Учреждение высшего образования
«Белорусский государственный технологический университет»

УТВЕРЖДАЮ
Проректор по учебной работе БГТУ

_____ А.А. Сакович
23.12. 2016 г.

Регистрационный № УД-7220 /уч.

Криптографические методы защиты информации

Учебная программа учреждения высшего образования
по учебной дисциплине для специальностей:

1-40 01 01 «Программное обеспечение информационных технологий»,
специализация: 1-40 01 01 10 «Программирование интернет-приложений»;
1-47 01 02 «Дизайн электронных и веб-изданий»

2016 г.

Учебная программа составлена на основе образовательных стандартов высшего образования для специальности 1-40 01 01 «Программное обеспечение информационных технологий» (утвержден и введен в действие постановлением Министерства образования Республики Беларусь № 88 от 30.08.2013) и для специальности 1-47 01 02 «Дизайн электронных и веб-изданий» (утвержден и введен в действие постановлением Министерства образования Республики Беларусь № 40 от 12.05.2015) по дневной и заочной формам обучения

СОСТАВИТЕЛЬ:
П.П. Урбанович, профессор кафедры информационных систем и технологий, профессор, д.т.н.

РЕЦЕНЗЕНТЫ:
Н.И. Листопад, заведующий кафедрой информационных радиотехнологий УО «Белорусский государственный университет информатики и радиоэлектроники»,
Д.М. Романенко, заведующий кафедрой информатики и веб-дизайна УО «Белорусский государственный технологический университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационных систем и технологий учреждения образования «Белорусский государственный технологический университет»
(протокол № 4 от 19.12.2016);

Учебно-методическим советом учреждения образования «Белорусский государственный технологический университет»
(протокол № от г.).

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебная программа по дисциплине «Криптографические методы защита информации» разработана для студентов специальностей 1-40 01 01 «Программное обеспечение информационных технологий»,
специализация: 1-40 01 01 10 «Программирование интернет-приложений»;
1-47 01 02 «Дизайн электронных и веб-изданий» в соответствии с требованиями образовательных стандартов ОСВО 1-40 01 01-2013 (для специализации 1-40 01 01 10) и ОСВО 1-47 01 02-1014 (для специальности 1-47 01 02).

ЦЕЛИ, ЗАДАЧИ, РОЛЬ ДИСЦИПЛИНЫ

Цели преподавания дисциплины:

изучение криптографических методов и средств повышения информационной безопасности систем хранения, преобразования и передачи информации и защиты информации в информационно-вычислительных системах (ИВС), освоение и закрепление практических навыков по созданию и использованию методов и средств повышения информационной безопасности систем.

Задачи изучения дисциплины:

- изучение особенностей ИВС как объекта защиты;
- изучение организационных методов защиты информации в ИВС;
- ознакомление с программно-техническими средствами преобразования и защиты информации в ИВС, повышения надежности ИВС;
- изучение методов и инструментальных средств криптографической защиты информации и ИВС.

Связь с другими дисциплинами.

Изучению дисциплины должно предшествовать усвоение базовых дисциплин «Математика»,, «Основы информационных технологий», «Основы алгоритмизации и программирования», «Объектно-ориентированное программирование», «Базы данных».

В процессе изучения дисциплины студент должен освоить основы создания защищенных информационно-вычислительных систем, включающие анализ угроз, перечень атак, методов и средств криптографической защиты информации, методологию оценки информационной безопасности.

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины формируются следующие компетенции:

академические:

1) уметь применять базовые научно-теоретические знания для решения теоретических и практических задач,

2) уметь работать самостоятельно,

3) применять соответствующий физико-математический аппарат, методы математического анализа и моделирования, теоретического и экспериментального исследования для решения проблем, возникших в ходе профессиональной деятельности,

4) владеть основными методами, способами и средствами получения, хранения, переработки информации, наличием навыков работы с компьютером как средством управления информацией;

социально-личностные:

1) уметь работать в команде,

2) иметь способность находить правильные решения в условиях чрезвычайных ситуаций;

профессиональные:

1) владеть современными методами, языками, технологиями и инструментальными средствами проектирования и разработки программных продуктов, основанных на использовании криптографического преобразования информации;

2) разрабатывать требования на внедрение и эксплуатацию информационных систем и программных разработок,

3) рассчитывать и анализировать эффективность, оценку риска, безопасность программных разработок и проектов внедрения информационных технологий,

4) анализировать и оценивать собранные данные.

В результате изучения дисциплины обучаемый должен:

знать:

1) особенности информационной системы, как объекта защиты,

2) организационные методы защиты информации в информационных системах,

3) программные и технические средства криптографического преобразования и защиты информации,

4) программные и технические средства повышения безопасности ИВС,

5) новейшие достижения в области защиты информации и перспективы их использования для создания программно-технических средств,

уметь:

1) строить системы защиты информации в информационных системах, основу которых составляют методы зашифрования/расшифрования данных;

2) применять технические и программные средства защиты информации,

3) использовать технические и программные средства, повышающие безопасность информационной системы,

4) применять методы криптографии;

владеть:

1) навыками принятия обоснованных решений по организационному и правовому регулированию проблем, относящихся к состоянию безопасности ИВС, обеспечению необходимого уровня защиты информации в ИВС,

2) основными приемами анализа вероятных угроз информационной безопасности ИВС,

3) математическим аппаратом и прикладными программными средствами для анализа, моделирования и оптимизации параметров ИВС, функционирующих на основе криптографических методов защиты информации.

2. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

Программа рассчитана на объем 141 учебный час (для специальности 1-40 01 01 «Программное обеспечение информационных технологий», специализация: 1-40 01 01 10 «Программирование интернет-изданий») и 144 часа – для специальности 1-47 01 02 «Дизайн электронных и веб-изданий», из них – 72 аудиторных (для всех специальностей). Распределение аудиторных часов по видам занятий (дневная форма): лекций – 36 ч., лабораторных работ – 36 ч. Дисциплина изучается в 6-м семестре. Форма контроля знаний – экзамен. По заочной форме обучения: лекций – 8 ч. (4ч. – 7 семестр, 4ч. – 8 сем.), лаб. работ – 10 ч. (8 сем.). Форма контроля знаний – экзамен.

3. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Раздел 1. Информационно-вычислительные системы (ИВС) как объекты защиты информации и повышения функциональной надежности

Тема 1. Фундаментальные понятия и определения из области информационной безопасности систем. Объекты и методы защиты информации

Понятия безопасность, надежность, целостность объекта и системы. Краткая историческая информация и тенденции развития ИВС. Общая характеристика факторов, влияющих на безопасность и надежность ИВС. Особенности использования и угрозы со стороны деструктивных программных средств. Компьютерные преступления и ответственность нарушителей. Основные методы защиты информации.

Тема 2. Общая характеристика, структура и математическое описание каналов передачи и хранения информации.

Описание и характеристика ИВС на структурно-функциональном уровне. Особенности и математическое описание каналов передачи и каналов хранения информации. Двоичные каналы. Факторы, определяющие безопасность и надежность каналов.

Раздел 2. Основы теории информации

Тема 3. Понятие информации. Энтропия источника сообщений.

Основы теории информации К. Шеннона. Понятие алфавита источника сообщения. Энтропия Шеннона и Хартли.

Тема 4. Количество информации. Энтропийная оценка потерь при передаче информации.

Количество информации в сообщении. Информационная избыточность сообщений. Потери информации в зашумленных каналах. Условная энтропия и ее использование для оценки потерь информации в двоичных каналах передачи.

Раздел 3. Теоретические основы криптографии

Тема 5. Основы теории чисел и теории вычетов.

Математические основы шифрования данных. Проблема дискретного логарифма. Основы теории больших чисел. Простые и взаимно простые числа. Проблемы факторизации и дискретного логарифма. Алгоритм Евклида. Арифметика вычетов. Китайская теорема об остатках. Модулярная арифметика в криптопреобразованиях данных.Обратные значения по модулю. Функция Эйлера и Малая теорема Ферма.

Тема 6. Классификация и принципы функционирования криптографических систем.

Понятие криптостойкости шифра. Характеристика методов. Подстановочные и перестановочные шифры. Шифр Цезаря и другие шифры на его основе. Блочные и потоковые шифры. Симметричные и асимметричные криптосистемы. Атаки на криптосистемы.

Раздел 4. Симметричные криптосистемы

Тема 7. Алгоритмы DES, 3DES, Lucifer, Blowfish, IDEA.

Алгоритм DES. Общая структура. Преобразование блока данных в одном раунде. Криптостойкость алгоритма. Достоинства и недостатки алгоритма. Алгоритмы 3DES. Стандарт шифрования ГОСТ 28147-89.

Алгоритмы шифрования Lucifer, Blowfish, IDEA. Особенности. Криптостойкость.

Тема 8. Особенности потоковых шифров.

Синхронные и асинхронные шифры. Шифр Вернама. Генераторы ключевой информации. Генераторы ПСП на основе регистров сдвига. Особенности алгоритмов RC4 и SEAL. Криптостойкость потоковых шифров.

Раздел 5. Асимметричные криптосистемы

Тема 9. Алгоритм Диффи-Хеллмана и ранцевый алгоритм.

Алгоритм Диффи-Хеллмана согласования ключевой информации по открытым каналам. Задача об укладке ранца. Алгоритм Меркла-Хеллмана. Варианты ранцевых схем. Особенности криптографических систем на основе нейросетевых технологий.

Тема 10. Алгоритмы RSA и Эль-Гамаля.

Криптосистема RSA. Криптосистема Эль-Гамаля. Атаки на асимметричные шифры. Криптостойкость асимметричных криптосистем.

Раздел 6. Криптосистемы на основе эллиптических кривых

Тема 11. Основы алгебраической геометрии.

Представление и описание эллиптической кривой на основе алгебраической геометрии. Арифметические операции в эллиптической криптографии. Порядок точки на кривой. Генерирующая точка кривой.

Тема 12. Система распределения криптографических ключей на основе эллиптической кривой.

Рекомендации по выбору параметров эллиптической кривой. Криптосистема распределения (обмена) тайной ключевой информации. Виды эллиптических криптосистем.

Раздел 7. Электронная цифровая подпись

Тема 13. Назначение, генерация и использование ЭЦП

Определение, функции и назначение ЭЦП. Алгоритмы и терминология. Основные типы ЭЦП. Сферы применения ЭЦП.

Тема 14. Хеширование сообщений

Определение и однонаправленность хеш-функции. Коллизии. Особенности алгоритмов класса MD и класса SHA. Имитовставки. Стойкость алгоритмов хеширования и выбор однонаправленных функций.

Тема 15. Рассмотрение и анализ основных типов ЭЦП.

ЭЦП на основе симметричной и асимметричной криптографии без использования хеша сообщения. ЭЦП на основе открытого ключа и хеша. Алгоритм DSA. Генерация простых чисел для DSA. Стойкость DSA. ЭЦП на основе дискретных логарифмов: алгоритмы Эль-Гамаля и Шнорра. Стандарт ЭЦП в РБ. Практика использования ЭЦП.

Раздел 8. Стеганографические и иные методы защиты информации

Тема 16. Сущность, принципы функционирования и модели стеганосистем

Назначение, классификация, структура стеганографических систем. Понятие контейнера. Стеганография и криптография. Модели и криптостойкость стеганосистем. Защита прав интеллектуальной собственности с помощью стеганосистем.

Тема 17. Текстовая стеганография

Основные синтаксические и лингвистические методы. Методы на основы модификации пространственных и цветовых параметров символов текста. Использование модели RGB для осаждения информации в текстах-контейрах. Математические модели систем на основе текстовой стеганографии.

Тема 18. Графическая стеганография

Сущность и особенности метода младших значащих бит. Математические модели систем на основе графической стеганографии. Особенности стегоанализа. Прикладные компьютерные программы

Тема 19. Защита кодов программ методами обфускации

Сущность и классификация методов обфускации. Защита программного кода на основе запутывания потока выполнения, замены имен объектов и непрозрачных предикатов. Реализация обфускации кода.

Раздел 9. Архивация данных как метод их защиты

Тема 20. Цели, классификация и характеристика основных методов сжатия данных. Особенности словарных, вероятностных и арифметических методов сжатия информации.

Раздел 10. Защита ИС от деструктивных программных средств

Тема 21. Классификация и принципы действия деструктивных программ. Компьютерные вирусы

Классификация вредоносных программ. Компьютерные вирусы и «троянские кони». Классификация и принципы действия. Вирусы для мобильных приложений. Методы защиты. Другие типы подобных программ. Спам. Антивирусное ПО.

Тема 22. Парольная защита ИВС. Идентификация и проверка подлинности

Бреши в ПО. Их поиск и устранение. Парольная защита. Безопасное время и безопасная длина пароля. Формула Андерсена. Взаимная проверка подлинности субъектов. Протоколы идентификации. Особенности протокола Kerberos.

Тема 23. Основные итоги изучения дисциплины. Направления разработки новых средств повышения надежности и безопасности ИС

Сфера деятельности администратора информационной безопасности. Особенности биотехнических и антропометрических методов идентификации пользователя. Направления разработки защищенных веб-ресурсов.

4. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА ДИСЦИПЛИНЫ

4.1 (дневная форма получения образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов			Количество часов УСР	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические (семинарские)	лабораторные занятия				
1	2	3	4	5	6	7	8	9
1.	**Информационные и информационно-вычислительные системы (ИВС) как объекты защиты**	**2**		**2**	**4**			
1.1.	Тема 1. Фундаментальные понятия и определения из области информационной безопасности систем. Объекты и методы защиты информации	1			1	компьютер, проектор		
	Лабораторная работа № 1. Разработка политики безопасности конкретного предприятия, учреждения или организации.			2	2	компьютер		отчет
1.2.	Тема 2. Общая характеристика, структура и математическое описание каналов передачи и хранения информации	1			1	компьютер, проектор		

2.	**Основы теории информации**.	**2**		**4**	**6**			
2.1	Тема 3. Понятие информации. Энтропия источника сообщений	1			1	компьютер, проектор		
	Лабораторная работа № 2. Энтропия Шеннона и Хартли.			2	2	компьютер		отчет
2.2	Тема 4. Количество информации. Энтропийная оценка потерь при передаче информации	1			1	компьютер, проектор		
	Лабораторная работа № 3. Энтропия Шеннона и Хартли.			2	2	компьютер		отчет
3.	**Теоретические основы криптографии**	**4**		**2**	**6**			
3.1	Тема 5. Основы теории чисел и теории вычетов.	2			2	компьютер, проектор		
3.2	Тема 6. Классификация и принципы функционирования криптографических систем	2			1	компьютер, проектор		
	Лабораторная работа № 4. Разработка приложений для реализации и анализа шифров на основе базового шифра Цезаря.			2	3	компьютер		отчет
4.	**Симметричные криптосистемы**	**4**		**6**	**10**			
4.1.	Тема 7. Алгоритмы DES, 3DES, Lucifer, Blowfish, IDEA.	2			1	компьютер, проектор		
	Лабораторная работа № 5. Разработка приложений для реализации выбранного симметричного алгоритма			4	4	компьютер		отчет
4.2	Тема 8. Особенности потоковых шифров	2			1	компьютер, проектор		

	Лабораторная работа № 6. Разработка приложений для изучения свойств ПСП			2	4	компьютер		отчет
5.	**Асимметричные криптосистемы**	**4**		**6**	**10**			
5.1.	Тема 9. Алгоритм Диффи-Хеллмана и ранцевый алгоритм	2			1	компьютер, проектор		
	Лабораторная работа № 7. Разработка приложения для реализации алгоритмов Диффи-Хеллмана и ранцевого алгоритма			2	3	компьютер		отчет
5.2.	Тема 10. Алгоритмы RSA и Эль-Гамаля. Распределение и хранение ключевой информации	2			2	компьютер, проектор, коллоквиум		
	Лабораторная работа № 8. Разработка приложений для реализации асимметричных шифров			4	4	компьютер		отчет, коллоквиум
6.	**Криптосистемы на основе эллиптических кривых**	**4**		**2**	**6**			
6.1.	Тема 11. Основы алгебраической геометрии	2			2	компьютер, проектор		
6.2.	Тема 12. Система распределения криптографических ключей на основе эллиптической кривой	2			1	компьютер, проектор		
	Лабораторная работа № 9. ЭЦП на основе эллиптических кривых. Разработка приложения для реализации заданного преподавателем вида кривой.			2	3	компьютер		отчет
7.	**Электронная цифровая подпись**	**6**		**6**	**12**			

7.1.	Тема 13. Классификация, назначение, генерация и использование ЭЦП	2			1	компьютер, проектор		
7.2.	Тема 14. Хеширование сообщений. Алгоритмы хеширования семейств MD и SHA	2			2	компьютер, проектор		
	Лабораторная работа № 10. Разработка приложения для реализации заданного преподавателем алгоритма хеширования			2	4	компьютер		отчет
7.3.	Тема 15. Рассмотрение и анализ основных типов ЭЦП.	2			1	компьютер, проектор		
	Лабораторная работа № 11. Разработка приложения для реализации ЭЦП на основе стандарта РБ			4	4	компьютер		отчет
8.	**Стеганографические и иные методы защиты информации**	**4**		**6**	10			
8.1.	Тема 16. Сущность, принципы функционирования и модели стеганосистем	1			1	компьютер, проектор		
8.2.	Тема 17. Текстовая стеганография	1			1			
	Лабораторная работа № 12. Разработка приложения для реализации методов (по указанию преподавателя) текстовой стеганографии			4	4	компьютер		отчет
8.3.	Тема 18. Графическая стеганография	1			1			
8.4	Тема 19. Защита кодов программ методами обфускации	1			1	компьютер, проектор		
	Лабораторная работа № 13. Разработка приложения для реализации методов обфускации			2	2	компьютер		отчет

9.	**Архивация данных как метод их защиты информации**	**2**		**4**	**4**			
	Тема 20. Цели, классификация и характеристика основных методов сжатия данных	2			1	компьютер, проектор		
	Лабораторная работа № 14. Разработка приложения для реализации методов сжатия (по указанию преподавателя)			4	3	компьютер		отчет
10.	**Раздел 10. Защита ИС от деструктивных программных средств**	**4**		**2**	**6 (3*)**			
10.1.	Тема 21. Классификация и принципы действия деструктивных программ. Компьютерные вирусы	2			1	компьютер, проектор		
10.2.	Тема 22. Парольная защита ИВС. Идентификация и проверка подлинности. Основные итоги изучения дисциплины. Направления разработки новых средств повышения надежности и безопасности ИС.				1	компьютер, проектор, коллоквиум		
	Лабораторная работа № 15. Разработка приложения для исследования безопасности пароля			2	4(1*)			отчет, коллоквиум
				4				
				6				отчет
Итого (144 ч. - для ДЭВИ**):** **(141 ч. –** для ПОИТ*)		**36**		**36**	**72 (69*)**			

4.2 (заочная форма получения образования)

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов			Количество часов УСР	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические (семинарские)	лабораторные занятия				
1	2	3	4	5	6	7	8	9
1.	**Информационные и информационно-вычислительные системы (ИВС) как объекты защиты**	**1**			**2**			
1.1.	Тема 1. Фундаментальные понятия и определения из области информационной безопасности систем. Объекты и методы защиты информации	1			2	компьютер, проектор		
2.	**Основы теории информации**.	**1**		**2**	**8**			
2.1	Тема 2. Понятие информации. Энтропия источника сообщений. Количество информации.	1			4	компьютер, проектор		
	Лабораторная работа № 1. Энтропия Шеннона и Хартли.			2	4	компьютер		отчет
3.	**Теоретические основы криптографии**	**1**		**2**	**22**			

3.1	Тема 3. Основы теории чисел и теории вычетов.	1			10	компьютер, проектор		
	Лабораторная работа № 2. Разработка приложений для реализации и анализа шифров на основе базового шифра Цезаря.			2	12	компьютер		отчет
4.	**Симметричные криптосистемы**	**1**			**10**			
4.1.	Тема 4. Алгоритмы DES, 3DES, Lucifer, Blowfish, IDEA.	1			10	компьютер, проектор		
5.	**Асимметричные криптосистемы**	**2**		**2**	**21**			
5.1.	Тема 5. Алгоритм Диффи-Хеллмана и ранцевый алгоритм	1			5	компьютер, проектор		
5.2.	Тема 6. Алгоритмы RSA и Эль-Гамаля. Распределение и хранение ключевой информации	1			10	компьютер, проектор, коллоквиум		
	Лабораторная работа № 3. Разработка приложений для реализации асимметричных шифров			2	6	компьютер		отчет, коллоквиум
6.	**Криптосистемы на основе эллиптических кривых**	**1**			**6**			
6.1.	Тема 7. Основы алгебраической геометрии	1			2	компьютер, проектор		
6.2.	Тема 12. Система распределения криптографических ключей на основе эллиптической кривой				4	компьютер, проектор		
7.	**Электронная цифровая подпись**	**1**		**2**	**12**			
7.1.	Тема 13. Классификация, назначение, генерация и использование ЭЦП				1	компьютер, проектор		

7.2.	Тема 14. Хеширование сообщений. Алгоритмы хеширования семейств MD и SHA	1			3	компьютер, проектор		
	Лабораторная работа № 4. Разработка приложения для реализации заданного преподавателем алгоритма хеширования			2	4	компьютер		отчет
7.3.	Тема 15. Рассмотрение и анализ основных типов ЭЦП.				4	компьютер, проектор		
8.	**Стеганографические и иные методы защиты информации**			**2**	**28**			
8.1.	Тема 16. Сущность, принципы функционирования и модели стеганосистем				2	компьютер, проектор		
8.2.	Тема 17. Текстовая стеганография				6			
	Лабораторная работа № 5. Разработка приложения для реализации методов (по указанию преподавателя) текстовой стеганографии			2	10	компьютер		отчет
8.3.	Тема 18. Графическая стеганография				4			
8.4	Тема 19. Защита кодов программ методами обфускации				6	компьютер, проектор		
9.	**Архивация данных как метод их защиты информации**				**7**			
	Тема 20. Цели, классификация и характеристика основных методов сжатия данных				7	компьютер, проектор		
10.	**Раздел 10. Защита ИС от деструктивных программных средств**				**10**			

10.1.	Тема 21. Классификация и принципы действия деструктивных программ. Компьютерные вирусы				4	компьютер, проектор		
10.2.	Тема 22. Парольная защита ИВС. Идентификация и проверка подлинности. Основные итоги изучения дисциплины. Направления разработки новых средств повышения надежности и безопасности ИС.				6	компьютер, проектор, коллоквиум		
	Итого 144 ч.	**8**		**10**	**126**			

5. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

МЕТОДЫ (ТЕХНОЛОГИИ) ОБУЧЕНИЯ

Характеристика методов обучения.

В числе наиболее перспективных и эффективных современных инновационных образовательных методик и технологий, способствующих вовлечению студентов в поиск и управление знаниями, приобретению опыта самостоятельного решения разнообразных задач, следует выделить:
– технологии проблемно-модульного обучения,
– технологии учебно-исследовательской деятельности,
– проектные технологии,
– коммуникативные технологии (дискуссия, пресс-конференция, учебные дебаты и другие активные формы и методы),
– метод кейсов (анализ ситуации),
– игровые технологии, в рамках которых студенты участвуют в ролевых, имитационных играх, и др.

Для управления учебным процессом и организации контрольно-оценочной деятельности рекомендуется использовать рейтинговые, кредитно-модульные системы оценки учебной и исследовательской деятельности студентов, вариативные модели управляемой самостоятельной работы, учебно-методические комплексы, информационные технологии.

Целесообразно внедрять в практику проведения семинарских и практических занятий методики активного обучения и дискуссионные формы в целях формирования современных социально-личностных и социально-профессиональных компетенций выпускника вуза.

Организация самостоятельной работы студентов.

Аудиторную самостоятельную работу при проведении семинарских и практических занятий целесообразно строить в несколько этапов:

1. Вводная установка преподавателя (постановка цели занятия, формулировка основных вопросов для рассмотрения).
2. Устный экспресс-опрос по теоретическому материалу, необходимому для выполнения работы.
3. Решение типовых задач у доски.
4. Самостоятельное решение задач.
5. Разбор типовых ошибок при решении (в конце текущего занятия или в начале следующего).

При проведении лабораторных, практических и других видов занятий студенты могут выполнять самостоятельную работу как индивидуально, так и малыми творческими группами, каждая из которых разрабатывает свой проект (задачу). Выполненный проект (решение проблемной задачи) затем представляется другим творческим группам. Публичное обсуждение и защита своего варианта повышают роль самостоятельной

работы студентов и усиливают стремление к ее качественному выполнению. Данная система организации практических занятий позволяет вводить в задания научно-исследовательские элементы, упрощать или усложнять задания.

Содержание и формы самостоятельной работы студентов, а также модель рейтинговой системы оценки знаний (кредитно-модульной системы), обеспечивающие контрольно-оценочную деятельность преподавателя за результатами самостоятельной работы студентов, разрабатываются (или выбираются и адаптируются) вузами и кафедрами в соответствии с целями и задачами подготовки специалистов.

ДИАГНОСТИКА КОМПЕТЕНЦИЙ СТУДЕНТА

Типовым учебном планом специальности в качестве формы итогового контроля по дисциплине «Криптографические методы защиты информации» предусмотрен зачет (в первом семестре изучения дисциплины) и экзамен (во втором семестре изучения), а также курсовая работа. Оценка учебных достижений студента осуществляется на экзамене (зачете, защите курсовой работы) и производится по десятибалльной шкале.

1. Требования к осуществлению диагностики

– *определение* объекта диагностики;
– *выявление* факта учебных достижений студента с помощью критериально-ориентированных тестов и других средств диагностики;
– *измерение* степени соответствия учебных достижений студента требованиям стандарта;
– *оценивание* результатов выявления и измерения соответствия учебных достижений студента требованиям стандарта (с помощью шкалы оценок).

2. Шкалы оценок

Оценка учебных достижений студента на экзаменах для цикла общепрофессиональных и специальных дисциплин производится по десятибалльной шкале (1, 2, … 9, 10).

Оценка учебных достижений студентов, выполняемая поэтапно по конкретным модулям учебной дисциплины, осуществляется кафедрой в соответствии с избранной вузом шкалой оценок.

3. Диагностический инструментарий

Для диагностики компетенций студентов «на выходе» из модуля и при итоговом оценивании рекомендуется использовать следующий диагностический инструментарий:

1) педагогические тесты и тестовые задания (Приложение 1),
2) коллоквиум,
3) собеседование,
4) письменные контрольные работы,
5) устный опрос,

6) защита лабораторных работ,

7) проведение текущих опросов по отдельным разделам (темам) дисциплины,

8) критериально-ориентированные компьютерные тесты по отдельным разделам (темам) дисциплины,

9) выступление студента по разработанной им теме,

10) решение проблемных (творческих) задач, предполагающих неформализованный ответ,

11) экзамен.

ЛИТЕРАТУРА

Основная

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации: учебно-методическое пособие/ П.П. Урбанович. – – Мн.: БГТУ, 2014 – 219 с.

2. Урбанович, П.П. Защита информации и надежность информационных систем: пособие для студентов направления специальности 1-40 05 01-03/ П.П. Урбанович, Д.В. Шиман. – Мн.: БГТУ, 2014. – 95 с.

3. Урбанович, П. П. Информационная безопасность и надежность систем: учеб.-метод. пособие / П. П. Урбанович, Д. М. Романенко, Е. В. Романцевич. – Мн.: БГТУ, 2007.

4. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты ная языке Си/ Б. Шнайер. – М.: Издательство ТРИУМФ, 2003.

5. Мельников, В. В. Защита информации в компьютерных системах / В. В. Мальников. – М.: Финансы и статистика, 1997.

6. Харин, Ю. С. Математические основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Мн.: БГУ, 1999.

Дополнительная

1. Герасименко, В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: Московский государственный инженерно-физический институт, 1997.

2. Теория прикладного кодирования: учеб. пособие: в 2 т. / Под редакцией В. К. Конопелько. – Мн.: БГУИР, 2004.

3. Зима, В. М. Компьютерные сети и защита передаваемой информации / В. М. Зима, А. А. Молдавян, Н. А. Молдовян. – С-Петербург, 1998.

4. Мельников, В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – М.: Финансы и статистика, 2003.

5. Ботт, Э. Безопасность Windows / Э. Ботт, К. Зихерт. – С.П.: Питер, 2003.

6. Фористайл, Д. Защита от хакеров / Д. Фористайл. – М.: ДМК Пресс, 2003.

7. Ховард, М. Защищенный код / М. Ховард, Д. Лебланк. – М.: Издательский дом «Русская редакция», 2005.

8. Ярмолик, В.Н. Криптография, стеганография и охрана авторского права/ В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. – Минск: Издательский центр БГУ, 2007.