Учреждение образования «Гомельский государственный технический университет имени П.О. Сухого»

УТВЕРЖДАЮ
Первый проректор
ГГТУ им.П.О.Сухого
_____ Асенчик О.Д.
«17» 10. 2014
Регистрационный № УД-2230-57/р.

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:
1-36 04 02 «Промышленная электроника»

Факультет автоматизированных и информационных систем

Кафедра Промышленная электроника

Курс 2

Семестр 4

Лекции 34 ч.

Экзамен _____
(семестр)

Практические (семинарские) занятия 17 ч.

Зачет 4
(семестры)

Лабораторные занятия -

Курсовой проект (работа) -

Всего аудиторных часов по дисциплине 51 ч.

Всего часов по дисциплине 94

Форма получения высшего образования дневная

Составитель: Храбров Е. А., к.т.н., доцент

2014 г.

Учебная программа составлена на основе учебной программы учреждения высшего образования по учебной дисциплине «Основы защиты информации» для специальности 1-36 04 02 Промышленная электроника, № УД-1018/уч от 11.11.2014.

Рассмотрена и рекомендована к утверждению кафедрой «Промышленная электроника»

28.08.2014 пр. №1
(дата, номер протокола)

Заведующий кафедрой

(подпись) Крышнев Ю.В.
(И.О. Фамилия)

Одобрена и рекомендована к утверждению научно-методическим советом факультета автоматизированных и информационных систем

05.09.2014 №: 1
(дата, номер протокола)

Председатель

(подпись) Селиверстов Г.И.
(И.О. Фамилия)

1. Пояснительная записка

Учебная программа по дисциплине «Основы защиты информации» для студентов дневной формы обучения специальности I ступени высшего образования 1-36 04 02 «Промышленная электроника» учреждения образования «Гомельский государственный технический университет имени П.О.Сухого» разработана в соответствии с учебной программой учреждения высшего образования № УД-1018/уч от 11.11.2014.

1.1. Цели и задачи учебной дисциплины

Целью преподавания учебной дисциплины является формирование у студентов знаний в области защиты информации и управления интеллектуальной собственностью.

Задачи учебной дисциплины:

- изучение областей применения средств защиты информации;
- получение навыков реализации мероприятий и устройств, обеспечивающих защиту информации;
- изучение номенклатуры и технических характеристик существующих средств защиты информации;
- ознакомление с авторским правом и смежными правами, патентованием технических решений и регистрацией компьютерных программ.

В результате изучения дисциплины обучаемый должен

знать:

- системную методологию, правовое и нормативное обеспечение защиты информации; организационные и технические методы защиты информации;
- активные и пассивные мероприятия по защите информации и средства их реализации;
- основы криптологии;
- технические каналы утечки информации, их обнаружение и обеспечение информационной безопасности;

уметь характеризовать:

- основные направления современной теории кодирования;
- виды защиты информации в системах различного назначения от случайных и преднамеренных воздействий, приводящих к искажению, уничтожению или утечке информации, а также навязыванию ложной информации или ложных режимов работы;
- методы и средства блокирования каналов утечки информации;
- рекомендации по защите объектов различного типа от несанкционированного доступа;
- основные положения международного и национального законодательства в области интеллектуальной собственности;

уметь анализировать:

- вероятные угрозы информационной безопасности для заданных объектов; определять возможные каналы утечки информации;
- информационные потоки на предприятии и производстве;
- алгоритмы, реализующие криптографическую защиту информации, процедуры аутентификации и контроля целостности;
- заявки на выдачу охранных документов на объекты промышленной собственности;

владеть:

- основными приемами анализа вероятных угроз информационной безопасности для заданных объектов;
- способами введения объектов интеллектуальной собственности в гражданский оборот;
- способами передачи прав на использование объектов интеллектуальной собственности.

приобрести навыки:

- проектирования технических средств защиты данных;
- реализации мероприятий и устройств, обеспечивающих защиту информации;
- патентного поиска по заданному техническому решению;
- введения объектов интеллектуальной собственности в гражданский оборот;
- передачи прав на использование объектов интеллектуальной собственности.

1.2. Освоение учебной дисциплины согласно стандарту специальности должно обеспечить формирование следующих компетенций:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным порождать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-8. Обладать навыками устной и письменной коммуникации.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

АК-10. Использовать основные законы естественнонаучных дисциплин в профессиональной деятельности.

АК-11. Применять соответствующий физико-математический аппарат, методы математического анализа и моделирования, теоретического и экспериментального исследования в физике, химии, экологии для решения проблем, возникших в ходе профессиональной деятельности.

АК-14. На научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности.

СЛК-1. Обладать качествами гражданственности.

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике.

СЛК-6. Уметь работать в команде.

ПК-1. В составе группы специалистов разрабатывать технологическую документацию, принимать участие в создании стандартов и нормативных документов

ПК-8. В составе группы специалистов осуществлять метрологическую аттестацию и сертификацию изготовляемых радиоэлектронных средств промышленной электроники.

ПК-11. Проводить монтаж, наладку, испытания электронного оборудования, в том числе информационных каналов и каналов связи, устройств автоматики.

ПК-13. Разрабатывать технические задания на проектируемый объект, выбирать структуру и элементную базу радиоэлектронных средств промышленной электроники, рассчитывать и анализировать режимы работы как отдельных узлов, так и изделия в целом.

ПК-21. Владеть современными средствами информационных коммуникаций.

1.3. Изучение дисциплины «Основы защиты информации» опирается на материал дисциплин «Метрология, стандартизация и сертификация в электронике», «Схемотехника аналоговых устройств», «Схемотехника цифровых устройств», «Микроэлектроника и микросхемотехника», «Теоретические основы информационно-измерительной техники» учебного плана специальности 1-36 04 02 «Промышленная электроника» I ступени высшего образования.

1.4. Программа дисциплины рассчитана на объем 94 учебных часа, из них аудиторных – 51. Распределение аудиторных часов по видам занятий: лекций – 34 часа; практических занятий – 17 часов.

2. Содержание учебного материала

2.1. Лекционные занятия

№ п.п.	Название темы, содержание лекции	Объем в часах
4-й семестр		
Раздел 1. Правовые и организационные основы защиты информации		
1.	Системная и правовая методология защиты информации: основные понятия и терминология, классификация угроз информационной безопасности, классификация методов защиты информации. Анализ международных и национальных стандартов управления информационной безопасностью	4
2.	Организационные методы защиты информации: государственное регулирование в области защиты информации, лицензирование деятельности юридических и физических лиц по защите информации, сертификация и аттестация средств защиты и объектов информации, управление рисками, физическая защита информации, комбинированные методы защиты информации.	4
Раздел 2. Защита технических каналов информации		
3	Технические каналы утечки информации. Пассивные и активные методы защиты информации от утечки по техническим каналам. Основы построения защит от угроз нарушения конфиденциальности и целостности информации. Основы построения защит от угроз раскрытия параметров информационной системы и от угроз отказа доступа.	4
4	Анализ вероятности неприема некоторых видов информации и вероятности ложного их приема различными декодирующими устройствами. Анализ способов повышения надежности приема данных при соотношении сигнал/шум меньше единицы.	4
Раздел 3. Физические характеристики каналов передачи информации		
5	Основные свойства и параметры электромагнитных волн различных частотных диапазонов, способы и устройства возбуждения и приема волн, электромагнитное экранирование объектов. Основные свойства и параметры акустических волн различных частотных диапазонов, особенности акустики речи и восприятия звука человеком, основные акустические характеристики помещений, принципы звукоизоляции.	4
6	Анализ схем подавления работы устройств, предназначенных для несанкционированного доступа к информации в помещениях. Разработка схем скремблирования телефонных сигналов с инвертированием частотного спектра речи, с разбиением спектра на отрезки и перемешиванием отрезков спектра.	4
Раздел 4. Математические и схемотехнические аспекты защиты информации		
7	Криптография и криптоанализ сигналов и информационных систем. Кодирование и шифрование информации. Алгоритмы обработки данных устройствами, позволяющими обнаружить и исправить ошибки. Схемотехника электронных устройств передачи, приема и обработки сигналов, обеспечивающих защиту информации. Полиномиальные кодеры и декодеры.	4

Раздел 5. Особенности защиты информации в компьютерных сетях		
8	Программно-техническое обеспечение защиты информации: алгоритмы шифрования, электронно-цифровая подпись, защита информации в электронных платежных системах, методы разграничения доступа и способы их реализации. Защита объектов от несанкционированного доступа: интегральные системы безопасности, противодействие техническим средствам разведки. Анализ простых программ вирусов и антивирусов.	6
Итого: 4 семестр		34
Всего за учебный год		34

2.3. Практические занятия

№ п.п.	Название темы, содержание	Объем в часах
Восьмой семестр		
1.	Параметрический синтез устройств обработки данных с функциями обнаружения и исправления ошибок.	2
2.	Разработка схем полиномиального кодирования и декодирования информации.	2
3.	Анализ международных и национальных стандартов управления информационной безопасностью.	2
4.	Расчет вероятности неприема некоторых видов информации и вероятности ложного их приема различными декодирующими устройствами.	2
5.	Анализ средств подавления работы в помещениях устройств, предназначенных для несанкционированного доступа к информации.	2
6.	Разработка схем скремблирования телефонных сигналов с инвертированием частотного спектра речи, с разбиением спектра на отрезки и перемешиванием отрезков спектра.	2
7.	Разработка простых программ вирусов и антивирусов.	2
8.	Расчет устройств, обеспечивающих надежный прием данных при соотношении сигнал/шум меньше единицы.	3
Итого: 8 семестр		17
Всего за учебный год		17

3. Учебно-методическая карта дисциплины

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов						Форма контроля знаний
		лекции	практические занятия	Семинарские занятия	лабораторные занятия	Управляемая самостоятельная работа	Иное	
1	2	3	4	5	6	7	8	9
	ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ (51 ч.)	34	17					
4-й семестр								
	Правовые и организационные основы защиты информации (12ч.)	8	4					
1.	Системная и правовая методология защиты информации: основные понятия и терминология, классификация угроз информационной безопасности, классификация методов защиты информации. Анализ международных и национальных стандартов управления информационной безопасностью.	4	2					Опрос студентов, подготовка к экзамену
2.	Организационные методы защиты информации: государственное регулирование в области защиты информации, лицензирование деятельности юридических и физических лиц по защите информации, сертификация и аттестация средств защиты и объектов информации, управление рисками, физическая защита информации, комбинированные методы защиты информации.	4	2					Опрос студентов, подготовка к экзамену
	Защита технических каналов информации (12ч.)	8	4					
3.	Технические каналы утечки информации. Пассив-	4	2					Опрос

	ные и активные методы защиты информации от утечки по техническим каналам. Основы построения защит от угроз нарушения конфиденциальности и целостности информации. Основы построения защит от угроз раскрытия параметров информационной системы и от угроз отказа доступа.							студентов, подготовка к экзамену
4.	Анализ вероятности неприема некоторых видов информации и вероятности ложного их приема различными декодирующими устройствами. Анализ способов повышения надежности приема данных при соотношении сигнал/шум меньше единицы.	4	2					Опрос студентов, подготовка к экзамену
	Физические характеристики каналов передачи информации (12 ч.)	8	4					
5.	Основные свойства и параметры электромагнитных волн различных частотных диапазонов, способы и устройства возбуждения и приема волн, электромагнитное экранирование объектов. Основные свойства и параметры акустических волн различных частотных диапазонов, особенности акустики речи и восприятия звука человеком, основные акустические характеристики помещений, принципы звукоизоляции.	4	2					Опрос студентов, подготовка к экзамену
6.	Анализ схем подавления работы устройств, предназначенных для несанкционированного доступа к информации в помещениях. Разработка схем скремблирования телефонных сигналов с инвертированием частотного спектра речи, с разбиением спектра на отрезки и перемешиванием отрезков спектра.	4	2					Опрос студентов, подготовка к экзамену
	Математические и схемотехнические аспекты защиты информации(6 ч.)	4	2					
7.	Криптография и криптоанализ сигналов и информационных систем. Кодирование и шифрование информации. Алгоритмы обработки данных уст-	4	2					Опрос студентов, подготовка к экзамену

	ройствами, позволяющими обнаружить и исправить ошибки. Схемотехника электронных устройств передачи, приема и обработки сигналов, обеспечивающих защиту информации. Полиномиальные кодеры и декодеры.							
	Особенности защиты информации в компьютерных сетях (8 ч.)	6	2					
8.	Программно-техническое обеспечение защиты информации: алгоритмы шифрования, электронно-цифровая подпись, защита информации в электронных платежных системах, методы разграничения доступа и способы их реализации. Защита объектов от несанкционированного доступа: интегральные системы безопасности, противодействие техническим средствам разведки. Анализ простых программ вирусов и антивирусов.	6	2					Опрос студентов, подготовка к экзамену

4. Информационно-методическая часть

4.1. Основная литература

1.Аверченков, В. И. Криптографические методы защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. - Брянск : БГТУ, 2011. - 216 с.. - (Организация и технология защиты информации)

2. Бузов Г.А. Защита от утечки информации по техническим каналам : учеб пособие. - Москва : Горячая линия-Телеком, 2005. - 414с.

3. Защита информации в системах мобильной связи : учеб. пособие для вузов / А. А. Чекалин [и др.]. - Москва : Горячая линия-Телеком, 2005. - 171с.

4.Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

5.Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

4.2. Дополнительная литература

1. Шаньгин В. Ф. Защита компьютерной информации.Эффективные методы и средства : учеб. пособие для вузов. - Москва : ДМК, 2008. - 542 с.

2.Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. – М.: Мир, 1976. – 412 с.

3.Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн. – М.:Энергоатомиздат,1994.

4.Введение в криптографию/ Под общей ред. В.В. Ященко. 2-е изд. – М.: МЦНМЦ «ЧеРо», 1999.

5.Стивенсон Н. Криптономикон/ Пер. с англ.-М: АСТ, 2006. – 910 с.

6.Бузов Г. А. Б90 Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. — М.: Горячая линия Телеком, 2010. 240 с.; ил.

4.3. Учебно-методические комплексы

1. Электронный учебно-методический комплекс по дисциплине «Основы защиты информации» для студентов специальности 1-36 04 02 «Промышленная электроника» дневной и заочной форм обучения авторов к.т.н., доцента Храброва Е.А., Котовой Ю.Е. – Гомель: УО «ГГТУ им. П.О. Сухого», 2013.

4.4. Перечень компьютерных программ, наглядных и других пособий, методических указаний, материалов и технических средств обучения

1. Храбров Е.А., Основы защиты информации: пособие по одноименному курсу для студентов специальности 1-36 04 02 «Промышленная электроника» дневной и заочной форм обучения. Часть 1. Гомель, ГГТУ, 2009. – 52 с.

Список литературы сверен

5. Протокол согласования учебной программы по изучаемой учебной дисциплине с другими дисциплинами специальности

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1. Метрология, стандартизация и сертификация в электронике	Промышленная электроника		28.08.14 пр. №1
2. Схемотехника аналоговых устройств	Промышленная электроника		28.08.14 пр. №1
3. Теоретические основы информационной измерительной техники	Промышленная электроника		28.08.14 пр. №1
4. Схемотехника цифровых устройств	Промышленная электроника		28.08.14 пр. №1
5. Микроэлектроника и микросхемотехника	Промышленная электроника		28.08.14 пр. №1

Зав. кафедрой _____ Ю.В. Крышнев
(ФИО, подпись)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на _____/_____ учебный год