Учреждение высшего образования
«Белорусский государственный технологический университет»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.А. Касперович
29. 07. 2015 г.

Регистрационный № УД- 253/уч.

Защита информации и надежность информационных систем

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности:

1-40 05 01 Информационные системы и технологии,
направление специальности: 1-40 05 01-03 Информационные системы и технологии (издательско-полиграфический комплекс)

2015 г.

Программа разработана на основе образовательного стандарта ОСВО 1-40 05 01-2013 и типового учебного плана, утвержденного Министерством образования Республики Беларусь 30.08.2013, рег. № I 40-1-011/ тип

СОСТАВИТЕЛЬ:
П.П. Урбанович, заведующий кафедрой информационных систем и технологий Учреждения образования «Белорусский государственный технологический университет», профессор, д.т.н.

РЕЦЕНЗЕНТЫ:
Л.М. Лыньков, заведующий кафедрой защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»,
Д.М. Романенко, заведующий кафедрой информатики и веб-дизайна Учреждения образования «Белорусский государственный технологический университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой информационных систем и технологий Учреждения образования «Белорусский государственный технологический университет», (протокол № 10 от 25 мая 2015 г.);

Методической комиссией факультета информационных технологий Учреждения образования «Белорусский государственный технологический университет», (протокол № 12 от 26.06.15)

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа по дисциплине «Защита информации и надежность информационных систем» разработана для студентов специальности 1-40 05 01 «Информационные системы и технологии (по направлениям)» (направление специальности: 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс))». Указанная дисциплина изучается на 3 курсе в течение двух семестров и является одной из профильных, формирующих основные компетенции специалиста.

ЦЕЛИ, ЗАДАЧИ, РОЛЬ ДИСЦИПЛИНЫ

Цели преподавания дисциплины:

– изучение методов и средств повышения информационной безопасности и надежности 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 и надежности 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 криптографической защиты информации и ИВС.

МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СИСТЕМЕ ПОДГОТОВКИ СПЕЦИАЛИСТА С ВЫСШИМ ОБРАЗОВАНИЕМ

Изучению дисциплины должно предшествовать усвоение базовых дисциплин «Высшая математика», «Физика», «Логические основы цифровых вычислительных машин», «Информационные технологии», «Основы алгоритмизации и программирования», «Объектно-ориентированное программирование», «Проектирование информационных систем», «Базы данных», «Системы управления базами данных».

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

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

3) рассчитывать и анализировать эффективность, оценку риска, надежность 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 преобразования и защиты информации,

4) программные и технические средства повышения надежности,

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

6) методы криптографической защиты информации в информационных системах;

уметь:

1) строить системы защиты информации в информационных системах,

2) применять технические и программные средства защиты информации,

3) использовать технические и программные средства, повышающие надежность 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 и надежности функционирования ИВС,

2) основными приемами анализа вероятных угроз информационной безопасности ИВС,

3) математическим аппаратом и прикладными программными средствами для анализа, моделирования и оптимизации параметров надежности и безопасности ИВС.

ОБЪЕМ АКАДЕМИЧЕСКИХ ЧАСОВ ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Общее количество часов – 238

Количество аудиторных часов – 140, из них лекции – 70: 5-й семестр – 34, 6-й семестр – 36, лабораторные работы – 70: 5-й семестр – 34, 6-й семестр – 36; курсовая работа – 30 часов.

ФОРМЫ ТЕКУЩЕЙ АТТЕСТАЦИИ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Оценка учебных достижений студента осуществляется на экзамене (зачете, защите курсовой работы) и производится по десятибалльной шкале: зачет – 5 семестр, экзамен – 6 семестр, курсовая работа – 6-й семестр.

Форма получения высшего образования - очная

2. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

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

Тема 1. Фундаментальные понятия и определения из области информационной безопасности и надежности систем.

Понятия безопасность, надежность, целостность объекта и системы. Краткая историческая информация и тенденции развития ИВС. Общая характеристика факторов, влияющих на безопасность и надежность ИВС.

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.

Тема 3. Потенциальные угрозы безопасности информации в ИВС. Объекты и методы защиты информации.

Естественные и искусственные помехи. Ионизирующие излучения. Особенности их влияния на аппаратные и аппаратно-программные средства ИВС. Хакеры и кракеры. Особенности использования и угрозы со стороны деструктивных программных средств. Компьютерные преступления и ответственность нарушителей. Основные методы защиты информации.

Раздел 2. Основы теории информации

Тема 4. Понятие информации. Энтропия источника сообщений.

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

Тема 5. 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. Аппаратно-программные методы и средства повышения надежности ИС и ИВС

Тема 6. Методы структурной, информационной и временной избыточности в ИВС.

Характеристика базовых методов преобразования информации. Основные цели применения. Сущность методов структурной, информационной и временной избыточности в ИВС; комбинирование методов.

Тема 7. Основы теории прикладного избыточного кодирования информации .

Помехоустойчивое кодирование информации. Классификация кодов и их граничные характеристики. Математические основы избыточного кодирования. Линейные и нелинейные коды. Коды Хемминга. Циклические коды. Низкоплотностные коды. Турбо-коды.

Методы кодирования и декодирования сообщений. Синдромное декодирование сообщений. Особенности аппаратной, программной и аппаратно-программной реализации кодеров и декодеров.

Использование методов кодирования информации в ЗУ.

Тема 8. Методы сжатия и пермутации данных и их влияние на безопасность и целостности информации.

Классификация и цели использования методов сжатия сообщений. Словарные, вероятностные, арифметические и комбинированные методы сжатия.

Методы Берроуза-Уиллера, Шеннона-Фано, Хаффмана, Лемпеля-Зива. Алгоритмы и математическое описание. Особенности программной реализации методов.

Оценка эффективности методов сжатия (архивации) данных.

Особенности современных компьютерных архиваторов. Их применение для преобразования файлов различных форматов.

Перемежители данных.Типы. Применение для коррекции группирующихся ошибок в сообщениях.

Раздел 4. Математические основы описания и моделирование надежности ИВС

Тема 9. Факторы, влияющие на надежность ИВС.

Климатические, вибрационные и иные типы факторов. Влияние ионизирующих излучений на полупроводниковые структуры; последствия.

Отказы и сбои. Распределение во времени, в пространстве (по площади). Равномерное и сгруппированное распределение. Надежность цифровых си-

стем и каналов передачи информации. Количественные показатели надежности ИВС.

Тема 10. Моделирование надежности цифровых устройств ИВС.

Методы повышения аппаратной надежности ИВС. Аппаратная, временная и информационная избыточность. Надежность ИС при параллельном и последовательном соединении элементов. Статистические методы исследований надежности ИВС. кодирования. Марковские процессы в исследовании надежности ИВС. Надежность функционирования программного обеспечения (ПО). Цели и виды сертификационных испытаний программ. Математические модели описания статистических характеристик ошибок в ПО.

Надежность резервируемых ИВС и систем с использованием помехоустойчивого кодирования.

Тема 11. Тенденции и направления разработки ИС с заданными показателями надежности

Тенденции повышения надежности и быстродействия полупроводниковых изделий, внешней памяти ПК и каналов передачи данных.

Итоговое занятие в семестре.

Раздел 5. Теоретические основы криптографии

Тема 12. Основы теории чисел и теории вычетов.

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

Тема 13. Классификация и принципы функционирования криптографических систем.

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

Раздел 6. Симметричные криптосистемы

Тема 14. Алгоритм DES, 3DES.

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

Алгоритмы Lucifer, Blowfish, IDEA. Особенности. Криптостойкость.

Тема 15. 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 7. Асимметричные криптосистемы

Тема 16. Алгоритм Диффи-Хеллмана и ранцевый алгоритм.

Алгоритм Диффи-Хеллмана согласования ключевой информации по открытым каналам. Задача об укладке ранца. Алгоритм Меркла-Хеллмана. Вариан-

ты ранцевых схем. Особенности криптографических систем на основе нейросетевых технологий.

Тема 17. Алгоритмы RSA и Эль-Гамаля.

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

Раздел 8. Криптосистемы на основе эллиптических кривых

Тема 18. 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 19. Система распределения криптографических ключей на основе эллиптической кривой.

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

Раздел 9. Электронная цифровая подпись

Тема 20. Назначение, генерация и использование ЭЦП

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

Тема 21. Хеширование сообщений

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

Тема 22. 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 10. Стеганографические и иные методы защиты информации

Тема 23. 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 24. 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 25. Графическая стеганография

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

Тема 26. 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 11. Защита ИС от деструктивных программных средств

Тема 27. 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 28. 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 29. 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.

3. ТРЕБОВАНИЯ К КУРСОВОЙ РАБОТЕ

Курсовая работа выполняется в 6 семестре. На ее выполнение отводится 30 часов.

Целью работы является закрепление студентами знаний по основным разделам курса, получение практических навыков самостоятельной работы при решении задач по обеспечению необходимого уровня надежности ИС и защиты информации при ее хранении, передаче и обработке в ИС. При выполнении работы студент анализирует и решает две задачи: теоретическое обоснование метода повышения надежности и безопасности ИС и практическая реализация выбранного приложения с обоснование среды и языка разработки.

Примерный объем – 30 страниц стандартного текста с необходимыми графическими иллюстрациями, оформленными на основе принятых в университете требований. Обязательной частью пояснительной записки является код листинг программы в виде приложения (дополнение к основной части записки). Разработанное приложение представляется в виде исполнительного файла.

4. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов				Количество часов УСР	Форма контроля знаний
		Всего	Лекции	Лабораторные занятия	Иное (коллоквиум)		
1	2	3	4	5	6	7	8
5 семестр							
1	**Раздел 1. Информационные и информационно-вычисли-тельные системы (ИВС) как объекты защиты информации и повышения функциональной надежности**	**10**	**6**	**4**		**4**	
1.1	Тема 1. Фундаментальные понятия и определения из области информационной безопасности и надежности систем	2	2			1	Опрос, тест
1.2	Тема 2. Общая характеристика, структура и математическое описание каналов передачи и хранения информации	4	2	2		1	Опрос, Защита отчета по лаб. работе
1.3	Тема 3. Потенциальные угрозы надежности и безопасности информации в ИВС. Объекты и методы защиты информации	4	2	2		2	Опрос, Защита отчета по лаб. работе
2.	**Раздел 2. Основы теории информации**.	**10**	**4**	**6**		**6**	
2.1	Тема 4. Понятие информации. Энтропия источника сообщений	6	2	4		3	Опрос, Защита отчета по лаб. работе
2.2	Тема 5. Количество информации. Энтропийная оценка потерь при передаче информации	4	2	2		3	Опрос, Защита отчета по лаб. работе
3.	**Раздел 3. Аппаратно-программные методы и средства повышения надежности ИС и ИВС**	**32**	**12**	**20**		**14**	
3.1	Тема 6. Методы структурной, информационной и временной избыточности в ИВС	4	2	2		1	Опрос, Защита отчета по лаб. ра-

							боте
3.2	Тема 7. Основы теории прикладного избыточного кодирования информации 7.1 Математические основы линейных кодов. Коды Хемминга 7.2 Циклические коды 7.3. Итерационные коды и перемежение данных	14 6 4 4	6 2 2 2	8 4 2 2		5	Опрос, Защита отчета по лаб. работе
3.2	Тема 8. Методы сжатия и перестановки данных и их влияние на безопасность и целостности информации	14	4	10		8	Опрос, Защита отчета по лаб. работе
4.	**Раздел 4. Математические основы описания и моделирование надежности ИВС**	**16**	**12**	**4**		**8**	
4.1.	Тема 9. Факторы, влияющие на надежность ИВС	4	4			2	Опрос, тест
4.2	Тема 10. Моделирование надежности цифровых устройств ИВС	10	6	4		4	Опрос, Защита отчета по лаб. работе
4.3	Тема 11. Тенденции и направления разработки ИС с заданными показателями надежности	2	2		+	2	Опрос, Защита отчета по лаб. работе
	За семестр	**68**	**34**	**34**		**32**	
6 семестр							
5.	**Раздел 5. Теоретические основы криптографии**	**8**	**6**	**2**		**8**	
5.1	Тема 12. Основы теории чисел и теории вычетов.	6	4	2		5	Опрос, Защита отчета по лаб. работе
5.2	Тема 13. Классификация и принципы функционирования криптографических систем	2	2			3	Опрос, тест
6.	**Раздел 6. Симметричные криптосистемы**	**10**	**4**	**6**		**8**	
6.1	Тема 14. Алгоритм DES, 3DES. Алгоритмы Lucifer, Blowfish, IDEA.	6	2	4		5	Опрос, Защита отчета по лаб. работе
6.2	Тема 15. Особенности потоковых шифров	4	2	2		3	Опрос, Защита отчета по лаб. работе

7.	**Раздел 7. Асимметричные крипто-системы**	**10**	**4**	**6**		**8**	
7.1	Тема 16. Алгоритм Диффи-Хеллмана и ранцевый алгоритм	4	2	2		3	Опрос, Защита отчета по лаб. работе
7.2	Тема 17. Алгоритмы RSA и Эль-Гамаля. Распределение и хранение ключевой информации	6	2	4		5	Опрос, Защита отчета по лаб. работе
8.	**Раздел 8. Криптосистемы на основе эллиптических кривых**	**8**	**4**	**4**		**8**	
8.1	Тема 18. Основы алгебраической геометрии	4	2	2		4	Опрос, Защита отчета по лаб. работе
8.2	Тема 19. Система распределения криптографических ключей на основе эллиптической кривой	4	2	2		4	Опрос, Защита отчета по лаб. работе
9.	**Раздел 9. Электронная цифровая подпись**	**12**	**6**	**6**		**12**	
9.1	Тема 20. Назначение, генерация и использование ЭЦП	2	2			2	
9.2	Тема 21. Хеширование сообщений	6	2	4		6	Опрос, Защита отчета по лаб. работе
9.3	Тема 22. Рассмотрение и анализ основных типов ЭЦП.	4	2	2		8	Опрос, тест
10.	**Раздел 10. Стеганографические и иные методы защиты информации**	**16**	**8**	**8**		**16**	
10.1	Тема 23. Сущность, принципы функционирования и модели стеганосистем	2	2			4	Опрос, тест
10.2	Тема 24. Текстовая стеганография	6	2	4		4	Опрос, Защита отчета по лаб. работе
10.3	Тема 25. Графическая стеганография	4	2	2		4	Опрос, Защита отчета по лаб. работе
10.4	Тема 26. Защита кодов программ методами обфускации	4	2	2		4	Опрос, Защита отчета по лаб. работе
11.	**Раздел 11. Защита ИС от деструк-**	**8**	**4**	**4**		**7**	

	тивных программных средств						
11.1	Тема 27. Классификация и принципы действия деструктивных программ. Компьютерные вирусы	4	2	2		3	Опрос, Защита отчета по лаб. работе
11.2	Тема 28. Парольная защита ИВС. Идентификация и проверка подлинности	3	1	2		2	Опрос, Защита отчета по лаб. работе
11.3	Тема 29. Основные итоги изучения дисциплины. Направления разработки новых средств повышения надежности и безопасности ИС	1	1		+	2	Опрос, тест
	Всего за семестр	**70**	**36**	**36**		**66**	
	ВСЕГО по дисциплине	**140**	**70**	**70**		**98**	

5. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Оценка учебных достижений студентов, выполняемая поэтапно по конкретным модулям учебной дисциплины, осуществляется кафедрой в соответствии с учебным планом:

семестровые: зачет, экзамен, курсовая работа.

текущие:

1) коллоквиум,
2) письменные контрольные работы,
3) устный опрос,
4) защита лабораторных работ,
5) проведение текущих опросов по отдельным разделам (темам) дисциплины,
6) критериально-ориентированные компьютерные тесты по отдельным разделам (темам) дисциплины,
7) выступление студента по разработанной им теме,
8) решение проблемных (творческих) задач, предполагающих неформализованный ответ.

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ УСР

Управляемая самостоятельная работа предусматривает выполнение студентом заданий в соответствии с программой дисциплины, а также выполнение контрольных заданий, примерный состав которых приводится ниже.

ПРИМЕРЫ КОНТРОЛЬНЫХ ЗАДАНИЙ

Контрольные задания по теме «Криптографические методы повышения информационной безопасности»

Вариант 1

1. Укажите, какое из утверждений верно: функция Эйлера $\varphi(n)$ указывает 1) количество положительных целых чисел меньших n, 2) количество простых чисел меньших n и взаимно простых с n для любого $n > 1$, 3) количество взаимно простых чисел меньших n, 4) количество положительных чисел меньших n и взаимно простых с n для любого $n > 1$.
2. Перечислите требования (не менее 5), предъявляемые к современным системам криптографической защиты информации.
3. Используя любой из известных вам подстановочных методов (название метода в решении указать) зашифруйте сообщение «ВЫЛЕТАЮ ПЯТОГО».
4. Разбейте, приведенное множество криптографических методов на две группы: 1) симметричные методы, 2) ассиметричные методы. Методы: RSA, DES, IDEA, ГОСТ28147-89, схема шифрования Эль Гамаля.
5. Поясните сущность основных методов вычисления обратных значений по модулю n.
6. Охарактеризуйте в чем заключается основное отличие блочных и потоковых шифров.
7. Укажите, какие из приведенных наборов чисел являются взаимно простыми: 1) 8, 15; 2) 6, 8, 9; 3) 8, 15, 49.

Вариант 2

1. Чему равно значение функции Эйлера для следующих предложенных вариантов: 1) $\varphi(1)$, 2) $\varphi(11)$, 3) $\varphi(3)$, 4) $\varphi(5)$, 5) $\varphi(121 \cdot 119)$.
2. Перечислите основные задачи, составляющие проблематику современной криптографии.
3. Используя любой из известных вам перестановочных методов (название метода в решении указать) зашифруйте сообщение «ВЫЛЕТАЮ ШЕСТОГО».
4. Разбейте, приведенное множество методов на две группы: 1) подстановочные методы, 2) перестановочные методы. Методы: шифр Цезаря, магические квадраты, шифр Трисемиуса, шифрующие таблицы, шифр Плейфера.
5. Поясните суть проблемы дискретного логарифма.
6. Поясните, в чем состоят основные различия методов симметричного и ассиметричного криптопреобразования.

Укажите, какие из наборов натуральных чисел являются попарно взаимно простыми: 1) 2, 7, 11; 2) 6, 8, 9; 3) 8, 15, 49; 4) 2,

Триумф, 2003.

ПРИМЕРНАЯ ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

1. Энтропия Шеннона и Хартли.
2. Количество информации в сообщениях на основе произвольного алфавита.

3. Подготовка приложения для оценки количества информации.
4. Избыточный код Хемминга.
5. Подготовка приложения для изучения и технологии применения кода.
6. Расчет надежностных параметров канала передачи с использованием кода.
7. Изучение методов сжатия данных.
8. Подготовка приложения для изучения и анализа статистических методов сжатия.
9. Исследование методов сжатия на основе созданного приложения.
10. Асимметричные криптосистемы.
11. Подготовка приложения для изучения и анализа ЭЦП.
12. Генерация ЭЦП и идентификация электронного документа.
13. Практика внедрения закрытых данных в электронный документ.
14. Подготовка приложения для изучения и анализа стеганографических методов..
15. Исследование стеганографических методов на основе созданного приложения.
16. Изучение особенностей системы Kerberos.
17. Программная реализация обфускатора и деобфускатора.
18. Выполнение контрольных заданий.

ЛИТЕРАТУРА

Основная

1. 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.

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

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

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

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

5. Урбанович, П. П. Надежность полупроводниковых интегральных микросхем памяти / В. Ф. Алексеев, Е. А. Верниковский. – Мн.: Наука и техника, 1992.

6. Черкесов, Г. Н. Надежность аппаратно-программных комплексов / Г. Н. Черкесов. – Питер, 2005.

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.