 544 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЩАЮЩИХСЯ

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

изучение накануне каждой лекции материала предыдущих лекций, пользуясь конспектом лекций с устранением возможных ошибок и пропусков;

выполнение лабораторных работ с качественным оформлением отчетов;

изучение дополнительного материала;

повторение пройденного теоретического материала;

подготовка сообщений, тематических докладов, рефератов, презентаций;

выполнение обзора научной литературы по заданной теме.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ КОМПЕТЕНЦИЙ ОБУЩАЮЩИХСЯ

Примерным учебным планом по специальности 7-06-0713-03 «Радиосистемы и радиотехнологий» в качестве формы промежуточной аттестации по учебной дисциплине «Технологии обеспечения информационной безопасности в радиосистемах» рекомендуется зачет. Оценка учебных достижений обучающихся производится по системе «зачтено/не зачтено».

Для текущего контроля по учебной дисциплине и диагностики компетенций могут использоваться следующие формы:

собеседования;

коллоквиумы;

выполнение лабораторных работ с оформлением и защитой отчетов по результатам.

РЕКОМЕНДУЕМЫЕ МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

Основные рекомендуемые методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

лекционные занятия, имеющие объяснительно-иллюстративный характер с использованием метода проблемного изложения материала и компьютерного сопровождения (активное применение современных мультимедийных средств с программным обеспечением, разработанным преподавателем и обучающимися);

лабораторные занятия с использованием аппаратных средств и пакетов прикладных программ, позволяющих производить оценку информационной безопасности в радиосистемах с целью практического освоения научно-теоретических положений учебной дисциплины.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Технологии анализа трафика и состояния сетей передачи данных.
2. Конфигурирование межсетевого экрана
3. Криптографические хэш-функции.
4. Электронные цифровые подписи.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ

1. ОС Microsoft Windows.
2. Пакет математического моделирования: Cisco Packet Traiser.
3. Пакет инженерного проектирования: Matlab.