Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
и менеджменту качества
_____Е. Н. Живицкая
20.01.2016

Регистрационный № УД-5-397/р

«Методы защиты информации»

Учебная программа учреждения высшего образования по учебной дисциплине для специальности
1-40 04 01 Информатика и технологии программирования

Кафедра информатики

Всего часов
по дисциплине 120

Зачетных единиц 3

2015

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-40 04 01-2013 и учебных планов специальности 1-40 04 01 Информатика и технологии программирования.

Составитель:
В.В. Сергейчик, ассистент кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», магистр технических наук.

Рецензенты:
А.М. Седун, проректор по учебной работе учреждения образования «Белорусский государственный экономический университет», кандидат технических наук, доцент;
Н.В. Лапицкая, заведующая кафедрой программного обеспечения информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент.

Рассмотрена и рекомендована к утверждению:
Кафедрой информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 2 от 21.09.2015);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 4 от 15.01.2016).

СОГЛАСОВАНО

Эксперт-нормоконтролер

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов				Академ. часов на курс. работу (проект)	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары		
1-40 04 01	Информатика и технологии программирования	3	6	64	32	32	-	-	Зачет

План учебной дисциплины в дистанционной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Всего	Количество работ			Академ. часов на курс. работу (проект)	Форма текущей аттестации
					Контрольные работы	Лабораторные занятия	Индивидуальные практические работы		
1-40 04 01	Информатика и технологии программирования	5	9	120	2	-	1	-	Зачет

Место учебной дисциплины

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.

З**адачи 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) владеть навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;
2) уметь учиться, повышать свою квалификацию в течение всей жизни;
3) использовать основные законы естественнонаучных дисциплин в профессиональной деятельности;
4) владеть основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;

социально-личностные:

1) уметь работать в команде;

профессиональные:

1) владеть современными технологиями анализа предметной области и разработки требований к создаваемым программным средствам, разрабатывать математические модели процессов, документацию и спецификации для создания программного обеспечения.
2) владеть современными технологиями проектирования и применять их в разработке программного обеспечения и информационных систем.
3) владеть методами технико-экономического анализа выбора технологий разработки программного обеспечения и информационных систем, оказывать содействие заказчикам в выборе варианта оптимизации процессов

производства с использованием знаний системного анализа и программных средств.

4) систематизировать результаты и составлять отчеты по выполненной работе, обеспечивать контроль качества выполнения работ.
5) использовать современные информационные технологии для получения новых знаний.

В результате изучения учебной дисциплины студент должен

знать:

– технические каналы утечки информации, их обнаружение и обеспечение информационной безопасности;

– основы криптографической и стеганографической защиты информационных ресурсов;

– типы удаленных атак на распределенные компьютерные системы и способы защиты от них;

уметь:

– проводить анализ вероятных угроз информационной безопасности для заданных объектов;

– обнаруживать и устранять уязвимости, приводящие к реализации атак на программные продукты, компьютерные системы и сети;

– качественно оценивать алгоритмы, реализующие криптографическую защиту информационных ресурсов, процедуры аутентификации и контроля целостности;

– разрабатывать рекомендации по защите от несанкционированного доступа объектов различного типа.

владеть:

– базовыми представлениями о различных видах угроз информационной безопасности и способах их предотвращения в современных компьютерных системах и сетях.

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

1. Содержание учебной дисциплины

№ темы	Название темы	Содержание
1.	Общие определения	Основные понятия и терминология. Классификация угроз информационной безопасности. Классификация методов защиты информации.
2.	Введение в криптографию	Симметричная криптография. Криптография с открытым ключом. Стеганография.
3.	Идентификация и проверка подлинности	Аутентификация сообщений. Электронная цифровая подпись. Идентификация и аутентификация пользователей.
4.	Сетевые протоколы	Многоуровневые модели. Модель OSI. Физический уровень. Канальный уровень. Протокол Ethernet. Сетевой уровень. Протокол IP. Транспортный уровень. Протокол TCP. Протокол UDP. Сеансовый уровень. Уровень представления. Прикладной уровень. Протокол HTTP.
5.	Методы и средства защиты от удаленных атак	Удаленные атаки на распределенные вычислительные системы. Типовые атаки. Атака типа ложный ARP-сервер. Ложный DNS-сервер. Подмена одного из субъектов TCP-соединения в сети Internet. Методы удаленного сканирования портов. Защита от удаленных атак в сети Internet. Методы обнаружения анализаторов сетевого трафика. Защищенные сетевые протоколы. Протоколы SSL, IPsec, SET.Защита электронных банковских платежных систем. Защита конфиденциальности информации в мобильных устройствах. Защита медицинских цифровых устройств.
6.	Методы и средства защиты программного обеспечения и мультимедиа информации.	Средства защиты от несанкционированного использования. Средства защиты ПО от обратного проектирования. Средства защиты от модификации. Атаки на переполнение буфера. Переполнение стека. Переполнение кучи. Целочисленное переполнение. Защита от переполнения буфера. Внедрение SQL-кода (SQL-injection). Защита от атак типа SQL-injection. Проверка входных данных. Защита от атак, основанных на изменении входных данных. Классификация вредоносного ПО. Защита от вредоносного ПО. Методы анализа вредоносного ПО. Стеганографические методы защиты информации. Водяные знаки для мультимедиа информации. Водяные знаки в ПО. Методы обфускации.
7.	Методы и средства защиты аппаратного обеспечения	Классификация угроз. Классификация методов и средств защиты. Водяные знаки и отпечатки пальцев. Обфускация. Идентификация. Активное измерение. ФНФ.

2. Информационно-методический раздел

2.1 Литература

2.1.1 Основная

1. Б. Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф. – 2002 г. – 816 с.

2. В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. Криптография, стеганография и охрана авторского права. – Мн.: Издательский центр БГУ. – 2007 г. – 241 с.

3. В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.

4. В. Олифер, Н. Олифер Компьютерные сети: принципы, технологии, протоколы. – 4-е издание. – СПб.: Питер. – 2015 г. – 944 с.

5. Э. Таненбаум, Д. Уэзеролл. Компьютерные сети. 5-е изд. – СПб.: Питер, 2015. – 960 с.

6. С. Норткат, Д. Новак. Обнаружение нарушений безопасности в сетях. 3-е изд. – М.: Издательский дом «Вильямс». – 2003 г. – 447 с.

7. В. Зима, А. Молдовян, Н. Молдовян. Безопасность глобальных сетевых технологий. – СПб.: BHV. – 2000 г. – 320 с.

8. Б. Анин. Защита компьютерной информации. – СПб.: BHV. – 2002 г. – 376 с.

9. В. Цирилов. Основы информационной безопасности автоматизированных систем. Краткий курс. – М.: Феникс. – 2008 г. – 173 с.

2.1.2 Дополнительная

10. К. Касперски Техника сетевых атак. Приемы противодействия. – Том 1. – М.: Солон-Р. – 2001 г. – 400 с.

11. M. Tehranipoor, C. Wang Introduction to Hardware Security and Trust. – New York: Springer. – 2012. – 421 p.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

1. Среды программирования и отладки языков высокого уровня.
2. Сетевые утилиты операционной системы.
3. Средства анализа сетевого траффика. Например, WireShark.
4. Средства управления базами данных. Например, MySQL.

2.3 Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспечен-ность по пункту 2.2
6	Атаки на переполнение буфера	Реализовать программу, демонстрирующую атаку на переполнение буфера.	1
6	Атака внедрением SQL-кода	Провести атаку SQL-injection.	4
2, 3, 4	Идентификация и аутентификация пользователей. Протокол Kerberos.	Реализовать программно протокол Kerberos.	1
4, 5	Атака при установке TCP-соединения	Реализовать атаку при установке TCP-соединения.	1, 2, 3
4, 5	Атака протокола прикладного уровня	Провести атаку в рамках заданного протокола прикладного уровня.	1, 3
2, 6	Стеганографические методы защиты информации	Реализовать метод LSB и метод Patchwork для изображений.	1
2, 6	Защита ПО от несанкционированного использования	Провести обфускацию заданной программы и внедрить динамический цифровой водяной знак.	1

2.4 Контрольная работа

№ темы по п.1	Наименование контрольной работы	Содержание	Обеспеченность по пункту 2.2
5	Методы и средства защиты от удаленных атак	Удаленные атаки на распределенные вычислительные системы. Типовые атаки. Атака типа ложный ARP-сервер. Ложный DNS-сервер. Подмена одного из субъектов TCP-соединения в сети Internet. Методы удаленного сканирования портов. Защита от удаленных атак в сети Internet. Методы обнаружения анализаторов сетевого трафика. Защищенные сетевые протоколы. Протоколы SSL, IPsec, SET. Защита электронных банковских платежных систем. Защита конфиденциальности информации в мобильных устройствах. Защита медицинских цифровых устройств.	2, 3
6	Методы и средства защиты программного, аппаратного обеспечения, мультимедиа информации от	Средства защиты от несанкционированного использования. Средства защиты ПО от обратного проектирования. Средства защиты от модификации. Атаки на переполнение буфера. Переполнение стека. Переполнение кучи. Целочисленное	1, 4

№ темы по п.1	Наименование контрольной работы	Содержание	Обеспеченность по пункту 2.2
	несанкционированного использования	переполнение. Защита от переполнения буфера. Внедрение SQL-кода (SQL-injection). Защита от атак типа SQL-injection. Проверка входных данных. Защита от атак, основанных на изменении входных данных. Классификация вредоносного ПО. Защита от вредоносного ПО. Методы анализа вредоносного ПО. Стеганографические методы защиты информации. Водяные знаки для мультимедиа информации. Водяные знаки в ПО. Методы обфускации. Классификация угроз. Классификация методов и средств защиты. Водяные знаки и отпечатки пальцев. Обфускация. Идентификация. Активное измерение. ФНФ.	

2.5 Индивидуальная практическая работа

№ темы по п.1	Наименование индивидуальной практической работы	Содержание	Обеспеченность по пункту 2.2
3	Криптографические и стеганографические методы защиты информации	Реализовать на выбор: программное средство идентификации и аутентификации пользователей с использованием протокола Kerberos; программное средство стеганографической защиты изображений; программное средство защиты ПО от несанкционированного использования путем обфускации и постановки цифровых водяных знаков.	1

3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер темы по п. 1	Название темы	Количество аудиторных часов		Самостоятельная работа, часы	Форма контроля знаний студентов
		ЛК	Лаб. зан.		
6 семестр					
1	Общие определения	2		2	Текущий опрос
2	Введение в криптографию	4	6	8	Текущий опрос, защита лабораторных работ
3	Идентификация и проверка подлинности	4	6	10	Текущий опрос, защита лабораторных работ
4	Сетевые протоколы	6	6	12	Текущий опрос, защита лабораторных работ
5	Методы и средства защиты от удаленных атак	8	8	12	Текущий опрос, защита лабораторных работ
6	Методы и средства защиты программного обеспечения и мультимедиа информации	6	6	8	Текущий опрос, защита лабораторных работ
7	Методы и средства защиты аппаратного обеспечения	2		4	Текущий опрос
	Текущая аттестация				Зачет
	Итого	**32**	**32**	**56**	

3.2 Учебно-методическая карта учебной дисциплины в дистанционной форме обучения

Номер темы по п.1	Название темы	Количество работ			Самостоятельная работа, часы	Форма контроля знаний
		КР	Лаб. зан.	ИПР		
9 семестр						
1	Общие определения				10	
2	Введение в криптографию				17	
3	Идентификация и проверка подлинности			1	17	Зачет по индивидуальной практической работе
4	Сетевые протоколы				24	
5	Методы и средства защиты от удаленных атак	1			25	Зачет по контрольной работе
6	Методы и средства защиты программного обеспечения и мультимедиа информации	1			17	Зачет по контрольной работе
7	Методы и средства защиты аппаратного обеспечения				10	
	Текущая аттестация					Зачет
	Итого	**2**		**1**	**120**	

Рейтинг-план дисциплины
«Методы защиты информации»
для студентов дневной формы обучения

Специальность 1-40 04 01 Информатика и технологии программирования

курс 3, семестр 6

Количество часов по учебному плану 120, в т. ч. аудиторная работа 64, самостоятельная работа 56

Преподаватель: Сергейчик Владимир Валентинович
Кафедра Информатики

Приложение к учебной программе учреждения высшего образования по учебной дисциплине
рег. № УД -5-397 /р

Рекомендовано на заседании кафедры информатики
Протокол № 2 от «21 » сентября 2015 г.

Зав. кафедрой _____/Волорова Н. А.

Преподаватель _____ /Сергейчик В. В.

Виды учебной деятельности студентов	Модуль 1 (весовой коэффициент вк1 = 0,25)		Модуль 2 (весовой коэффициент вк2 = 0,25)		Модуль 3 (весовой коэффициент вк3 = 0,25)		Модуль 4 (весовой коэффициент вк4 = 0,25)		Итоговый контроль по всем модулям
	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	
1. Лекционные занятия									
1 – 4	15.03	к11=0,3							
5 – 8			15.04	к12=0,3					
9 – 12					15.05	к13=0,3			
13 – 16							31.05	к14=0,3	
2. Лабораторные занятия									
1 – 4	15.03	к21=0,7							
5 – 8			15.04	к22=0,7					
9 – 12					15.05	к23=0,7			
13 – 16							31.05	к24=0,7	
Модульный контроль		МР1		МР2		МР3		МР4	ИР

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Перечень учебных дисциплин	Кафедра, обеспечивающая учебную дисциплину	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего кафедрой, обеспечивающей учебную дисциплину с указанием номера протокола и даты заседания кафедры
«Современные средства проектирования информационных систем»	Информатики	нет	_____ подпись (протокол № 2 от 21.09.2015 г.)
«Тестирование и верификация программ»	Информатики	нет	
«Математическое моделирование»	Информатики	нет	
«Операционные системы и среды»	Информатики	нет	

Зав. кафедрой информатики Н. А. Волорова