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

УТВЕРЖДАЮ
Первый проректор ГГТУ им. П.О.Сухого
_____ О.Д.Асенчик
04.12.2016

Регистрационный № УД-43-24/уч.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности

1-40 04 01 «Информатика и технологии программирования»

2016

Учебная программа составлена на основе образовательного стандарта ОСВО 1-40 04 01-2013, учебных планов учреждения образования «Гомельский государственный технический университет имени П.О. Сухого» специальности 1-40 04 01 «Информатика и технологии программирования» № I 40-1-03/уч. 12.02.2015, № I 40-1-06/уч. 11.02.2016, 40-1-37/уч. 17.04.2014

СОСТАВИТЕЛЬ:
Д.В. Прокопенко, старший преподаватель кафедры « Информатика» учреждения образования «Гомельский государственный технический университет имени П.О. Сухого».

Рецензенты:
И.А Мурашко, профессор кафедры «Информационные технологии» учреждения образования «Гомельский государственный технический университет имени П.О. Сухого», доктор технических наук, профессор;
Е.И. Сукач, доцент кафедры "Математические проблемы управления и информатика" учреждения образования «Гомельский государственый университет имени Ф. Скорины», кандидат технических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой «Информатика» учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 5 от 28.11.2016 г.);
Научно-методическим советом факультета автоматизированных и информационных систем учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 4 от 28.11.2016 г.); УДФ-03-21/уч.
Научно-методическим советом учреждения образования «Гомельский государственный технический университет имени П.О. Сухого»
(протокол № 2 от 06.12.2016).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цель преподавания учебной дисциплины: формирование у обучаемого профессиональных навыков, приобретение знаний и умений, касающихся основ защиты информации в компьютерных системах и сетях от различного рода внешних воздействий, которые способны привести к потере или искажению обрабатываемой или управляющей информации, вопросов санкционирования локального и удаленного доступа к информационным ресурсам.

Задачи изучения учебной дисциплины:

– приобретение знаний о концепциях, положенных в основу современных криптографических и стеганографических способов защиты данных, а также об особенностях и видах удаленных (сетевых) атак на компьютерные системы и способы защиты от них;

– формирование навыков, необходимых для изучения новых способов программной и аппаратной защиты программного обеспечения от нелицензионного использования;

– формирование навыков, необходимых для изучения новых способов защиты цифровых устройств от несанкционированного использования;

– формирование навыков разработки защищенных программ с использованием современных инструментальных средств.

В результате изучения учебной дисциплины «Методы защиты информации» формируются следующие компетенции:

академические:

1) иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;

2) владеть основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;

социально-личностные:

1) уметь работать в команде;

профессиональные:

1) разрабатывать программное обеспечение с использованием современных технологий и автоматизированных средств разработки, используя знания процессов жизненного цикла и методов обеспечения компьютерной безопасности;

2) эффективно работать с современными базами данных, владеть компьютерными методами сбора, хранения и обработки информации, администрирование компьютерных систем и сетей;

3) инсталлировать, настраивать и обслуживать системное, инструментальное и прикладное программное обеспечение вычислительных и автоматизированных систем;

4) владеть современными средствами инфокоммуникаций;

5) уметь применять основные математические модели и методы в научных исследованиях в области профессиональной деятельности.

В результате изучения учебной дисциплины студент должен ***знать:***

область применения основных разделов криптографии при решении задач в соответствии с профилем специальности;

модели информационной безопасности, основные виды уязвимостей и иных угроз безопасности информации в компьютерных системах;

существующие стандарты информационной безопасности;

математические основы методов защиты информации;

методы и алгоритмы криптографической защиты информации в компьютерных системах;

методы и алгоритмы проверки подлинности информации, включая электронную подпись;

современные приложения криптографической защиты и аутенфикации;

уметь:

выполнять анализ источников и направлений угроз информационной безопасности объектов;

выполнять анализ последствий нарушения информационной безопасности объектов;

использовать криптографические средства защиты информации;

программировать и итлаживать элементы криптографической защиты информации;

проектировать программные продукты с учетом требований безопасности;

владеть:

подходами к построению комплексных систем информационной безопасности;

приемами администрирования компьютерных систем с учетом требований информационной безопасности;

основными практическими приемами криптоанализа.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины.

№ пп	Название учебной дисциплины	Раздел, тема
1.	«Архитектура вычислительных систем»	Все разделы дисциплины
2.	«Теория вероятностей и математическая статистика»	Все разделы дисциплины
3.	«Системное программирование»	Все разделы дисциплины

Форма получения высшего образования дневная. Распределение аудиторного времени по видам занятий, курсам и семестрам:

Курс	3
Семестр	6
Лекции (часов)	32
Лабораторные занятия (часов)	32
Всего аудиторных (часов)	64

Формы текущей аттестации по учебной дисциплине

Зачет – 6 семестр.

Общее количество часов по учебной дисциплине 108, аудиторных часов 64. Трудоемкость учебной дисциплины 3 зачетные единицы.

СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1 Общие определения

Основные понятия и терминология. Классификация угроз информационной безопасности. Классификация методов защиты информации.

Тема 2. Введение в криптографию

История и перспективы развития систем защиты информации. Симметричная и асимметричная криптография.

Тема 3. Идентификация и проверка подлинности

Аутентификация сообщений. Электронная цифровая подпись. Идентификация и аутентификация пользователей.

Тема 4. Сетевые протоколы

Многоуровневые модели. Физический уровень. Канальный уровень. Протокол Ethernet. Сетевой уровень. Протокол IP. Протокол TCP. Протокол UDP. Сеансовый уровень. Прикладной уровень. Протокол HTTP.

Тема 5. Методы и средства защиты от удаленных атак

Удаленные атаки на распределенные вычислительные системы. Типовые атаки.

Тема 6. Методы и средства защиты программного обеспечения и мультимедиа информации.

Средства защиты от несанкционированного использования. Атаки на переполнение буфера. Переполнение стека. Стеганографические методы защиты информации.

Тема 7. Методы и средства защиты аппаратного обеспечения

Классификация угроз. Классификация методов и средств защиты. Водяные знаки и отпечатки пальцев.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(Дневная форма получения образования)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов				Иное	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия		
1	2	3	4	5	6	7	9
1.	Общие определения	2					О, ЗЛР, З
2.	Введение в криптографию	6			8		О, ЗЛР, З
3.	Идентификация и проверка подлинности	6			6		О, ЗЛР, З
4.	Сетевые протоколы	6			6		О, ЗЛР, З
5.	Методы и средства защиты от удаленных атак	4			6		О, ЗЛР, З
6.	Методы и средства защиты программного обеспечения и мультимедиа информации	6			6		О, ЗЛР, З
7.	Методы и средства защиты аппаратного обеспечения	2					О, ЗЛР, З
	ИТОГО	32			32		

Принятые обозначения:
О - отчет по лабораторной работе;
ЗЛР - защита лабораторной работы;
З - зачет

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Анин, Б. Защита компьютерной информации / Б. Анин. – СПб.: BHV. – 2000. – 376 с.
2. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков: под ред. С. А. Клейменова: учебное пособие для вузов. – Москва :Академия, 2009. – 331 с.
3. Олифер, В. Компьютерные сети: принципы, технологии, протоколы / В. Олифер, Н. Олифер. –Питер. – 4-е издание, 2015. – 944 с.
4. Таненбаум, Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл. – Питер. – 4-е изд, 2011. – 991 с.
5. Шаньгин, В. Ф. Защита компьютерной информации- Эффективные методы и средства: / В. Ф. Шаньгин: учеб. пособие для вузов. – Москва: ДМК, 2008. – 542 с.

Дополнительная литература

6. Зима, В. Безопасность глобальных сетевых технологий / В. Зима, А. Молдовян, Н. Молдовян. – СПб.: BHV. – 2000. – 320 с.
7. Касперски, К. Техника сетевых атак. Приемы противодействия / К. Касперски. – М.: Солон-Р. – Том 1, 2001. – 400 с.
8. Норткат, С. Обнаружение нарушений безопасности в сетях / С. Норткат, Д. Новак. – М.: Издательский дом «Вильямс». – 3-е изд ., 2003. – 447 с.
9. Цирилов, В. Основы информационной безопасности автоматизированных систем. Краткий курс / В.Цирилов. – М.: Феникс, 2008. – 173 с.
10. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2002. – 816 с.
11. Ярмолик, В.Н. Криптография, стеганография и охрана авторского права / В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. – Мн.: Издательский центр БГУ. – 2007. – 241 с.

Средства диагностики компетенций студента

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

- устные: собеседование;
- письменные: тесты; контрольные работы;
- устно-письменные: отчеты по лабораторным работам с их устной защитой; зачет.

Список литературы оверен (Бритова А.В.)

Примерный перечень тем лабораторных занятий

1. Простейшие алгоритмы шифрования: перестановочные и подстановочные
2. Криптографические системы с открытым ключом
3. Электронная цифровая подпись
4. Идентификация и аутентификация пользователей.
5. Атака при установке TCP-соединения.
6. Стеганографические методы защиты информации.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название дисциплины, с которой требуется согласование	Кафедра	Предложения об изменениях в содержании учебной программы по изучаемой дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Технологии разработки программного обеспечения	Информатика		Рабочую программу утвердить, протокол № 5, от 23.11. 2016

Зав. кафедрой «Информатика» Т.В. Тихоненко