БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
Толстик А.Л.
4.7.17
Регистрационный № УД-4742/уч.

ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

1-98 80 03 Аппаратное и программно-техническое обеспечение информационной безопасности

2017 г.

Учебная программа составлена на основе ОСВО 1-98 80 03-2012 и учебного плана № Р98-286/уч от 26.05.2017

СОСТАВИТЕЛИ:
Е.Е.Попко, старший преподаватель кафедры телекоммуникаций и информационных технологий Белорусского государственного университета

А.Л.Труханович, старший преподаватель кафедры телекоммуникаций и информационных технологий Белорусского государственного университета

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета
(протокол № 6 от 12.12.2017 г.);

Учебно-методической комиссией факультета радиофизики и компьютерных технологий Белорусского государственного университета
(протокол № 4 от 19.12.2017 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Программно-технические средства компьютерной безопасности» разработана для студентов специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности» и относится к циклу дисциплин специальной подготовки компонента учреждения высшего образования.

В курсе рассматриваются такие темы, как: основные понятия в области технической защиты информации; генерация случайных числовых последовательностей для криптографических систем; построение ключевой информации в программно-технических средствах защиты информации; симметричные и асимметричные алгоритмы криптографического преобразования данных; функции хеширования; цифровые подписи; аппаратные средства криптозащиты информации.

При изучении курса акцент делается на выработку у студентов навыков практической работы с современными средствами защиты информации.

Цели и задачи учебной дисциплины

Целью изучения данной дисциплины является формирование у студентов знаний принципов построения и использования программно-технических средств защиты информации.

Основные задачи дисциплины:

- научить студентов анализировать основные угрозы компьютерной безопасности,
- изучить основные принципы работы программно-технических средств компьютерной безопасности,
- изучить программно-технические средства обеспечения компьютерной безопасности.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием, связи с другими учебными дисциплинами

Дисциплина посвящена изучению основных навыков работы с программно-техническими средствами защиты информации. Изучаются способы построения надежных криптографических систем и применение их в построении комплексов для предотвращения несанкционированного доступа к информации. Акцент делается на изучение белорусских стандартов криптографических преобразований.

Дисциплина «Программно-технические средства компьютерной безопасности» базируется на курсах «Микропроцессоры и аппаратные средства вычислительной техники», «Программно-аппаратные средства обеспечения информационной безопасности», «Технологии программирования».

Требования к освоению учебной дисциплины в соответствии с образовательным стандартом

В результате изучения учебной дисциплины студент должен:

знать:

- методы и аппаратно-технические средства комплексной защиты информационных систем на уровнях защиты программ и данных ПЭВМ;
- основные алгоритмы криптографического преобразования данных и принципы их работы;
- способы построение систем предотвращения несанкционированного доступа к данным.

уметь:

- применять методы и средства защиты ПЭВМ;
- применять алгоритмы криптографического преобразования данных;
- использовать программно-технические средства компьютерной безопасности;
- строить решения по защите корпоративных информационных систем.

владеть:

- основными приемами обеспечения компьютерной безопасности с использованием средств криптографической защиты информации, защиты программ и данных;
- знаниями, навыками и умениями в области обеспечения безопасности информации, обрабатываемой на компьютерах.

Состав компетенций специалиста

Требования к профессиональным компетенциям специалиста:

- работать с научно-технической информацией с использованием современных информационных технологий;
- разрабатывать и совершенствовать методы исследования проблем информационной безопасности;
- осуществлять постановку и проведение теоретических и экспериментальных исследований в области информационной безопасности;
- обосновывать достоверность полученных научных результатов;
- формулировать выводы и рекомендации по применению результатов научно-исследовательской работы.

Требования к социально-личностным компетенциям специалиста:

- формировать и аргументировать собственные суждения и профессиональную позицию;
- анализировать и принимать решения по социальным, этическим, научным и техническим проблемам, возникающим в профессиональной деятельности.

Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с образовательным стандартом

Отводится на изучение во 2 семестре всего 168 часов, из них аудиторные - 56 часов: 20 часов – лекции, 36 часов – лабораторные работы. Число зачетных единиц - 4, форма текущей аттестации – зачет.

Форма получения образования – очная.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1.Введение. Основные понятия в области технической защиты информации и компьютерной безопасности.

Классификация программно-аппаратных средств обеспечения информационной безопасности. Требования к защите информации. Доступность, целостность и конфиденциальность информации.

Тема 2. Генерация случайных числовых последовательностей (СЧП) для криптографических систем.

Методы генерации СЧП. Генерация СЧП с использованием математических вычислений. Генерация СЧП с использованием случайных параметров. Генерация СЧП на физических источниках шума. Методы проверки качества СЧП для криптографической системы.

Тема 3. Построение ключевой информации в программно-технических средствах защиты информации.

Способы формирования ключевой информации. Контроль целостности ключевой информации. Способы хранения ключевой информации. Способы установки ключевой информации. Протокол формирования общего ключа и транспортного ключа СТБ 34.101.66-214.

Тема 4.Симметричные алгоритмы криптографического преобразования данных.

Алгоритмы шифрования: ГОСТ 28147-89,AES,DES, 3DES,RC5, СТБ 34.101.31-2011.

Тема 5.Ассиметричные алгоритмы криптографического преобразования данных.

Алгоритмы шифрования: СТБ 34.101.45, ГОСТ Р 34.10-2012, RSA, DSA, Elgamal.

Тема 6. Функции хеширования.

Алгоритм криптографического преобразования данных СТБ 1176.1-99.

Тема 7. Цифровые подписи.

Алгоритмы криптографического преобразования данных СТБ 1176.2-99 и СТБ 34.101.45-2013.

Тема 8. Аппаратные и программные средства защиты информации.

Системы защиты информации от несанкционированного доступа (Кристалл, Аккорд). Смарт-карты. Электронные ключи. Защита программ от отладки. Защита программ от модификации исполняемого кода. Привязка программ к аппаратному окружению и физическому носителю.

Тема 9. Способы построения программно-технических систем компьютерной безопасности.

Основные принципы построения систем компьютерной безопасности.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4		5	6	8	9
1.	Тема 1. Введение. Основные понятия в области технической защиты информации и компьютерной безопасности.	2						тест
1.1.	Изучение аппаратно-программного комплекса «КриптоЛаб».				4			
2.	Тема 2. Генерация случайных числовых последовательностей для криптографических систем.	2						
2.1.	Случайная числовая последовательность.				4			отчет по лабораторной работе с устной защитой
3.	Тема 3. Построение ключевой информации в программно-технических средствах защиты информации.	2						
3.1.	Генерация и работа с ключевой информацией на АПК «Криптолаб».				4			отчет по лабораторной работе с устной защитой
4.	Тема 4. Симметричные алгоритмы криптографического преобразования данных.	2						

4.1.	Алгоритм криптографического преобразования данных ГОСТ 28147-89.				8			отчет по лабораторной работе с устной защитой
5.	Тема 5. Ассиметричные алгоритмы криптографического преобразования данных.	2						
5.1.	Алгоритм криптографического преобразования данных СТБ 34.101.31-2011				8			отчет по лабораторной работе с устной защитой
6.	Тема 6. Функции хеширования.	2						
6.1.	Алгоритм криптографического преобразования данных СТБ 1176.1-99. (функция хеширования)				4			отчет по лабораторной работе с устной защитой
7.	Тема 7. Цифровые подписи.	2						
7.1.	Алгоритм криптографического преобразования данных СТБ 1176.2-99. (электронная цифровая подпись)				2			отчет по лабораторной работе с устной защитой
8.	Тема 8. Аппаратные и программные средства защиты информации.	2						рефераты
9.	Тема 9. Способы построения программно-технических средств компьютерной безопасности.	4						тест
	Итого	**20**			**36**			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень литературы:

Основная

1. Словарь основных терминов по криптологии / Ю.С. Харин [и др.]. - Минск: БГУ, 2013. - 66 с.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / Шаньгин В.Ф. - М.: Инфра-М, 2016 - 416 с.
3. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах / П.Б. Хорев. -М.: ACADEM A, 2005. 254с.
4. Проскурин, В.Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах. Уч. пособие для ВУЗов / С.В. Крутов, И.В. Мацкевич, В.Г. Проскурин. -М. Радио и связь. 2000. 168с.
5. Кузнецов, А.А. Защита деловой информации (секреты безопасности) / А.А. Кузнецов. -М.: Экзамен, 2008. 255 с.
6. Жадаев, А. Г. Как защитить компьютер на 100% / А.Г. Жадаев. -СПб.: Питер, 2012. 304 с.
7. Бойцев О. М. Защити свой компьютер на 100% от вирусов и хакеров / О.М. Бойцев. -СПб.: Питер, 2008. 288 с.
8. Васильков, А.В. Безопасность и управление доступом в информационных системах. Учебное пособие/ А.В.Васильков, И.А. Васильков. -М.: Форум, Инфра-М, 2017. 368 с.

Дополнительная:

1. Нестеров С.А. Основы информационной безопасности. Учебник и практикум / С.А. Нестеров. – М.: Изд-во “Юрайт”, 2017 - 322 с.
2. Руденков Н.А. / Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – М: НОУ Интуит, 2016 - 368 с.

Примерный перечень лабораторных работ

1. Изучение аппаратно-программного комплекса «КриптоЛаб».
2. Случайная числовая последовательность.
3. Генерация и работа с ключевой информацией на АПК «Криптолаб».
4. Алгоритм криптографического преобразования данных ГОСТ 28147-89.
5. Алгоритм криптографического преобразования данных СТБ 34.101.31-2011
6. Алгоритм криптографического преобразования данных СТБ 1176.1-99. (функция хеширования)
7. Алгоритм криптографического преобразования данных СТБ 1176.2-99. (электронная цифровая подпись)

Перечень используемых средств диагностики

Для контроля качества обучения используются следующие средства диагностики:

- тесты;
- отчеты по лабораторным работам с их устной защитой;
- рефераты;
- зачет.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной 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
«Микропроцессоры и аппаратные средства вычислительной техники»	кафедра телекоммуникаций и информацион-ных технологий	нет	изменений не требуется протокол №6 от 12.12.2017
«Технологии программирования»	кафедра телекоммуникаций и информацион-ных технологий	нет	изменений не требуется протокол №6 от 12.12.2017
«Программно-аппаратные средства обеспечения информационной безопасности»	кафедра телекоммуникаций и информацион-ных технологий	нет	изменений не требуется протокол №6 от 12.12.2017

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

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 20___ г.)

Заведующий кафедрой

_____	_____	_____
(ученая степень, звание)	(подпись)	(И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____	_____	_____
(ученая степень, звание)	(подпись)	(И.О. Фамилия)