Приложение 3
к основной профессиональной образовательной программе
по направлению подготовки 38.03.02 Менеджмент
направленность (профиль) программы
Менеджмент организации

Министерство образования и науки Российской Федерации
Пермский институт (филиал)
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»

Одобрено
на заседании Учебно-методического совета
Пермского института (филиала)
протокол № 9 от «20» июня 2018 г.

Председатель совета _____ В.Н. Яковлев

Факультет Менеджмента

Кафедра Торгового дела и информационных технологий

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
для набора 2018 года

Б1.В.ДВ.02.02 Основы информационной безопасности

Направление подготовки 38.03.02
«Менеджмент»

Направленность (профиль) программы
«Менеджмент организации»

Уровень высшего образования ***Бакалавриат***

Программа подготовки ***Прикладной бакалавриат***

Пермь – 2018 г.

Рецензенты:

1. Катанова Татьяна Николаевна, кандидат физико-математических наук, доцент, доцент кафедры информатики и вычислительной техники Пермского государственного гуманитарно-педагогического университета
2. Елтышев С.А., генеральный директор ООО «Фараон»

Аннотация рабочей программы дисциплины

Цель дисциплины

В результате изучения дисциплины «Основы информационной безопасности» у обучающихся формируются знания по общим вопросам информационной безопасности, а также защите информации в информационных системах. В курсе основное внимание уделяется изложению общих положений информационной безопасности и защиты информации, моделей безопасности, защиты информации в информационных системах, глобальных и локальных сетях ЭВМ, персональных компьютерах, криптографических методов, антивирусной защиты.

Задачи дисциплины:

- усвоение основных понятий в области информационной безопасности;
- овладение основами защиты информации. Освоение практических методов защиты информационных систем организации;
- приобретение обучающимися навыков квалифицированной работы с криптографическими методами защиты информации;
- подготовка студентов к последующей образовательной и профессиональной деятельности;
- формирование логического мышления.

Рабочая программа составлена на основании Федерального государственного образовательного стандарта по направлению 38.03.02 – «Менеджмент».

Составитель: Ильин В.В., к.т.н., доцент кафедры торгового дела и информационных технологий

Рабочая программа утверждена на заседании кафедры Торгового дела и информационных технологий протокол № 10 от «31» мая 2018 г.

Зав. кафедрой /Писарева Е.В.

Дополнения и изменения, внесенные в рабочую программу, утверждены на заседании кафедры Товароведения и экспертизы товаров, протокол № 13 от «03» июня 2019 г.

Заведующий кафедрой Мазунина Т.А.

Одобрено УМС Пермского института (филиала) РЭУ им. Г.В.Плеханова, протокол № 9 от «26» июня 2019 г.

Председатель Яковлев В.Н.

Дополнения и изменения, внесенные в рабочую программу, утверждены на заседании кафедры экономического анализа и статистики
протокол № 8 от «28» мая 2020 г.

Заведующий кафедрой _____ О.И.Агеева
(подпись)

Одобрено УМС Пермского института (филиала) РЭУ им. Г.В. Плеханова
протокол № 9 от «21» мая 2020 г.

Председатель _____ В.Н. Яковлев
(подпись)

Содержание

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ 5

Цель дисциплины 5
Место дисциплины в структуре ОПОП ВО (основной профессиональной образовательной программы высшего образования) 5
Требования к результатам освоения содержания дисциплины 6
Формы контроля 6

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 8

III. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 11

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 11

Рекомендуемая литература 11
Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля) 12
Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости) ..... **Ошибка! Закладка не определена.**
Средства антивирусной защиты информации 13
Шифр Цезаря. 14
Электронная цифровая подпись 16
Межсетевые экраны 20
Программно – аппаратные средства защиты от НСД 21

V. ТЕМАТИЧЕСКИЙ ПЛАН ИЗУЧЕНИЯ ДИСЦИПЛИНЫ 22

(*СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ЧАСОВ И ВИДОВ ЗАНЯТИЙ)* 22

(*ОЧНАЯ ФОРМА ОБУЧЕНИЯ)* 22

VI. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ 23

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы (см. таблицу раздела II) 23
6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (см. таблицу раздела II и раздел VIII) 23
6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы 23

VIII. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ 29

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель дисциплины

В результате изучения дисциплины «Основы информационной безопасности» у обучающихся формируются знания по общим вопросам информационной безопасности, а также защите информации в информационных системах. В курсе основное внимание уделяется изложению общих положений информационной безопасности и защиты информации, моделей безопасности, защиты информации в информационных системах, глобальных и локальных сетях ЭВМ, персональных компьютерах, криптографических методов, антивирусной защиты.

Задачи дисциплины:

- усвоение основных понятий в области информационной безопасности;
- овладение основами защиты информации. Освоение практических методов защиты информационных систем организации;
- приобретение обучающимися навыков квалифицированной работы с криптографическими методами защиты информации;
- подготовка обучающихся к последующей образовательной и профессиональной деятельности;
- формирование логического мышления.

Место дисциплины в структуре ОПОП ВО (основной профессиональной образовательной программы высшего образования)

Дисциплина «Основы информационной безопасности», относится к вариативной части учебного плана и является дисциплиной по выбору.

Объем дисциплины и виды учебной работы

Показатели объема дисциплины	Всего часов по формам обучения		
	очная	*Заочная ф.о.*	*Ускоренная на базе СПО или ВО*
Объем дисциплины в зачетных единицах	**4 ЗЕТ**		
Объем дисциплины в часах	**144**		
Контактная работа обучающихся с преподавателем (Контакт. часы), всего:	**42**	**14,25**	**10,25**
1. Аудиторная работа (Ауд.), всего:	**40**	**14**	**10**
в том числе:			
• лекции	*14*	*6*	*4*
• лабораторные занятия			
• практические занятия	*26*	*8*	*6*
2. Контактная работа по промежуточной аттестации (Катт)	**2**	**-**	**-**
3. Контактная работа по промежуточной аттестации в период экз. сессии / сессии заочников (Каттэк)	**-**	**0,25**	**0,25**
Самостоятельная работа (СР), всего:	**102**	**129,75**	**133,75**
в том числе:			
• самостоятельная работа в семестре (СР)	102	126	130
• самостоятельная работа в период экз. сессии (Контроль)		3,75	3,75

Дисциплина «Основы информационной безопасности» базируется на входных знаниях, умениях и компетенциях, полученных студентами в процессе освоения школьной программы среднего (полного) общего образования по следующим предметам: «Математика», «Физика», «Информатика», а также при усвоении дисциплин бакалавриата «Информационные технологии», «Информационно-коммуникационные технологии».

Для успешного освоения дисциплины «Основы информационной безопасности», студент должен:

1. знать сущность информационных процессов и их взаимосвязи;
2. уметь применять математический аппарат при исследовании процессов;
3. уметь использовать современные технические средства и информационные технологии для решения проблемных ситуаций.

Изучение дисциплины «Основы информационной безопасности» необходимо для дальнейшего ведения профессиональной деятельности.

Требования к результатам освоения содержания дисциплины

В результате освоения дисциплины должны быть сформированы следующие компетенции:

Вид деятельности: информационно-аналитическая

ПК-11 - владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов.

В результате освоения компетенции **ПК-11**обучающийся должен:

Знать: составляющие внутреннего документооборота организации, методы и принципы его организации; современные программные средства офисного назначения.

Уметь: анализировать внешнюю и внутреннюю информацию, ее влияние на функционирование организации;

Владеть: навыками ведения внутреннего документооборота организации; навыками работы в современных программных средствах офисного назначения.

ПК-12 – умение организовать и поддерживать связи с деловыми партнерами, используя системы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления).

В результате освоения компетенции ПК-12 обучающийся должен:

1. **Знать**: методы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проект.
2. **Уметь:** организовать и поддерживать связи с деловыми партнерами.
3. **Владеть**: методами обмена опытом при реализации проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления)

Формы контроля

Текущий и рубежный контроль осуществляется лектором и преподавателем, ведущим лабораторные занятия, в соответствии с тематическим планом.

Промежуточная аттестация в 4 семестре – **зачет.**

Результаты текущего контроля и промежуточной аттестации формируют рейтинговую оценку работы студента. Распределение баллов при формировании

рейтинговой оценки работы студента осуществляется в соответствии с «Положением о рейтинговой системе оценки успеваемости и качества знаний студентов в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский экономический университет имени Г.В. Плеханова». Распределение баллов по отдельным видам работ в процессе освоения дисциплины «Основы информационной безопасности» осуществляется в соответствии с разделом VIII.

II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

и описание показателей и критериев оценивания компетенций на различных этапах их формирования в процессе освоения образовательной программы

№ п/п	Наименование раздела дисциплины (темы)	Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть, понимать)	Образовательные технологии
1.	Общие сведения о защите информации	Национальные интересы и безопасность. Основные угрозы безопасности России. Информационная безопасность. Жизненно важные интересы в информационной сфере и угрозы им. Информационная война. Информационное оружие. Принципы, основные задачи и функции обеспечения информационной безопасности. Функции государственной системы по обеспечению информационной безопасности. Ответственность за нарушение законодательства в информационной сфере. Характеристики информации. Угрозы защищенности информации. Защита информации. Задачи защиты информации. Основные предметные направления защиты информации. Примеры способов защиты информации. Стандарты в области защиты информации.	ПК-12 ПК-11	Знать: – основные понятия и определения информационной безопасности; – виды информации, классификацию угроз информационной безопасности. Уметь: – анализировать типы атак и угроз информационной безопасности; – формулировать соответствующие требования к системам защиты информации. Владеть: – базовыми навыками построения и управления систем защиты информации; – навыками отражения типовых атак на информационные системы.	Лекции, практические занятия, деловая игра, самостоятельная работа с литературой, консультации преподавателей, письменное домашнее задание
2.	Защита информации в информационных	Предмет и объекты защиты информации в ИС. Надежность информации. Уязвимость информации.	ПК-12 ПК-11	Знать: – основные понятия и концепции современных технологий защиты	Лекции, практические занятия,

	системах	Элементы и объекты защиты в ИС. Дестабилизирующие факторы ИС. Причины нарушения целостности информации (ПНЦИ). Каналы несанкционированного получения информации в ИС (КНПИ). Преднамеренные угрозы безопасности ИС. Функции и задачи защиты информации. Методы и средства защиты информации. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре. Использование простого пароля. Использование динамически изменяющегося пароля. Методы идентификации и установления подлинности субъектов и объектов. Своевременное обнаружение несанкционированных действий пользователей. Общие сведения о контроле информационной целостности.		информации; – основные методы создания систем защиты информации. Уметь: – анализировать причины нарушения целостности информации; – своевременно обнаруживать несанкционированные действия пользователей. Владеть: – базовыми методами идентификации и установления подлинности субъектов и объектов.; – навыками контроля информационной целостности.	индивидуальное домашнее задание, самостоятельная работа с литературой задание
3.	Криптографические методы защиты информации	Методы криптографического преобразования данных. Электронная цифровая подпись. Проблемы реализации методов криптографической защиты в ИС. Характеристики криптографических средств защиты.	ПК-12 ПК-11	Знать: - основы криптографии; - российские и американские стандарты шлифования. Уметь: - передавать конфиденциальную информацию по открытым каналам; - пользоваться шифром одноразового блокнота.	Лекции, практические занятия, индивидуальное домашнее задание, самостоятельная работа с литературой задание

				Владеть: - протоколами электронной подписи.	
4.	Особенности защиты информации в ПК.	Стандарты информационной безопасности. Защита в средах Windows. Классификация компьютерных вирусов. Средства и способы защиты информации. Каналы и причины утечки информации.	ПК-12 ПК-11	Знать - встроенные средства обеспечения безопасности; - архитектуру системы безопасности операционных систем . Уметь: - использовать инструментальные средства защиты информации. Владеть: - базовыми навыками работы администратором безопасности компьютерных систем.	Лекции, самостоятельная работа с литературой, индивидуальное домашнее задание, консультация преподавателей
5.	Проблемы защиты информации в сетях ЭВМ	Цели, функции и задачи защиты информации в сетях ЭВМ. Понятие сервисов безопасности. Международные стандарты X.800 и X.509. Методы цифровой подписи данных, передаваемых в сети. Пример системы защиты локальной вычислительной сети. Межсетевые экраны – брандмауэры (FireWall). Прокси (Proxy) серверы	ПК-12 ПК-11	Знать: - специализированные аппаратно- программные системы защиты безопасности Уметь: - ориентироваться в системах безопасности «Криптоцентр», «Криптон», «Верба», «Крипто-Про» и др. Владеть - базовыми навыками работы администратором компьютерных систем безопасности.	Лекции, практические занятия, самостоятельная работа с литературой, расчетно-аналитическое задание, консультации преподавателей

III. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе освоения дисциплины «Основы информационной безопасности» используются следующие образовательные технологии:

1. **Стандартные методы обучения:**

- лекции;
- практические занятия, на которых обсуждаются основные информационные технологии обработки информации, освещенные в лекциях и сформулированные в домашних заданиях;
- лабораторные работы;
- письменные или устные домашние задания;
- расчетно-аналитические, расчетно-графические задания;
- консультации преподавателей;
- самостоятельная работа студентов, в которую входит освоение теоретического материала, подготовка к практическим/лабораторным занятиям, выполнение указанных выше письменных/устных заданий, работа с литературой.

2. **Методы обучения с применением интерактивных форм образовательных технологий:**

- компьютерные симуляции;
- деловые игры.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Рекомендуемая литература

Основная литература

1. Мельников В. П. Информационная безопасность и защита информации : учеб. пособие для студ. учреждений высш. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под. ред. С. А. Клейменова. — 6-е изд., стер. — М.: Издательский центр «Академия», 2012. — 336 с.
2. Малюк А. А. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - М.: Гор. линия-Телеком, 2011. - 288 с.

Нормативно-правовые документы:

1. Конституция Российской Федерации (основной закон).
2. Федеральный закон «Об информационной безопасности» от 15.12.2005 №164.
3. Федеральный закон «Об информации и информатизации» от 17.03.2006 №263 с изменениями и дополнениями от 03.11.2007 № 345.
4. Федеральный закон № 149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации».

Дополнительная литература:

1. Партыка Т. Л. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.
3. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.

4. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.
5. Гришина Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с.
6. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с.
7. Барнс К. Защита от хакеров беспроводных сетей [Электронный ресурс] / Кристиан Барнс, Тони Боутс, Дональд Лойд и др.; пер. с англ. А. В. Семенова. - М.: Компания АйТи; ДМК Пресс, 2015. - 480 с.

Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. Study Stuff. Интеллектуальные информационные системы http://studystuff.ru/articles/prezentaczii-intellektualnyie-informaczionnyie-sistemyi.html
2. Банковские информационные системы — www.bis.ru
3. Диасофт – www.diasoft.ru
4. Инверсия – www.inversion.ru
5. ИНЭК — www.inec.ru
6. ПрограмБанк — www.programbank.ru
7. Про-инвест-ИТ — www.pro-invest.com/it
8. http://www.citforum.ru
9. http://www.habarov.da.ru

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Программное обеспечение:
Операционная система Microsoft Windows 7, Пакет прикладных программ Microsoft Office: 2010, Visual Studio 2017-2019 community, Acrobat Reader DC, 7-Zip, Notepad ++, Графический редактор GIMP, Inkscape, Электронный справочник 2GiS, Справочная Правовая система «Консультант плюс Эксперт», Электронный справочник "Система Гарант", Браузер: Google Chrome, Mozilla Firefox, MS Internet Explorer, Антивирусная программа Windows defender, Антивирусная программа 360 Total Security.

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Тема 1. Общие сведения о защите информации

Литература: О-1; О-2; Д-1; Д-3..
Вопросы для самопроверки:
1. Типы атак и угроз. Активные и пассивные противники.
2. Каналы утечки информации.
3. Стандарты информационной безопасности.
4. Основные методы обеспечения информационной безопасности.
5. Принципы построения защищенных систем.
6. Принципы, основные задачи и функции обеспечения информационной безопасности.
7. Функции государственной системы по обеспечению информационной безопасности. Ответственность за нарушение законодательства в информационной сфере.

8. Характеристики информации.
9. Угрозы защищенности информации.

Задания для самостоятельной работы:

1. Выбор эффективных средств защиты.
2. Типология компьютерных вирусов.
3. Антивирусное программное обеспечение. Обзор и анализ.
4. Экономическая оценка информационной безопасности

Средства антивирусной защиты информации

Задание 1.

1. Найти в Интернете методы профилактики от заражения вирусами компьютера, признаки заражения и действия пользователя при наличии признаков заражения.
2. Зайти на сайт www.kaspersky.ru. Изучить понятия и терминологию, используемые в антивирусных программах.

Заполнить таблицу:

Лаборатория Касперского	
Клиенты	
Продукты	
Защита от следующих видов угроз:	
Защита типов устройств:	
Обслуживание (сервис)	
Kaspersky **Internet Security 2010**	
Поддерживаемые ОС	
Аппаратные требования	
Содержание данного продукта	
Новинки продукта	
Дополнительные возможности	

Задание 2.

Заполнить таблицу сведениями об антивирусных программах.

Технические характеристики программы	**AVP**	**Dr.Web**
Поддерживаемые ОС		
Монитор. Сканер		
Ревизор		
Эвристический анализатор		
Проверка архивов		
Проверка электронной почты		

Доклады:

1.Аудит систем и сканирование уязвимостей.
2.Различные архитектуры с применением межсетевых экранов.

Тема 2. Защита информации в информационных системах

Литература: О-1; О-2; Д-1; Д-2; Д-3-7.

Вопросы для самопроверки:

1. Основные атаки и угрозы информационным системам.
2. Политики безопасности.
3. Модель системы защиты.
4. Этапы проектирования системы безопасности.

Задания для самостоятельной работы:

1.Сетевые атаки.

2.Централизованные DoS-атаки и DDoS-атаки.

Доклады:

1. Моделирование и проектирование систем защиты информации.

Тема 3. Криптографические методы защиты информации.

Литература: О-1; О-2; Д-1; Д-2, Д-3-7.

Вопросы для самопроверки:

1. Основы криптографии.
2. Передача конфиденциальной информации по открытым каналам. Симметричные криптосистемы.
3. Потоковые и блочные шифры.
4. Криптографические генераторы псевдослучайных последовательностей. Шифр одноразового блокнота.
5. Протоколы электронной подписи.

Задания для самостоятельной работы:

1. Криптография. Основные понятия и виды криптографических алгоритмов.
2. Надежность криптографического алгоритма и лобовая атака.
3. Симметричные криптоалгоритмы.
4. Криптоалгоритмы с открытым ключом.
5. Алгоритм RSA.
6. Шифр Цезаря.

Шифр Цезаря.

Цель работы: Освоить технологию шифрования и дешифрования информации в среде Excel с использованием шифра Цезаря.

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

При шифровании исходного текста каждая буква заменяется другой буквой того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту к концу от исходной буквы на ***k*** букв. При достижении конца алфавита выполняется циклический переход к его началу.

Например: пусть **A** – используемый алфавит:

A={a1, a2,…,am,...,aN},

где a1, a2,…,am,...,aN – символы алфавита; N ширина алфавита.

Пусть k – число позиций сдвига символов алфавита при шифровании, $0<k<N$. При шифровании каждый символ алфавита с номером m из кодируемого текста заменяется на символ этого же алфавита с номером m+k. Если $m+k>N$, номер символа в алфавите A определяется как m+k-N.

Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как m-k. Если $m-k<0$, то вычисление этого номера производится как m-k+N.

Достоинством этой системы является простота шифрования и дешифрования. К недостаткам системы Цезаря следует отнести:

- подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного и отрытого текста;

- сохраняется алфавитный порядок в последовательности заменяющих букв;

- при изменении значения k изменяются только начальные позиции такой последовательности;

- число возможных ключей k мало;

- шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифре.

Задание 1.

Зашифровать текст с помощью шифра Цезаря.

Порядок выполнения задания

1. Войти в среду **Excel**. Создать новый документ, перейти на второй лист этого документа. Начиная с ячейки А1 до А40 набрать алфавит, как показано на рисунке 20.

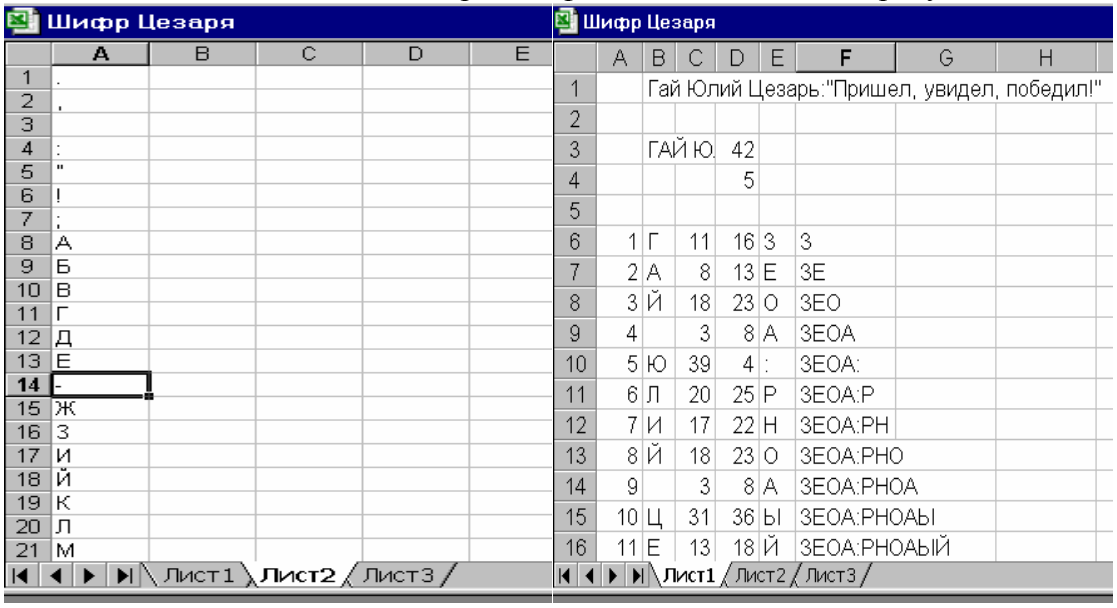

Рис. 20 Шифр Цезаря

Выделить весь диапазон алфавита и назначить ему имя “АВС” (через контекстное меню).

2. На первом листе документа в ячейке В1 набрать текст, который необходимо зашифровать, например: Гай Юлий Цезарь:”Пришел, увидел, победил!” При наборе текста необходимо использовать только те символы, которые входят в алфавит.

3. В ячейке В3 записать формулу «=ПРОПИСН(В1)», функция ПРОПИСН переводит буквенные символы в строке в прописные буквы.

4. В ячейке D3 записать формулу «=ДЛСТР(В3)», функция ДЛСТР позволяет определить длину строки, что необходимо пользователю, для кодировки исходной строки.

5. В ячейку D4 записать значение k, например, 5.

6. В столбце А, начиная с ячейки А6, пронумеровать ячейки числами последовательного ряда от 1 до N, где N – число символов в тексте, включая пробелы.
N рассчитано в ячейке D3.

7. В ячейку В6, записать формулу “=ПСТР(В$3;А6;1)”, которая разделяет кодируемый текст на отдельные символы. Скопировать эту формулу в ячейки В7- В47.

8. В ячейку С6 записать формулу “=ПОИСКПОЗ(В6;АВС;0)”. Функция ПОИСКПОЗ производит поиск индекса (номера позиции) символа в массиве АВС, который был определен на листе 2. Скопировать содержимое ячейки С6 в ячейки С7, С8….

9. Получив номер символа в алфавите АВС, произвести сдвиг нумерации алфавита для кодируемой последовательности символов. В ячейку D6 записать формулу: “=ЕСЛИ(ПОИСКПОЗ(В6;АВС;0)+$D$4>36;ПОИСКПОЗ(В6;АВС;0)+$D$4-36;ПОИСКПОЗ(В6;АВС;0)+$D$4)”. **(1)**

Эта формула производит сдвиг номеров символов алфавита на величину k и определяет номер заменяющего символа из алфавита АВС. Содержимое D6 скопировать в область D7,D8….

10. Выбрать символы из алфавита ABC в соответствии с новыми номерами. В ячейку E6 записать формулу “=ИНДЕКС(ABC;D6)”. Скопировать содержимое ячейки E6 в область E7,E8….

11. Для получения строки закодированного текста необходимо в ячейку F6 записать “=E6”, в ячейку F7 соответственно – “=F6&E7”. Далее скопировать содержимое ячейки F7, в область F8,F9…. В последней ячейке FN прочитать зашифрованный текст.

12. Для проверки шифрования произвести дешифрование полученного текста и сравнить его с исходным. На третьем листе выполнить дешифрование аналогично пунктам 2-11 задания. При этом необходимо учесть следующие особенности: в п. 2 набрать зашифрованный текст; в п. 9 в ячейку D6 записать формулу: =ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)-$D$4<0;ПОИСКПОЗ(B6;ABC;0)-

$D$4+40;ПОИСКПОЗ(B6;ABC;0)-$D$4). **(2)**

Получение исходного текста в итоговой ячейке F третьей страницы свидетельствует о корректном выполнении задания.

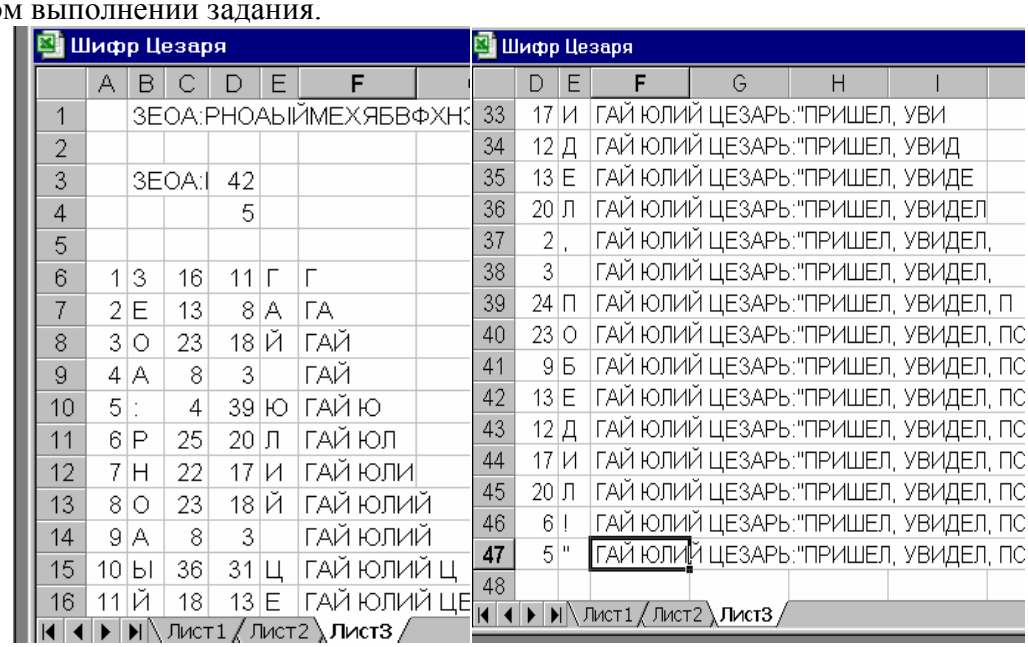

Рис. 21 Результат шифрования (шифр Цезаря)

Электронная цифровая подпись

Цель работы: изучить основы работы с программным средством ЭЦП на основе программы **Pretty Good Privacy** (PGP).

В России имеются нормативно-правовые акты, ограничивающие эксплуатацию нелицензированных программных средств, основанных на криптографии. В связи с этим правовой режим практической эксплуатации программы PGP на территории России в настоящее время не определен. В данном случае речь идет только об ее использовании в качестве наиболее доступной учебной модели.

Задание 1.

Создание ключей в системе PGP

Это и последующие упражнения предполагают, что на компьютере установлена программа PGP, автоматически стартующая при запуске операционной системы.

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys.**
2. Щелкните на кнопке **Generate new keypair** (Сгенерировать новую пару ключей). Произойдет запуск **Мастера генерации ключей** (Key Generation Wizard). Щелкните на кнопке **Далее.**
3. Введите свое полное имя в поле **Full name** (Полное имя) и свой адрес электронной почты в поле **Email address** (Адрес электронной почты). Щелкните на кнопке **Далее.**

4. Установите переключатель **Diffie-Hellman/DSS**. Это более современный алгоритм генерации пары ключей. Щелкните на кнопке **Далее.**
5. Установите переключатель 2048 bits (2048 бит), определяющий длину ключа. Щелкните на кнопке **Далее**. (По надежности ключ такой длины соответствует примерно 128-битному ключу для симметричного шифрования.)
6. Для данного упражнения установите переключатель **Key pair never expires** (Пара ключей действует бессрочно). На практике рекомендуется задавать ограниченный срок действия ключей. Щелкните на кнопке **Далее.**
7. Дважды введите произвольную **парольную фразу** (Passphrase) в соответствующие поля. Так как в данном случае реальная секретность не существенна, можно **сбросить флажок Hide Typing** (Скрыть ввод), чтобы вводимый текст отображался на экране. Рекомендуется, чтобы парольная фраза легко запоминалась, но при этом содержала пробелы, буквы разного регистра, цифры, специальные символы. Качество (трудность подбора) ключевой фразы отображается с помощью индикатора **Passphrase Quality** (Качество ключевой фразы). Удобно использовать какую-нибудь известную цитату или пословицу на русском языке, но вводить ее в латинском регистре. После того как парольная фраза введена дважды, щелкните на кнопке **Далее.**
8. Просмотрите за процессом генерации пары ключей, что может занять до нескольких минут. После появления сообщения Complete **(Готово)** щелкните на кнопке **Далее.** Затем может потребоваться еще несколько щелчков на кнопках **Далее** и, в конце, **Готово**, чтобы завершить создание ключей (публикацию ключа на сервере выполнять не следует).
9. Посмотрите, как отображается только что созданный ключ в списке **Keys** (Ключи). Убедитесь, что этот ключ автоматически подписывается его создателем, который, как предполагается, абсолютно доверяет самому себе.
10. Щелкните на ключе правой кнопкой мыши и выберите в контекстном меню пункт **Key Properties** (Свойства ключа). Убедитесь, что установлен флажок **Implicit Trust** (Полное доверие), указывающий, что вы доверяете владельцу данного ключа, то есть самому себе.

В этом упражнении мы научились создавать пару ключей, используемых для несимметричного шифрования в системе PGP. Мы также познакомились с механизмом доверия, используемым для подтверждения подлинности ключей.

Задание 2.

Передача открытого ключа PGP корреспондентам

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys.**
2. Выберите в списке ключ, который планируется передать корреспонденту, и дайте команду **Edit ► Copy** (Правка ► Копировать).
3. Запустите используемую по умолчанию программу электронной почты. **Далее** мы будем предполагать, что это программа Outlook Express (Пуск ► Программы ► Outlook Express).
4. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите условный адрес корреспондента, тему сообщения (например, Мой открытый ключ) и произвольный текст сообщения, объясняющий его назначение.
5. Поместите курсор в конец сообщения и щелкните на кнопке **Вставить** на панели инструментов. Убедитесь, что в текст сообщения был вставлен символьный блок, описывающий открытый ключ. Сохраните сообщение (отправлять его не обязательно).
6. Проверьте, можно ли перенести ключ в сообщение электронной почты методом перетаскивания.
7. Теперь предположим, что только что созданное сообщение на самом деле было получено по электронной почте. Порядок действий в этом случае очень похож на тот, который использовался для отправки ключа.
8. Выделите текст ключа, включая специальные строки, описывающие его начало и конец.

9. Скопируйте ключ в буфер обмена с помощью комбинации клавиш CTRL+C.
10. Переключитесь на программу PGPkeys.
11. Нажмите комбинацию клавиш CTRL+V. В открывшемся диалоговом окне щелкните на кнопке **Select All** (Выбрать все), а затем на кнопке **Import** (Импортировать).
12. В самом окне **PGPkeys** вы после этого никаких изменений не обнаружите, так как соответствующий ключ уже хранится на данном компьютере.
13. На самом деле, пересылать ключи по электронной почте не вполне корректно, так как в таком случае корреспондент имеет естественное право на сомнение: действительно ли ключ поступил от вас. Ключ можно сохранить в файле и передать корреспонденту лично, при встрече.
14. Чтобы экспортировать ключ в файл, выберите его и дайте команду **Keys ► Export** (Ключи ► Экспортировать).
15. Выберите каталог и укажите имя файла. Щелкните на кнопке **Сохранить**, чтобы записать ключ в текстовый файл.

В этом упражнении мы научились передавать открытые ключи системы PGP своим корреспондентам, а также получать ключи для расшифровки поступающих сообщений. Мы узнали, что ключ может передаваться по электронной почте или, что предпочтительнее, при личной встрече. Мы также выяснили, что ключ, фактически, представляет собой длинную последовательность алфавитно-цифровых символов.

Задание 3.

Передача защищенных и подписанных сообщений с помощью системы PGP

1. Запустите программу Outlook Express (Пуск ► Программы ► Outlook Express).
2. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите адрес электронной почты, использованный при создании пары ключей, в качестве адреса отправителя, а также произвольные тему и текст сообщения.
3. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys**. Выбирите **Gurrent Windows**, далее **Sign** (Подписать). В открывшемся диалоговом окне введите парольную фразу, заданную при создании ключей, и щелкните на кнопке **ОК**. Обратите внимание на добавленные служебные строки и электронную подпись в виде последовательности символов, не имеющей видимой закономерности.
4. Выделите весь текст сообщения и нажмите комбинацию клавиш CTRL+C. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Decrypt & Verify** (Буфер обмена ► Расшифровать и проверить). В открывшемся диалоговом окне обратите внимание на сообщение *** PGP Signature Status: good, указывающее на целостность сообщения.
5. Откройте это сообщение, внесите произвольные (большие или небольшие) изменения в текст сообщения или в саму подпись, после чего выполните повторную проверку, как описано в п. 6. Убедитесь, что программа PGP обнаружила нарушение целостности сообщения.
6. Создайте новое сообщение.
7. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства PGPkeys. Выбирите **Gurrent Windows**, далее **Encrypt & Sign** (Зашифровать и подписать).
8. Скопируйте текст зашифрованного сообщения в буфер обмена и выполните его расшифровку. По запросу введите парольную фразу. Убедитесь, что при этом как отображается текст исходного сообщения, так и выдается информация о его целостности.
9. Щелкните на кнопке **Copy to Clipboard** (Копировать в буфер обмена), чтобы поместить расшифрованный текст в буфер обмена.
10. Вставьте расшифрованный текст в любом текстовом редакторе и сохраните его как файл.

В этом упражнении мы научились создавать сообщения, снабженные электронной цифровой подписью, а также зашифрованные сообщения.

Задание 4.

Шифрование данных на жестком диске при помощи системы PGP

Система PGP может также использоваться для защищенного хранения файлов на жестком диске. Для шифрования и расшифровки файлов могут использоваться различные механизмы.

1. С помощью текстового процессора **WordPad** создайте произвольный документ и сохраните его под именем **pgp-test.doc**. Можно также скопировать под этим именем какой-либо из уже существующих файлов документов.
2. Откройте этот документ в программе **WordPad** и дайте команду **Правка ► Выделить все**. Нажмите комбинацию клавиш CTRL+C.
3. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Encrypt & Sign** (Буфер обмена ► Зашифровать и подписать).
4. В открывшемся диалоговом окне перетащите созданный вами ключ в список **Recipients** (Получатели) и щелкните на кнопке **ОК**.
5. Введите парольную фразу, используемую для электронной подписи, и щелкните на кнопке **ОК**.
6. Вернитесь в программу WordPad, нажмите клавишу **DELETE** и далее комбинацию CTRL+V. Сохраните документ под именем **pgp-test-clp.doc**. Закройте программу WordPad.
7. Любым способом запустите программу Проводник и откройте папку, в которой лежит файл **pgp-test.doc**.
8. Щелкните правой кнопкой мыши на значке файла и выберите в контекстном меню команду **PGP ► Encrypt & Sign** (PGP ► Зашифровать и подписать). Далее действуйте в соответствии с пп. 4-5.
9. Убедитесь, что в папке появился **файл pgp-test.doc.pgp.**
10. Теперь расшифруем созданные файлы. Запустите программу WordPad и откройте файл **pgp-test-clp.doc**.
11. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Current Window ► Decrypt & Verify** (Текущее окно ► Расшифровать и проверить).
12. Введите парольную фразу и щелкните на кнопке ОК.
13. В открывшемся диалоговом окне **Text Viewer** (Просмотр текста) щелкните на кнопке **Copy to Clipboard** (Скопировать в буфер обмена).
14. Вставьте текст в окно программы WordPad и сохраните полученный файл.
15. Откройте программу Проводник и разыщите файл **pgp-test.doc.pgp**. Дважды щелкните на его значке.
16. Введите парольную фразу и щелкните на кнопке **ОК**.
17. Так как оригинал файла не был уничтожен, программа предложит указать, под каким именем следует сохранить файл. Введите это имя по своему усмотрению.

Мы научились отправлять файлы на защищенное хранение, шифруя их при помощи программы PGP. Мы выяснили, что для текстовых данных эту операцию можно применять непосредственно в текущем окне редактора или к данным, находящимся в буфере обмена. Для произвольных файлов выполнить шифрование можно через контекстное меню. Мы также узнали, как расшифровывать зашифрованные файлы, используя разные способы.

Доклады:

1. Российский и американский стандарты шифрования (ГОСТ, DES, AES).
2. Асимметрические криптосистемы (RSA, El Gamal).

Тема 4. Особенности защиты информации в ПК

Литература: **О-1; О-2; Д-1; Д-2; Д-3-7.**

Вопросы для самопроверки

1. Встроенные средства обеспечения безопасности распространенных операционных систем и серверов различных сетевых протоколов.
2. Архитектура системы безопасности операционных систем.
3. Локальный администратор безопасности, центр аутентификации, диспетчер учетных записей, монитор безопасности.
4. Механизм контроля доступа.
5. Система аудита.

Задания для самостоятельной работы

1. Безопасность серверов SMB, RAS, IIS...
2. Защищенные сетевые протоколы (SSL, TSL, IPsec и др.).
3. Программно-технической меры. Роль и место программно-технических мер в информационной безопасности.
4. Архитектурная безопасность.

Тема 5. Проблемы защиты информации в сетях ЭВМ

Литература О-1; О-2; **Д-1; Д-2; Д-3-7.**

Вопросы для самопроверки

1. Беседа по специализированным аппаратно-программным системам защиты безопасности.
2. Системы безопасности «Криптоцентр», «Криптон», «Верба», «Крипто-Про» и др.

Задания для самостоятельной работы

1. Защита информации в информационных системах.
2. Идентификация и аутентификация.
3. Экранирование, анализ защищенности.

Межсетевые экраны

Цель работы: Анализ возможностей межсетевых экранов.

Задание 1.

Используя поисковые системы, проанализировать информацию о межсетевых экранах, например, FireWall – 1, Agnitum Outpost Firewall, ZoneAlarm Anti-Spyware, Comodo Firewall Pro.

Показатели	Брандмауэр 1	Брандмауэр 2
Название		
Производитель		
Назначение		
Поддерживаемые ОС		
Ключевые возможности		
Поддерживаемые протоколы		
Тип системы (программный, программно-аппаратный)		
Статистическая фильтрация		
Динамическая фильтрация		
Проксирование		

Программно – аппаратные средства защиты от НСД

Цель работы: Анализ возможностей программно-аппаратных средств защиты от несанкционированного доступа к информации.

Задание 1.

Проанализировать возможности и основные характеристики программно – аппаратных средств «СЗИ НСД Аккорд-АМДЗ» и «ПСКЗИ ШИПКА» на сайте http://www.accord.ru. Составить отчет, содержащий краткие сведения о данных продуктах.

Задание 2.

В сети Интернет с помощью средств поиска или по адресам, указанных преподавателем, найти и проанализировать информацию о программно-аппаратных средствах, обеспечивающих защиту от несанкционированного доступа к информации:

1. Программно-аппаратный комплекс «Аккорд»
2. Программно-аппаратная система защиты «Secret-Net»
3. Программно-аппаратная система «Криптон-Вето»,

Заполнить таблицу:

Характеристики системы	«Аккорд»	«Secret-Net»	«Криптон-Вето»
Поддерживаемые ОС			
Момент загрузки системы (н-р, перед ОС)			
Блокировка физических каналов			
Разграничение доступа к ресурсам системы			
Идентификация/ аутентификация			
Ведение журнала событий			
Контроль целостности аппаратных и программных средств			
Подсистемы (компоненты)			
Особенности			

Материально-техническое обеспечение дисциплины (разделов)

Дисциплина обеспечена:

- учебной аудиторией для проведения занятий лекционного типа, оборудованной мультимедийными средствами обучения для демонстрации лекций-презентаций,
- учебной аудиторией для проведения занятий семинарского типа (семинары, практические занятия) для групповых и индивидуальных консультаций, промежуточной аттестации, оборудованной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации студентам;
- помещениями для самостоятельной работы, оснащенной компьютерной техникой с возможностью подключения к сети «Интернет» и обеспеченной доступом в электронную информационно-образовательную среду Института.

V. ТЕМАТИЧЕСКИЙ ПЛАН ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

(*Содержание дисциплины, структурированное по темам (разделам) с указанием часов и видов занятий)*
(*очная форма обучения)*

№ п/п	Наименование разделов и тем	Контактные часы								Самостоятельная работа		Формы текущего/ рубежного контроля
		Аудиторные часы						Конт. часы по промежуточной аттестации (Катт)	Конт. часы по промежуточной аттестации в период экз. сессии (Каттэк)	формы	часы	
		Лекции	Лабора-торные работы	Практи-ческие занятия	Всего ауд.	в том числе интерактив-ные: формы	в том числе интерактив-ные: часы					
1.	Общие сведения о защите информации	2		2	4					Лит., индивид. задание,	20	анализ ДИ, тест
2.	Защита информации в информационных системах	4		6	10		4			Лит., подго-товка к тестам	20	защита индивид. задания
3.	Криптографические методы защиты информации	4		6	10		4			Лит., П.з., подгот. к тестам	20	устный опрос, проверка письм.дом.задания
4.	Особенности защиты информации в ПК	2		6	8	Копм. симуляции	2			Лит., комп.з.	20	Устный опрос, защита индивид. задания, тест
5.	Проблемы защиты информации в сетях ЭВМ	2		6	8	Копм. симуляции	2			Лит., комп.з.	22	Устный опрос, защита индивид. задания, тест
Итого:		**14**		**26**	**40**		**12**	**2**			**102**	
Всего по дисциплине		**14**		**26**	**40**			**2**			**102**	**зачет**

Сокращения, используемые в Тематическом плане изучения дисциплины:

№ п/п	Сокращение	Вид работы
1.	Лит	Работа с литературой
2.	П.з.	Выполнение письменной домашней работы
3.	ДИ	Деловая игра
4.	И.л.	Интерактивная лекция

VI. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства по дисциплине разработаны в соответствии с Положением о фонде оценочных средств в ФГБОУ ВО «РЭУ им. Г.В.Плеханова».

Фонд оценочных средств хранится на кафедре торгового дела и информационных технологий.

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы (см. таблицу раздела II)

6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (см. таблицу раздела II и раздел VIII)

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

- **Тематика курсовых работ**

Согласно учебному плану, выполнение курсовой работы по дисциплине «Основы информационной безопасности» не предусмотрено.

- **Вопросы к зачету:**

1. Дать определение понятия «информационная безопасность» и основных ее составляющих.
2. Основные положения «Доктрины информационной безопасности России».
3. Статьи Конституции РФ, относящиеся к проблеме информационной безопасности.
4. Законы РФ, имеющие отношение к проблеме компьютерной безопасности.
5. Что такое «Оранжева книга»?
6. Развернутое определение понятия «политика безопасности».
7. Перечислить возможные организационные мероприятия, повышающие уровень компьютерной безопасности.
8. Цели государства в области обеспечения информационной безопасности.
9. Основные нормативные акты РФ, связанные с правовой защитой информации.
10. Виды компьютерных преступлений.
11. 4.Способы и механизмы совершения информационных компьютерных преступлений.
12. Основные параметры и черты информационной компьютерной преступности в России.
13. Компьютерный вирус. Основные виды компьютерных вирусов.
14. Методы защиты от компьютерных вирусов.
15. Типы антивирусных программ.
16. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
17. Основные угрозы компьютерной безопасности при работе в сети Интернет.
18. Виды защищаемой информации.
19. Государственная тайна как особый вид защищаемой информации.
20. Конфиденциальная информация.
21. Система защиты государственной тайны.
22. Правовой режим защиты государственной тайны.
23. Защита интеллектуальной собственности средствами патентного и авторского права.
24. Международное законодательство в области защиты информации.
25. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
26. Симметричные методы шифрования.
27. Ассиметричные методы шифрования.
28. Криптографические хеш-функции.

29. Электронная цифровая подпись.
30. Организационное обеспечение информационной безопасности.
31. Служба безопасности организации в организации.
32. Методы защиты информации от утечки в технических каналах.
33. Инженерная защита и охрана объектов.

- ***Перечень вопросов текущего контроля***

1. Доктрина информационной безопасности Российской Федерации.
2. Информационная безопасность. Доступность, целостность и конфиденциальность информационных ресурсов.
3. Российское и зарубежное законодательство в области информационной безопасности.
4. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
5. Обзор международных и национальных стандартов и спецификаций в области информационной безопасности.
6. Политики безопасности. Уровень гарантированности. Доверенная вычислительная база. Периметр безопасности. Классы безопасности.
7. Организационные мероприятия, повышающие уровень информационной безопасности.
8. Выбор эффективных средств защиты.
9. Типология компьютерных вирусов.
10. Антивирусное программное обеспечение. Обзор и анализ.
11. Сетевые атаки.
12. Централизованные DoS-атаки и DDoS-атаки.
13. Маршрутизаторы. Прокси-серверы. Межсетевые экраны.
14. Программа Outpost Pro.
15. Настройка правил безопасности брандмауэров.
16. Экономическая оценка информационной безопасности.
17. Аудит систем и сканирование уязвимостей.
18. Различные архитектуры с применением межсетевых экранов.
19. Криптография. Основные понятия и виды криптографических алгоритмов.
20. Надежность криптографического алгоритма и лобовая атака.
21. Симметричные криптоалгоритмы.
22. Криптоалгоритмы с открытым ключом.
23. Алгоритм RSA.
24. Хэш-функции и цифровые подписи.
25. Программно-технической меры. Роль и место программно-технических мер в информационной безопасности.
26. Архитектурная безопасность.
27. Идентификация и аутентификация.
28. Экранирование, анализ защищенности.

- ***Примеры тестовых заданий***

1. Выделите основные составляющие национальных интересов Российской Федерации в информационной сфере:

a) Защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем

b) Законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи

c) Усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ

d) Развитие современных информационных технологий, отечественной индустрии информации

e) Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России

f) Разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли

g) Информационное обеспечение государственной политики Российской Федерации

h) Совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации

1. Протоколы сети интернет – это:

a) рекомендации по использованию сети

b) правила передачи пакетов информации

c) правила для пользователей по использованию сети

3. RFC – это:

a) рекомендации для сети Интернет

b) инструкции для пользователей Интернет

4. Шлюз – это:

a) программа для связи двух удаленных компьютеров.

b) компьютер, соединяющий сети с различными протоколами.

c) устройство обмена данными в Интернет

5. Задачи протокола IP:

a) повторная отправка недоставленных пакетов в случае сбоев в работе

b) доставка всей информации получателю

c) адресация

d) контроль последовательности

e) маршрутизация

f) разбивка больших пакетов на блоки

6. Сетевая утилита PING позволяет:

a) протестировать передачу пакетов хосту

b) просмотреть путь прохождения пакетов до хоста

c) узнать IP-адрес хоста

7. **Укажите опасные типы файлов-вложений:**

a) xls b) pif c) ppt d) reg e) scr f) wma

1. Отметьте типичные функции, которые выполняет брандмауэр (файеруолл):

a) Обеспечение доступа с компьютеров локальной сети в Интернет

b) Обеспечение оптимальной доставки от источника к получателю

c) Сжатие данных

d) Обеспечение контроля и фильтрации пакетов информации

e) Защита локальной сети от внешнего доступа

f) Ограничение доступа из локальной сети к внешней

g) Анонимизация доступа к различным ресурсам

h) Соединение подсетей с разными протоколами

i) Кэширование данных

2. Укажите приложения, имеющие встроенные языки программирования:

a) Windows Explorer

b) Internet Explorer

c) Microsoft PowerPoint

d) WordPad

e) Adobe Photoshop

10. Какие проявления в поведении компьютера могут являться симптомами его заражения:

a) Изменение длины и/или даты создания программ;

b) Замедление выполнения программ;

c) Необъяснимые зависания или перезагрузка системы;

d) Потеря работоспособности некоторых резидентных программ или драйверов;

e) Аварийное завершение ранее нормально функционирующих программ;
f) Уменьшение объема системной памяти или свободной памяти после загрузки;

11. Для получения управления вирус записывает свою голову в:

a) Загрузочные модули (COM- , EXE- файлы);
b) FAT
c) MBR (Master Boot Record – главная загрузочная запись);
d) Сбойный кластер
e) Модули библиотек .DLL;
f) BAT-файл;
g) Файл-документы, созданные приложениями обработки данных, которые поддерживают работу на макроязыках.

15. Задачи протокола TCP:

a) повторная отправка недоставленных пакетов в случае сбоев в работе
b) доставка всей информации получателю
c) адресация
d) контроль последовательности
e) маршрутизация
f) разбивка больших пакетов на блоки

16. Протоколы IPX/SPX входят в стек протоколов:

a) Интернет TCP/IP b) IBM/Microsoft c) Novell

17. Номер хоста в IP-адресе занимает:

a) 1 байт b) 12 бит c) 16 бит
d) Разное число бит в зависимости от класса сети

19. Укажите безопасные типы файлов-вложений:

a) vbs b) mp3 c) rar d) jpg e) gif f) bat g) txt

20. Укажите возможные состояния активных TCP и UDP-портов:

a) NOT_ACTIVE
b) LISTENING
c) WAITING_FOR
d) ESTABLISHED
e) TIME_WAIT

21. Атака модификации включает в себя следующие действия:

a) Подслушивание c) Добавление e) Удаление
b) Замена d) Перехват

22. Для проведения централизованных DoS-атак используется протокол:

a) ICMP b) UDP c) TCP d) ARP

23. Отметьте типичные функции, которые выполняет прокси-сервер:

a) Обеспечение доступа с компьютеров локальной сети в Интернет
b) Обеспечение оптимальной доставки от источника к получателю
c) Сжатие данных
d) Обеспечение контроля и фильтрации пакетов информации
e) Защита локальной сети от внешнего доступа
f) Ограничение доступа из локальной сети к внешней
g) Анонимизация доступа к различным ресурсам
h) Соединеие подсетей с разными протоколами
i) Кэширование данных

24. Укажите режимы работы брандмауэра Outpost:

a) Обучения
b) Разрешение
c) Внутренней защиты
d) Фоновый
e) Игровой
f) Блокирование

25. Укажите политики брандмауэра Outpost:

a) Игровая d) Блокирование g) Запрещение
b) Разрешение e) Внутренней защиты
c) Отключение f) Обучение

26. Какие группы приложений в брандмауэре Outpost существуют?

a) Запрещенные
b) Глобальные
c) Доверенные
d) Локальные

e) Пользовательский уровень

27. Можно ли в брандмауэре Outpost отключить глобальное правило, не удаляя его?

a) Да b) Нет

28. Какие уровни тревоги существуют в детекторе атак брандмауэра Outpost?

a) Высокий. Оповещение об атаке отображается даже если обнаружено единичное сканирование одного из ваших портов.

b) Средний. Оповещение об атаке отображается, если просканировано 3-5 портов

c) Обычный. Оповещение об атаке отображается если просканировано несколько портов или если просканирован один из портов, которые, по мнению Outpost Firewall Pro, обычно используются для атаки.

d) Низкий. Оповещение об атаке отображается при обнаружении нескольких попыток атаки.)

29. Какие существуют механизмы назначения DHCP IP-адресов?

a) Серверный

b) Динамический

c) Клиентский

d) Автоматический

e) Ручной

VII. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Положение об интерактивных формах обучения (http://www.rea.ru)
Положение об организации самостоятельной работы студентов (http://www.rea.ru)
Положение о рейтинговой системе оценки успеваемости и качества знаний студентов (http://www.rea.ru)
Положение об учебно-исследовательской работе студентов в ФГБОУ ВО "РЭУ им. Г.В. Плеханова" (http://www.rea.ru)

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практические занятия	Проработка рабочей программы, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (указать текст из источника и др.). Прослушивание аудио- и видеозаписей по заданной теме, решение расчетно-графических заданий, решение задач по алгоритму и др.
Контрольная работа / индивидуальные задания	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.
Курсовая работа	Курсовая работа: изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной цели и задачи; проведение практических исследований по данной теме. Методические указания по выполнению требований к оформлению курсовой работы находится в методических материалах по дисциплине.
Деловая игра	Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для участия в деловой игре. Выполнение предварительных заданий преподавателя с целью подготовки. Деление на микрогруппы, работы внутри микрогрупп.

VIII. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Формирование балльной оценки по дисциплине «Основы информационной безопасности»

В соответствии с «Положением о рейтинговой системе оценки успеваемости и качества знаний студентов в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Российский экономический университет имени Г.В. Плеханова» распределение баллов, формирующих рейтинговую оценку работы студента, осуществляется следующим образом:

Виды работ	Максимальное количество баллов
Выполнение учебных заданий на аудиторных занятиях	20
Текущий и рубежный контроль	20
Творческий рейтинг	20
Промежуточная аттестация (экзамен/ зачет)	40
ИТОГО	100

1. **Текущий рубежный контроль**

Расчет баллов по результатам текущего и рубежного контроля в 4 семестре:

Наименование темы, выносимой на контроль	**Форма проведения контроля**	**Количество баллов, максимально**
Общие сведения о защите информации	Письменная домашняя работа	**2**
Защита информации в информационных системах	Письменная домашняя работа	**2**
Криптографические методы защиты информации	Письменная домашняя работа Тестирование	**2** **4**
Особенности защиты информации в ПК	Письменная домашняя работа Тестирование	**2** **4**
Проблемы защиты информации в сетях ЭВМ	Письменная домашняя работа Тестирование	**2** **2**
ИТОГО		**20**

* - Тестирование студентов, которое включено в модульный график учебного процесса (рабочий учебный план) ***не включается*** в количество баллов, отводимых на проведение текущего и рубежного контроля.

2. **Творческий рейтинг**

Распределение баллов осуществляется по решению методической комиссии кафедры и результат распределения баллов за соответствующие виды работ представляются в виде следующей таблицы

Наименование раздела/ темы дисциплины	**Вид работы**	**Количество баллов**
Криптографические методы защиты	Реферат	**10**

информации		
Защита информации в информационных системах	Реферат	**10**
ИТОГО		**20**

3. Промежуточная аттестация

Зачет по результатам изучения учебной дисциплины «Основы информационной безопасности» проводится устно по вопросам, включающим теоретические вопросы.

Итоговый балл формируется суммированием баллов за промежуточную аттестацию и баллов, набранных перед аттестацией. Приведение суммарной балльной оценки к четырехбалльной шкале производится следующим образом:

Оценка по результатам зачета выставляется исходя из следующих критериев:

- теоретические вопросы – по 20 баллов каждый;

В случае частично правильного ответа на вопрос или решение ситуационной задачи, студенту начисляется определяемое преподавателем количество баллов.

Итоговый балл формируется суммированием баллов за промежуточную аттестацию и баллов, набранных перед аттестацией в каждом семестре отдельно. Приведение суммарной балльной оценки к четырехбалльной шкале производится следующим образом:

Показатели и критерии оценивания планируемых результатов освоения компетенций и результатов обучения, шкала оценивания

100-балльная система оценки	**Традиционная четырехбалльная система оценки**	**Формируемые компетенции (индикаторы компетенций)**	**Критерии оценивания**
85 – 100 баллов	«отлично»	ПК-11	**Знает верно и в полном объеме:** методы анализа информации о функционировании системы внутреннего документооборота организации **Умеет верно и в полном объеме:** проводить анализ предметной области, вести базы данных по различным показателям **Владеет навыками верно и в полном объеме:** способами формирования информационного обеспечения участников организационных проектов
		ПК-12	**Знает верно и в полном объеме:** методы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проект **Умеет верно и в полном объеме:** организовать и поддерживать связи с деловыми партнерами **Владеет навыками верно и в полном объеме:** методами обмена опытом при реализации

			проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления)
70 – 84 баллов	«хорошо»	ПК-11	**Знает с незначительными замечаниями:** методы анализа информации о функционировании системы внутреннего документооборота организации **Умеет с незначительными замечаниями:** проводить анализ предметной области, вести базы данных по различным показателям **Владеет навыками с незначительными замечаниями:** способами формирования информационного обеспечения участников организационных проектов
		ПК-12	**Знает с незначительными замечаниями:** методы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проект **Умеет с незначительными замечаниями:** организовать и поддерживать связи с деловыми партнерами **Владеет навыками с незначительными замечаниями:** методами обмена опытом при реализации проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления)
50 – 69 баллов	«удовлетвори-тельно»	ПК-11	**Знает на базовом уровне, с ошибками:** методы анализа информации о функционировании системы внутреннего документооборота организации **Умеет на базовом уровне, с ошибками:** проводить анализ предметной области, вести базы данных по различным показателям **Владеет на базовом уровне, с ошибками:** способами формирования информационного обеспечения участников организационных проектов
		ПК-12	**Знает на базовом уровне, с ошибками:** методы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проект **Умеет на базовом уровне, с ошибками:** организовать и поддерживать связи с деловыми партнерами **Владеет на базовом уровне, с ошибками:**

			методами обмена опытом при реализации проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления)
менее 50 баллов	«неудовлетвори-тельно»	ПК-11	**Не знает на базовом уровне:** методы анализа информации о функционировании системы внутреннего документооборота организации **Не умеет на базовом уровне:** проводить анализ предметной области, вести базы данных по различным показателям **Не владеет на базовом уровне:** способами формирования информационного обеспечения участников организационных проектов
		ПК-12	**Не знает на базовом уровне:** методы сбора необходимой информации для расширения внешних связей и обмена опытом при реализации проект **Не умеет на базовом уровне:** организовать и поддерживать связи с деловыми партнерами **Не владеет на базовом уровне:** методами обмена опытом при реализации проектов, направленных на развитие организации (предприятия, органа государственного или муниципального управления)

Карта обеспеченности дисциплины «Основы информационной безопасности»
учебными изданиями и иными информационно-библиотечными ресурсами

Кафедра Торгового дела и информационных технологий
ОПОП ВО по направлению подготовки 38.03.02 Менеджмент
Уровень подготовки бакалавриат

№п/п	Наименование, автор	Выходные данные	Библиотека Пермского института (филиала) РЭУ им Г.В.Плеханова		Количество экземпляров на кафедре (в лаборатории) (шт.)	Численность студентов (чел.)	Показатель обеспеченности студентов литературой: = 1 (при наличии в ЭБС); или =(колонка 4/ колонка 7) (при отсутствии в ЭБС)
			количество печатных экземпляров (шт.)	наличие в ЭБС (да/нет), название ЭБС			
1	2	3	4	5	6	7	8
Основная литература							
1.	Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для студ. учреждений высш. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под. ред. С. А. Клейменова. — 6-е изд., [Электронный ресурс]	М. : Издательский центр «Академия», 2012. — 336 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
2.	Малюк А. А. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатова.	М.: Гор. линия-Телеком, 2011. - 288 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**

Дополнительная литература							
1.	Партыка Т. Л. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. [Электронный ресурс]	М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
2.	Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. [Электронный ресурс]	М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
3.	Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп.	М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
4.	Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. -	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
5.	Гришина Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп.	М. : ФОРУМ : ИНФРА-М, 2017. — 239 с.					
6.	Баранова Е. К.	М.: РИОР: ИНФРА-М,	X	да,	X	X	**1,0**

	Информационная безопасность и защита информации: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп.	2017. — 322 с.		ЭБС «ZNANIUM»			
7.	Барнс К. Защита от хакеров беспроводных сетей [Электронный ресурс] / Кристиан Барнс, Тони Боутс, Дональд Лойд и др.; пер. с англ. А. В. Семенова.	М.: Компания АйТи; ДМК Пресс, 2015. - 480 с.	X	да, ЭБС «ZNANIUM»	X	X	**1,0**
	Всего:						
Профессиональные базы данных, информационно-справочные системы							
1	Единое окно доступа к образовательным ресурсам. Раздел Информатика и иформационные технологии - http://window.edu.ru/catalog/?p_rubr=2.2.75.6		x	x	x	x	**1**
2	База книг и публикаций Электронной библиотеки "Наука и Техни-ка" - http://www.n-t.ru		x	x	x	x	**1**
3.	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/		x	x	x	x	**1**

Зав. кафедрой /Кочинов Ю.А./

29.08.2016 г.

Согласовано:

Зав. библиотекой /Любимова Л.Б./
29.08.2016 г.