МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сыктывкарский лесной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный лесотехнический университет имени С. М. Кирова»

Кафедра информационных систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебно-методический комплекс по дисциплине
для студентов специальности
230201 "Информационные системы и технологии"
всех форм обучения

Самостоятельное учебное электронное издание

Сыктывкар 2012

УДК 004
ББК 67.404.3
И74

Рекомендован к изданию в электронном виде кафедрой информационных систем Сыктывкарского лесного института

Утвержден к изданию в электронном виде советом технологического факультета Сыктывкарского лесного института

С о с т а в и т е л ь :
Асадуллин Ф. Ф., доктор физико-математических наук, профессор

Ответственный редактор:
Лавреш И. И., к.т.н., заведующий кафедрой информационные системы

И74 **Информационная безопасность и защита информации** [Электронный ресурс] : учеб.-метод. комплекс по дисциплине для студентов специальности 230201 "Информационные системы и технологии" всех форм обучения : самост. учеб. электрон. изд. / Сыкт. лесн. ин-т ; сост.: Ф. Ф. Асадуллин. – Электрон. дан. – Сыктывкар : СЛИ, 2012. – Режим доступа: http://lib.sfi.komi.com. – Загл. с экрана.

В издании помещены материалы для освоения дисциплины «Информационная безопасность и защита информации». Приведены рабочая программа курса, методические указания по различным видам работ.

УДК 004
ББК 67.404.3

Самостоятельное учебное электронное издание

Составитель: **Асадуллин** Фанур Фаритович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Электронный формат – pdf. Объем 0,9 уч.-изд. л.
Сыктывкарский лесной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный лесотехнический университет имени С. М. Кирова» (СЛИ),
167982, г. Сыктывкар, ул. Ленина, 39, institut@sfi.komi.com, www.sli.komi.com

Редакционно-издательский отдел СЛИ.

СОДЕРЖАНИЕ

1. ВЫПИСКА ИЗ ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА СПЕЦИАЛЬНОСТИ

1.1. Общие требования к основной образовательной программе

1.1.1. Основная образовательная программа подготовки инженера разрабатывается на основании настоящего государственного образовательного стандарта и включает в себя учебный план, программы учебных дисциплин, программы учебных и производственных практик.

1.1.2. Требования к обязательному минимуму содержания основной образовательной программы подготовки инженера, к условиям ее реализации и срокам ее освоения определяются настоящим государственным образовательным стандартом.

1.1.3. Основная образовательная программа подготовки инженера состоит из дисциплин федерального компонента, дисциплин национально-регионального (вузовского) компонента, дисциплин по выбору студента, а также факультативных дисциплин. Дисциплины вузовского компонента и по выбору студента в каждом цикле должны содержательно дополнять дисциплины, указанные в федеральном компоненте цикла.

1.1.4. Основная образовательная программа подготовки инженера должна предусматривать изучение студентом следующих циклов дисциплин:

- цикл ГСЭ – Общие гуманитарные и социально-экономические дисциплины;
- цикл ЕН – Общие математические и естественнонаучные дисциплины;
- цикл ОПД – Общепрофессиональные дисциплины;
- цикл СД – Специальные дисциплины, включая дисциплины специализации;
- ФТД – Факультативные дисциплины.

1.1.5. Содержание национально-регионального компонента основной образовательной программы подготовки инженера должно обеспечивать подготовку выпускника в соответствии с квалификационной характеристикой, установленной настоящим государственным образовательным стандартом.

2. ВЫПИСКА ИЗ ФГОС С ТРЕБОВАНИЯМИ ПО ДИСЦИПЛИНЕ

Общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Сыктывкарский лесной институт (филиал)
федерального государственного бюджетного образовательного
учреждения высшего профессионального образования
«Санкт-Петербургский государственный
лесотехнический университет имени С. М. Кирова»
(СЛИ)

СОГЛАСОВАНО
Декан технологического факультета
_____А.А. Самородницкий

"_____"_____2012 г.

УТВЕРЖДАЮ
Зам. директора по учебной и научной работе
_____Л.А. Гурьева

"_____"_____2012 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине: **“Информационная безопасность и защита информации”**
Обязательная

Для направления подготовки дипломированного специалиста
230000 "Информатика и вычислительная техника" специальности
230201 "Информационные системы и технологии"

Кафедра информационные системы

Очная форма		Очно-заочная форма		заочная форма.	
Курс 4		Курс 5		Курс 5	
Семестр 7		Семестр 10		Семестр 10	
Всего часов	136	Всего часов	136	Всего часов	136
В том числе	68	В том числе	40	В том числе	18
аудиторных:		аудиторных:		аудиторных:	
из них:		из них:		из них:	
лекции	34	лекции	20	лекции	10
лабораторные	34	лабораторные	20	лабораторные	8
Самостоятельная работа	68	Самостоятельная работа	96	Самостоятельная работа	118
Контрольная работа 7 семестр				Контрольная работа 5 курс	
Экзамен 7 семестр		Экзамен 10 семестр		Экзамен 5 курс	

Сыктывкар 2012

Рабочая программа составлена в соответствии с Государственным образовательным стандартом высшего профессионального образования для подготовки дипломированного специалиста по направлению подготовки 230000 "Информатика и вычислительная техника" специальности 230201 "Информационные системы и технологии"

Программу составил: доктор физико-математических наук, профессор кафедры Сыктывкарского лесного института Санкт-Петербургского государственного лесотехнического университета Ф. Ф. Асадуллин, г. Сыктывкар

Переработанная учебная программа обсуждена на заседании кафедры Информационных систем
Протокол № 9 от 11.05.2012

Заведующий кафедрой _____И. И. Лавреш

Учебная программа рассмотрена и одобрена методической комиссией технологического факультета.
Протокол № ____ от _____ 20 г.

Председатель комиссии: _____А. А. Самородницкий

Библиографический список рабочей программы полностью соответствует сведениям книгообеспеченности образовательного процесса СЛИ

_____И. И. Лавреш

1. Цели и задачи дисциплины, и ее место в учебном процессе

1.1. Основные цели преподавания дисциплины

Основными целями преподавания дисциплины являются:

- изучение методов построения технических средств защиты объектов и информации;
- изучение методов защиты автоматизированных систем обработки данных от несанкционированного доступа к информации;
- изучение математических и методических средств защиты;
- изучение законодательных мер по защите информации.

1.2. Задачи изучения дисциплины.

В результате изучения дисциплины студенты должны

ЗНАТЬ:

- основные устройства и системы защиты объектов и информации;
- основные типы методов, устройств и систем технической разведки;
- методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе:
  - специальные технические средства опознавания пользователя ПЭВМ;
  - специальное программное обеспечение по защите информации ПЭВМ;
  - специальные средства защиты от несанкционированного доступа;
  - организацию вычислительных работ, минимизирующую риск потери информации.

УМЕТЬ:

- применять парольную идентификацию;
- применять средства шифрования информации;
- применять средства защиты от несанкционированного копирования программных продуктов;
- использовать программное обеспечение для надежного уничтожения информации;
- создавать архивы;
- применять программное обеспечение для защиты от "вирусов";
- организовать вычислительную работу с минимумом риска потери информации.

БЫТЬ ОЗНАКОМЛЕНЫ:

- с техническими средствами разведки, защиты информации и противодействия коммерческой разведке;
- законодательными мерами по защите информации.

1.3. Перечень дисциплин и тем, усвоение которых студентами необходимо для изучения данной дисциплины

Для полноценного усвоения учебного материала по дисциплине "Информационная безопасность и защита информации" студентам необходимо иметь прочные знания по технологии программирования, теории вычислительных сетей, информационным технологиям.

1.4. Нормы государственного стандарта

Общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.

2. Содержание дисциплины

2.1. Наименование тем, их содержание, объем в часах лекционных занятий

№ № п/п	Темы лекции, краткое содержание	Количество часов
Раздел 1. Общая проблема информационной безопасности информационных систем. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа.		
1	**Концепция информационной безопасности.** Концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией.	2
2	**Направления обеспечения информационной безопасности.** Правовая защита. Организационная защита. Инженерно-техническая защита.	2
3	**Способы защиты информации.** Общие положения. Характеристика защитных действий.	2
4	**Пресечение разглашения конфиденциальной информации.** Общие положения. Способы пресечения разглашения.	2
5	**Защиты информации от утечки по техническим каналам.** Общие положения. Защита информации от утечки по визуально-оптическим, акустическим, электромагнитным и материально-вещественным каналам.	2
6	**Противодействие несанкционированному доступу к конфиденциальной информации.** Способы несанкционированного доступа к конфиденциальной информации. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. Противодействие незаконному подключению к линиям связи. Защита от перехвата.	2
Раздел 2. Математические и методические средства защиты информации. Компьютерные средства реализации защиты в информационных системах.		
1	**Основные понятия теории защиты информации.** Базовая терминология. Основные алгоритмы шифрования. Цифровые подписи, криптографические хэш-функции и генераторы случайных чисел. Шифровальный алгоритм, симметричные криптоалгоритмы. Скремблеры. Блочные шифры. Сеть Фейштеля. Блочный шифр TEA. Криптоанализ и атаки на криптосистемы, функции криптосистем и алгоритмы создания цепочек. Методы рандомизации сообщений. Архивация. Транспортное кодирование. Асимметричные криптоалгоритмы. Алгоритм RSA. Технологии цифровых подписей. Механизм распространения открытых ключей. Обмен ключами по алгоритму Диффи-Хеллмана.	4
2	**Защита информации.** Хеши. Табличное реверсирование. Алгоритмы генерации. Области применения хэш-функций. Шифрование в каналах связи компьютерной сети. Шифрование файлов. Аппаратное и программное шифрование.	4
3	**Криптосистемы с открытым ключом.** Предыстория и основные идеи. Первая система с открытым ключом - система Диффи-Хеллмана. Элементы теории чисел. Шифр Шамира. Шифр Эль-Гамаля. Одностороння функция с	4

	«лазейкой» и шифр RSA.	
4	**Электронная, или цифровая подпись.** Электронная подпись RSA. Электронная подпись на базе шифра Эль-Гамаля. Стандарты на электронную (цифровую) подпись.	4
5	**Современные шифры с секретным ключом.** Введение. Блоковые шифры: шифр ГОСТ 28147-89; шифр RC6; шифр Rijndael (AES). Основные режимы функционирования блоковых шифров: режим ECB; режим CBC. Потоковые шифры: режим OFB блокового шифра; режим CTR блокового шифра; алгоритм R.C4. Криптографические хеш-функции.	2
6	**Сетевая безопасность.** Сервера. Рабочие станции. Среда передачи информации. Узлы коммутации сетей. Уровни сетевых атак согласно модели OSI.	2
7	**Программное обеспечение и информационная безопасность.** Операционные системы. Прикладные программы. Ошибки, приводящие к возможности атак на информацию. Основные положения по разработке программного обеспечения.	2
8	**Комплексная система безопасности.** Классификация информационных объектов. Политика ролей. Создание политики информационной безопасности. Методы обеспечения безотказности.	2
Всего часов		34 ч.

2.2. Лабораторные занятия, их наименование, краткое содержание и объем в часах

№ п/п	Темы практических занятий	Кол-во часов
Программа информационной безопасности России и пути ее реализации. Криптографическая система PGP.		
1	**Программа информационной безопасности России и пути ее реализации.** Виды и источники угроз информационной безопасности РФ. Состояние и методы обеспечения информационной безопасности РФ. Особенности обеспечения информационной безопасности РФ. Международное сотрудничество РФ в области обеспечения информационной безопасности. Основные положения государственной политики обеспечения и первоочередные мероприятия по реализации информационной безопасности РФ. Основные элементы и функции системы информационной безопасности РФ.	6
2	**Криптографическая система PGP.** Принцип работы. Установка и использование. Шифрование сообщения для нескольких адресатов. Подписание сообщения и шифрование. Использование стандартного шифрования. Дешифровка и проверка подписей. Работа с ключами. Генерация ключа RSA. Защита открытые ключи от подделки. Проверка корректности ключей системой PGP. Установка параметров конфигурации. Справочник команд.	10
Криптографическая система PGP. Криптографическая система Microsoft Cryptographic Application Programming Interface (CryptoAPI).		
1	**Криптографическая система PGP 5.0.** Использование PGP в Linux. Как работает криптография открытого ключа. Версии PGP для различных дистрибутивов Linux. Установка и конфигурация. Работа с ключами. Как подписывается сообщение. Декодирование. Обработка текстовых файлов. «Отпечатки (fingerprints)». Шифрование электронной почты и файлов. PGP	2

	Enterprise Security 3.0.	
2	**Криптографическая система Microsoft Cryptographic Application Programming Interface (CryptoAPI).** Криптографические интерфейсы. Общие положения. Особенности внешнего разделяемого сервиса безопасности. Microsoft Cryptographic Application Programming Interface (CryptoAPI). Обзор функции CryptoAPI 1.0. Принципы реализации интерфейса вызовов CryptoAP11.0. Получение информации о криптопровайдерах, установленных в системе. Использование CryptoAPI для обмена защищенными сообщениями. Использование CryptoAPI 1.0 для реализации схемы симметричного шифрования. Использование CryptoAPI 1.0 для реализации схем несимметричного шифрования и схемы цифровой подписи.	12
3	**Решение задач по криптографическим методам защиты информации.**	4

Всего часов 34 ч.

Содержание и методика выполнения лабораторных работ приведены в методических указаниях.

2.3. Самостоятельная работа и контроль успеваемости

(очная форма обучения)

Вид самостоятельной работы	Число часов	Вид контроля успеваемости
1. Проработка лекционного материала по конспекту	30	Экзамен
2. Подготовка к лабораторным занятиям	21	КО, КР, ТФП
3. Подготовка к экзамену	17	Экзамен
Всего	68	

(очно-заочная форма обучения)

Вид самостоятельной работы	Число часов	Вид контроля успеваемости
1. Проработка лекционного материала по конспекту	22	Экзамен
2. Подготовка к лабораторным занятиям	14	КО, ЛР, ТФП
3. Изучение материала, не рассматриваемого на лекциях	31	КО
4. Подготовка к экзамену	29	Экзамен
Всего	96	

(заочная форма обучения)

Вид самостоятельной работы	Число часов	Вид контроля успеваемости
1. Проработка лекционного материала по конспекту	34	Экзамен
2. Подготовка к лабораторным занятиям	24	КО, ЛР, ТФП
3. Изучение материала, не рассматриваемого на лекциях	31	КО
4. Подготовка к экзамену	29	Экзамен
Всего	118	

Текущая успеваемость контролируется контрольным опросом на лекциях, учетом выполнения лабораторных работ, тестовой формой проверки по темам на лекциях.

2.4.Распределение часов по темам и видам занятий.

(очная форма обучения)

№ раздела	Объем работы студента, ч.				Форма Контроля успеваемости
темы дисциплины	Лекции	Лабор. зан.	Самост. работа	Всего	
1. Концепция информационной безопасности	2	0	2	4	-
2. Направления обеспечения информационной безопасности	2	0	3	5	КО, зачет
3. Способы защиты информации	2	0	3	5	КО, зачет
4. Пресечение разглашения конфиденциальной информации	2	0	2	4	КО, зачет
5. Защита информации от утечки по техническим каналам	2	0	3	5	КО, зачет
6. Противодействие несанкционированному доступу к конфиденциальной информации	2	0	3	5	КО, зачет
7. Основные понятия теории защиты информации	2	0	3	5	КО, зачет
8. Защита информации	2	0	3	5	КО, зачет
9. Криптосистемы с открытым ключом	2	0	3	5	КО, зачет
10. Электронная, или цифровая подпись	2	0	3	5	КО, зачет
11. Современные шифры с секретным ключом	2	0	3	5	КО, зачет
12. Сетевая безопасность	2	0	3	5	КО, зачет
13. Программное обеспечение и информационная безопасность	2	0	3	5	КО, зачет
14. Комплексная система безопасности	2	0	3	5	КО, зачет
15. Программа информационной безопасности России и пути ее реализации	2	6	3	11	КО, ТФП
16. Криптографическая система PGP	2	10	5	17	ЛП, ТФП
17. Криптографическая система PGP 5.0	0	2	3	5	ЛП, ТФП
18. Криптографическая система CryptoAPI	0	12	6	18	ЛП, ТФП
19. Решение задач по криптографическим методам защиты информации	0	4	2	6	ЛП, ТФП
20. Подготовка к экзамену			9	9	
Всего:	34	34	68	136	экзамен

(очно-заочная форма обучения)

№ раздела	Объем работы студента, ч.				Форма контроля успеваемости
темы дисциплины	Лекции	Лабор. зан.	Самост. работа	Всего	
1. Концепция информационной безопасности	2	0	2	4	-
2. Направления обеспечения информационной безопасности	2	0	2	4	КО, зачет
3. Способы защиты информации	2	0	2	4	КО, зачет
4. Пресечение разглашения конфиденциальной информации	2	0	3	5	КО, зачет
5. Защита информации от утечки по техническим каналам	2	0	3	5	КО, зачет
6. Противодействие несанкционированному доступу к конфиденциальной информации	2	0	3	5	КО, зачет
7. Основные понятия теории защиты информации	2	0	3	5	КО, зачет
8. Защита информации	2	0	3	5	КО, зачет
9. Криптосистемы с открытым ключом	2	0	3	5	КО, зачет
10. Электронная, или цифровая подпись		0	6	6	КО, зачет
11. Современные шифры с секретным ключом	2	0	3	5	КО, зачет
12. Сетевая безопасность	0	0	6	6	КО, зачет
13. Программное обеспечение и информационная безопасность	0	0	3	3	КО, зачет
14. Комплексная система безопасности	0	0	6	6	КО, зачет
15. Программа информационной безопасности России и пути ее реализации	0	3	3	6	КО, ТФП
16. Криптографическая система PGP	0	6	5	11	ЛП, ТФП
17. Криптографическая система PGP 5.0	0	1	3	4	ЛП, ТФП
18. Криптографическая система CryptoAPI	0	8	5	13	ЛП, ТФП
19. Решение задач по криптографическим методам защиты информации	0	2	3	5	ЛП, ТФП
20. Подготовка к экзамену			29	29	
Всего:	20	20	96	136	экзамен

(заочная форма обучения)

№ раздела	Объем работы студента, ч.				Форма контроля успеваемости
темы дисциплины	Лекции	Лабор. зан.	Самост. работа	Всего	
1. Концепция информационной безопасности	1	0	3	4	-
2. Направления обеспечения информационной безопасности	1	0	3	4	КО, зачет
3. Способы защиты информации	1	0	3	4	КО, зачет
4. Пресечение разглашения конфиденциальной информации	1	0	4	5	КО, зачет
5. Защита информации от утечки по техническим каналам	1	0	4	5	КО, зачет
6. Противодействие несанкционированному доступу к конфиденциальной информации	1	0	4	5	КО, зачет
7. Основные понятия теории защиты информации	1	0	4	5	КО, зачет
8. Защита информации	1	0	4	5	КО, зачет
9. Криптосистемы с открытым ключом	1	0	4	5	КО, зачет
10. Электронная, или цифровая подпись		0	6	6	КО, зачет
11. Современные шифры с секретным ключом	1	0	4	5	КО, зачет
12. Сетевая безопасность	0	0	6	6	КО, зачет
13. Программное обеспечение и информационная безопасность	0	0	4	4	КО, зачет
14. Комплексная система безопасности	0	0	6	6	КО, зачет
15. Программа информационной безопасности России и пути ее реализации	0	0	4	4	КО, ТФП
16. Криптографическая система PGP	0	2	5	7	ЛП, ТФП
17. Криптографическая система PGP 5.0	0		3	3	ЛП, ТФП
18. Криптографическая система CryptoAPI	0	4	5	9	ЛП, ТФП
19. Решение задач по криптографическим методам защиты информации	0	2	3	5	ЛП, ТФП
20. Подготовка к экзамену			29	29	
Всего:	10	8	118	136	экзамен

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная учебная литература

1. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студ. вузов, обучающихся по спец. "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 6-е изд., стер. – Москва : Академия, 2012. – 336 с. – (Высшее профессиональное образование).

Дополнительная учебная, учебно-методическая литература

1. Аверченков, В. И. Организационная защита информации [Электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков ; Университетская библиотека онлайн (ЭБС). – Москва : Флинта, 2011. – 184 с. – (Организация и технология защиты информации). – Режим доступа: http://www.biblioclub.ru/book/93343/.

2. Барнс, К. Защита от хакеров беспроводных сетей [Электронный ресурс] / К. Барнс ; Университетская библиотека онлайн (ЭБС). – [Б. м.] : ДМК Пресс, Б. г. – 478 с. – (Информационная безопасность). – Режим доступа: http://www.biblioclub.ru/book/85095/.

3. Башлы, П. Н. Информационная безопасность [Электронный ресурс] : учеб.-практ. пособие для студ. вузов / П. Н. Башлы ; Университетская библиотека онлайн (ЭБС). – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: http://www.biblioclub.ru/book/90539/.

4. Расторгуев, С. П. Основы информационной безопасности [Текст] : учеб. пособие для студ. вузов, обучающихся по спец. "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" и "Информационная безопасность телекоммуникационных систем" / С. П. Расторгуев. – 2-е изд., стер. – Москва : Академия, 2009. – 192 с. – (Высшее профессиональное образование).

5. Фостер, Д. Защита от взлома: сокеты, эксплойты, shell-код [Электронный ресурс] / Д. Фостер ; Университетская библиотека онлайн (ЭБС). – [Б. м.] : ДМК Пресс, Б. г. – 784 с. – (Информационная безопасность). – Режим доступа: http://www.biblioclub.ru/book/85068/.

6. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : учеб. пособие для студ. вузов / В. Ф. Шаньгин ; Университетская библиотека онлайн (ЭБС). – Москва : ДМК Пресс, 2010. – 544 с. – Режим доступа: http://www.biblioclub.ru/book/86475/.

7. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Электронный ресурс] : учеб. пособие для студ. вузов / А. Ю. Щербаков ; Университетская библиотека онлайн (ЭБС). – Москва : Книжный мир, 2009. – 352 с. – (Высшая школа). – Режим доступа: http://www.biblioclub.ru/book/89798/.

Дополнительная литература

1. Technet magazine/ Русская версия [Текст] : microsoft для ИТ-профессионалов. – Выходит ежемесячно.

2008 № 8-10,12;

2. Защита персональных данных [Текст]. – Выходит ежемесячно.

2010 № 1-6.

5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

- Компьютерный класс, оснащенный современными персональными компьютерами.
- Операционная система не ниже Windows 98 с приложениями MS Office Word и MS Office Excel.
- Криптографическая система PGP (Pretty Good Privacy) фирмы Phil's Pretty Good Software.
- Криптографический модуль операционной системы Microsoft Cryptographic Application Programming Interface (CryptoARI) и ее версии (CryptoARI 2.0).

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ СТУДЕНТАМ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

6.1. Методические указания по самостоятельному изучению лекций

Самостоятельная работа студентов по изучению отдельных тем дисциплины включает поиск учебных пособий по данному материалу, проработку и анализ теоретического материала, самоконтроль знаний по данной теме с помощью нижеприведенных контрольных вопросов и заданий.

6.2. Методические рекомендации по самостоятельной подготовке к лабораторным работам

Самостоятельная работа студентов по подготовке к лабораторным работам, оформлению отчетов и защите лабораторных работ включает проработку и анализ теоретического материала, описание проделанной экспериментальной работы с приложением таблиц, запросов, а и также самоконтроль знаний по теме лабораторной работы с помощью нижеприведенных контрольных вопросов и заданий.

7. МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ ЗНАНИЙ СТУДЕНТОВ

7.1. Промежуточный контроль

Текущая успеваемость студентов контролируется выполнением, оформлением и защитой отчетов по лабораторным работам, промежуточной аттестацией в виде контрольной работы. Контрольные вопросы для аттестации включают: теоретический материал, пройденный на лекциях, практический материал по лабораторным работам.

7.2. Итоговый контроль

Вопросы к экзамену

Основные

1. Основные концептуальные положения системы защиты информации.
2. Концептуальная модель информационной безопасности.
3. Угрозы конфиденциальной информации.
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
5. Направления обеспечения информационной безопасности. Правовая защита.
6. Направления обеспечения информационной безопасности. Организационная защита.
7. Направления обеспечения информационной безопасности. Инженерно-техническая защита.
8. Способы защиты информации. Общие положения.
9. Способы защиты информации. Характеристика защитных действий.
10. Пресечение разглашения конфиденциальной информации. Общие положения.
11. Пресечение разглашения конфиденциальной информации. Способы пресечения разглашения.
12. Защиты информации от утечки по техническим каналам. Общие положения.
13. Защита информации от утечки по визуально-оптическим каналам.
14. Защита информации от утечки по акустическим каналам.
15. Защита информации от утечки по электромагнитным каналам.
16. Защита информации от утечки по материально-вещественным каналам.
17. Способы несанкционированного доступа к конфиденциальной информации.
18. Технические средства несанкционированного доступа к информации.
19. Противодействие несанкционированному доступу к конфиденциальной информации. Защита от наблюдения и фотографирования.
20. Противодействие несанкционированному доступу к конфиденциальной информации. Защита от подслушивания.
21. Противодействие незаконному подключению к линиям связи.
22. Противодействие несанкционированному доступу к конфиденциальной информации. Защита от перехвата.
23. Основные понятия теории защиты информации. Базовая терминология. Основные алгоритмы шифрования.
24. Цифровые подписи, криптографические хэш-функции и генераторы случайных чисел.
25. Шифровальный алгоритм, симметричные криптоалгоритмы. Скремблеры. Блочные шифры. Сеть Фейштеля. Блочный шифр TEA

26. Криптоанализ и атаки на криптосистемы, функции криптосистем и алгоритмы создания цепочек.

27. Методы рандомизации сообщений.

28. Архивация. Транспортное кодирование.

29. Асимметричные криптоалгоритмы. Алгоритм RSA. Технологии цифровых подписей. Механизм распространения открытых ключей. Обмен ключами по алгоритму Диффи-Хеллмана.

30. Защита информации. Хеши.

31. Защита информации. Табличное реверсирование.

32. Защита информации. Алгоритмы генерации.

33. Области применения хэш-функций.

34. Шифрование в каналах связи компьютерной сети.

35. Шифрование файлов.

36. Аппаратное и программное шифрование.

37. Криптосистемы с открытым ключом. Предыстория и основные идеи.

38. Первая система с открытым ключом - система Диффи-Хеллмана.

39. Элементы теории чисел.

40. Шифр Шамира.

41. Шифр Эль-Гамаля.

42. Одностороння функция с «лазейкой» и шифр RSA.

43. Электронная подпись RSA.

44. Электронная подпись на базе шифра Эль-Гамаля.

45. Стандарты на электронную (цифровую) подпись.

46. Современные шифры с секретным ключом. Введение.

47. Блоковые шифры: шифр ГОСТ 28147-89; - шифр RC6; - шифр Rijndael (AES).

48. Основные режимы функционирования блоковых шифров: режим ECB; режим CBC.

49. Потоковые шифры: режим OFB блокового шифра; режим CTR блокового шифра; алгоритм R.C4.

50. Криптографические хеш-функции.

51. Сетевая безопасность. Серверы.

52. Сетевая безопасность. Рабочие станции.

53. Сетевая безопасность. Среда передачи информации.

54. Сетевая безопасность. Узлы коммутации сетей.

55. Сетевая безопасность. Уровни сетевых атак согласно модели OSI

55. Программное обеспечение и информационная безопасность. Операционные системы.

56. Программное обеспечение и информационная безопасность. Прикладные программы.

57. Информационная безопасность. Ошибки, приводящие к возможности атак на информацию.

58. Информационная безопасность. Основные положения по разработке программного обеспечения.

59. Комплексная система безопасности.

60. Комплексная система безопасности. Классификация информационных объектов.

61. Комплексная система безопасности. Политика ролей.

62. Создание политики информационной безопасности.

63. Комплексная система безопасности. Методы обеспечения безотказности.

Дополнительные

1. Информационная безопасность Российской Федерации.

2. Виды угроз информационной безопасности Российской Федерации.

3. Источники угроз информационной безопасности Российской Федерации.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

5. Общие методы обеспечения информационной безопасности Российской Федерации.

6. Особенности обеспечения информационной безопасности Российской федерации в различных сферах общественной жизни.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.

10. Основные функции системы обеспечения информационной безопасности Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

12. Криптографическая система PGP. Принцип работы. Установка и использование.

13. Криптографическая система PGP. Шифрование сообщения для нескольких адресатов.

14. Криптографическая система PGP. Подписание сообщения и шифрование.

15. Криптографическая система PGP. Дешифровка и проверка подписей.

16. Криптографическая система PGP. Работа с ключами. Генерация ключа RSA.

17. Криптографические интерфейсы. Общие положения.

18. Особенности внешнего разделяемого сервиса безопасности.

19. Microsoft Cryptographic Application Programming Interface (CryptoAPI).

20. Обзор функции CryptoAPI 1.0.

21. Принципы реализации интерфейса вызовов CryptoAP11.0.

22. Получение информации о криптопровайдерах, установленных в системе.

23. Использование CryptoAPI для обмена защищенными сообщениями.

24. Использование CryptoAPI 1.0 для реализации схемы симметричного шифрования.

25. Использование CryptoAPI 1.0 для реализации схем несимметричного шифрования.

26. Использование CryptoAPI 1.0 для реализации схемы цифровой подписи.

7.3. Критерии оценки знаний студентов

Оценка "**отлично**" выставляется студенту за:

а) глубокое усвоение программного материала по всем разделам курса, изложение его на высоком научно-техническом уровне.

б) ознакомление с дополнительной литературой и передовыми научно-техническими достижениями в области производства пищевой продукции;

в) умение творчески подтвердить теоретические положения процессов и расчета аппаратов соответствующими примерами, умелое применение теоретических знаний при решении практических задач.

Оценка "**хорошо**" выставляется студенту за:

а) полное усвоение программного материала в объеме обязательной литературы по курсу;

б) владение терминологией и символикой изучаемой дисциплины при изложении материала:
в) умение увязывать теоретические знания с решением практических задач;
г) наличие не искажающих существа ответа погрешностей и пробелов при изложении материала.

Оценка "**удовлетворительно**" выставляется студенту за:
а) знание основных теоретических и практических вопросов программного материала;
б) допущение незначительных ошибок и неточностей, нарушение логической последовательности изложения материала, недостаточную аргументацию теоретических положений.

Оценка "**неудовлетворительно**" выставляется студенту за:
а) существенные пробелы в знаниях основного программного материала.
б) недостаточный объем знаний по дисциплине для дальнейшей учебы и профессиональной деятельности.