БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.В. Данильченко
(подпись)
«28» декабря 2015г.
(дата утверждения)
Регистрационный № УД-1366/уч.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-31 03 07 Прикладная информатика (по направлениям).
Направление специальности:
1-31 03 07-03 Прикладная информатика
(веб-программирование и компьютерный дизайн)

2015 г.

Учебная программа составлена на основе образовательного стандарта высшего образования первой ступени специальности 1-31 03 07-2013 «Прикладная информатика» (по направлениям) 1-31 03 07 и учебного плана БГУ по специальности 1-31 03 07-03 «Прикладная информатика» (веб-программирование и компьютерный дизайн) G31-188/уч. 2013 г.

СОСТАВИТЕЛЬ:

Ю. А. Пикман, старший преподаватель кафедры информационных технологий факультета социокультурных коммуникаций Белорусского государственного университета;

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационных технологий
(протокол №2 от 20.10.2015г.);

Учебно-методической комиссией факультета социокультурных коммуникаций БГУ
(протокол от 26.10.2015г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Быстрое развитие информационных технологий и глобальной сети Интернет привело к формированию информационной среды, оказывающей существенное влияние на все сферы человеческой деятельности. Корпоративные информационные системы стали одним из важнейших средств производства современной компании. Социальные сети позволяют обмениваться информацией миллионам пользователей вне зависимости от их географического местоположения. Важнейшим условием существования и полноценного функционирования информационных систем любого масштаба является информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, способных нанести ущерб владельцам или пользователям информации. Поэтому подготовка грамотного специалиста в области информатики и информационных технологий не может обойтись без изучения основ информационной безопасности, основных видов угроз, способов их обнаружения, предотвращения и нейтрализации.

Целью изучения дисциплины является формирование у студентов базовых знаний о принципах построения и использования современных систем защиты информации, техническом и программном обеспечения этих систем, правовом регулировании правоотношений, возникающих в информационной сфере, об актуальных угрозах безопасности информационных систем.

Основные **задачи** дисциплины:

- научить студентов анализировать и выявлять основные угрозы информационной безопасности;
- изучить основные принципы обеспечения информационной безопасности, методы и средства защиты программных и аппаратных средств от несанкционированного доступа и копирования;
- изучить программно-аппаратные средства обеспечения информационной безопасности;
- сформировать у студентов навыки использования специальных знаний при реагировании на нарушения информационной безопасности;

В результате изучения дисциплины «**Безопасность информационных систем**» студент должен:

знать:

- проблемы и задачи, решение которых имеет важное значение для обеспечения защищенности информации в информационных системах;
- аппаратно-программные средства защиты персонального компьютера от несанкционированного доступа;

- методы и аппаратно-программные средства комплексной защиты информационных систем;
- современные научно-технические решения по обеспечению защиты информации в информационных системах.

уметь:

- использовать современные средства защиты персонального компьютера от несанкционированного доступа;
- строить решения по защите информационных систем;
- применять современные методы и технологии при создании и для оценки защищенных систем;

владеть:

- основными подходами к анализу задач информационной безопасности;
- аппаратными и программными методами обеспечения информационной безопасности;

Проведение лабораторных занятий по дисциплине «Безопасность информационных систем» имеет целью:

1). закрепление и реализация знаний, полученных студентами на лекциях;
2). развитие умений и навыков по работе со специальным программным обеспечением, которые будут способствовать более глубокому пониманию теоретических основ;
3). развитие навыков решения задач информационной безопасности.

Программа дисциплины «Безопасность информационных систем» рассчитана на 90 часов, из них 60 часов – аудиторные:

- 30 часов – лабораторные занятия,
- 30 часов – лекции,

– с итоговым контролем в форме зачёта. Форма получения образования – очная.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

6-ой семестр

Раздел 1. *Введение. Информационная система как объект защиты.*

Тема 1. *Что такое информационная система?*

Структура и принципы функционирования ИС. Основные понятия информационной безопасности и защиты информации. Угрозы информационной безопасности. Проблемы защиты ИС. Характеристики, влияющие на безопасность. Пути решения проблем информационной безопасности.

Тема 2. *Безопасность в Internet.*

Internet как объект защиты. Хосты и протоколы Internet. Типовые сервисы. Угрозы для протоколов и служб Internet.

Тема 3. *Политика информационной безопасности.*

Определение понятия политики информационной безопасности, основные понятия. Структура политики безопасности предприятия. Разработка политики безопасности предприятия. Политики безопасности для Internet.

Тема 4. *Стандарты информационной безопасности.*

Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты информационной безопасности.

Тема 5. *Организационное и правовое обеспечение информационной безопасности.*

Информационное право. Основные нормативно-правовые акты обеспечения ИБ процессов обработки информации. Защита государственной тайны. Подсистема организационно-правовой защиты.

Раздел 2. *Технологии защиты данных.*

Тема 6. *Криптографическая защита информации.*

Основные понятия. Управление криптоключами.

Тема 7. *Программно-технические методы и средства защиты информации.*

Методы идентификации и аутентификации пользователей. Управление идентификацией и доступом. Обеспечение конфиденциальности и целостности данных и сообщений.

Раздел 3. *Многоуровневая защита корпоративных информационных систем* (*КИС*).

Тема 8. *Принципы многоуровневой защиты корпоративной информации.*

Структура корпоративной информационной системы. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений.

Тема 9. *Обеспечение безопасности операционных систем.*

Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС. Обеспечение безопасности в ОС UNIX. Обеспечение безопасности в ОС Windows 7.

Тема 10. *Защита каналов связи. Протоколы защищённых каналов.*

Модель взаимодействия ISO/OSI и стек протоколов TCP/IP. Защита на канальном уровне – протоколы PPTP и L2TP. Защита на сетевом уровне – протокол IPSec. Защита на сеансовом уровне – протоколы SSL, TLS и SOCKS. Защита беспроводных сетей.

Тема 11. *Технологии межсетевого экранирования.*

Функции межсетевых экранов. Функционирование межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе межсетевых экранов.

Тема 12. *Технологии виртуальных защищённых сетей VPN.*

Концепция построения виртуальных защищённых сетей VPN. VPN-решения для построения защищённых сетей. Современные VPN-продукты.

Тема 13. *Защита удалённого доступа.*

Особенности удалённого доступа. Организация защищённого удалённого доступа. Протокол Kerberos.

Тема 14. *Технологии обнаружения и предотвращения вторжений.*

Основные понятия. Обнаружение вторжений системой IPS. Предотвращение вторжений системного и сетевого уровней. Защита от DDoS-атак.

Тема 15. *Технологии защиты от вредоносных программ и спама.*

Классификация вредоносных программ. Основы работы антивирусных программ. Защита ПК и корпоративных систем от воздействия вредоносных программ и вирусов.

Раздел 4. *Управление информационной безопасностью (ИБ).*

Тема 16. *Управление средствами обеспечения ИБ*

Задачи управления ИБ. Архитектура управления ИБ КИС. Функционирование системы управления ИБ КИС. Аудит и мониторинг безопасности КИС.

Тема 17. *Обзор современных систем управления безопасностью ИС.*

Продукты компании Cisco для управления безопасностью сетей. Продукты компании IBM для управления средствами безопасности. Продукты компании Check Point Software Technologies для управления средствами безопасности.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы.	Название раздела, темы занятия; перечень изучаемых вопросов	Количество аудиторных часов					Количество часов УСР	Формы контроля
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	**Раздел 1.** ***Информационная система как объект защиты***							
1.1	*Тема 1.1.* Что такое информационная система Структура и принципы функционирования ИС. Основные понятия информационной безопасности и защиты информации. Угрозы информационной безопасности. Проблемы защиты ИС. Характеристики, влияющие на безопасность. Пути решения проблем информационной безопасности.	2						Фронтальный опрос
1.2	*Тема 1.2.* Безопасность в Internet. Интернет как объект защиты. Хосты и протоколы Интернет. Типовые сервисы. Угрозы для протоколов и служб Интернет.	2						Фронтальный опрос
1.3	*Тема 1.3.* Политика информационной безопасности Определение политики информационной безопасности, основные понятия. Структура политики безопасности	2			4			Фронтальный опрос

	предприятия. Разработка политики безопасности предприятия. Политики безопасности для Internet.							
1.4	*Тема 1.4.* Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты информационной безопасности.	1						Фронтальный опрос
1.5	*Тема 1.5.* Организационное и правовое обеспечение информационной безопасности. Информационное право. Основные нормативно-правовые акты обеспечения ИБ процессов обработки информации. Защита государственной тайны. Подсистема организационно-правовой защиты.	1						Фронтальный опрос
2.	**Раздел 2. *Технологии защиты данных***							
2.1	*Тема 2.1.* Криптографическая защита информации. Основные понятия. Управление криптоключами.	2						Фронтальный опрос
2.2	*Тема 2.2.* Программно-технические методы и средства защиты информации. Методы идентификации и аутентификации пользователей. Управление идентификацией и доступом. Обеспечение конфиденциальности и целостности данных и сообщений.	2			4			Фронтальный опрос
3.	**Раздел 3. *Многоуровневая защита корпоративных информационных систем* (*КИС*)**							
3.1	*Тема 3.1.* Принципы многоуровневой защиты корпоративной информации. Структура корпоративной информационной системы. Системы «облачных» вычислений. Многоуровневый	2						Фронтальный опрос

	подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений.							
3.2	*Тема 3.2.* Обеспечение безопасности операционных систем. Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС. Обеспечение безопасности в ОС UNIX. Обеспечение безопасности в ОС Windows 7.	2			4			Фронтальный опрос
3.3	*Тема 3.3.* Защита каналов связи. Протоколы защищённых каналов. Модель взаимодействия ISO/OSI и стек протоколов TCP/IP. Защита на канальном уровне – протоколы PPTP и L2TP. Защита на сетевом уровне – протокол IPSec. Защита на сеансовом уровне – протоколы SSL, TLS и SOCKS. Защита беспроводных сетей.	2			4			Фронтальный опрос
3.4	*Тема 3.4.* Технологии межсетевого экранирования. Функции межсетевых экранов. Функционирование межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе межсетевых экранов.	2			4			Фронтальный опрос
3.5	*Тема 3.5.* Технологии виртуальных защищённых сетей VPN. Концепция построения виртуальных защищённых сетей VPN. VPN-решения для построения защищённых сетей. Современные VPN-продукты.	2						Фронтальный опрос
3.6	*Тема 3.6.* Защита удалённого доступа. Особенности удалённого доступа. Организация защищённого удалённого доступа. Протокол Kerberos.	2						Фронтальный опрос
3.7	*Тема 3.7.* Технологии обнаружения и предотвращения вторжений. Основные понятия. Обнаружение вторжений системой IPS. Предотвращение вторжений системного и сетевого уровней. Защита от DDoS-атак.	2			4			Фронтальный опрос

3.8	*Тема 3.8.* Технологии защиты от вредоносных программ и спама. Классификация вредоносных программ. Основы работы антивирусных программ. Защита ПК и корпоративных систем от воздействия вредоносных программ и вирусов.	2			2			Фронтальный опрос
4.	**Раздел 4. *Управление информационной безопасностью (ИБ).***							
4.1	*Тема 4.1.* Управление средствами обеспечения ИБ Задачи управления ИБ. Архитектура управления ИБ КИС. Функционирование системы управления ИБ КИС. Аудит и мониторинг безопасности КИС.	1			4			Фронтальный опрос
4.2	*Тема 4.2.* Обзор современных систем управления безопасностью ИС. Продукты компании Cisco для управления безопасностью сетей. Продукты компании IBM для управления средствами безопасности. Продукты компании Check Point Software Technologies для управления средствами безопасности.	1						Фронтальный опрос
	Всего – 60 аудиторных часов	**30**			**30**			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – Москва: ДМК Пресс, 2014. – 416 с.
2. Информационная безопасность открытых систем. В 2-х томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.]; под общ. ред. С.В. Запечникова. – Москва: Горячая линия-Телеком, 2007. – 536 с.
3. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов [и др.]; под общ. ред. Е.Б. Белова. – Москва: Горячая линия-Телеком, 2006. – 544 с.
4. Домарёв, В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарёв. – Киев: ООО ТИД "ДС", 2002. – 688 с.
5. Галатенко, В.А. Стандарты информационной безопасности. Курс лекций. Учебное пособие / В.А. Галатенко; под ред.чл.-корр. РАН В.Б. Бетелина. – Москва: ИНТУИТ.РУ Интернет-университет информационных технологий, 2008. – 328с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Ярочкин, В.И. Информационная безопасность: Учебник для студентов вузов / В.И. Ярочкин. – 2-е изд. – Москва: Академический проект; Гаудеамус, 2008. – 544 с.
2. Галатенко, В.А. Основы информационной безопасности. Курс лекций. Учебное пособие / В.А. Галатенко; под ред.чл.-корр. РАН В.Б. Бетелина. – 2-е изд. – Москва: ИНТУИТ.РУ Интернет-университет информационных технологий, 2008. – 264с.
3. Лапонина, О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Курс лекций. Учебное пособие / О.Р. Лапонина. – Москва: ИНТУИТ.РУ Интернет-университет информационных технологий, 2009. – 608с.
4. Домарёв, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарёв. – Киев: ООО ТИД "ДС", 2004. – 992 с.
5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин. – Москва: Инфра-М, 2010. – 592 с.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х томах. Том 2. Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – Москва: Горячая линия-Телеком, 2008. – 558 с.

ФОРМА ИТОГОВОГО КОНТРОЛЯ

В качестве средств текущего и итогового контроля за учебным процессом предусматриваются: устные вопросы и письменные экспресс-тесты (5-7 минут). Итоговая оценка формируется на основании результатов текущего контроля в ходе лабораторных занятий и результатов зачета. Ликвидация задолженности по отдельным контролируемым темам дисциплины в рамках текущего контроля может проводиться в форме дополнительного контрольного опроса или тестирования по материалу тем дисциплины в часы дополнительных занятий или консультаций.

Оценка промежуточных учебных достижений студента осуществляется по десятибалльной шкале. Для оценки достижений студента используется следующий диагностический инструментарий:

– защита выполненных на лабораторных занятиях индивидуальных работ;

– проведение текущих контрольных вопросов по отдельным темам;

– сдача зачета по дисциплине.

ПРИМЕРНЫЕ ВОПРОСЫ К ЗАЧЁТУ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

1. Определение информационной системы (ИС). Структура, типовые компоненты, принципы функционирования. Информационная система как объект защиты. Многоуровневая модель ИС.
2. Основные понятия информационной безопасности и защиты информации. Защищённая ИС. Классификация и анализ угроз информационной безопасности. Классификация и анализ угроз корпоративных и беспроводных сетей.
3. Обеспечение информационной безопасности компьютерных систем. Принципы и методы обеспечения информационной безопасности. Базовые сервисы и механизмы обеспечения безопасности.
4. Политика информационной безопасности. Определение, основные принципы построения и компоненты архитектуры информационной безопасности (ИБ). Роли и ответственности в безопасности сети. Политики безопасности для Интернет.
5. Стандарты информационной безопасности. Международные стандарты информационной безопасности ISO.
6. Подсистема управления криптоключами. Инфраструктура управления открытыми ключами PKI.
7. Методы аутентификации – с паролем, строгая аутентификация, биометрическая аутентификация.
8. Управление доступом по схеме Single Sign-on.
9. Управление идентификацией и доступом.

10. Системы «облачных» вычислений. Модели, архитектура, основные характеристики.
11. Многоуровневый подход к обеспечению информационной безопасности корпоративных информационных систем (КИС). Подсистемы информационной безопасности традиционных КИС.
12. Проблемы безопасности «облачной» инфраструктуры. Средства защиты в виртуальных средах.
13. Обеспечение безопасности ОС. Типичные угрозы. Защищённая ОС.
14. Архитектура подсистемы защиты ОС.
15. Обеспечение безопасности ОС Windows 7(8).
16. Структура и функциональность стека протоколов TCP/IP.
17. Защита на канальном уровне. Протоколы PPTP и L2TP.
18. Защита на сетевом уровне. Протокол IPSec.
19. Защита на сеансовом уровне. Протоколы SSL, TLS и SOCKS.
20. Обеспечение безопасности беспроводных сетей.
21. Понятие брандмауэра. Виртуальные сети. Схемы подключения. Администрирование. Политика и компоненты брандмауэра.
22. Шлюзы уровня приложений и посредники. Шлюзы сеансового и прикладного уровней. Шлюз экспертного уровня.
23. Формирование политики межсетевого взаимодействия. Основные схемы подключения межсетевых экранов (МЭ). Персональные и распределённые сетевые экраны.
24. Примеры современных МЭ. Тенденции развития.
25. Основные понятия и функции сети VPN. Варианты построения и средства обеспечения безопасности VPN.
26. Классификация сетей VPN. Основные варианты архитектуры и виды технической реализации.
27. Методы управления удалённым доступом. Функционирование системы управления доступом.
28. Средства и протоколы аутентификации удалённых пользователей. Централизованный контроль удалённого доступа.
29. Протокол Kerberos.
30. Технологии обнаружения и предотвращения вторжений. Основные понятия. Системы IPS и IDS.
31. Предотвращение вторжений системного и сетевого уровней. Защита от DDoS-атак.
32. Классификация вредоносных программ. Основы работы антивирусного ПО.
33. Современные средства защиты ПК и корпоративных систем от вредоносных программ и вирусов.
34. Задачи управления информационной безопасностью. Архитектура управления информационной безопасностью КИС.
35. Аудит и мониторинг безопасности КИС.
36. Современные системы управления безопасностью.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГАММЫ УВО

Название дисциплины, изучение которой связано с дисциплиной учебной программы	Кафедра, обеспечивающая изучение этой дисциплины	Предложения кафедры об изменениях в содержании учебной программы	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1	2	3	4
Компьютерные сети	Кафедра информационных технологий	Нет	Рекомендована к утверждению на заседании кафедры инф. технологий (пр. №2 от 20.10.2015г.)
Криптографические методы защиты информации	Кафедра информационных технологий	Нет	Рекомендована к утверждению на заседании кафедры инф. технологий (пр. №2 от 20.10.2015г.)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО НА 2015 / 2016 УЧЕБНЫЙ ГОД

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры информационных технологий (протокол № ___ от _____г.)

Заведующий кафедрой

кандидат физ.-мат. наук, доцент _____ В. А. Нифагин
(подпись)

УТВЕРЖДАЮ
декан факультета

кандидат техн. наук, доцент _____ В. Е. Гурский
(подпись)