МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
_____ А.Н. Марьенков

_____

«2» июня 2022 г.

УТВЕРЖДАЮ
И.о. заведующего кафедрой ИБ
_____ Р.Ю. Демина
протокол заседания кафедры № 2
от «2» июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ

(наименование)

Составитель(-и)	**Демина Р.Ю., к.т.н., доцент, и.о.заведующего кафедрой ИБ**
Направление подготовки	**09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ**
Направленность (профиль) ОПОП	**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ**
Квалификация (степень)	**бакалавр**
Форма обучения	**очно-заочная**
Год приема	**2021**
Курс	**2**
Семестр	**4**

Астрахань, 2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины (модуля) «Безопасность информационных технологий и систем» формирование у студентов необходимого объема знаний идейных и концептуальных основ информационной безопасности, изучение основных принципов безопасности информационных технологий и систем, ознакомление студентов с современными криптосистемами, методами идентификации при проектировании информационных систем

1.2. Задачами освоения дисциплины (модуля) *являются*:

знакомство с правовыми основами и стандартами в области защиты компьютерной информации;

– знакомство с программными методами защиты информации в компьютерных системах;

– знакомство с современными криптосистемами;

– изучение методов идентификации при проектировании информационных систем;

– научиться применять современные методы и алгоритмы защиты информации при проектировании информационных систем в различных областях.

Вместе с другими дисциплинами цикла профессиональных дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

- строгость в суждениях;
- творческое мышление;
- организованность и работоспособность;
- дисциплинированность;
- самостоятельность и ответственность.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Безопасность информационных технологий и систем**»** Б1.Б.11 входит в обязательную (базовую) часть учебного плана направления подготовки 09.03.02 **ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ, профиль БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ** 2021 года набора и относится к базовой части. Дисциплина изучается в 4 семестре, общая трудоемкость дисциплины – 3 ЗЕ, 108 часов, итоговая форма контроля – зачет.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

- Математические основы информационных технологий и вычислительной техники
- Информатика.
- Основы программирования.

Знания: основных понятий информатики, структуры систем документационного обеспечения, методов защиты информации, языков программирования, основ алгоритмизации, архитектуры ЭВМ и устройства ПК, представления данных в ЭВМ..

Умения: использовать программные и аппаратные средства персонального компьютера, программировать, алгоритмизировать и программировать порядок решения задач по оценке и исследованию уровней защищенности компьютерных систем.

Навыки и (или) опыт деятельности: навыки поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): навыки разработки приложений, навыки инженерно-технической защиты информации, практические навыки обработки информации с использованием

информационных технологий и средств вычислительной техники при решении профессиональных задач.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Методы и средства криптографической защиты информации.

Знания, полученные в результате изучения дисциплины, используются студентами при прохождении преддипломной практики и написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) общепрофессиональных (ОПК): ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем.

Таблица 1 - Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ИОПК-5.1. Знать: основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.	ИОПК-5.2. Уметь: выполнять параметрическую настройку информационных и автоматизированных систем.	ИОПК-5.3. Иметь навыки: инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем, в том числе программно-аппаратных средств защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ «Безопасность информационных технологий и систем»

Объем дисциплины (модуля) 3 з.е., 108 часов, 18 часов выделено на контактную работу обучающихся с преподавателем (из них 18 часов – лабораторные работы), 90 часов – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Введение в дисциплину	4	1-2			2		11	Опрос по теме. входное тестирование,

									лабораторная работа 1
2	Обеспечение ИБ на уровне государства		3-4			2		11	Опрос по теме. лабораторная работа 2
3	Система безопасности		5-6			2		11	Опрос по теме. контрольная работа 1
4	Основы криптографии		7-8			2		11	Опрос по теме. лабораторная работа 3
5	Электронная подпись		9-10			2		11	Опрос по теме. лабораторная работа 4
6	Компьютерная стеганография		11-12			2		11	Опрос по теме. лабораторная работа 5
7	Построение защищенных экономических систем		13-14			2		11	Опрос по теме. лабораторная работа 6
8	Защищенные компьютерные системы		15-18			4		13	Опрос по теме. контрольная работа 2, итоговое тестирование
ИТОГО			**108**			**18**		**90**	**зачет**

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3 - Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции*	*Σ общее количество компетенций*
		ОПК 5	
Введение в дисциплину	13	+	1
Обеспечение ИБ на уровне государства	13	+	1
Система безопасности	13	+	1
Основы криптографии	13	+	1
Электронная подпись	13	+	1
Компьютерная стеганография	13	+	1
Построение защищенных экономических систем	13	+	1
Защищенные компьютерные системы	17	+	1
ИТОГО	108		

Содержание дисциплины

Введение в дисциплину

Основные положения теории информационной безопасности: информация и информационные отношения; субъекты информационных отношений, их безопасность. Три вида возможных нарушений ИС. Определение требований к защищенности информации. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Обеспечение ИБ на уровне государства

Законодательные и правовые основы защиты компьютерной информации и информационных технологий. Международные стандарты информационного обмена. ИБ в условиях функционирования в России глобальных сетей. Назначение и задачи в сфере обеспечения ИБ на уровне государства. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1 – аудит ИБ 78. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст). Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 № 479-ст).

Система безопасности

Проблемы защиты информации в информационных системах. Задачи системы безопасности. Меры противодействия угрозам безопасности. Классификация мер. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные механизмы защиты АС. Модели безопасности и их применение. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – требования к СУИБ ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ.

Основы криптографии

Современные криптосистемы для защиты компьютерной информации. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования. Основные понятия и классификация средств криптографической защиты информации. Абсолютно стойкий шифр. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрических криптосистем. Методы криптографии. Классификация шифров по различным признакам.

Электронная подпись

Электронная цифровая подпись и ее использование. Основные понятия и свойства. Аппаратно-программные средства защиты информации. Средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей.

Компьютерная стеганография
Компьютерная стеганография и ее применение. Базовые понятия стеганографии Модель стеганографической системы.. Понятие контейнера, виды контейнеров. Методы сокрытия информации в мультимедийных файлах. Направления развития компьютерной стеганографии.

Построение защищенных экономических систем
Методы идентификации и проверки подлинности пользователей информационных систем. Основные технологии построения защищенных ЭИС. Место ИБ экономических систем в национальной безопасности страны. Концепция ИБ. Особенности работы с персоналом, владеющим конфиденциальной информацией. Технологические основы обработки конфиденциальных документов. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ. ISO/IEC 27011:2008 – руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002

Защищенные компьютерные системы
Использование защищенных компьютерных систем. Защита операционной системы и других системных программных средств. Организация доступа в локальных сетях. ISO/IEC 27013 – руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001. ISO/IEC 27014 – инфраструктура руководства ИБ. ISO/IEC 27015 – руководство по управлению ИБ для финансовых сервисов. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (основной). Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (дополнительной).

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-источниками.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
1.	Подготовка к опросу по теме. Подготовка к входному тестированию. Подготовка отчета по лабораторной работе 1	11	Внеаудиторная, изучение учебных пособий

2.	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 2	11	Внеаудиторная, изучение учебных пособий
3.	Подготовка к опросу по теме. Подготовка к контрольной работе 1	11	Внеаудиторная, изучение учебных пособий
4.	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 3	11	Внеаудиторная, изучение учебных пособий
5.	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 4	11	Внеаудиторная, изучение учебных пособий
6.	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 5	11	Внеаудиторная, изучение учебных пособий
7.	Подготовка к опросу по теме. Подготовка отчета по лабораторной работе 6	11	Внеаудиторная, изучение учебных пособий
8.	Подготовка к опросу по теме. Подготовка к контрольной работе 2. Подготовка к итоговому тестированию	13	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно

Правила оформления текста пояснительной записки реферата

На титульном листе прописываются: название университета, факультета, кафедры, название дисциплины, темы реферата, Ф.И.О. студента, номер группы, Ф.И.О. преподавателя и оставляется место для проставления оценки и подписи преподавателя . Внизу пишется город и год написания.

Текстовая часть

Изложение текста и оформление работы следует выполнять в соответствии с требованиями.

Текст ПЗ оформляется на одной стороне листа формата А4.

Основной текст набирается шрифтом *Times New Roman 12,* с выравниванием *по ширине*, абзацный отступ должен быть одинаковым по всему тексту и равен *1,25 см*; строки разделяются *полуторным интервалом*.

Поля страницы: верхнее -2,5см, нижнее – 2,5 см, левое – 3,5 см, правое – 1,0 см.

Структурные элементы пояснительной записки **СОДЕРЖАНИЕ, ВВЕДЕНИЕ, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ, ПРИЛОЖЕНИЕ** должны начинаться с нового листа.

Их заголовки оформляются ***прописными буквами, шрифтом 14 Ж***, располагаются *в середине строки без точки в конце*. Дополнительный *интервал после* заголовка - 12 *пт*.

Основную часть работы разделяют на разделы, подразделы и, при необходимости, на пункты.

Каждый раздел необходимо начинать с нового листа. Разделы нумеруют арабскими цифрами в пределах всего текста. После номера и в конце заголовка раздела *точка не ставится*.

Если заголовок состоит из двух предложений, их разделяют точкой. *Переносы слов в заголовках не допускаются.*

Заголовки разделов оформляются ***с прописной буквы, шрифтом 14 Ж,*** с абзацного отступа *1,25* см. Дополнительный *интервал после заголовка - 6 пт.*

(Если заголовок раздела занимает две и большее число строк, то интервал между этими строками – *полуторным*).

Подразделы нумеруются в пределах каждого раздела. Номер подраздела состоит из номера раздела и порядкового номера подраздела, разделенных точкой. После номера подраздела точку не ставят.

Заголовки подразделов печатаются с абзацного отступа, ***с прописной буквы шрифтом 12 Ж,*** без точки в конце заголовка.

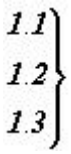
Дополнительный *интервал перед* заголовком подраздела – *6 пт, после* заголовка - 6 *пт*.

Пункты нумеруются в пределах каждого подраздела. Номер пункта состоит из номеров раздела, подраздела и пункта, разделенных точкой. После номера пункта точку не ставят.

Нельзя писать заголовок в конце страницы, если на ней не умещаются, по крайней мере, две строки текста, идущего за заголовком.

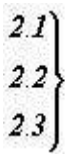
Пример оформления заголовков текста:

1 Разработка аппаратных средств



Нумерация пунктов первого раздела отчета

2 Технические характеристики



Нумерация пунктов второго раздела отчета

В пояснительной записке после титульного листа помещается лист **СОДЕРЖАНИЕ**, в котором указываются номера и наименования разделов, подразделов и приложений ТД с указанием номеров страниц, где они начинаются.

Разделы, подразделы записываются в содержании в точном соответствии с их наименованиями без сокращений *строчными буквами кроме первой прописной.*

Перечисления

В тексте пояснительной записки перечисления производятся с абзацного отступа, каждое с новой строки с *дефисом***.**

Примеры написания:

- текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
- приложения;
- перечень терминов;
- перечень сокращений;
- перечень литературы.

При необходимости ссылки в тексте отчета на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

При необходимости дальнейшей детализации перечислений используются арабские цифры и строчные буквы русского алфавита, после которых ставятся скобки:

а)…;

б)…;

1)…;

2)…;

в).

Примеры написания:

1) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
2) приложения;
3) перечень терминов;
4) перечень сокращений;
5) перечень литературы.

Примеры написания:

а) текст пояснительной записки (ПЗ) (с рисунками, таблицами и т. п.);
б) приложения;
в) перечень терминов;
г) перечень сокращений;
д) перечень литературы.

Сокращения слов

Сокращение слов в тексте, как правило, не допускается. Исключение составляют сокращения, общепринятые в русском языке: т. е. (то есть), и т. п. (и тому подобное), и т. д. (и так далее), и др. (и другие).

При необходимости применения специфических терминов или сокращений нужно дать их разъяснение при первом упоминании. Например «…создание систем автоматического проектирования (САПР)». В последующем тексте принятые сокращения пишутся без скобок.

Формулы

Составной частью текста пояснительной записки являются математические формулы и соотношения. Формулы создаются в редакторе формул.

Формулы располагают в середине строки и выделяют из текста свободными строками.

Пример оформления расчетов:

Количество населения в заданном пункте и подчиненных окрестностях с учетом среднего прироста населения определяется по формуле (3.1):

$$H_t = H_0 \left(1 + \frac{\Delta H}{100}\right)^t, \qquad ((3.1)$$

где H_0 – число жителей на время проведения переписи населения, тыс. чел.;

ΔH – средний годовой прирост населения в данной местности, % (принимается 2…3%);

t – период, определяемый как разность между назначенным годом перспективного проектирования и годом проведения переписи населения, год.

$$H_t = 32{,}6\left(1 + \frac{2}{100}\right)^8 = 38{,}2 \text{ тыс. чел.}$$

Расшифровка формулы, при необходимости, приводится непосредственно под формулой. В конце формулы ставится запятая, пояснение значений символов дают с новой строки в той последовательности, в какой они приведены в формуле.

Формулы нумеруются в пределах раздела. Номер формулы состоит из номера раздела и порядкового номера формулы в этом разделе. Номер формулы в круглых скобках помещается в крайнем правом положении на строке.

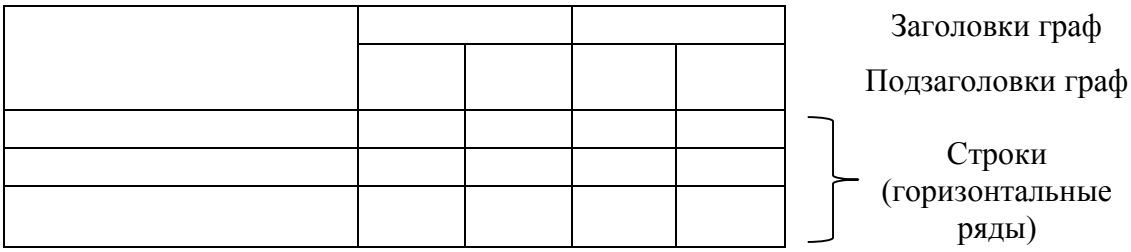
Ссылка в тексте на формулу: «…в формуле (3.1)».

Таблицы

Цифровой материал оформляется в виде таблиц. Таблицу следует располагать непосредственно после ссылки на нее.

Размеры таблиц выбираются произвольно, в зависимости от представляемого материала. Высота строк таблицы должна быть не менее 8 мм

Таблица 2.1 – Наименование таблицы



Заголовки граф и строк таблицы должны начинаться с прописной буквы, а подзаголовки граф – со строчной буквы, если они составляют одно предложение с заголовком. Если подзаголовки граф имеют самостоятельное значение, то их начинают с прописной буквы.

Заголовки указывают в единственном числе. В конце заголовков и подзаголовков таблицы точки не ставят.

Разделять заголовки боковика и граф диагональными линиями не допускается. Графу

«Номер по порядку» в таблицу включать не допускается.

Таблицы нумеруются в пределах раздела. Номер таблицы состоит из номера раздела и порядкового номера таблицы в этом разделе. Номер и наименование таблицы следует помещать над таблицей слева через тире.

Пример оформления таблицы:

Таблица 3.1– Длина участков трассы

Протяженность участка проектируемой трассы, км	Тип кабеля
0,084	ДПС-04-24А06-7,0
0,167	ДПС-04-24А06-7,0
0,301	ДПС-04-24А06-7,0
0,779	ДПС-04-24А06-7,0
Общая длина кабеля: 1,331 км	ДПС-04-24А06-7,0

Примечание – Толщину линий таблицы задайте 1 пт.

Таблицу с большим числом строк допускается переносить на другой лист. При этом в первой части таблицы нижнюю горизонтальную линию не проводят. Над второй частью слева пишут: «Продолжение Таблицы 2.1».

Продолжение Таблицы 2.1

Дата	Наименование	Стоимость

Рисунки

Графический материал располагают, возможно, ближе к тексту, в котором о нём упоминается.

Все рисунки нумеруются в пределах раздела и должны иметь наименование, Номер рисунка и его наименование располагают под рисунком следующим образом:

Рисунок 2.12 – Кривая коэффициента восприятия речи

Ссылка в тексте на рисунок: «…в соответствии с рисунком 4.3».

Если в разделе ВВЕДЕНИЕ есть рисунки, то они нумеруются как :

Рисунок В.1 – Название рисунка

Список использованных источников

Список использованных источников приводится в конце пояснительной записки. Список использованных учебников, справочников, статей, стандартов и др. следует располагать в порядке появления ссылок на источники в тексте работы и нумеровать арабскими цифрами без точки, печатать с абзацного отступа.

Список литературы должен быть составлен в алфавитном порядке. Список адресов серверов Internet указывается после литературных источников. При указании веб-адреса рекомендуется давать заголовок данного ресурса (заголовок веб-страницы).

При составлении списка литературы в алфавитном порядке следует придерживаться следующих правил:

1) законодательные акты и постановления правительства РФ;

2) специальная научная литература;

3) методические, справочные и нормативные материалы, статьи периодической печати.

Для многотиражной литературы при составлении списка указываются: полное название источника, фамилия и инициалы автора, издательство и год выпуска (для статьи – название издания и его номер). Полное название литературного источника приводится в начале книги на 2-3 странице.

Для законодательных актов необходимо указывать их полное название, принявший орган и дату принятия.

При указании адресов серверов Internet сначала указывается название организации, которой принадлежит сервер, а затем его полный адрес.

Примеры записей:

1 Глухов В. А. Исследование, разработка и построение системы электронной доставки документов в библиотеке: Автореф. дис. канд. техн. наук. – Новосибирск, 2000. – 18 с.

2 Экономика и политика России и государств ближнего зарубежья : аналит. обзор, апр. 2007, Рос. акад. наук, Ин-т мировой экономики и муждунар. отношений. – М. : ИМЭМО, 2007. – 39 с.

3 Фенухин В. И. Этнополитические конфликты в современной России: на примере Северо-Кавказкого региона : дис. … канд. полит. наук. – М., 2002. – с. 54–55.

4 Официальные периодические издания : электронный путеводитель / Рос. нац. б-ка, Центр правовой информации. [СПб], 200520076. URL: http://www.nlr.ru/lawcrnter/izd/index.html (дата обращения: 18.01.2007).

5 Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).

6 Рынок тренингов Новосибирска: своя игра [Электронный ресурс]. – Режим доступа: http://nsk.adme.ru/news/2006/07/03/2121.html (дата обращения: 17.10.08).

Оформление приложений

Нумерация приложений осуществляется русскими буквами, кроме букв Ё, Й, Ъ, Ь, Ы, О.

В разделе СОДЕРЖАНИЕ название приложения оформляется следующим образом:

ПРИЛОЖЕНИЕ А – Диаграмма классов

В самом приложении, слово **ПРИЛОЖЕНИЕ А** пишется жирным шрифтом по центру, на следующей строке пишется название приложения, по центру жирным шрифтом, например,

ПРИЛОЖЕНИЕ А
Диаграмма классов

Если приложение продолжается на следующей странице, то необходимо сверху по центру, нежирным шрифтом написать слова:

Продолжение Приложения А

Если в приложении, например, в приложении А есть таблицы, то они нумеруются как:

Таблица А.1– Название таблицы

Если в приложении есть рисунки, например, в приложении А, то они нумеруются как:

Рисунок А.1 – Название рисунка

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Введение в дисциплину	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы, теста
Обеспечение ИБ на уровне государства	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Система безопасности	Лекция - презентация	Не предусмотрено	выполнение контрольной работы
Основы криптографии	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Электронная подпись	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Компьютерная стеганография	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Построение защищенных экономических систем	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Защищенные компьютерные системы	Обзорная лекция	Не предусмотрено	выполнение контрольной работы выполнение теста

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
2. Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.

3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
4. Электронно-библиотечная система elibrary. http://elibrary.ru
5. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
6. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Безопасность информационных технологий и систем» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Введение в дисциплину	ОПК 5	Вопросы для обсуждения. лабораторная работа 1 .Входной тест
2.	Обеспечение ИБ на уровне государства	ОПК 5	Вопросы для обсуждения. лабораторная работа 2
3.	Система безопасности	ОПК 5	Вопросы для обсуждения. контрольная работа 1
4.	Основы криптографии	ОПК 5	Вопросы для обсуждения. лабораторная работа 3
5.	Электронная подпись	ОПК 5	Вопросы для обсуждения. лабораторная работа 4
6.	Компьютерная стеганография	ОПК 5	Вопросы для обсуждения. лабораторная работа 5
7.	Построение защищенных экономических систем	ОПК 5	Вопросы для обсуждения. лабораторная работа 6
8.	Защищенные компьютерные системы	ОПК 5	Вопросы для обсуждения. контрольная работа 2, итоговый тест

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания

5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для результатов обучения по дисциплине (модулю)

Тема 1. Введение в дисциплину

1. Вопросы для обсуждения

Основные положения теории информационной безопасности: информация и информационные отношения; субъекты информационных отношений, их безопасность. Три вида возможных нарушений ИС. Определение требований к защищенности информации.

2. Лабораторная работа 1

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные;
- технологические;
- правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой

точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке (plaintext-equivalent);
- по некоторому проверочному значению (verifier-based);
- без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
- с использованием пароля для получения криптографического ключа (cryptographic).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной

системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем
и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:
   - подбор в интерактивном режиме;
   - подсматривание;
   - преднамеренную передачу пароля его владельцем другому лицу;
   - захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
   - перехват переданной по сети информации о пароле;
   - хранение пароля в доступном месте.
2. Вмешательство в функционирование компонентов парольной системы через:
   - внедрение программных закладок;
   - обнаружение и использование ошибок, допущенных на стадии разработки;
   - выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние:
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия,

нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароля	**Получаемый эффект**
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи

2. Примеры.

Пример 1.
Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.
Длина пароля 6 символов k=6.
Таким образом, получаем количество вариантов: $C=n^k=10^6$
Примем скорость перебора s=10 паролей в секунду. Получаем время перебора всех паролей $t= C/s=10^5$секунд≈1667минут≈28часов≈1,2 дня.
Примем, что после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей
T=t*5/3=16667секунд≈2778минут≈46часов≈1,9 дня.
$T_{итог}$ = t+T = 1,2 + 1,9 = 3,1 дня

Пример 2.
Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
Алфавит составляют символы n=10.
Длина пароля рассчитывается: $k=\log_n C= \lg C$.
Определим количество вариантов C= t * s=10лет*10 паролей в сек. = 10*10*365*24*60*60≈3,15* 10^9 вариантов
Таким образом, получаем длину пароля: $k=\lg (3,15*10^9) = 9,5$ Очевидно, что длина пароля должна быть не менее 10 символов.

3. Задания.

1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.
Длина пароля символов k.
Скорость перебора s паролей в секунду.
После каждого из m неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	m	v
1	33	10	100	0	0
2	26	12	13	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

2. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.
Скорость перебора s паролей в секунду.

вариант	n	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20

5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.
Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

3. Тест входной

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. По объекту воздействия угрозы бывают:
- воздействующие на информационную среду в целом
- воздействующие на отдельные элементы информационной среды
- активные
- пассивные

2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнес-операции и создания угрозы
- инцидент
- нарушение
- сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется
- событием (информационной безопасности)
- инцидентом (информационной безопасности)
- угрозой (информационной безопасности)

4. Первым шагом в управлении сетью является ее

- документирование
- ревизия
- оформление

5. Какова цель ревизии эффективности?

- Мониторинг и анализ работы сети.
- Определение того, работает ли сеть в соответствии со своим потенциалом.
- Идентификация типов оборудования и устройств, сети.
- Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

Тема 2. Угрозы информационной безопасности. Меры защиты

1. Вопросы для обсуждения

1) Понятие угрозы. Защита.
2) Классификация угроз и мер защиты информации.
3) Таксономия нарушений ИБ вычислительной системы и причины, обуславливающие их существование.
4) Состав и содержание средств защиты, объекты и элементы защиты.

2. Лабораторная работа 2

Архивирование с паролем

1. Теория.

Архиваторы – это программы для создания архивов. Архивы предназначены для хранения данных в удобном компактном виде. В качестве данных обычно выступают файлы и папки. Как правило, данные предварительно подвергаются процедуре сжатия или упаковки. Поэтому почти каждый архиватор одновременно является программой для сжатия данных. С другой стороны, любая программа для сжатия данных может рассматриваться как архиватор. Эффективность сжатия является важнейшей характеристикой архиваторов. От нее зависит размер создаваемых архивов. Чем меньше архив, тем меньше места требуется для его хранения. Для передачи нужна меньшая пропускная способность канала передачи или затрачивается меньшее время. Преимущества архивов очевидны, если учесть, что данные уменьшаются в размере и в 2 раза, и в 5 раз.

Сжатие данных используется очень широко. Можно сказать, почти везде. Например, документы PDF , как правило, содержат сжатую информацию. Довольно много исполняемых файлов EXE сжаты специальными упаковщиками. Всевозможные мультимедийные файлы (GIF , JPG , MP 3, MPG) являются своеобразными архивами.

Основным недостатком архивов является невозможность прямого доступа к данным. Их сначала необходимо извлечь из архива или распаковать. Операция распаковки, впрочем, как и упаковки, требует некоторых системных ресурсов. Это не мгновенная операция. Поэтому архивы в основном применяют со сравнительно редко используемыми данными. Например, для хранения резервных копий или установочных файлов.

В данный момент существует много архиваторов. Они имеют разную распространенность и эффективность. Некоторые интересные архиваторы не известны широкому кругу потенциальных пользователей. Особый интерес представляют оценка и сравнение эффективности сжатия популярных архиваторов.

Методы сжатия архиваторов.

Разработано большое количество разнообразных методов, их модификаций и подвидов для сжатия данных. Современные архиваторы, как правило, одновременно используют несколько методов одновременно. Можно выделить некоторые основные.

Кодирование длин серий (RLE - сокращение от run - length encoding - кодирование длин серий).

Очень простой метод. Последовательная серия одинаковых элементов данных заменяется на два символа: элемент и число его повторений. Широко используется как дополнительный, так и промежуточный метод. В качестве самостоятельного метода применяется, например, в графическом формате BMP .

Словарный метод (LZ - сокращение от Lempel Ziv - имена авторов).

Наиболее распространенный метод. Используется словарь, состоящий из последовательностей данных или слов. При сжатии эти слова заменяются на их коды из словаря. В наиболее распространенном варианте реализации в качестве словаря выступает сам исходный блок данных.

Основным параметром словарного метода является размер словаря. Чем больше словарь, тем больше эффективность. Однако для неоднородных данных чрезмерно большой размер может быть вреден, так как при резком изменении типа данных словарь будет заполнен неактуальными словами. Для эффективной работы данного метода при сжатии требуется дополнительная память. Приблизительно на порядок больше, чем нужно
для исходных данных словаря. Существенным преимуществом словарного метода является простая и быстрая процедура распаковки. Дополнительная память при этом не требуется. Такая особенность особенно важна, если необходим оперативный доступ к данным.

Энтропийный метод (Huffman - кодирование Хаффмена, Arithmetic coding - арифметическое кодирование)

В этом методе элементы данных, которые встречаются чаще, кодируются при сжатии более коротким кодом, а более редкие элементы данных кодируются более длинным кодом. За счет того, что коротких кодов значительно больше, общий размер получается меньше исходного.

Широко используется как дополнительный метод. В качестве самостоятельного метода применяется, например, в графическом формате JPG .

Метод контекстного моделирования (CM - сокращение от context modeling - контекстное моделирование)

В этом методе строится модель исходных данных. При сжатии очередного элемента данных эта модель выдает свое предсказание или вероятность. Согласно этой вероятности, элемент данных кодируется энтропийным методом. Чем точнее модель будет соответствовать исходным данным, тем точнее она будет выдавать предсказания, и тем короче будут кодироваться элементы данных.

Для построения эффективной модели требуется много памяти. При распаковке приходится строить точно такую же модель. Поэтому скорость и требования к объему оперативной памяти для упаковки и распаковки почти одинаковы. В данный момент методы контекстного моделирования позволяют получить наилучшую степень сжатия, но отличаются чрезвычайно низкой скоростью.

PPM (PPM - Prediction by Partial Matching - предсказание по частичному совпадению).

Это особый подвид контекстного моделирования. Предсказание выполняется на основании определенного количества предыдущих элементов данных. Основным параметром является порядок модели, который задает это количество элементов. Чем больше порядок модели, тем выше степень сжатия, но требуется больше оперативной памяти для хранения данных модели. Если оперативной памяти недостаточно, то такая модель с большим порядком показывает низкие результаты. Метод PPM особенно эффективен для сжатия текстовых данных.

Предварительные преобразования или фильтрация.

Данные методы служат не для сжатия, а для представления информации в удобном для дальнейшего сжатия виде. Например, для несжатых мультимедиа данных характерны плавные изменения уровня сигнала. Поэтому для них применяют дельта-преобразование, когда вместо абсолютного значения берется относительное. Существуют фильтры для текста, исполняемых файлов, баз данных и другие.

Метод сортировки блока данных (BWT - сокращение от Burrows Wheeler Transform - по имени авторов).

Это особый вид или группа преобразований, в основе которых лежит сортировка. Такому преобразованию можно подвергать почти любые данные. Сортировка производится над блоками, поэтому данные предварительно разбиваются на части. Основным параметром является размер блока, который подвергается сортировке. Для распаковки данных необходимо проделать почти те же действия, что и при упаковке. Поэтому скорость и требования к оперативной памяти почти одинаковы. Архиваторы, которые используют данный метод, обычно показывают высокую скорость и степень сжатия для текстовых данных.

Непрерывные блоки или непрерывный режим (Solid mode - непрерывный режим). Во многих методах сжатия начальный участок данных или файла кодируется плохо. Например, в словарном методе словарь пуст. В методе контекстного моделирования модель не построена. Когда количество файлов большое, а их размер маленький, общая степень сжатия значительно ухудшается за счет этих начальных участков. Чтобы этого не происходило при переходе на следующий файл, используется информация, полученная исходя из предыдущих файлов. Аналогичного эффекта можно добиться простым представлением исходных файлов в виде одного непрерывного файла.

Этот метод используется во многих архиваторах и имеет существенный недостаток. Для распаковки произвольного файла необходимо распаковать и файлы, которые оказались в начале архива. Это необходимо для правильного заполнения словаря или построения модели. Существует и промежуточный вариант, когда используются непрерывные блоки фиксированного размера. Потери сжатия получаются минимальными, но для извлечения одного файла, который находится в конце большого архива, необходимо распаковать только один непрерывный блок, а не весь архив.

Сегментирование.

Во всех методах сжатия при изменении типа данных собственно сам переход кодируется очень плохо. Словарь становится не актуальным, модель настроена на другие данные. В этих случаях применяется сегментирование. Это предварительная разбивка на однородные части. Затем эти части кодируются по отдельности или группами.

Особо хочется подчеркнуть, что существует большое количество методов сжатия. Каждый метод обычно ориентирован на один вид или группу реальных данных. Хорошие результаты показывает комплексное использование методов.

Особенности данных

Степень сжатия в основном зависит от исходных данных. Хорошо сжимаются почти все предварительно несжатые данные, например, исполняемые файлы (EXE), тексты (TXT , DOC), базы данных (DBF), простые несжатые изображения (BMP). Ограниченно сжимаются несжатый звук (WAV), сложные несжатые изображения (BMP). Не сжимаются почти все уже сжатые данные, например, архивы (ZIP , CAB), сжатые документы (PDF), сжатая графика и видео (JPG , GIF , AVI , MPG), сжатый звук (MP 3). Их сжатие находится в пределах пары процентов за счет служебных блоков и небольшой избыточности.

Для сжатия некоторых специфических данных (текст, несжатые изображения, несжатый звук) существуют специальные методы и архиваторы. Такие архиваторы обеспечивают высокую степень сжатия и высокую скорость. Однако так называемые универсальные архиваторы постепенно дополняются подобными методами. В данный

момент только для несжатого звука существуют высокоэффективные специальные архиваторы, такие, как OptimFROG , Monkey Audio . Для текстов и изображений лучшие универсальные архиваторы показывают лучшую степень сжатия. Например, архив изображений получится меньше, если использовать формат BMP и архиватор WinRK вместо специализированных графических форматов, таких как JPEG 2000 (LossLess - сжатие без потерь).

Большое количество типов данных уже являются сжатыми. Использование архиваторов дает мизерное уменьшение размера. Тем не менее даже в таких случаях эффективное сжатие теоретически возможно. Это обусловлено тем, что в большинстве распространенных форматов файлов, использующих сжатие, применены не самые эффективные методы. Например, в основе формата JPG лежит энтропийное сжатие, которое используется после преобразований Фурье. Данные кодируются неоптимальными блоками, что обусловлено желанием сделать формат JPG устойчивым к повреждениям и возможности частичного извлечения информации. Перекодировав файлы JPG при помощи высокоэффективных методов, можно добиться сжатия порядка 75% от исходного файла (архиватор StuffIt). Собственно сам исходный файл JPG сжимается обычными архиваторами только до 96%. Однако подобные манипуляции с файлами JPG стали возможны только недавно и еще не получили распространения. В большинстве случаев сжимать уже сжатые данные бесполезно.

Следует различать собственно программу-архиватор, формат архивов и методы сжатия. Даже один и тот же метод сжатия может иметь варианты реализации. Например, существует более десятка программ-архиваторов, которые могут создавать архивы в формате ZIP. В свою очередь данные в формате ZIP могут быть сжаты различными методами: Deflate, Deflate64, BZip2. Метод Deflate имеет несколько реализаций с разной скоростью и степенью сжатия (разница порядка 5%). С помощью этого метода архиватор 7-zip позволяет создавать архивы в формате ZIP и 7Z.

Обычно архиваторы могут создавать архивы в собственном эксклюзивном формате с использованием своих оригинальных методов. Например, архиватор RAR позволяет создавать архивы RAR. В формате архива и методах сжатия заключаются основные преимущества того или иного архиватора.

В простейшем случае архиватор позволяет только упаковать или распаковать один файл. Кроме собственно сжатия данных, современные архиваторы обеспечивают некоторые дополнительные функции. Можно выделить несколько основных:

сжатие некоторых файлов и целых директорий;

создание самораспаковывающихся (SFX) архивов. То есть для распаковки архива программа-архиватор не требуется;

изменение содержимого архива; шифрование содержимого архива;

информация для восстановления архива при частичном повреждении и возможность восстановления поврежденных архивов;

разбивка архива на несколько частей или томов;

консольная версия программы для работы из командной строки; графическая (GUI) версия программы.

Стоит отметить, что, несмотря на формальное наличие, реализация каждой дополнительной функции может быть выполнена на совершенно разном уровне.

Кроме различий в функциональности, можно разбить архиваторы на две группы: асимметричные и симметричные. Асимметричные архиваторы требуют для операции распаковки значительно меньше времени и оперативной памяти, чем для операции упаковки. Это позволяет быстро получать содержимое архива на маломощных компьютерах. Симметричные архиваторы требуют для операций упаковки и распаковки одинаковое время и объем оперативной памяти. Использование таких архиваторов на широком парке компьютеров или для оперативного доступа к содержимому архива ограничено. Известный архиватор RAR в качестве основного использует

асимметричный словарный метод сжатия, а для текстов может использовать симметричный PPM-метод. Таким образом, распаковка архивов RAR, сжатых с максимальной степенью сжатия, может быть невозможна на компьютерах с ограниченным объемом оперативной памяти. Все или почти все передовые архиваторы с высокой степенью сжатия являются симметричными.

Точной статистики по распространенности архиваторов у меня нет. Я выскажу свою субъективную точку зрения на основе личного опыта. Безусловно, самым распространенным архиватором являются ZIP и его модификации. По своей распространенности он значительно превосходит ближайших конкурентов. Следом идут RAR и ACE. В последние годы встречается архиватор 7-zip. Других архиваторов и архивов лично мы не встречали. Исключение составляют некогда популярные ARJ и LHA. В данный момент они не актуальны из-за очень низкой степени сжатия.

Несмотря на очень скромные данные о распространенности архиваторов, их существует большое множество. Основная масса относится к категории экспериментальных и архиваторов с ограниченной функциональностью. Тем не менее, каждый их них позволяет выполнять собственно процедуру сжатия данных. Меньшая распространенность увеличивает вероятность ошибок в программе.

2. Практика.

1. Необходимо создать текстовый файл, содержащий фамилию, имя, отчество студента в объеме 50 записей. Провести архивирование файла. Любым редактором внести изменения согласно задания. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.
2. Провести архивацию файла с паролем. Внести искажения, попробовать разархивировать. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.
3. Провести архивацию файла с паролем, состоящим из 3-х цифр. Провести попытку подбора пароля с использованием программного обеспечения. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения, время подбора.

Варианты:

1. архиватор zip. Искажение двух байт.
2. архиватор arj. Искажение трех байт.
3. архиватор rar. Искажение трех байт.
4. архиватор zip. Удаление двух байт.
5. архиватор arj. Удаление трех байт.
6. архиватор rar. Удаление трех байт.
7. архиватор arj. Добавление трех байт.
8. архиватор rar. Добавление трех байт.
9. архиватор zip. Добавление двух байт.
10. архиватор zip. Удаление двух байт.

Тема 3. Каналы утечки информации. Модель нарушителя

1. Вопросы для обсуждения

1) Классификация каналов проникновения в систему и утечки информации.
2) Неформальная модель нарушителя в АС.
3) Виды противников или «нарушителей».
4) Анализ способов нарушений ИБ.
5) Понятия о видах вирусов.

2. Контрольная работа 1

Вопросы к контрольной работе 1

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации
3. Задание требований к информационной безопасности организации
4. Понятие угрозы информационной безопасности. Классификация угроз ИБ
5. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
6. Объект и субъект защиты информации
7. Каналы утечки информации. Классификация каналов утечки информации
8. Модель нарушителя информационной безопасности
9. Классификация нарушителей информационной безопасности
10. Компьютеные «Вирусы». Их виды
11. Способы борьбы с компьютерными вирусами

Тема 4. Система безопасности

1. Вопросы для обсуждения

1) Задачи системы безопасности.
2) Меры противодействия угрозам безопасности.
3) Классификация мер.
4) Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
5) Основные механизмы защиты АС.
6) Модели безопасности и их применение.

2. Лабораторная работа 3

Шифр простой замены. Таблица Вижинера

1. Теория.

Современные криптографические системы тесно связаны с методами шифрования сообщений, которые, в свою очередь, зависят от способа использования ключей. Предлагаемая программа отличается простотой понимания смысла шифрования, позволяет получить криптограммы одного и того же исходного текста в зависимости от выбранного ключевого слова. Кроме того, такой подход шифрования может быть применен в одноключевых криптосистемах для защиты информации в локальных сетях.

Одноключевые криптографические системы являются классическими системами криптографической защиты информации. Для шифрования и расшифрования сообщений в них используется один и тот же ключ, сохранение которого в тайне обеспечивает надежность защиты информации. Шифровальную схему в этом случае можно представить следующим образом:

$$Y = E_Z(X)$$
$$X = D_Z(Y) = D_Z(E_Z(X)),$$

где X — открытый текст; Y — шифротекст;

D_Z — функция шифрования с секретным ключом z;

E_Z — функция расшифрования с секретным ключом z.

Открытый текст, как правило, имеет произвольную длину. В связи с этим он разбивается на блоки фиксированной длины и каждый блок шифруется в отдельности, независимо от его получения во входной последовательности. Соответствующие методы шифрования называются блочными, а наиболее важными шифрами при этом являются шифры замены (подстановки). Шифры замены образуются с помощью замены знаков исходного сообщения на другие знаки.

Простейшим шифром замены является шифр Цезаря. В этом шифре буквы исходного сообщения латинского алфавита заменяются буквами, расположенными тремя позициями правее. Однако вскрытие таких шифров легко осуществляется путем

перебора всех возможных ключей, в качестве которых используется величина сдвига букв сообщения в алфавите, до появления осмысленного текста.

Устойчивость шифра замены можно повысить за счет использования «перемешанного» алфавита. Однако наиболее стойким к расшифрованию сообщений из данного класса шифров является шифр полиалфавитной замены, в котором применяется несколько алфавитов, поочередно используемых для замены букв открытого текста.

Разновидностью шифрования с использованием полиалфавитной замены знаков сообщения является метод Вижинера (или шифр Вижинера), в котором важную роль играет ключевое слово.

Приведем в качестве примера программу шифрования текста сообщения с помощью шифра Вижинера. Программа может быть применена для создания шифротекстов с последующей передачей их в одноключевых криптосистемах.

Математическая постановка такой задачи заключается в следующем. Множество из 26 алфавитов, для английского текста (по числу букв), формируется последовательным циклическим сдвигом букв исходного алфавита (аналогично принципу формирования шифра Цезаря). Совокупность всех алфавитов образует так называемую таблицу Вижинера.

При шифровании буквы ключевого слова определяют выбор конкретного сдвинутого алфавита, используемого при замене соответствующей буквы сообщения.

Процесс шифрования может быть описан как процесс суммирования по модулю 26 номеров соответствующих друг другу букв открытого текста и ключевого слова.

В данном случае для уяснения принципа получения криптограмм с использованием шифра Вижинера применим ключевое слово и один алфавит английского языка.

Каждой букве алфавита сопоставим цифру (A $^{\Omega\Omega}$ 0, B $^{\Omega\Omega}$ 1, …, Z $^{\Omega\Omega}$ 25). Ключевое слово k_i задается определенным количеством букв d и повторно записывается под шифруемым сообщением m_i. В дальнейшем в i-м столбце из двух букв буква сообщения m_i складывается по модулю 26 со стоящей под ней буквой ключевого слова k_i в виде:

$$g_i = m_i + k_i \bmod 26,$$

где g_i — буквы полученной криптограммы.

Расшифровка криптограммы осуществляется вычитанием ключевого слова по модулю 26. При $d = 1$ шифр Вижинера является шифром Цезаря.

2. Примеры.

Пример 1. Шифр Цезаря

Получим криптограмму с использованием шифра Цезаря с ключом $d = 1$ на базе английского алфавита, строчный регистр.

Исходное сообщение	i	n	f	o	r	m	f	t	i	o	n
Криптограмма	j	o	g	p	s	n	g	u	j	p	o

Для русского языка с ключом $d = 10$

Исходное сообщение	И	Н	Ф	О	Р	М	А	Ц	И	Я
Криптограмма	Т	Ч	Ю	Ш	Ь	Ц	Й	А	Т	И

Пример 2. Шифр Вижинера

Получим криптограмму с использованием шифра Цезаря с ключевым словом «code» (ключи «c=2», «o=14», «d=3», «e=4») на базе английского алфавита, строчный регистр.

Исходное сообщение	i	n	f	o	r	m	f	t	i	o	n
Ключевое слово	c	o	d	e	c	o	d	e	c	o	d
Криптограмма	k	b	i	s	t	a	i	x	k	c	q

Для русского языка с ключевым словом «код» (ключи «к=10», «о=14», «д=4»).

Исходное сообщение	И	Н	Ф	О	Р	М	А	Ц	И	Я
Ключевое слово	К	О	Д	К	О	Д	К	О	Д	К
Криптограмма	Т	Ы	Ш	Ш	Ю	Р	Й	Д	М	И

3. Практика.

Составьте алгоритмическое и программное обеспечение:

1. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
2. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
3. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
4. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
5. Постройте программно таблицу Вижинера и выведите в файл.

Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 5. Построение защищенных экономических систем

1. Вопросы для обсуждения

1) Основные технологии построения защищенных ЭИС.
2) Место ИБ экономических систем в национальной безопасности страны.
3) Концепция ИБ.
4) Особенности работы с персоналом, владеющим конфиденциальной информацией.
5) Технологические основы обработки конфиденциальных документов.

2. Лабораторная работа 4

Обмен ключами по Диффи-Хелману

1. Теория.

Для защиты информации в вычислительных сетях используется такой Е криптографического преобразования как шифрование, в котором всегда различают два элемента: ключ и алгоритм. При этом ключом является секретное состояние некоторых параметров алгоритма криптопреобразования сообщения.

На практике в зависимости от способа применения ключа различают *i* типа криптографических систем:

- Одноключевые (симметричные)
- Двухключевые (несимметричные)

В одноключевых системах, называемых традиционными, ключи шифрования и расшифрования (л.р.2) либо одинаковы, либо легко выводятся один из другого, об' печивая таким образом единый общий ключ. Такой ключ является секретные передается получателю сообщения только по защищенному каналу связи.

Однако при этом имеет место следующий парадокс: если для обмена ее секретного ключа используется защищенный канал, то нет необходимости шифровать конфиденциальные сообщения, гораздо проще отправить их по это: каналу.

Отмеченный парадокс может быть исключен использованием идеи Диффи и Хеллмана, которые предложили способ выработки секретного ключа без предварительного согласования между абонентами сети путем обмена информацией по открытому каналу. Этот способ был предложен Диффи и Хеллманом в 1976 году и опубликован в ряде работ по криптографии. Реализация такого способа привела к появлению открытого шифрования. Абонент сего открыто сообщал о том, каким образом зашифровать к нему сообщение, расшифровать же его мог только он сам.

Основную роль при выработке секретного ключа в данном случае играют математические операции, когда прямая операция сравнительно проста, а обратная — практически трудно реализуема.

Прямая операция: возвести основание a в степень p и взять остаток по модулю m вида:

$L = a^p \bmod m$.

Обратная операция: найти p, зная L, a и m.

Обратная операция (задача) при этом может быть решена простым перебором значений p, но практически не решается при больших значениях p .

В предлагаемом алгоритме выработки секретного ключа известны основание a и mod m.

Отправитель сообщения с помощью генератора случайных чисел (ГСЧ) получает случайное число X ($1 < x < m$), вычисляет значение $L_0 = a^y \bmod m$ и посылает L_0 получателю.

Получатель принимает L_0 вырабатывает с помощью своего ГСЧ случайное число Y ($1 < y < m$), вычисляет значение $L_p = a^y \bmod m$ и посылает L_p отправителю.

x x_i $= a^{yx} \bmod m$. Получатель вычисляет

Отправитель принимает Lp, вычисляет $K0=Lp$

$K_p = L_0^y = a^{yx} \bmod m$.

Так как $K_0 = K_p$., то это число и является общим секретным ключом.

Злоумышленник, перехватив L_0 и L_p , не знает случайных чисел x и y и не сможет расшифровать исходный текст сообщения.

3. Практика.

Составьте программное обеспечение, реализующее алгоритм обмена ключами. Ключи должны автоматически формироваться в файлы. Должна быть обеспечена наглядность выполнения алгоритма. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 6. Защищенные компьютерные системы

1. Вопросы для обсуждения

1) Использование защищенных компьютерных систем.
2) Защита операционной системы и других системных программных средств.
3) Организация доступа в локальных сетях.

2. Лабораторная работа 5

Шифр RSA

1. Теория.

Защита данных с помощью криптографического преобразования является эффективным решением проблемы их безопасности. Зашифрованные данные доступны лишь тем, кто знает, как их расшифровать, то есть тем, кто обладает соответствующим ключом шифрования.

Одним из наиболее перспективных криптографических стандартов на шифрование данных являются системы с открытым ключом. В таких системах для шифрования используется один ключ, а для расшифрования другой. Первый ключ является открытым

и может быть опубликован для шифрования своей информации любым пользователем сети. Получатель зашифрованной информации для расшифровки данных использует второй ключ, являющийся секретным. При этом должно соблюдаться следующее условие: секретный ключ не может быть определен из опубликованного открытого ключа.

Криптографические системы с открытым ключом используют необратимые или односторонние функции, обладающие важным свойством: при заданном значении x относительно просто вычислить значение $f(x)$, однако, если $y = f(x)$, то нет простого пути для вычисления значения x, то есть очень трудно рассчитать значение обратной функции 1
// $f(y)$.

В настоящее время широко используется метод криптографической защиты данных с открытым ключом RSA, получившим название по начальным буквам фамилий его изобретателей (Rivest, Shamir, Adleman). На основе метода RSA разработаны алгоритмы шифрования, успешно применяемые для защиты информации. Он обладает высокой криптостойкостью и может быть реализован при использовании относительно несложных программных и аппаратных средств. Данный метод позволил решить проблему обеспечения персональных подписей в условиях безбумажной передачи и обработки данных. Описание схем формирования шифротекста в алгоритмах типа RSA приведено в различной литературе.

Использование метода RSA для криптографической защиты информации может быть пояснено с помощью структурной схемы, представленной на рисунке.

Функционирование криптосистемы на основе метода RSA предполагает формирование открытого и секретного ключей. С этой целью необходимо выполнить следующие математические операции:

- Выбираем два больших простых числа p и q, понимая под простыми числами такие числа, которые делятся на само себя и число 1
- Определяем $n = p \times q$,
- Вычисляем число $k = (p-1)\ (q-1)$,
- Выбираем большое случайное число d, взаимно простое с числом k (взаимно простое число — это число, которое не имеет ни одного общего делителя, кроме числа 1)
- Определяем число e, для которого истинным является соотношение

$$(e \times d) \bmod k = 1$$

- Принимаем в качестве открытого ключа пару чисел $\{e, n\}$
- Формирование секретного ключа в виде пары чисел $\{d, n\}$

Для зашифровки передаваемых данных с помощью открытого ключа $\{e, n\}$ необходимо выполнить операции:

- Разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде чисел $M(i) = 0,1,..., n-1$
- Зашифровать текст в виде последовательности чисел $M(i)$ по формуле

$$C(i) = (M(i)^e) \bmod n$$

- Расшифрование шифротекста производится с помощью секретного ключа $\{d, n\}$ при выполнении следующих вычислений:

$$M(i) = (C(i)^d) \bmod n$$

В результате получаем последовательность чисел $M(i)$, представляющих исходные данные. На практике при использовании метода RSA длина p и q составляет 100 и более десятичных знаков, что обеспечивает высокую криптостойкость шифротекста.

$$M(I) = (C(I) \times \bmod n \qquad \{e, n\}$$

3. Практика.

Составьте программное обеспечение, реализующее алгоритм RSA. Исходные данные должны передаваться через файлы: файл с открытым ключом, закрытым

ключом и шифруемая информация. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 7. Основы криптографии

1. Вопросы для обсуждения

1) Методы криптографии.
2) Классификация шифров по различным признакам.
3) Шифры перестановки.
4) Шифры замены.
5) Шифры гаммирования.
6) Надежность шифров.

2. Лабораторная работа 6

Циклические коды

1. Теория.

Принцип работы – метод проверки целостности массива бит, основанный на свойствах операции взятия остатка в полиномиальной арифметике по модулю 2 с основными операциями 0+0=0, 0+1=1, 1+0=1, 1+1=0, 0*0=0, 0*1=0, 1*0=0, 1*1=1.

CRC Cyclic Redundancy Check - (Циклический избыточный контрольный код) результат операции взятия остатка от деления проверяемого битового массива на некоторое число-делитель, которое обладает специфическими свойствами равномерно "размазывать" изменение в некотором бите массива на возможно большее число бит результата. Это число-делитель, называемое образующим полиномом, выбирается так, чтобы само являлось полиномиально простым - не делилось полиномиально нацело на любые числа от 2 до самого себя. кроме того, есть и другие критерии выбора полинома, направленные на уменьшение вероятности пропуска типичных ошибок в каналах передачи данных, так что самостийно выдумывать полиномы - дело не только трудное, но и вредное.

Полином может быть записан как в виде суммы степеней с ненулевыми (а значит - единичными) коэффициентами, так и маской этих единичек. Порядок записи единиц в маске однозначно связан с порядком обработки бит в проверяемом массиве, потому что в процессе расчета CRC промежуточный результат необходимо циклически сдвигать в ту же сторону, что и биты проверяемого массива, причем сдвигать так, чтобы вытеснялись старшие степени полинома. Самая старшая степень в маске не учитывается, она определяет только число бит маски. Ниже старшие степени отделены пропусками. Чтобы реализовать проверку с применением CRC, помимо маски полинома и порядка следования бит в массиве (определяющего направление циклического сдвига), необходимо знать начальное значение CRC и метод завершающей модификации результата вычисления CRC.

Типичные методы, применяемые для контроля целостности данных при передаче и хранении:

CCITT-CRC-32 [Все распространенные архиваторы и протоколы с CRC-32] биты массива обрабатываются, начиная с младшего бита в байте - LSB. Образующий полином: X^0+X^1+X^2+X^4+X^5+X^7+X^8+X^10+X^11+X^12+X^16+X^22+X^23+X^26 +X^32 Маска = EDB88320h, в которой правые цифры соответствуют старшим степеням, сдвиг выполняется вправо. Начальное значение - 0xFFFFFFFF. Конечная модификация - поразрядная инверсия всех битов результата.

CCITT-DOS-16 [архиватор LHA и, вероятно, некоторые другие с CRC-16] биты массива обрабатываются, начиная с младшего бита в байте - LSB. Образующий полином: X^0+X^2+X^15 +X^16 Маска = A001h, в которой правые цифры соответствуют старшим степеням, сдвиг выполняется вправо. Начальное значение - 0000. Конечная модификация - отсутствует.

CCITT-CRC-16 [протоколы передачи данных с CRC-16, Контроль EMSI] биты массива обрабатываются, начиная со старшего бита в байте - MSB. Образующий полином: X^16+ X^12+X^5+X^0 Маска = 0x1021, в которой левые цифры соответствуют старшим степеням, сдвиг выполняется влево. Начальное значение - 0x0000. Конечная модификация
- отсутствует.

Теперь собственно описание вычисления: Рабочая переменная W соответствующей разрядности, в которой будет накапливаться результат, инициализируется начальным значением. Затем для каждого бита *m* входного массива выполняются следующие действия: *W* сдвигается на 1 бит (о направлении сдвига см. выше) В освободившийся бит *W* помещается нуль. Бит, только что вытолкнутый из *W*, сравнивается с битом *m*. если они не совпали, выполняется операция исключающего ИЛИ над *W* и маской полинома, результат заносится в *W*. И так, пока не будут обработаны все биты массива. После чего над *W* производится конечная модификация.

Можно сказать, что обычно так CRC считают только в схемных реализациях. Потому, что это очень медленно - ведь число циклов равно числу бит массива. При реализации на программном уровне обработка ведется восьмерками бит - байтами. Заводится табличка из 256 элементов. Каждое значение - результат расчета CRC над восьмеркой бит индекса элемента: for i := 0 to 255 do tab[i] := count_crc(*i*); После этого расчет CRC для массива можно вести байтами. Начало и конец расчета, как и раньше. А цикл идет для каждого байта *Q*: *W* := *W* XOR *Q*; *W* := сдвиг(*W*, 8) XOR tab[*W*]

При LSB-порядке Q операция XOR выполняется над младшими битами W, а при MSB-порядке - над старшими. Индексом в таблице служат именно эти биты.

Байтовый табличный метод требует ощутимых затрат памяти под таблицу. Для CRC-32 требуется таблица размером в килобайт. Если килобайт памяти для реализации с одним циклом на байт массива это перебор, можно предложить компромиссный вариант - считать CRC, не восьмерками, а четверками бит. CRC-32-таблица из 16 значений займет 64 байта, но скорость будет несколько ниже, чем при большой таблице, хотя существенно выше, чем без нее вообще.

В реализации расчета CRC для z-modem'a есть один тонкий момент. Там допущено отклонение от базовой схемы. Две строки поменяли местами: *W* := сдвиг(*W*, 8) XOR tab[
W]; *W* := *W* XOR *Q*

В результате получается не чистый CRC: контрольный код z-modem'a для массивов до двух байт размером "равен" самому массиву. Например, для массива из двух байт 3 и 8, контрольный код будет равен 0308h.

[И наконец, одно маленькое замечание. Операция вычисления CRC обратима. Не в том смысле, конечно, что по CRC можно восстановить весь массив, а в том, что если дано CRC разрядности *N* и дан некоторый массив, в котором где-нибудь можно поменять подряд *N* бит, то подогнать этот массив под заданную CRC не сложнее, чем посчитать CRC. CRC не является криптографически устойчивой хеш-функцией.]

3. Практика.

Составьте алгоритмическое и программное обеспечение, реализующее алгоритм CRC. В качестве исходных данные – файл. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

Тема 8. Обеспечение ИБ на уровне государства

1. Вопросы для обсуждения

1) Международные стандарты информационного обмена. ИБ в условиях функционирования в России глобальных сетей.
2) Назначение и задачи в сфере обеспечения ИБ на уровне государства.

2. Контрольная работа 2

Вопросы к контрольной работе 2

1. Опреление понятия «Система информационной безопасности»
2. Элементы системы информационной безопасности
3. Определение понятия «Государственная тайна»
4. Регулирование правовых отношений в области защиты государственной тайны
5. Модели безопасности их применение
6. Место ИБ экономических систем в национальной безопасности страны
7. Основы конфиденциального документооборота
8. Особенности работы с персоналом, владеющим конфиденциальной информацией
9. Принципы построения защищенных компьютерных систем
10. Элементы операционной системы
11. Управление доступом пользователей в опреационных системах
12. Парольная политика популярных операционных систем
13. Состав локально-вычислительных сетей
14. Коммутаторы, концентраторы, маршрутизаторы
15. Организация доступа в локальных сетях
16. Контроль сетевых подключений
17. Управление сетевой маршрутизацией
18. Управление доступом к компьютерам
19. Система управления паролями
20. Управление доступом к приложениям
21. Управление доступом к библиотекам исходных текстов программ

3. Тест итоговый

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. Какова цель ревизии установленного оборудования?

- Идентификация типов оборудования и устройств, сети.
- Идентификация местонахождения каждого элемента сети.
- Мониторинг и анализ работы сети.
- Перенос информации на чертежи здания для создания карты нарезки.

2. Действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов - это

- Защитные меры
- Комплексные меры
- Превентивные меры
- Организационные меры

3. Какова цель ревизии средств защиты сети?

- Согласование требований по защите сети со строительными нормами и
- нормами секретности.
- Оценка способностей клиентов пользоваться сетевым оборудованием и
- программным обеспечением.
- Выяснение способности сети гарантировать целостность данных.
- Определение состава аппаратно-программного комплекса, требующегося
- для обеспечения защиты сети.

4. Какие шаги следует предпринять для анализа и решения проблемы в сети после сбора данных о работе?

- Определить, является ли проблема периодической или устойчивой; составить список возможных причин; расставить приоритеты причин.
- Расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины; отследить тенденции с целью предвидения возникновения проблем в будущем.
- Составить список возможных причин; расставить приоритеты причин; используя средства управления сетью или метод замены, идентифицировать причины.
- Определить, можно ли воспроизвести проблему; расставить приоритеты возможных причин; используя средства управления сетью или метод замены, идентифицировать причины.

5. Что из приведенного ниже должно быть включено в отчет о проведении оценки?

- Состав сетевой аппаратуры и программного обеспечения, которые не удовлетворяют промышленным стандартам.
- Журналы, показывающие тенденцию к уменьшению скорости трафика в определенных сегментах сети.
- Описание случаев и мест несанкционированного доступа к файлам.
- Описание типов пользователей, наиболее часто сталкивающихся с проблемами при пользовании сетью.

Перечень основных вопросов, выносимых на зачет

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации
3. Задание требований к информационной безопасности организации
4. Виды возможных нарушений информационной системы. Общая классификация информационных угроз.
5. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор.
6. Угрозы компьютерной информации, реализуемые на аппаратном уровне.
7. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей.
8. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
9. Объект и субъект защиты информации
10. Каналы утечки информации. Классификация каналов утечки информации
11. Модель нарушителя информационной безопасности
12. Классификация нарушителей информационной безопасности
13. Компьютерные вирусы. История. Определение по УК РФ.
14. Определение понятия «Система информационной безопасности»
15. Элементы системы информационной безопасности
16. Определение понятия «Государственная тайна»
17. Регулирование правовых отношений в области защиты государственной тайны
18. Модели безопасности их применение
19. Место ИБ экономических систем в национальной безопасности страны
20. Основы конфиденциального документооборота
21. Особенности работы с персоналом, владеющим конфиденциальной информацией
22. Принципы построения защищенных компьютерных систем
23. Элементы операционной системы
24. Управление доступом пользователей в операционных системах
25. Парольная политика популярных операционных систем

26. Состав локально-вычислительных сетей
27. Коммутаторы, концентраторы, маршрутизаторы
28. Организация доступа в локальных сетях
29. Контроль сетевых подключений
30. Управление сетевой маршрутизацией
31. Управление доступом к компьютерам
32. Система управления паролями
33. Управление доступом к приложениям
34. Управление доступом к библиотекам исходных текстов программ
35. Правовое урегулирование защиты информации. Стандарты ИБ
36. Защита данных криптографическими методами. Методы шифрования.
37. Защита данных криптографическими методами. Алгоритмы шифрования.

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем				
1.	Задание закрытого типа	Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя: а. сокрытие. б. мощность. в. сбор информации. г. отсутствие последствий после вторжения	г	2
2.		Укажете два основных метода анализа, связанных с выявлением атак в системах обнаружения вторжений. а. сигнатурный метод и метод, связанный с выявлением аномального поведения. б. сигнальный метод и метод, связанный с выявлением аномального поведения. в. сигнатурный и сигнальный методы. г. структурный и сигнальный методы.	а	2
3.		Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться (выберите все возможные варианты)? а. использовать максимально возможное количество символов в пароле; б. использовать в качестве пароля имя супруга/супруги, ребенка или кличку собаки (чтобы не забыть пароль);	в, г	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		в. использовать хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ; г. использовать пароль, который трудно угадать по смыслу.		
4.		Уязвимость информации — это: а. Возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. б. Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. в. Это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.	б	2
5.		Под угрозой безопасности информации в компьютерной системе (КС) понимают: а) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. б) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. с) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости	с	2
6.	Задание открытого типа	Основные задачи при эксплуатации механизмов аутентификации	При эксплуатации механизмов аутентификации основными задачами являются: генерация или изготовление идентификаторов, их учет и хранение, передача	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.	
7.		Что понимается под системой защиты от несанкционированного использования и копирования	Под системой защиты от несанкционированного использования и копирования понимается комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.	3
8.		Что должен выполнить для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы?	Для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы должен выполнить следующие функции: − анализ аппаратно-программной среды компьютера, на котором должна будет выполняться инсталлируемая программа, и формирование на основе этого анализа эталонных характеристик среды выполнения программы; − запись криптографически преобразованных эталонных характеристик аппаратно-программной среды компьютер на винчестер.	3
9.		Основные компоненты системы защиты программных	Основные компоненты системы защиты программных	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		продуктов от несанкционированного копирования	продуктов от несанкционированного копирования: модуль проверки ключевой информации (некопируемой метки на дистрибутивном диске, уникального набора характеристик компьютера, идентифицирующей информации для легального пользователя) – может быть добавлен к исполнимому коду защищаемой программы по технологии компьютерного вируса, в виде отдельного программного модуля или в виде отдельной функции проверки внутри защищаемой программы; модуль защиты от изучения алгоритма работы системы защиты; модуль согласования с работой функций защищаемой программы в случае ее санкционированного использования; модуль ответной реакции в случае попытки несанкционированного использования (как правило, включение такого модуля в состав системы защиты нецелесообразно по морально-этическим соображениям).	
10.		Основные требования, предъявляемые к системе защиты от копирования	Основные требования, предъявляемые к системе защиты от копирования: обеспечение некопируемости дистрибутивных дисков стандартными средствами (для такого копирования нарушителю по	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			требуется тщательное изучение структуры диска с помощью специализированных программных или программно-аппаратных средств); обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без применения специализированных программно-аппаратных средств (нарушитель должен быть специалистом высокой квалификации); обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами (нарушителю потребуется использование или разработка специализированных дисассемблеров); обеспечение сложности изучения алгоритма распознавания индивидуальных параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты (нарушителю будет сложно эмулировать легальную среду запуска защищаемой программы).	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению зачета

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по лабораторной работе должно содержаться:

Титульный лист в соответствии с рекомендации кафедры информационной безопасности (//fileserver)

Задание на лабораторную работу.

Краткую теорию.

Ход выполнения работы: алгоритмы, программное обеспечение (исходный код), результаты тестирования.

Выводы.

Критерии оценки лабораторных работ:

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретических заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине отводится 100 баллов (90 баллов на текущие формы контроля и до 10 баллов отводится на бонусы), которые накапливаются студентом в течение всего семестра изучения дисциплины.

отсутствие пропусков практических занятий – максимально 1 балл.

Оценивание студентов на зачете осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений по разработке документов различных видов. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Критерии оценки зачета:

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

Таблица 10 – Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Выполнение лабораторной работы*	6/11	66	По расписанию
2.	*Выполнение контрольной работы*	2/6	12	
3.	*Тест*	2/6	12	
Всего			**90**	-
Блок бонусов				
4.	*Посещение занятий без пропусков*	1	3	
5.	*Своевременное выполнение всех заданий*	1	3	
6.	*Активность студента на занятии*	1	4	
Всего			**10**	-
ИТОГО			**100**	-

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1

Показатель	Балл
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	незачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Шаньгин В.Ф., Информационная безопасность и защита информации/ Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 -URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).
2. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). - URL: http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).
3. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202381.html (ЭБС «Консультант студента»).
4. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

1. Защита информации : Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2011. - URL: http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).
3. Галатенко, В. А. Защита информации: курс лекций: учеб.пособие / В. А. Галатенко ; под ред. В. Б. Бетелина.- 2-е изд., испр. - М. : Интернет-Ун-т Информ. Технологий, 2004. - 264 с. (45 экз.)
4. Девянин П.Н. Модели безопасности компьютерных систем.-М.: Академия, 2005. 144 с. (50 экз.)

5. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч. (45 экз.)

6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : уч.пособие. – М.: Издат центр «Академия», 2005, – 256 с. (69 экз.)

7. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ; стер. - М. : Академия, 2009. - 336 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46. (19 экз.)

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения публичной защиты проектов, необходима мультимедийная аудитория с проектором.

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет.

Учебные аудитории, библиотеки АГУ, центр мониторинга и аудита качества образования, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).