МИНОБРНАУКИ РОССИИ

**Орский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования «Оренбургский государственный университет»
(Орский гуманитарно-технологический институт (филиал) ОГУ)**

Кафедра программного обеспечения

Методические указания по выполнению и защите лабораторных работ по дисциплине «Б1.Д.Б.20 Информационная безопасность»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.03 Прикладная информатика

(код и наименование направления подготовки)

Прикладная информатика в экономике

(наименование направленности (профиля) образовательной программы)

Тип образовательной программы

Программа бакалавриата

Квалификация

Бакалавр

Форма обучения

Очная

Год начала реализации программы (набора)

2019

г. Орск 2018

Методические указания предназначены для обучающихся очной формы обучения направления подготовки 09.03.03 Прикладная информатика профилю Прикладная информатика в экономике по дисциплине «Б1.Д.Б.20 Информационная безопасность»

Составитель _____ В.С. Богданова
_____ О.В. Подсобляева

Методические указания рассмотрены и одобрены на заседании кафедры программного обеспечения, протокол № 1 от «01» сентября 2018 г.

Заведующий кафедрой _____ Е.Е. Сурина

Согласовано:
Председатель методической комиссии по направлению подготовки 09.03.03 Прикладная информатика

_____ Е.Е.Сурина
«12» сентября 2018 г.

Пояснительная записка

В результате изучения дисциплины «Б1.Д.Б.20 Информационная безопасность» у обучающихся должны быть сформированы знания, умения и навыки:

- изучение программно-аппаратных средств защиты информации, методов анализа и планирования информационной защиты компьютерных систем, сетей и их компонентов, средств защиты сетевых служб;
- формирование базовых знаний в области информационной защиты телекоммуникационных и компьютерных систем и сетей на основе современных программных и операционных систем.

Одной из наиболее эффективных форм закрепления теоретических знаний и выработки навыков самостоятельной работы являются лабораторные занятия.

Целью проведения лабораторных занятий является:

- закрепление знаний студентов по основам проектной деятельности.
- формирование у студентов навыков использования современных технических средств и технологий для решения проектных и исследовательских задач.

Тематический план

Таблица 1 – Тематический план выполнения лабораторных работ по дисциплине «Б1.Д.Б.20 Информационная безопасность» для обучающихся направления подготовки 09.03.03 Прикладная информатика профиль подготовки Прикладная информатика в экономике

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
№ 1	1	Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия	4
№ 2	2	Защищенная информационная система. Уровни и структура ИБ	4
№ 3	3	Модели и стандарты в сфере ИБ и управления рисками ИБ	4
№ 4	4	Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры	6
		Итого:	18

Методические указания по выполнению и оформлению лабораторных работ

Лабораторные работы по дисциплине «Информационная безопасность» предполагают решение задач по темам, представленным в тематическом плане.

В практической работе должны быть выполнены все предусмотренные задания. В работе должна просматриваться логическая последовательность и взаимная увязка основных частей работы.

Рекомендуемая структура лабораторных работ:

1) цель практической работы;

2) задание в соответствии с выбранным вариантом;

3) теоретическая часть, включающая краткое изложение теоретических положений по теме практической работы, формулы для решения задания;

4) практическая часть, включающая решение задания по теме практической работы. Дополнительно для наглядности расчетный материал может быть представлен в виде таблиц, графиков;

5) выводы по практической работе;

6) список использованной литературы.

Лабораторные работы могут быть оформлены:

- машинописным текстом на листах формата А4.

Титульный лист оформляется на основе СТО 02069024. 101 – 2014 «РАБОТЫ СТУДЕНЧЕСКИЕ. Общие требования и правила оформления».

Работа защищается устно и принимается к зачету, если нет замечаний по ее выполнению и оформлению. При отсутствии зачтенных лабораторных работ студент не допускается к зачету по дисциплине «Б1.Д.Б.20 Информационная безопасность».

Лабораторная работа №1 Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Порядок оформления:

1. Ознакомьтесь с описанием деятельности компании в соответствии с вашим вариантом.
2. Шрифт Tahoma 10. Интервал 1,5. Поля стандартные. Страницы работы должны быть пронумерованы. Формат документов MS Office полностью совместимым с версией 97-2003
3. Каждая таблица и рисунок должны быть пронумерованы и иметь название;
4. На каждую таблицу или рисунок должны быть ссылки из текста. При этом таблица или рисунок должны начинаться не далее следующей страницы;
5. Пункт не должен начинаться или заканчиваться списком, таблицей, рисунком;
6. Материал должен иметь четкую структуру изложения
7. Работы в электронном виде отправляются на ящик преподавателя. Тема письма «Практикум ИБ».
8. Крайний срок сдачи лабораторного практикума для проверке преподавателем за 3 календарных дня до проведения итогового мероприятия.
9. Работы, оформленные не в соответствии с требованиями или сданные после завершения срока сдачи работ, к защите не принимаются.

1. Ознакомление с представленными средства инструментального контроля

а) Изучение возможностей представленных средств контроля.

б) Проведение пробных проверок систем/компьютеров установленных в учебном классе.

в) Получение одного либо нескольких отчётов и подготовка предложений по устранению выявленных несоответствий.

2. Подготовка плана мероприятий по аудиту информационной безопасности

а) Выбор одной из представленных компаний.

б) Формулирование требований аудита на основании одного из стандартов информационной безопасности.

в) Разработка плана мероприятий с указанием сроков, подразделений и видов проверок для выбранной компании.

3. Разработка итогового отчёта по результатам аудита

а) Подготовка простейшей методики анализа результатов аудита.

б) Подготовка формы аудиторского отчёта с указанием персонала, его заполняющего, и плана проведения повторных проверок.

Варианты компаний:

1. Компания имеет 5 представительств, все пять в разных странах (.com, .ru и тд). Имеет 5 представительств в каждом от 50-100 чел. Головная компания 1000 чел в России. Отдел продаж в региональное представительство, административный отдел и отдел обработки данных. Направление деятельности компании - транснациональные грузовые перевозки.
2. Компания имеет одно представительство в России, которое является компанией, купленной годом ранее, занимающееся разработкой ПО. Головная компания до 500 чел. Представительство - до 300 чел. (Разные бренды). 2 домена – 2 бренда

3. Компания имеет головной офис со штатом 300 чел. Занимается продажей сотовых телефонов. По всей России 2000-3000 представительств – магазинах, есть упр. Менеджер (локальный отд. продаж) и тарифный отдел и отд. логистики.
4. Компания – 100 чел. Сфера деятельности аутсорсинг, услуги администрирования различных систем на базе Майкрософт. Клиенты в большинстве стран мира. Компания обеспечивает полную поддержку инфраструктуры клиента.
5. Компания состоит из 3-х филиалов на территории РФ. ЦО в Москве. Численность ЦО 100 чел., в филиалах 20 чел. Занимается производством и разработкой средств аутентификации. Производство в филиалах, ЦО выполняет только административные действия.
6. Компания - холдинг с центральным офисом в г. Москве. Занимается созданием и разработкой интернет сайтов и в неё входит ещё 4 компании, находящиеся в 4 странах мира. В каждой компании до 50 человек.

Лабораторная работа №2 Защищенная информационная система. Уровни и структура ИБ

Цель работы: Исследование структуры алгоритма и методики практической реализации криптосистемы шифрования Эль - Гамаля.

Основные теоретические положения:

Схема шифрования Эль - Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных. Безопасность схемы Эль - Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

При использовании алгоритма шифрования Эль - Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***M***.

В реальных схемах шифрования необходимо использовать в качестве модуля ***n*** большое простое число, имеющее в двоичном представлении длину ***512... 1024 бит***.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения ***k***, причём это значение должно выбираться случайным образом. Если нарушитель раскроет значение ***k***, повторно используемое отправителем, то может раскрыть и секретный ключ ***x*** отправителя.

Схема алгоритма шифрования данных Эль - Гамаля

1. Определение открытого *"y"* и секретного *"x"* ключей

1.1. Выбор двух взаимно простых больших чисел p и q, $q < p$

1.2. Выбор значения секретного ключа x, $x < p$

1.3. Определение значения открытого ключа y из выражения:

$$y = q^x \pmod p$$

2. Алгоритм шифрования сообщения M

2.1. Выбор случайного числа k, удовлетворяющего условию:

$$0 < k < p-1 \text{ и НОД } (k, p-1) = 1$$

2.2. Определение значения a из выражения: $a = q^k \pmod p$

2.3. Определение значения b из выражения: $b = y^k M \pmod p$

2.4. Криптограмма C, состоящая из a и b, отправляется получателю

2.5. Получатель расшифровывает криптограмму с помощью выражениями:

$$Ma^x = b \pmod p$$

3. Процедуру шифрования данных рассмотрим на следующем примере (для удобства расчётов в данном примере использованы числа малой разрядности):

3.1. Выбираем два взаимно простых числа $p = 11$ и $q = 2$;

3.2. Выбираем значение секретного ключа x, $(x < p)$, $x = 8$;

3.3. Вычисляем значение открытого ключа y из выражения

$$y=q^x \pmod p = 2^8 \pmod{11} = 256 \pmod{11} = 3$$

3.4.Выбираем значение открытого сообщения $M = 5$;

3.5. Выбираем случайное число $k = 9$; $НОД(9, 10) = 1$;

3.6. Определяем значение a из выражения:

$$a = q^k \pmod p = 2^9 \pmod{11} = 512 \pmod{11} = 6;$$

3.7. Определяем значение b из выражения:

$$b = y^k M \pmod p = 3^9 * 5 \pmod{11} = 98415 \pmod{11} = 9.$$

Таким образом, получаем зашифрованное сообщение как $(a, b) = (6, 9)$ и отправляем получателю.

3.8. Получатель расшифровывает данный шифротекст, используя секретный ключ x и решая следующее сравнение:

$$M*a^x = b \pmod p = 5*6^8 = 9 \pmod{11} = 8398080 = 9 \pmod{11}$$

Вычисленное значение сообщения $M = 5$ представляет собой заданное исходное сообщение.

4. Содержание отчёта

4.1. Составить блок-схему и программу алгоритма шифрования Эль - Гамаля.

4.2. Листинг программы шифрования заданного сообщения с использованием алгоритма Эль - Гамаля.

Лабораторная работа №3 Модели и стандарты в сфере ИБ и управления рисками ИБ

Цель работы: Исследование структуры алгоритма и методики практической реализации (ЭЦП) RSA.

Основные теоретические положения: Технология применения системы ЭЦП предполагает наличие сети абонентов, обменивающихся подписанными электронными документами. При обмене электронными документами по сети значительно снижаются затраты, связанные с их обработкой, хранением и поиском.

Одновременно при этом возникает проблема, как аутентификации автора электронного документа, так и самого документа, т.е. установление подлинности автора и отсутствия изменений в полученном электронном сообщении.

В алгоритмах ЭЦП как и в асимметричных системах шифрования используются однонаправленные функции. ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам.

ЭЦП представляет собой относительно небольшой объём дополнительной цифровой информации, передаваемой вместе с подписанным текстом.

Концепция формирования ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности подписи, которая реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП включает две процедуры:

- формирование цифровой подписи;
- проверку цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи — открытый ключ отправителя.

Безопасность системы RSA определяется вычислительной трудностью разложения на множители больших целых чисел. Недостатком алгоритма цифровой подписи RSA является уязвимость её к мультипликативной атаке. Другими словами, алгоритм ЭЦП RSA позволяет хакеру без знания секретного ключа сформировать подписи под теми документами, в которых результат - хэширования можно вычислить как произведение результата хэширования уже подписанных документов.

Алгоритм электронной цифровой подписи (ЭЦП) RSA

1.Определение открытого «e» и секретного «d» ключей (действия отправителя)

1.1. Выбор двух взаимно простых больших чисел p и q

1.2. Определение их произведения $n = p*q$

1.3. Определение функции Эйлера: $\phi(n) = (p-1)(q-1)$

1.4. Выбор секретного ключа d с учетом условий: $1 < d < \phi(n)$, $НОД(n, \phi(n)) = 1$

1.5. Определение значения открытого ключа e: $e < n$, $e*d(mod\ \phi(n))=1$

2. Формирование ЭЦП

2.1. Вычисление хэш - значения сообщения M: $m = h(M)$

2.2. Для получения ЭЦП шифруем хэш – значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d\ (mod\ n)$ и открытый текст сообщения M

3.Аутентификация сообщения - проверка подлинности подписи

3.1. Расшифровка цифровой подписи S с помощью открытого ключа e и вычисление её хэш - значения $m' = S^e (mod\ n)$

3.2. Вычисление хэш - значения принятого открытого текста M и $m=h(M)$

3.3. Сравнение хэш - значений m и m', если $m=m'$, то цифровая подпись **S** — достоверна.

Процедуру формирования ЭЦП сообщения M рассмотрим на следующем простом примере:

3.4. Вычисление хэш - значения сообщения M: $m = h(M)$.

Хэшируемое сообщение M представим как последовательность целых чисел

3.5. В соответствии с приведённым выше алгоритмом формирования ЭЦП RSA выбираем два взаимно простых числа $p = 3$, $q = 11$, вычисляем значение $n=p*q=3*11=33$, выбираем значение секретного ключа $d = 7$ и вычисляем значение открытого ключа $e = 3$. Вектор инициализации H_0 выбираем равным 6 (выбирается случайным образом).

Хэш - код сообщения **M =312** формируется следующим образом:

$H_1 = (M_1 + H_0)^2\ (mod\ n) = (3+6)^2\ (mod\ 33) = 81\ (mod 33) = 15;$

$H_2 = (M_2 + H_1)^2\ (mod\ n) = (1+15)^2\ (mod\ 33) = 256\ (mod\ 33) = 25;$

$H_3 = (M_3 + H_2)^2\ (mod\ n) = (2+25)^2\ (mod 33) = 729\ (mod 33) = 3,\ m=3$

3.6. Для получения ЭЦП шифруем хэш - значение m с помощью секретного ключа d и отправляем получателю цифровую подпись

$S = m^d\ (mod\ n)$ *и открытый текст сообщения* M

$S = 3^7\ (mod\ 33) = 2187 (mod 33) = 9$

3.7. Проверка подлинности ЭЦП

Расшифровка S (т. е. вычисление её хэш - значения m') производится с помощью открытого ключа **e**.

$$m' = S^e\ (mod\ n) = 9\ (mod\ 33) = 729 (mod\ 33) = 3$$

3.8. Если сравнение хэш - значений m' и m показывает их равенство, т.е. $m = m'$, то подпись достоверна.

4.Содержание отчета

4.1. Составить блок-схему алгоритма и программу формирования ЭЦП RSA.

4.2. Листинг программы расчета ЭЦП RSA в соответствии с заданием.

Лабораторная работа №4 Технологии и методы реализации ИБ. Комплексная защита информационной инфраструктуры

Простой столбцевой перестановочный шифр

В данном виде шифра текст пишется на горизонтально разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрование заключается в записи шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывании открытого текста горизонтально.

Пример:

МОСКОВСКАЯ ФИНАНСОВО-ЮРИДИЧЕСКАЯ АКАДЕМИЯ

М	О	С	К	О	В
С	К	А	Я		Ф
И	Н	А	Н	С	О
В	О	-	Ю	Р	И
Д	И	Ч	Е	С	К
А	Я		А	К	А
Д	Е	М	И	Я	

Зашифрованный текст:

МСИВДАДОКНОИЯЕСАА-Ч МКЯНЮЕАИО СРСКЯВФОИКА

М	О	С	К	О	В
С	К	А	Я		Ф
И	Н	А	Н	С	О
В	О	-	Ю	Р	И
Д	И	Ч	Е	С	К
А	Я		А	К	А
Д	Е	М	И	Я	

Задание: Реализовать на любом языке программирования работу данного шифра

Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации.

Открытый текст: Прикладная математика *Ключ*: Шифр

Ш	И	Ф	Р
4	1	3	2
П	р	и	к
л	а	д	н
а	я	м	а
т	е	м	а
т	и	к	а

Криптограмма: Раяеикнааидммкплатт

Ключевое слово (последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

Так как символы криптотекста те же, что и в открытом тексте, то частотный анализ покажет, что каждая буква встречается приблизительно с той же частотой, что и обычно. Это дает криптоаналитику информацию о том, что перестановочный шифр. Применение к криптотексту

второго перестановочного фильтра значительно повысит безопасность. Существуют и еще более сложные перестановочные шифры, но с применением компьютера можно раскрыть почти все из них.

Хотя многие современные алгоритмы используют перестановку, с этим связана проблема использования большого объема памяти, а также иногда требуется работа с сообщениями определенного размера.

Задание: Реализовать на любом языке программирования работу данного шифра

Шифр Полибия

Одной из наиболее древней из известных является система греческого историка Полибия. Его суть состоит в следующем: рассмотрим прямоугольник, что называется доской Полибия.

	А	Б	В	Г	Д	Е
А	А	Б	В	Г	Д	Е
Б	Ж	З	И	Й	К	Л
В	М	Н	О	П	Р	С
Г	Т	У	Ф	Х	Ц	Ч
Д	Ш	Щ	Ъ	Ы	Ь	Э
Е	Ю	Я	.	,	-	

Каждая буква может быть представлена парой букв, указывающих строку и столбец, в которых расположена данная буква. Так представления букв В, Г, П, У будут АВ, АГ, ВГ, ГБ соответственно, а сообщение

ПРИКЛАДНАЯ МАТЕМАТИКА

зашифруется как

ВГВДБВБДЬЕАААДВБААЕБЕЕВАААГААЕВАААГАБВБДАААЕЕ

Задание: Реализовать на любом языке программирования работу данного шифра

Рекомендуемая литература

Основная литература

1. Информационные системы и их безопасность [Текст] : учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. - Москва : Форум, 2015. - 528 с. - Библиогр. : с. 513-514. - ISBN 978-5-91134-289-0. (ОГТИ ч/з N4-1; аб.ТБ-18), коэфициент книгообеспеченности 1

Дополнительная литература

1. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 3-е изд., стер. - М. : Флинта, 2011. - 224 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. – URL: //biblioclub.ru/index.php?page=book_red&id=93351, коэффициент книгообеспеченности 1.

2. Основы информационной безопасности. Учебно-практическое пособие [Электронный ресурс] / Сычев Ю. Н. - Евразийский открытый институт, 2010.] - URL: //biblioclub.ru/index.php?page=book&id=93351, коэффициент книгообеспеченности 1.

3. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / Фаронов А. Е. - Интернет-Университет Информационных Технологий, 2011.- ,URL://biblioclub.ru/index.php?page=book_red&id=233763&sr=1, коэффициент книгообеспеченности 1.

4. Правовые основы информатики. Учебно-практическое пособие [Электронный ресурс] / Ефимова Л. Л. - Евразийский открытый институт, 2011. - URL://biblioclub.ru/index.php?page=book_red&id=93155&sr=1, коэффициент книгообеспеченности 1.

5. Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=277794, коэффициент книгообеспеченности 1.

6. Креопалов, В.В. Технические средства и методы защиты информации : учебно-практическое пособие / В.В. Креопалов. - М. : Евразийский открытый институт, 2011. - 278 с. - ISBN 978-5-374-00507-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=90753, коэффициент книгообеспеченности 1.

Периодические издания

1. Журнал «Вестник компьютерных и информационных технологий »
2. Журнал «Информационные технологии и вычислительные системы»
3. Журнал «Стандарты и качество»
4. Журнал «Прикладная информатика»