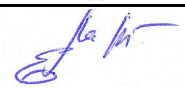
МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В	**Программно-аппаратное обеспечение информационной безопасности**

Код направления подготовки	44.04.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Управление информационной безопасностью в профессиональном образовании
Уровень образования	магистр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Программно-аппаратное обеспечение информационной безопасности» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.04.04 «Профессиональное обучение (по отраслям)» (уровень образования магистр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 5 з.е., 180 час.

1.3 Изучение дисциплины «Программно-аппаратное обеспечение информационной безопасности» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Дисциплины предметной подготовки».

1.4 Дисциплина «Программно-аппаратное обеспечение информационной безопасности» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Проектирование и модернизация учебных мастерских, лабораторий и классов», «Проектирование и мониторинг образовательных результатов», «Технологии свободнораспространяемого программного обеспечения», «Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации», «ЭИОС организаций профессионального образования», «выполнение и защита выпускной квалификационной работы».

1.5 Цель изучения дисциплины:

формирование у студентов системы теоретических знаний и практических навыков, необходимых для совершенствования управления информационной безопасностью в аспекте применения программнл-аппаратных средств

1.6 Задачи дисциплины:

1) дать студентам знания сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию;

понятие и современное состояние средств информационной защиты;

понятие семиуровневой системы обеспечения информационной безопасности;

компоненты программно-аппаратных средств обеспечения информационной защиты;системы оценки информационной защищенности

2) научить студентов давать оценку защищенности информационной системе;

применять на практике программно-аппаратные средства ОИБ;

3) научить выстраивать комплексную систему защиты информации по принципу разумной достаточности

1.7 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ПК-18 способен участвовать в мониторинге эффективности применяемых инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности
	ПК.18.1 Знает современные способы мониторинга эффективности применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП
	ПК.18.2 Умеет проводить мониторинг эффективности применения инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП
	ПК.18.3 Владеет способами управления мониторингом инженерно-техническими и программно-аппаратными средствами обеспечения информационной безопасности в организациях ВО, современного профессионального образования, ДПО и ДПП
2	ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности
	ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП
	ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП
	ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП

3	ПК-17 способен участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего состояния, в проведении технического обслуживания и текущего ремонта, выявлении технических каналов утечки информации и оценке возникающих опасностей, устранении отказов и восстановлении работоспособности
	ПК.17.1 Знает содержание теории и практики эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП
	ПК.17.2 Умеет квалифицированно проводить эксплуатацию, диагностику, техническое обслуживание и ремонт инженерно-технических средств обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП
	ПК.17.3 Владеет способами эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП
4	УК-3 способен организовать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
	УК.3.1 Знает жизненный цикл команды, основы ее формирования и развития; основы обеспечения эффективности командной работы и руководства ею; функции, обязанности проект-менеджера, требования к нему
	УК.3.2 Умеет разрабатывать стратегию командной работы; формировать команду, планировать командную работу, распределять поручения и делегировать полномочия, инструктировать членов команды, организовывать и управлять их конструктивным взаимодействием
	УК.3.3 Владеет инструментами и методами мотивации участников командной работы; методиками изучения и коррекции психологического климата группы, предупреждения и решения возникающих в команде разногласий и конфликтов; методами оценки компетенций и опыта участников команды; методами установления коммуникативных связей, организации и проведения совещаний, ведения переговоров

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.18.1 Знает современные способы мониторинга эффективности применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП	З.3 □ понятие и современное состояние средств информационной защиты; □ понятие семиуровневой системы обеспечения информационной безопасности
2	ПК.18.2 Умеет проводить мониторинг эффективности применения инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП	У.3 умеет прводить оценку информационной защищенности
3	ПК.18.3 Владеет способами управления мониторингом инженерно-техническими и программно-аппаратными средствами обеспечения информационной безопасности в организациях ВО, современного профессионального образования, ДПО и ДПП	В.3 владеет опытом управления ИБ посредством обучения сотрудников (студентов)

1	ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	З.1 сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию
2	ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	У.1 давать оценку защищенности информационной системе
3	ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП	В.1 опытом выстраивать комплексную систему защиты информации по принципу разумной достаточности
1	ПК.17.1 Знает содержание теории и практики эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП	З.2 компоненты программно-аппаратных средств обеспечения информационной защиты
2	ПК.17.2 Умеет квалифицированно проводить эксплуатацию, диагностику, техническое обслуживание и ремонт инженерно-технических средств обеспечения информационной безопасности в области организации ВО, современного профессионального образования, ДПО и ДПП	У.2 применять на практике программно-аппаратные средства ОИБ
3	ПК.17.3 Владеет способами эксплуатации, диагностики, технического обслуживания и ремонта инженерно-технических средств обеспечения информационной безопасности ВО, современного профессионального образования, ДПО и ДПП	В.2 владеет опытом применения информационной защиты
1	УК.3.1 Знает жизненный цикл команды, основы ее формирования и развития; основы обеспечения эффективности командной работы и руководства ею; функции, обязанности проект-менеджера, требования к нему	З.4 основы проектной технологии

2	УК.3.2 Умеет разрабатывать стратегию командной работы; формировать команду, планировать командную работу, распределять поручения и делегировать полномочия, инструктировать членов команды, организовывать и управлять их конструктивным взаимодействием	У.4 умеет руководить командной работой
3	УК.3.3 Владеет инструментами и методами мотивации участников командной работы; методиками изучения и коррекции психологического климата группы, предупреждения и решения возникающих в команде разногласий и конфликтов; методами оценки компетенций и опыта участников команды; методами установления коммуникативных связей, организации и проведения совещаний, ведения переговоров	В.4 владеет опытом управления командной работы

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Итого часов
	Л	ПЗ	СРС	
Итого по дисциплине	**6**	**18**	**120**	**144**
Первый период контроля				
Основные средства и методы программно-аппаратной защиты информации	***2***	***2***	***16***	***20***
Основные средства и методы программно-аппаратной защиты информации.	2		8	10
Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку.		2	8	10
Идентификация, аутентификация. Управление доступом.	***2***	***6***	***24***	***32***
Аутентификация и идентификация – основной сервис ИБ	2	2	8	12
Назначение прав пользователей при произвольном управлении доступом.		2	8	10
Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows.		2	8	10
. Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств		***4***	***16***	***20***
Протоколирование и аудит.		2	8	10
Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств.		2	8	10
Итого по видам учебной работы	4	12	56	72
Форма промежуточной аттестации				
Зачет				
Итого за Первый период контроля				**72**
Второй период контроля				
Шифрование. Криптография.	***2***	***2***	***24***	***28***
Шифрование и криптография	2	2	8	12
Решение криптогр.задач			8	8
ЭЦП			8	8
Экранирование. Классификация межсетевых экранов.		***2***	***16***	***18***
Классификация сетевых экранов		2	8	10
Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях			8	8
Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.		***2***	***24***	***26***
Компьютерные вирусы как особый класс разрушающих программных воздействий.			8	8
Общая организация защиты от компьютерных вирусов.			8	8
Установка антивирусного ПО. Сканирование внешнего носителя на наличие вирусов		2	8	10
Итого по видам учебной работы	2	6	64	72
Форма промежуточной аттестации				
Экзамен				36
Итого за Второй период контроля				**108**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации	***2***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	
1.1. Основные средства и методы программно-аппаратной защиты информации. 1. Обзор современных средств защиты информации 2. Классы сервисов ИБ 3. ГОСТы и стандарты в области ИБ Учебно-методическая литература: 1, 2, 3	2
2. Идентификация, аутентификация. Управление доступом.	***2***
Формируемые компетенции, образовательные результаты: ПК-16: В.1 (ПК.16.3) ПК-17: З.2 (ПК.17.1), У.2 (ПК.17.2)	
2.1. Аутентификация и идентификация – основной сервис ИБ 1. Парольная аутентификация, наложение технических ограничений на пароли. 2. Одноразовые и односторонние пароли. 3. Принцип действия сервера аутентификации. 4. Биометрическая идентификация и аутентификация. 5. Матрица доступа. Ролевой доступ. 6. Объектно-ориентированный подход в администрировании ролевого доступа. Учебно-методическая литература: 1, 2, 3, 4, 5	2
3. Шифрование. Криптография.	***2***
Формируемые компетенции, образовательные результаты: ПК-18: У.3 (ПК.18.2), В.3 (ПК.18.3)	
3.1. Шифрование и криптография 1. Основные термины и понятия криптографии открытые сообщения и их характеристики 2. модели открытых сообщений; 3. исторический очерк развития криптографии. 4. Типы криптографических систем. Учебно-методическая литература: 1, 2, 4, 5, 6	2

3.2 Практические

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации	***2***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	
1.1. Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку. 1. Установление пароля на текстовый документ 2. архивирование документов 3. установление пароля на архив 4. установление пароля на папку. Учебно-методическая литература: 3, 4	2
2. Идентификация, аутентификация. Управление доступом.	***6***

Формируемые компетенции, образовательные результаты: ПК-16: В.1 (ПК.16.3) ПК-17: З.2 (ПК.17.1), У.2 (ПК.17.2)	
2.1. Аутентификация и идентификация – основной сервис ИБ 1. Парольная аутентификация, наложение технических ограничений на пароли. 2. Одноразовые и односторонние пароли. 3. Принцип действия сервера аутентификации. 4. Биометрическая идентификация и аутентификация. 5. Матрица доступа. Ролевой доступ. 6. Объектно-ориентированный подход в администрировании ролевого доступа. Учебно-методическая литература: 3, 5, 6	2
2.2. Назначение прав пользователей при произвольном управлении доступом. 1. Пользователи ИС и их атрибуты 2. Назначение прав пользователей. 3. Реализация прав доступа Учебно-методическая литература: 3, 5 Профессиональные базы данных и информационные справочные системы: 1	2
2.3. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. 1. Ознакомление с интерфейсом и функционалом Ethernet 2. Способы администрирования ОС 3. Реализация администрирования через Ethernet Учебно-методическая литература: 1, 3, 4, 6 Профессиональные базы данных и информационные справочные системы: 1	2
3. . Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств	***4***
Формируемые компетенции, образовательные результаты: ПК-17: В.2 (ПК.17.3) ПК-18: З.3 (ПК.18.1)	
3.1. Протоколирование и аудит. 1. Общие сведения о нарушении доступа к дисковой и оперативной памяти. 2. Диагностирование и устранение логических и физических дефектов носителей информации. 3. Защита файлов от удаления и восстановление удаленных файлов. Ручное восстановление данных. Безопасное окончание работы на компьютере. Учебно-методическая литература: 2, 3, 4, 5	2
3.2. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. 1. Основные способы защиты от потери информации и нарушений работоспособности. вычислительных средств. 2. Способы резервирования информации. 3. Правила обновления резервных данных. 4. Методы сжатия информации. 5. Архивация файловых данных. 6. Безопасная инсталляция программных средств. Учебно-методическая литература: 3, 4 Профессиональные базы данных и информационные справочные системы: 1, 2	2
4. Шифрование. Криптография.	***2***
Формируемые компетенции, образовательные результаты: ПК-18: У.3 (ПК.18.2), В.3 (ПК.18.3)	

4.1. Шифрование и криптография 1. Простые методы шифрования: шифры подстановки и перестановки. 2. Использование псевдослучайных чисел для генерации ключей. 3. Режимы шифрования. 4. Особенности шифрования данных в режиме реального времени. 5. Стандарты шифрования. 6. Общая организация криптографической защиты информации. 7. Основные компоненты КСЗИ. Особенности применения симметрических и асимметрических систем шифрования. Учебно-методическая литература: 3, 5	2
5. Экранирование. Классификация межсетевых экранов.	***2***
Формируемые компетенции, образовательные результаты: УК-3: З.4 (УК.3.1), У.4 (УК.3.2)	
5.1. Классификация сетевых экранов 1. Поддержание целостности циркулирующих в сети сообщений. 2.Формирование и проверка цифровой подписи. 3. Защита от отрицания фактов отправки и приема сообщений. 4.Типы межсетевых экранов, их достоинства и недостатки Учебно-методическая литература: 3, 4, 5 Профессиональные базы данных и информационные справочные системы: 1	2
6. Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.	***2***
Формируемые компетенции, образовательные результаты: УК-3: В.4 (УК.3.3)	
6.1. Установка антивирусного ПО. Сканирование внешнего носителя на наличие вирусов 1.История появления компьютерных вирусов и факторы, влияющие на их распространение. 2.Понятие компьютерного вируса. 3.Основные этапы жизненного цикла вирусов. 4. Объекты внедрения, режимы функционирования и специальные функции вирусов. 5.Схемы заражения файлов. 6.Классификация компьютерных вирусов. Учебно-методическая литература: 3, 6 Профессиональные базы данных и информационные справочные системы: 1	2

3.3 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации	***16***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	
1.1. Основные средства и методы программно-аппаратной защиты информации. ***Задание для самостоятельного выполнения студентом:*** Анализ программных средств криптографической защиты информации. Исследование систем идентификации на основе устройств Bluetooth. - индивид. исследов. задания,, доклады, рефераты, статьи, в зависимости от объема и проработанности материала Учебно-методическая литература: 2, 3, 4, 5	8
1.2. Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку. ***Задание для самостоятельного выполнения студентом:*** 1. Установление пароля на текстовый документ 2. архивирование документов 3. установление пароля на архив 4. установление пароля на папку. Учебно-методическая литература: 2, 3, 4, 6	8
2. Идентификация, аутентификация. Управление доступом.	***24***

Формируемые компетенции, образовательные результаты:

ПК-16: В.1 (ПК.16.3)

ПК-17: З.2 (ПК.17.1), У.2 (ПК.17.2)

2.1. Аутентификация и идентификация – основной сервис ИБ ***Задание для самостоятельного выполнения студентом:***	8

ЛАБОРАТОРНАЯ РАБОТА: ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ (RSA, СХЕМЫ ШНОРРА И ФЕЙГЕ-ФИАТА-ШАМИРА)

Цель: В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:
- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

Теоретические сведения

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).
Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочитать как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).
Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. Авторизация (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.
Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.
Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.
Идентификация сродни присвоении имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).
Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.
Субъект может подтвердить свою подлинность, предъявив один из следующих аутентификаторов:
- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).
В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется многофакторной. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.
Основные программно-технические способы реализации идентификации и аутентификации: пароли, с использованием хеш-функции, на основе шифрования с открытым ключом, идентификационные карты и электронные ключи, сервер аутентификации Kerberos/
Введенный пользователем пароль сравнивается с паролем, имеющимся в БД, хранящейся в защищаемой ИС, и если они совпадают, то дается разрешение на использование защищаемых ресурсов.
Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в ОС, СУБД и программные продукты. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.
Парольная аутентификация имеет массу недостатков:
- как правило, пароль генерируется в одном месте (например, на сервере) и должен быть передан во второе (например, клиенту). При передаче пароль может быть

2.2. Назначение прав пользователей при произвольном управлении доступом. ***Задание для самостоятельного выполнения студентом:***	8

ПРАКТИЧЕСКАЯ РАБОТА: «РОЛЕВАЯ МАТРИЦА ДОСТУПА»

Цель: ознакомиться с моделями управления доступом, научиться составлять матрицу доступа и иерархию ролей для учреждения профессионального учреждения для целей реализации политики безопасности, получить опыт принятия мотивированного решения.

Методы и приемы: изучение теоретических источников, контент-анализ сайтов образовательных учреждений, моделирование (политики безопасности), структурное программирование, кейс-метод.

Ключевые слова: политика безопасности, матрица доступа, ролевое управление доступом, мандатное управление доступом, объектно-ориентированный подход в ролевом управлении доступом, наследование ролей, инкапсуляция ролей

Краткие теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа: дискретное (дискреционное, избирательное) управление доступом; мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля. Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации, в связи с чем, происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя [5].

Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности, поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в автоматизированной системе проводится анализ угроз и рисков для информации и информационного обмена и

2.3.	Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. ***Задание для самостоятельного выполнения студентом:***	8

Лабораторная работа: Изучение настроек Ethernet и способов анализа трафика на сетевых интерфейсах в ОС Windows.

1.Цели и задачи работы
Ознакомиться с настройками сетевой платы и встроенными инструментальными средствами ОС MS Windows анализа трафика на сетевых интерфейсах.

2. Теоретические сведения
Правильная настройка сетевой платы позволяет не только обеспечить соединение с сеть, но улучшить производительность сетевого подключения и получить необходимое качество сервиса предоставляемой локальной сетью.
Для просмотра состояния взаимодействия компьютера с локальной сетью различные разработчики операционных систем представляют средства диагностик.
Средства диагностики могут быть графическими или использовать командную строку (так называемый CLI - Command lininterface). Диагностика с помощью CLI позволяет создавать скрипты или программы для включения их в приложения занимающиеся мониторингом или анализом сети в целом.
В данной работе необходимы следующие понятия:
• Скрипт (script) - небольшая программа для выполнения средствами операционной системы и для расширения ее возможностей
• Loopback (обратная, возвратная петля) Тип диагностического интерфейса, при котором сигнал возвращается передающему устройству, пройдя по коммуникационному каналу в обоих направлениях.
• GUI - (Graphical User Interface) графический пользовательский интерфейс
• CLI - (Command Line Interface) Интерфейс командной строки, в котором инструкции компьютеру даются только путём ввода с клавиатуры текстовых строк (команд). Также известен под названием консоль.
• MMC (Microsoft Management Console) -средство для создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами операционной системы Windows.

3. Порядок выполнения работы
Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.
3.1. Описание свойств сетевой платы.
Выполнить в следующей последовательности доступ к настройкам сетевой платы:
Пуск - панель управления - подключение к локальной сети (сетевые подключения) – вызов контекстного меню- свойства- настроить.
Сохранить в отчет все свойства сетевой интерфейса виде таблицы 1:
<Название сетевой платы>

Свойство	Установленное значение	Возможные значение
Скорость и дуплекс	Автосогласование	От 10Мбит/с дуплекс…до 100Мбит/с полудуплекс
Wake Up Capabilities	Magic packet	None, Wake Up Frame, Both,

3.2. Изучить возможность консоли управления MMC по встроенной справке (Консоль - действия – справка). Кратко отразить полученные сведения в отчете.

3.3. Настройка консоли ОС MS Windows для анализа трафика сетевого интерфейса.
Панель управления – Администрирование – Производительность - контекстное меню – добавить счетчики - объект - сетевой интерфейс - добавить счетчики: «отправлено байт/сек», «получено байт/сек». В свойствах графика указать диапазон вертикальной шкалы =5. Вывести заголовок над динамическим графиком- «Сетевой трафик».

3.4. В окне командного процессора выполнить команду:
ping -l 10000 127.0.0.1 -t (Выход – ctrl+c)

В течении ~1 минуты снять статистику, проанализировать, сделать вывод. В отчет вставить формат отклика.

3.5. В окне командного процессора выполнить команду:
ping -l 65500 127.0.0.1 -t
В течении ~1 минуты снять статистику, проанализировать сделать вывод. В отчет вставить формат отклика.

3. . Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств	***16***
Формируемые компетенции, образовательные результаты: ПК-17: В.2 (ПК.17.3) ПК-18: З.3 (ПК.18.1)	
3.1. Протоколирование и аудит. ***Задание для самостоятельного выполнения студентом:*** Защита от атак WinNuke. Чтобы защититься от атаки WinNuke, нужно поставить соответствующий фильтр. Атака WinNuke заключается в посылке OOB-данных на 139 порт. Таким образом, достаточно будет заблокировать TCP-соединения с 139 портом. Однако 139 порт используется для NetBIOS и потому при работе в локальной сети его перекрывать не следует. Но если вы заходите в Сеть с домашнего компьютера, то блокируйте смело. В настройке Firewall добавляем новое правило – “Add”. Назовем “WinNuke”, действие – “Block”, направление только входящие – “Inbound”, протокол “TCP”. Далееназакладках: Any Application. Service: remote - "Any", local – single service 139 порт. Остальные настройки можно оставить по умолчанию. Включите протоколирование, чтобы можно было видеть, что вы подверглись атаке. По аналогии можно настроить и другие фильтры. Лабораторное задание Задание 1. Изучите функции программы, пользуясь данным описанием. Задание 2. Установить с диска, указанного преподавателем, 2 виртуальные машины. Настроить локальную сеть между двумя виртуальными машинами, если требуется. Задание 3. Установить с диска, указанного преподавателем, на обе виртуальные машины AtGuard. Задание 4. Попробуйте обменяться пакетами запрещенного типа при включенном и при выключенном AtGuard с другим компьютером сети. Задание 5. Создать правило запрещающее получение доступа к компьютеру с удаленного компьютера (с конкретного IP-адреса или с определенного имени компьютера), попытаться обратиться с запрещенного компьютера и отследить реакцию AtGuard. Задание 6. Подготовить компьютер к безопасной работе в Интернете (блокирование cookies, active-content, java-script). Задание 7. Ответить на контрольные вопросы. Сдать работу преподавателю Контрольные вопросы 1. Что такое ATGuard и для чего применяется? 2. От чего защищает и от чего не защищает ATGuard? 3. Как ATGuard вырезает баннеры и активное содержимое? 4. Зачем скрывать информацию о cookies файлах? 5. Как можно избирательно устанавливать настройки для определенных сайтов? 6. Как посмотреть статистику и лог-файлы? 7. Как работает ATGuard с прокси-серверами? Учебно-методическая литература: 3, 4, 5, 6	8

3.2.	Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. ***Задание для самостоятельного выполнения студентом:***	8

Цель: научиться ставить пароли на документы в MSWord и MS Excel.

Теоретические сведения

В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).

Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.

Пароль на открытие, пароль разрешения записи устанав-лива-ются на файл, то есть относятся к документу/книге в целом.

Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:

Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;

Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов),структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.

Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;

Разграничение доступа аутентифи-ци-ро-ванн-ных пользователей к фрагментам текста MS Word, задание ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиента управления правами Windows).

Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.

Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями.

Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен).

Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).

В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).

Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты selfcert.exe (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно. Кроме того, другие пользователи локального компьютера также не будут доверять такой подписи.

Один из самых простых, но в то же время надежных способов защиты своих документов – это установить пароль на документ Microsoft Word. Человек, не знающий пароля, попросту не сможет этот документ открыть. Есть несколько способов установить пароль. Один из них – это использование стандартных средств Microsoft Office. Причем можно установить пароль как и на открытие документа MS Word, так и на изменение содержимого документа.

4. Шифрование. Криптография.	*24*
Формируемые компетенции, образовательные результаты: ПК-18: У.3 (ПК.18.2), В.3 (ПК.18.3)	

4.1. Шифрование и криптография ***Задание для самостоятельного выполнения студентом:***	8

Практическая работа по шифрованию /дешифрованию в MSExcell
Форма работы: индивидуальная на компьютере
Аннотация: время выполнения задания – 90 мин. (1 пара)
Цель урока:изучение простейших методов криптографической зашиты информации и закрепление навыков работы в программной среде MicrosoftExcel.
Ход урока:
1. Изучение теоретического материала.
2. Зашифровывание своих фамилии и имени, используя метод Цезаря и среду MicrosoftExcel.
3. Расшифровывание фразы с карточки, используя метод Цезаря и среду MicrosoftExcel.
4. Зашифровать, расшифрованную в п.4 фразу методом перестановки с ключом. В качестве ключа взять свою фамилию.
5. Ответить устно на вопросы.
6. Предъявить работу преподавателю.
Теоретические сведения:
Система шифрования Цезаря – частный случай шифра простой замены. Метод основан на замене каждого символа сообщения (открытого текста) на другой символ того же алфавита, путем смещения от исходного на kпозиций (получаем закрытый текст). Величина k называется ключом шифра (ключ – это информация, необходимая для беспрепятственного дешифрования информации). Ключ в методе Цезаря – целое число. Если поставить в соответствие каждому символу используемого алфавита число, то процесс шифрования будет проходить по формуле:

где xi– номер i-того символа в открытом тексте, yi – номер i-того символа в закрытом тексте, k – ключ, n – число символов в алфавите. Операция mod – это взятие остатка от деления одного числа на другое (например: 5 mod 2 = 1, 10 mod 5 = 0, 20 mod 7 = 6).
Дешифрование (расшифровывание) будет проходить по формуле

Пример.
Зашифруем методом Цезаря с ключом k=7 слово «шифр».
Будем использовать русский алфавит без буквы ё, где букве А соответствует число 0, а следовательно букве Я – 31. Т.е. n=32.
Поставим в исходном слове в соответствие каждой букве число:
ш □ 24 = x1
и □ 8 = x2
ф □ 20 = x3
р □ 16 = x4
Тогда y1 = (x1 + k) mod 32 = (24 +7) mod 32 = 31 mod 32 = 31 □ я
y2 = (x2 + k) mod 32 = (8 +7) mod 32 = 15 mod 32 = 15 □п
y3 = (x3 + k) mod 32 = (20 +7) mod 32 = 27 mod 32 = 27 □ы
y4 = (x4 + k) mod 32 = (16 +7) mod 32 = 23 mod 32 = 23 □ч
Таким образом, получили слово «япыч»
Дешифрование.
Для дешифрования необходимо каждому символу слова «япыч» поставить в соответствие число:
я □ 31 = y1
п □ 15 = y2
ы □ 27 = y3
ч □ 23 = y4
Тогда x1 = (y1 + (32 – k)) mod 32 = (31 +(32 – 7)) mod 32 = 56 mod 32 = 24 □ш
x2 = (y2 + (32 – k)) mod 32 = (15 +25) mod 32 = 40 mod 32 = 8 □и
x3 = (y3 + (32 – k)) mod 32 = (27 +25) mod 32 = 52 mod 32 = 20 □ф
x4 = (y4 + (32 – k)) mod 32 = (23 +25) mod 32 = 48 mod 32 = 16 □р
Получили слово «шифр», следовательно шифрование было выполнено правильно.
Шифр перестановки с ключом – является одним из многочисленных видов шифров перестановки (символы исходного сообщения переставляются по определенным законам).
Для перестановки с ключом выбирается ключ – любое слово. Символы ключа нумеруется в порядке следования их в алфавите. Строится таблица, в которой количество столбцов равно количеству букв в ключе. Исходный текст вместе с пробелами и знаками препинания записывается в эту таблицу. Если последняя срока заполнена не полностью, до до конца строки записываются любые символы («пустышки»). Затем текст переписывается по столбцам, учитывая их нумерацию согласно ключу.
Пример.
Выберем в качестве ключа слово «информация». Пронумеруем ключ (первая, из

4.2. Решение криптогр.задач ***Задание для самостоятельного выполнения студентом:***	8

Контрольная работа «КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ»
Вариант 1
Кодирование информации
1. Дана кодовая таблица азбуки Морзе

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

2. Закодируйте с помощью азбуки Морзе слова СТЕНОГРАФИЯ, ШИФРОВАНИЕ, КОДИРОВАНИЕ.

3. Дана таблица ASCII-кодов
Расшифровать слово : 48 41 54 52 48 58(Шестнадцатеричная СС)

4. Зашифрованная пословица.
Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).
1. Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .
2. Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
3. Самый колючий зверь в лесу – это 12, 13.
А теперь прочитайте пословицу:
1, 2, 3, 4, 5, 1, 6
7, 8, 9, 10, 11
9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ КОДИРОВАТЬ ИНФОРМАЦИЮ”. Зашифрованный текст должен быть записан без пропусков.
,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ!
Используя эту же кодировочную таблицу, расшифруйте текст:
252015383503040538351115030400 38

Шифры замены.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

Какие сообщения закодированы с помощью этой таблицы?

8. При помощи таблицы Вижинера зашифровать текст «Полиалфавитная замена».
Ключ «Шифр»

9. Шифры перестановки
a) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Аутентификация
b) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Детектор движения

10. Аналитические методы шифрования
Зашифровать слово ТОМ
Ключ – матрица

1 1 3
-1 0 2
2 1 -2

A=

4.3. ЭЦП ***Задание для самостоятельного выполнения студентом:*** Юридические основания использования ЭЦП 10 января 2002 г. Президент Российской Федерации В.В. Путин подписал Федеральный закон "Об электронной цифровой подписи" № 1-ФЗ. Цель Федерального закона № 1-ФЗ - обеспечение правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В настоящий момент действует Федеральный закон "Об электронной подписи" № 63-ФЗ от 06.04.2011 г. Сфера действия (цель) Федерального закона № 63-ФЗ - регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами. В системах, где число пользователей исчисляется сотнями и тысячами, для проверки ЭЦП используются так называемые сертификаты ЭЦП (ЭП). Сертификат ЭЦП – открытый ключ с некоторой дополнительной информацией о его владельце (регистрационный номер сертификата, ФИО владельца, срок действия и т.д.), подписанный ключом Центра сертификации (ЦС, Certificate Authority, CA, Удостоверяющий центр, УЦ). В Федеральном законе "Об электронной подписи" № 63-ФЗ от 06.04.2011 г. даны следующие определения. Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП. Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП. При получении документа, подписанного ЭЦП, вначале подается запрос в ЦС, который высылает сертификат ЭЦП, информацию об окончании срока его действия или информацию об отсутствии сертификата. Если ЦС выслал сертификат, то считается, что документ послал именно тот, кто указан в сертификате. Для автоматизации деятельности ЦС применяется системы, называемые системы поддержки инфраструктуры открытых ключей (Public Key Infrastructure, PKI). Впервые ссуда под ЭЦП (на покупку дома) была выдана в США 25 июля 2000г. Контрольные вопросы 1. Дайте определение понятию "электронная цифровая подпись". 2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП. 3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП? 4. Опишите схему протокола ЭЦП на основе алгоритма RSA. 5. Перечислите специальные схемы ЭЦП. 6. Назовите цель введения в действие Федерального закона "Об электронной цифровой подписи". Учебно-методическая литература: 3 Профессиональные базы данных и информационные справочные системы: 1, 2	8
5. Экранирование. Классификация межсетевых экранов.	***16***
Формируемые компетенции, образовательные результаты: УК-3: З.4 (УК.3.1), У.4 (УК.3.2)	

5.1. Классификация сетевых экранов ***Задание для самостоятельного выполнения студентом:***	8

Лабораторная работа: Использование межсетевых экранов (брандмауэров) для защиты информации в сетях
Цель работы:овладеть навыками работы с сетевой программой ATGuard.
Теоретические сведения.
Требования к установке:Операционная система: Windows 95, Windows 98, WindowsNT 4.0 + ServicePack 3, Windows 2000 и выше. Неподдерживаются: Windows NT 3.51, Windows 3.1x, Windows ME, Mac, Linux/UNIX.
Компьютер: на Intel 80386DX или выше (для Windows 95), или на 486/25 или выше (для Windows NT 4.0).
Около 3 MB свободного дискового пространства.
Установленный протокол TCP/IP.
Общие сведения о межсетевых экранах.
Межсетевой экран(firewall или брандмауэр) является программно-аппаратным средством осуществления сетевой политики безопасности в выделенном сегменте IP-сети.
В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от вторжения злоумышленников во внутреннюю локальную сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров.
Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети (см. рис 1.)

Рис 1. Схема установления firewall.

Название «брандмауэр», может относиться к одному устройству или од¬ной программе. Термин «межсетевой экран» был принят для обозначения совокупности компонен¬тов, которые находятся между вашей сетью и внешним миром и образуют защит¬ный барьер.
Брандмауэр не может защитить от:
 вирусов.Хотя некоторые брандмауэры и способны распознавать вирусы в про-ходящем через них трафике, существует множество способов спрятать вирусы в программе. Если даже в описании вашего брандмауэра заявлена функция антивирусной проверки, не выключайте проверку вирусов на отдельных ком-пьютерах в сети;
 «троянских коней». Как и в случае с вирусами, блокировать проникновение в сеть «троянских коней» (Trojanhorses) достаточно сложно. Пользователь нередко поддается искушению загрузить программу из Internet или открыть прикрепленный к сообщению электронной почты файл, проложив тем самым путь в систему вредоносной программе;
 «социальной инженерии». Термин «socialengineering» возник недавно и при-меняется для описания методов получения хакерами информации от довер¬чивых пользователей. Часто люди готовы сообщить свой пароль любому, кто позвонил по телефону и отреко¬мендовался представителем службы безопасности, что-нибудь «проверяю¬щим». Межсетевой экран не в состоянии остановить невоздержного на язык сотрудника
 некомпетентности. Плохо подготовленные сотрудники или небрежное руко-водство приводят к ошибкам в настройках локальной сети и межсетевого экрана. Если сотрудники не понимают, как работает брандмауэр и как пра¬вильно его настраивать, не исключено, что это будет способствовать возник¬новению проблем;
 атаки изнутри. Межсетевой экран не может предотвратить злонамеренные дей-ствия внутри вашей сети. Это одна из причин, покоторой безопасность компью-теров в сети остается важной проблемой и после установки брандмауэра.
Интерфейс AtGuard.
После инсталляции программы и перезагрузки компьютера Вы обнаружите в системном трее (system tray) иконку запущенного AtGuard’a , а вверху экрана его же панель (dashboard)

Рис 2. Внешний вид dashboard
Это означает, что инсталляция и первый запуск прошли успешно. Двойной щелчок на иконке открывает окно настроек.
AtGuard Settings / Web

Рис 3. Окно настроек Web
Установка флажка Enable web filters включает блокирование, опции секретности и активные установки фильтров, определенные в диалоговом окне Web (HTTP) Filters. Уберите этот флажок, если Вы хотите выключить все web-фильтры.
Enable web filters действует как главный переключатель, который позволяет вам отменять индивидуальные установки фильтра в диалоговом окне Web (HTTP) Filters и отключать всю фильтрацию веб-трафика. Когда Вы отключаете web-фильтры,

5.2.	Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях ***Задание для самостоятельного выполнения студентом:***	8

Add Firewall Rule
Name. Это просто краткое описание вашего правила. Имя правила также появится в Firewall лог-файле, если вы выберете регистрацию события для этого правила.

Рис 5. Окно Add firewall rule
Action. Permit (разрешить), Block (запретить), Ignore (игнорировать). Регистрирует событие в лог-файле. Затем обработка события продолжается, пока не будет найдено соответствующее правило. Если никакое правило не будет найдено связь или блокируется (по умолчанию) или вызывается RuleAssistant.
Как использовать правило Ignore?Когда задано правило Ignore, происходит регистрация события и затем обработка продолжается пока не будет найдено правило разрешающее или запрещающее данный тип связи. Обратите внимание: для того чтобы правило Ignore сработало, оно должно появиться в списке правил firewall'a выше любого правила описывающего данный тип связи. Лучше поместить все правила Ignore в верхнюю часть списка firewall.

Действие Ignore предназначено, чтобы позволить Вам регистрировать события до предписания "Разрешить" или "Блокировать", которое применяется к этому типу связи. Например, есть разрешающее правило firewall, которое позволяет вашему FTP серверу связываться с любым сетевым адресом. Можно отследить, как часто пользователи с определенного сетевого адреса соединялись с вашим FTP сервером, задав игнорирующее правило для регистрации соединений. Правило Ignore должно предшествовать правилу Permit.
Direction. Inbound связь включает пакеты, посланные вашему компьютеру. Outbound связь включает пакеты, посланные вашим компьютером. Either - связь в любом направлении.
Protocol. Определяет, к какому протоколу связи применяется правило: TCP, UDP, или TCP и UDP, ICMP...
TCP - стандартный протокол Интернета транспортного уровня, обеспечивает надежную полнодуплексную связь. Программное обеспечение, реализующее протокол TCP, обычно постоянно находится в операционной системе и использует IP протокол, чтобы передать информацию. Примеры TCP приложений и сервисов - FTP, web-браузер, email и IRC.
UDP - транспортый уровень в TCP/IP сетях. UDP - низкоуровневый протокол, который использует IP, чтобы доставить пакеты. Примеры сервисов и приложений, которые используют UDP - DNS, NetBIOS.
ICMP - протокол межсетевых управляющих сообщений.
Application. Эта опция позволяет определять, применяется ли правило к конкретному приложению или к любому приложению, которое делает попытку сетевой связи, определенной правилом.
Service. Позволяет определять, применяется ли правило к локальным или удаленным сервисам и применяется ли это к одиночному определенному сервису или к любому сервису, который делает попытку сетевой связи, определенной правилом.

Сервисы - протоколы, которые используются, чтобы позволить одному компьютеру обращаться к специфическому виду данных, сохраненных в другом компьютере. Например, HTTP серверы используют протокол передачи гипертекста, чтобы обеспечить по всему миру сервис web, FTP серверы предлагают сервисы протокола передачи файла, SMTP серверы используют простой протокол транспорта почты, чтобы посылать почту, и POP серверы используют POP протокол, чтобы передать электронную почту.
Time Active. Используйте эти установки, чтобы определить время когда, правило будет действовать.
Logging. Определяет, что событие регистрируется в лог-файле, когда устанавливается описанное правилом соединение.
AtGuard settings / Options
Show taskbar icon - при запущенном AtGuard показывать его иконку в панели задач.
Show dashboard window - при запущенном AtGuard показывать dashboard.
Enable password protection - если выбрано, то как только вы попытаетесь открыть диалоговое окно AtGuard Settings, окно Dashboard Properties, Event Log, или окно статистики, вы будете должны ввести пароль.
StartUp Options / Run at network startup. Когда эта опция выбрана, AtGuard запускается автоматически, если вы открываете сетевое соединение, и останавливается также автоматически, когда вы закрываете ваше сетевое соединение.

Рис 6. Окно Options
AtGuard settings / Dashboard

Рис7. Панель AtGuard

6. Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.	***24***
Формируемые компетенции, образовательные результаты: УК-3: В.4 (УК.3.3)	

6.1.	Компьютерные вирусы как особый класс разрушающих программных воздействий. ***Задание для самостоятельного выполнения студентом:***	8

Лабораторная работа 5. Компьютерные вирусы и борьба с ними

1.Задание

Составьте инструкцию пользователю по применению антивирусной программы, указанной в индивидуальном задании:

1) Назначение программы.

2) Выполняемые функции.

3) Технология работы.

4) Рекомендации пользователю.

2. Индивидуальные задания

1) AidsTest.
2) ADinf.

3) Norton AntiVirus.
4) ADinf Cure Module.

5) AVZ.
6) Scan.

7) Symantec Endpoint Protection.
8) Антивирус Касперского.

9) Panda Antivirus.
10) Avast

11) McAfee
12) Nod32

13) Microsoft Security Essentials

14) USB Disk Security

15) NANO Антивирус

16) Zillya!

17) TrustPort Antivirus
18) ВирусБлокАда (VBA32)

19) ActiveVirusShield
20) Ashampoo AntiVirus

21) Outpost Antivirus
22) Winpooch

23) ClamWin
24) AVG

25) eScan Antivirus
26) Comodo AntiVirus

^ Номер варианта должен соответствовать порядковому номеру студента в учебном журнале

3.Примервыполнения.

Антивирусная программа Doctor Web.

6.2. Общая организация защиты от компьютерных вирусов. ***Задание для самостоятельного выполнения студентом:***	8

Изучить статью. Составить тезисный конспект
Методы и средства защиты от компьютерных вирусов

Александр Фролов, Григорий Фролов

alexandre@frolov.pp.ru; http://www.frolov.pp.ru, http://www.datarecovery.ru

В предыдущей статье, посвященной антивирусной защите, мы рассмотрели основные типы вирусов и способы их распространения. Теперь, основываясь на этих знаниях, мы займемся защитой от вирусов, троянских и других вредоносных программ. Мы расскажем о программно-технических и административно-технологических решениях и мероприятиях, необходимых для снижения риска вирусного заражения и уменьшения вреда, если такое заражение уже произошло.

Программно-технические методы обнаружения вирусов
Основным средством борьбы с вирусами были и остаются антивирусные программы. Можно использовать антивирусные программы (антивирусы), не имея представления о том, как они устроены. Однако без понимания принципов устройства антивирусов, знания типов вирусов, а также способов их распространения, нельзя организовать надежную защиту компьютера. Как результат, компьютер может быть заражен, даже если на нем установлены антивирусы.

Сегодня используется несколько основополагающих методик обнаружения и защиты от вирусов:

- сканирование;
- эвристический анализ;
- использование антивирусных мониторов;
- обнаружение изменений;
- использование антивирусов, встроенных в BIOS компьютера.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Конечно, если это возможно.

Сканирование
Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура. Применение простых программ-сканеров не защищает Ваш компьютер от проникновения новых вирусов.

Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

Эвристический анализ
Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе, как этого требует, например, рассмотренный ниже метод обнаружения изменений.

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы.

Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. На рис. 1 мы показали одну из таких программ —

6.3. Установка антивирусного ПО. Сканирование внешнего носителя на наличие вирусов ***Задание для самостоятельного выполнения студентом:***	8

Установка Антивируса Касперского из командной строки
Чтобы провести установку Антивируса Касперского/Kaspersky Internet Security 2011 из командной строки, выполните следующие действия:
- на компьютере, где необходимо провести установку продукта Лаборатории Касперского версии 2011, запустите командную строку;
- в левой нижней части экрана нажмите на кнопку Пуск;
- выберите пункты меню (Все) Программы – Стандартные – Командная строка.

Рисунок 11 – Запуск командной строки

В окне командной строки нужно ввести команду для запуска исполняемого файла setup.exe с различными параметрами и свойствами установки. Запуск файла сопровождается следующими ключами:
Основные параметры:
/s – неинтерактивный (silent) режим (без вывода диалоговых окон в процессе установки) (пример ввода команды в командной строке: setup.exe /s);
/p <свойство>=<значение> – задание свойства для установки (пример ввода команды в командной строке: setup.exe /p «ALLOWREBOOT=1 SKIPPRODUCTCHECK=1»);
/h – справка;

Рисунок 12 – Установка Kaspersky Internet Security 2011
через командную строку

Дополнительные параметры:
/a – административная установка (копирование файлов, необходимых для установки, в указанную сетевую папку) (пример ввода команды в командной строке: setup.exe /a «Z:\Kaspersky Lab»);
/x – удаление продукта (пример ввода команды в командной строке: setup.exe /x).
Наиболее значимые свойства установки:
ACTIVATIONCODE=<значение> – код активации продукта;

Рисунок 13 – Активация коммерческой версии

ALLOWREBOOT=1 – разрешить перезагрузку, если необходимо (пример ввода команды в командной строке: setup.exe /p «ALLOWREBOOT=1»);
INSTALLDIR=<значение> – место установки (пример ввода команды в командной строке: setup.exe /p «INSTALLDIR=C:\Documents and Settings\Администратор\kis2011»);
KLPASSWD=<значение> – установка пароля на различные функции продукт (пример ввода команды в командной строке: setup.exe /p «KLPASSWD=12345678»). Если при этом не задано значение параметра KLPASSWDAREA, то используется область действия пароля по умолчанию:
- изменение настроек продукта;
- завершение работы продукта.

KLPASSWDAREA=[SET|EXIT|PARCTL|UNINST] – область действия пароля, заданного параметром KLPASSWD:
SET – изменение настроек продукта;
EXIT – завершение работы продукта;
PARCTL – изменение настроек Родительского контроля (применение параметра возможно только для Kaspersky Internet Security 2011);
UNINST – удаление продукта.
SELFPROTECTION=1 – включить самозащиту продукта в процессе установки (пример ввода команды в командной строке: setup.exe /p «SELFPROTECTION=1»);
SKIPPRODUCTCHECK=1 – не выполнять поиск продуктов, несовместимых с продуктами Лаборатории Касперского версии 2011 (пример ввода команды в командной строке: setup.exe /p «SKIPPRODUCTCHECK=1»).
Например, при вводе и выполнении команды: setup.exe /p «ALLOWREBOOT=1 SKIPPRODUCTCHECK=1» во время установки продукта Лаборатории Касперского версии 2011 разрешена перезагрузка компьютера и не будет выполняться поиск несовместимых продуктов.

Рисунок 14 – Выполнение перезагрузки компьютера без поиска

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
	Основная литература	
1	Прокушев Я.Е. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие/ Прокушев Я.Е.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 160 c.	Режим доступа: http://www.iprbookshop.ru/66799.html.— ЭБС «IPRbooks»
2	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность»/ Л.Х. Мифтахова [и др.].— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2018.— 408 c.	Режим доступа: http://www.iprbookshop.ru/73644.html.— ЭБС «IPRbooks»
3	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс]/ — Электрон. текстовые данные.— Москва: Московский технический университет связи и информатики, 2016.— 31 c	Режим доступа: http://www.iprbookshop.ru/61529.html.— ЭБС «IPRbooks»
	Дополнительная литература	
4	Костин В.Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации [Электронный ресурс]: учебное пособие/ Костин В.Н.— Электрон. текстовые данные.— Москва: Издательский Дом МИСиС, 2018.— 21 c.	Режим доступа: http://www.iprbookshop.ru/98199.html.— ЭБС «IPRbooks»
5	Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс]: учебно-методическое пособие/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 218 c.	Режим доступа: http://www.iprbookshop.ru/77317.html.— ЭБС «IPRbooks»
6	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание/ А.И. Астайкин [и др.].— Электрон. текстовые данные.— Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 c.	Режим доступа: http://www.iprbookshop.ru/60959.html.— ЭБС «IPRbooks»

4.2. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Единое окно доступа к образовательным ресурсам	http://window.edu.ru
2	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru

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

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС									
Код образовательного результата дисциплины	Текущий контроль								Промежуточная аттестация
	Кейс-задачи	Опрос	Отчет по лабораторной работе	Реферат	Ситуационные задачи	Тест	Эссе	Задача	Зачет/Экзамен
ПК-16									
З.1 (ПК.16.1)						+			+
У.1 (ПК.16.2)		+							+
В.1 (ПК.16.3)			+						+
ПК-17									
З.2 (ПК.17.1)						+			+
У.2 (ПК.17.2)			+						+
В.2 (ПК.17.3)	+								+
ПК-18									
З.3 (ПК.18.1)						+			+
У.3 (ПК.18.2)	+								+
В.3 (ПК.18.3)								+	+
УК-3									
З.4 (УК.3.1)				+					+
У.4 (УК.3.2)					+				+
В.4 (УК.3.3)							+		+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Основные средства и методы программно-аппаратной защиты информации":

1. Опрос

Что такое программный вирус и какова его природа?

2.

В чем состоят вредные проявления компьютерных вирусов?

3.

Какие основные виды компьютерных вирусов вам известны?

4.

Какие существуют виды программ для обнаружения и защиты от вирусов?

5.

В чем состоят достоинства программ-ревизоров и программ-фильтров?

6.

Назовите основные меры по защите от компьютерных вирусов.

7.

Опишите технологию периодической проверки жесткого диска на наличие вирусов.

Количество баллов: 5

2. Тест

1. Выберите все правильные варианты ответов

Активным видом атак является

- отказ в обслуживании - DoS-атака (Denial of Service)
- модификация потока данных - атака "man in the middle"
- фальсификация (нарушение аутентичности) - попытка одного субъекта выдать себя за другого
- прослушивание (сниффинг)
- анализ трафика

2. Выберите все правильные варианты ответов

Алгоритм симметричного шифрования может быть применим в

- шифровании большого потока данных
- создании определенного количества случайных битов
- хэшировании данных
- секретной передаче ключа

3. Выберите все правильные варианты ответов

Односторонняя функция с секретом - это

- одностороння функция, которую легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация
- при наличии дополнительной информации инверсию можно вычислить за полиномиальное время
- при наличии дополнительной информации инверсию можно вычислить за экспоненциальное время

4 Выберите все правильные варианты ответов

Укажите основные угрозы информационной безопасности в вычислительных сетях

- несанкционированный доступ к информации
- искажение информации или подлог (имитация)
- отказ от авторства
- отказ от шифрования
- взлом сейфа с ценными бумагами

5. Выберите все правильные варианты ответов

В необходимый минимум средств защиты от вирусов входит:

- архивирование
- профилактика
- входной контроль

Количество баллов: 5

Типовые задания к разделу "Идентификация, аутентификация. Управление доступом.":

1. Отчет по лабораторной работе

Лабораторная работа: Установка паролей в документы MSWord и MS Excel.

Цель: научиться ставить пароли на документы в MSWord и MS Excel.

Теоретические сведения

В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).

Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.

Пароль на открытие, пароль разрешения записи устанав-лива-ются на файл, то есть относятся к документу/книге в целом.

Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:

Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;

Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов),структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.

Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;

Разграничение доступа аутентифи-ци-ро-ванн-ных пользователей к фрагментам текста MS Word, задание ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиента управления правами Windows).

Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.

Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями. Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен).

Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).

В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).

Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты selfcert.exe (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно. Кроме того, другие пользователи локального компьютера также не будут доверять такой подписи.

Один из самых простых, но в то же время надежных способов защиты своих документов – это установить пароль на документ Microsoft Word. Человек, не знающий пароля, попросту не сможет этот документ открыть. Есть несколько способов установить пароль. Один из них – это использование стандартных средств Microsoft Office. Причем можно установить пароль как и на открытие документа MS Word, так и на изменение содержимого документа.

Для того чтобы установить пароль для своего документа Microsoft Word, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 6).

Рисунок 6 – Меню Сервис MS Word

После выполнения всех действий появится окно Microsoft Word – Параметры. В этом окне Microsoft Word - Параметры нужно перейти на закладку Безопасность (см. рисунок 7); далее в строке «пароль для открытия файла» ввести пароль. После ввода пароля нажмите кнопку ОК.

Рисунок 7 – Меню Безопасность MS Word

Для безопасности документа Microsoft Excel можно установить свой пароль на открытие документа. После того как вы установили пароль на открытие документа Microsoft Excel, Excel будет требовать пароль на открытие вашего документа.

Для того чтобы установить пароль для своего документа Microsoft Excel, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 8).

Количество баллов: 5

2. Тест

.. Выберите правильный вариант ответа

Если n человек хотят обмениваться между собой конфиденциально (на основе симметричного криптоалгоритма) сообщениями, то необходимо

- n(n-1) ключей
- n(n-1)/2 ключей
- (n-1)! Ключей

7.Выберите все правильные варианты ответов

"Безопасное" хранение паролей можно обеспечить на основе

- упрятывания пароля в тело программы
- шифрования пароля
- хранения хэша пароля
- хранения "подсоленого" хэша пароля
- соль "подсоленого" хэша пароля является тайной
- соль "подсоленого" хэша пароля может храниться открыто

8. Выберите все правильные варианты ответов

Пространство имен System.Security.Cryptography содержит набор классов, обеспечивающий работу

- алгоритмов цифровой подписи данных
- алгоритмов вычисления контрольных избыточных кодов данных
- алгоритмов кодирования base64
- симметричных криптографических алгоритмов
- ассиметричных криптографических алгоритмов
- алгоритмов получения хэша данных

9.Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода.

- Макровирус
- Троянский конь
- Червь
- Файловый вирус

10. Выберите правильный вариант ответа

Прослушивание данных (sniffing) в локальных сетях Ethernet, построенных на основе коммутаторов, сопряжено с трудностями, поскольку коммутаторы передают трафик непосредственно получателю. Тем не менее, если в сети используется TCP/IP, то существует легко реализуемая на практике атака, позволяющая злоумышленнику встроиться между отправителем и получателем и прослушивать трафик. Это делается путем отправки обеим сторонам специальных пакетов. Уязвимость какого протокола эксплуатируется в этой атаке?

- TCP
- UDP
- IP
- ICMP
- ARP
- RIP

Количество баллов: 5

Типовые задания к разделу ". Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств":

1. Кейс-задачи

Задача 1: У менеджера компании есть личный электронный ящик, также что она пользуется социальными сетями (Вконтакте, Одноклассники, КрасМама и пр). При этом она закрывает браузер не нажимая кнопку "выход", использует Internet Explorer, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома. Девушка коммуникабельная, активная участница форумов. На сайтах регестрируется под ником ***

Студенты делятся на 2 группы: "Защитники" (Админы) и "Злоумышленники" (Хакеры),

Каждая команда сообразно своим интересам определяет для менеджера:

- Риски по аспектам информационной безопасности: целостность, доступность, конфиденциальность
- Уязвимости
- Угрозы
- Уровень неприемлемого ущерба
- Контрмеры - политику безопасности (для защитников)
- Порядок атак (для злоумышленников)

После обсуждения, студентам сообщается имя девушки и её ник (он виртуальный). Студенты выходят в Интернет, и кто первый успеет (найти почту, поменять пароли, сменить данные, чтоб не нашли другие и пр), тот и победил.

Количество баллов: 5

2. Тест

15. Выберите все правильные варианты ответов

Отметьте правильные рекомендации по обеспечению безопасной работы на рабочей станции

- Выполнение обновлений операционной системы
- Выполнение обновлений прикладных программ
- Установка антивирусной программы
- Настройка персонального брандмауэра
- Установка пароля на BIOS и экранную заставку
- Шифрование конфиденциальной информации (EFS, PGP ...)
- Установка антивирусной программы и регулярное обновление антивирусных баз
- Работа под учетной записью пользователя с минимальным необходимым уровнем привилегий

16. Выберите правильный вариант ответа

Что является наилучшим методом аутентификации?

- Чем пользователь характеризуется (например, биометрия)
- Что пользователь имеет
- Что пользователь знает
- Другое

17 Выберите правильный вариант ответа

Какое утверждение наиболее справедливо?

- Чем сложнее механизм защиты, тем меньшую безопасность он гарантирует
- Чем сложнее механизм защиты, тем большую безопасность он гарантирует
- Сложность механизм защиты не связана с уровнем гарантируемой им безопасности

18.Выберите правильный вариант ответа

Это код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы. Он обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. О какой вредоносной программе идет речь?

- вирусы
- "черви"
- троянские программы
- "бомбы"

19. Это код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы). Они ориентированы в первую очередь на путешествия по сети.О какой вредоносной программе идет речь?

- вирусы
- "черви"
- троянские программы
- "бомбы"
- "змеи"

20.Примером какой атаки является перехват злоумышленником передаваемых данных с одновременной их модификацией "прозрачно" для обеих участвующих в обмене сторон?

- Прослушивание сети (sniffing)
- Подмена или спуфинг (spoofing)
- Перехват соединения (hijacking)
- Повторная передача (replay)
- Человек в середине (man in the middle)

Количество баллов: 5

Типовые задания к разделу "Шифрование. Криптография.":

1. Задача

Контрольная работа «КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ»
Вариант 3
Кодирование информации
1. Дана кодовая таблица азбуки Морзе

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

2. Закодируйте с помощью азбуки Морзе слова КРИПТОГРАФИЯ, ВИРУС, ДЕКОДИРОВАНИЕ

3. Дана таблица ASCII-кодов
Закодировать при помощи таблицы ASCII кодов следующий текст Password. Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.
Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).
7. Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .
8. Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
9. Самый колючий зверь в лесу – это 12, 13.
А теперь прочитайте пословицу:
1, 2, 3, 4, 5, 1, 6
7, 8, 9, 10, 11
9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.
,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ!
Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

Шифры замены.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

Какие сообщения закодированы с помощью этой таблицы?

8. При помощи таблицы Вижинера зашифровать текст «Методы шифрования». Ключ «Шифр»

9. Шифры перестановки
c) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Кодирование
d) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Декодирование

10. Аналитические методы шифрования
Зашифровать слово ГАМ
Ключ – матрица
-1 0 4
0 2 2
3 1 -2

A=

Выполнить проверку (расшифровать слово)
Количество баллов: 10

2. Кейс-задачи

Контрольная работа «КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ»
Вариант 2
Кодирование информации
1. Дана кодовая таблица азбуки Морзе

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

2. Закодируйте с помощью азбуки Морзе слова КРИПТОАНАЛИЗ, КЛЮЧ, ШИФР

3. Дана таблица ASCII-кодов
Расшифровать слово при помощи таблицы ASCIIгкодов:
32 2A 78 2B 79 3D 30.

4. Зашифрованная пословица.
Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).
4. Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .
5. Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.
6. Самый колючий зверь в лесу – это 12, 13.
А теперь прочитайте пословицу:
1, 2, 3, 4, 5, 1, 6
7, 8, 9, 10, 11
9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.
,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ!
Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

Шифры замены.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

Какие сообщения закодированы с помощью этой таблицы?

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр»

9. Шифры перестановки
a) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Криптоанализ
b) Закодировать методом Гамильтона (создать свой маршрут(ы)).
Криптостойкость

10. Аналитические методы шифрования
Зашифровать слово БАР
Ключ-матрица
0 1 2
2 2 1
3 1 -1

A=

Выполнить проверку (расшифровать слово)

Количество баллов: 10

Типовые задания к разделу "Экранирование. Классификация межсетевых экранов.":

1. Реферат

Реферат — письменная работа, выполняемая обучающимся в течение длительного срока (от одной недели до месяца).
Реферат (от лат. referrer — докладывать, сообщать) — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.
Реферат отвечает на вопрос — что содержится в данной публикации (публикациях).
Однако реферат — не механический пересказ работы, а изложение ее существа.
В настоящее время, помимо реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата может предложить преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.
В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.
Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.
Структура реферата:
1. Титульный лист.
2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.
4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.
5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.
6. Приложение может включать графики, таблицы, расчеты.
7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.
Этапы работы над рефератом.
Работу над рефератом можно условно подразделить на три этапа:
1. Подготовительный этап, включающий изучение предмета исследования;
2. Изложение результатов изучения в виде связного текста;
3. Устное сообщение по теме реферата.
1. Подготовительный этап работы.
Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).
Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями (обращать особое внимание на список литературы, приведенный в конце тематической статьи); как работать с систематическими и алфавитными каталогами библиотек; как оформлять список литературы (выписывая выходные данные книги и отмечая библиотечный шифр).
Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.
Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.
Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.
Создание конспектов для написания реферата.
Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и

Количество баллов: 10

2. Ситуационные задачи

Задача 6 История вирусов

Александр Квасов, начальник управления информационных технологий Нижегородского регионального центра-филиала ОАО АКБ «СОЮЗ»:

— В конце 90-х много вирусов было настроено на остановку работоспособности компьютера — уничтожение информации в BIOS, и на жестких дисках. На себе я испытал поражение жесткого диска вирусом W95.CIH «Чернобыль». На офисных компьютерах стояла операционная система Windows 95, доступ в Интернет имел один компьютер, остальные были связаны с ним в локальной сети. 26 апреля 1999 года не загрузились все офисные компьютеры, информация на дисках стала недоступной. Данные, к счастью, удалось восстановить, однако это было не так просто. Фирма понесла большие убытки.
Пометка для педагога: Напомним, что W95.CIH заражал исполняемые файлы и обладал крайне деструктивной функциональностью. Он полностью уничтожал содержимое жесткого диска и перезаписывал флэш-BIOS материнской платы, после чего заражённый компьютер вообще переставал загружаться. Наиболее уязвимы для вируса компьютеры на базе операционных систем Windows 95, 98 и Me. В этом случае вирус ищет файлы с расширением .EXE и записывает свой код в неиспользуемые части этих файлов. Размер зараженных файлов при этом практически не увеличивается, и у пользователя не возникает никаких подозрений.
Участникам обсуждения проблемы предлагается представить себя на месте сотрудников ОАО АКБ «СОЮЗ», предложить варианты обнаружения заражения, проверки, профилактики, защиты данных.

Задача7: Классификация вирусов

У журналиста-фрилансера возникли проблемы с программным обеспечением:
1. Большинство программ перестают работать и "вылетают" с критической ошибкой
2. Загрузка в безопасном режиме невозможна
3. Сайты kaspersky.ru, drweb.ru, viruslist.ru и пр. не загружаются
4. Значительно снизилась производительность компьютера.
Он решил, что это - результат деятельности вируса.
Участникам обсуждения предлагается по симптомам определить, что за вирус, как его лечить

Пометка для педагога: Вирус, который Kaspersky определяет как VIRUS.WIN32.Sality.z, а Dr. Web - win32.sector.5, win32.sector.7 (подробное описание). Даже у опытных пользователей его уничтожение вызывает трудности.
Пример решения:
1. Отключаем сеть. Т.е. отключаем ADSLm Dial-up, LAN - любые сетевые подключения. Просто выдергиваем кабель.
2. Идем к неинфицированному компьютеру, т.к. на инфицированном не удастся получить доступ к сайту, и скачиваем Dr.Web CureIt!. Это бесплатное приложение, которое может работать даже без установки.
Скачанное приложение по возможности записываем на CD/DVD или флешку с защитой - дабы вирус не мог испортить программу. Если испортит - вместо приветственного окошка вы увидите окно стандартного распаковщика WinRAR SFX.
3. Чиним реестр с помощью установки ключа. Соглашаемся с внесением изменений в реестр.
4. Загружаемся в безопасном режиме, удерживая длительное время сразу после включения компьютера клавишу F8. Должно появиться меню с выбором вариантов загрузки. Нам нужен "Безопасный режим".
5. Лечим компьютер от вирусов. Для этого вставляем диск с записанным Dr.Web CureIt! и проводим полную проверку компьютера.
6. Перезагружаемся в обычном режиме.
7. Вновь проводим полную проверку.
8. Устанавливаем нормальный антивирус со свежими базами.

Количество баллов: 10

Типовые задания к разделу "Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.":

1. Эссе

Образец эссе.
Классификации современных программно-аппаратных комплексов
Бурное развитие средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий в нашей стране сопровождается появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и прежде всего несанкционированный доступ к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации. Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается так же и правовая база информационной безопасности, а именно, приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др. Целями защиты информации являются:
1. предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;
2. реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации
3. создание определенных программно-аппаратных средств защиты, соответствующих потребностям владельцев (пользователей) информации.
Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации, включающей не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах, прежде всего, программно-аппаратные.
Большинство функций современных КС реализованы в виде программ, поддержание целостности которых при запуске системы и особенно в процессе функционирования является трудной задачей. Значительное число пользователей в той или иной степени обладают познаниями в программировании, осведомлены об ошибках в построении операционных систем. Поэтому существует достаточно высокая вероятность применения ими имеющихся знаний для атак на программное обеспечение. Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя. В связи с этим к программным системам защиты от несанкционированного доступа следует относиться с особой осторожностью.
Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений вПО необходимо получить доступ к соответствующей плате и заменить микросхему. В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.
Для того, чтобы защитить информацию от НСД, существует ряд специально проводимых мер:
- Применение аппаратных средств:
  - установка фильтров, межсетевых экранов;
  - блокировка клавиатуры;
  - устройства аутентификации;
  - использование электронных замков на микросхемах.
- Применение программных средств:
  - использование пароля для доступа к компьютеру;
  - использование средств парольной защиты BIOS — как на сам BIOS, так и на ПК в целом.
- Применение аппаратно-программных средств:
  - использование аппаратно-программных средств доверенной загрузки
- Применение шифрования:
  - Шифрование — это преобразование (кодирование) открытой информации в зашифрованную, для передачи закрытой информации или сведений, составляющих государственную тайну информации по незащищенным каналам связи. Зачастую, сам алгоритм шифрования известен всем, а ключ, с помощью которого можно расшифровать данное сообщение засекречен.
- Проведение организационных мероприятий:
  - осуществление пропускного режима;
  - хранение носителей информации в закрытом доступе;
  - ограничение лиц, имеющих доступ к компьютеру.

Рассмотрим несколько программно-аппаратных комплексов защиты информации.
1) Программно-аппаратный комплекс «Аккорд – 1.95».
Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Аккорд – 1.95», далее комплекс «Аккорд», предназначен для применения на ПЭВМ типа IBM PC в целях защиты ПЭВМ и информационных ресурсов от НСД и обеспечения конфиденциальности информации, обрабатываемой и хранимой в ПЭВМ при многопользовательском режиме ее эксплуатации. Комплекс разработан ОКБ САПР при участии фирмы «Инфокрипт» на основании лицензии Государственной технической комиссии при Президенте РФ (Гостехкомиссии России) от 02.06.95 N 56. Комплекс «Аккорд» состоит из программно-аппаратных средств «Аккорд АМДЗ» и ПО разграничения доступа «Аккорд 1.95-00». В настоящее время комплекс «Аккорд-1.95» выпускается в трех основных версиях в зависимости от модификации аппаратных средств (контроллеров):

Количество баллов: 10

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. • Защита авторских прав на электронные документы в России. Правовая база.
2. • Применение электронной подписи (ЭП) в России (хранение ЭП, идентификация и аутентификация при помощи ЭП). Правовая база применения ЭП в России.
3. • Web-сайт. Выбор способа написания. Преимущества и недостатки.
4. • Продвижение сайта в поисковых системах.
5. • Защищенные централизованные хранилища данных (ЦХД): принципы построения, продукты-менеджеры, угрозы ЦХД.
6. • Утечка информации при помощи побочного электромагнитного излучения и наводок (ПЭМИН).
7. • Стандарт ISO/IEC 17799:2005.
8. • Стандарт ISO/IEC 27001:2005.
9. • Стандарт BS 7799-3:2006.
10. • Обзор новых и широко используемых криптографических стандартов и алгоритмов.
11. • Обзор современных программных средств криптографического управления данными (шифрование, удаление, создание защищенных дисков и т.д.).
12. • Протоколы шифрования при передаче по сети (в т.ч. беспроводной). Примеры (WPA и т.д.)
13. • Обзор программных средств выполнения активного аудита.
14. • Защита от копирования CD, DVD дисков.
15. • Целостность информации. Средства резервного копирования. Обзор имеющихся средств.
16. • Средства восстановления потерянных или удаленных файлов. Средства полного уничтожения информации.
17. • Виртуальные машины. Примеры. Работа с VMWare.
18. • Методы и средства идентификации и аутентификации в компьютерных системах.
19. • Устройство и работа бесконтактных карт, смарт-карт, электронных ключей и т.п.
20. • Наиболее известные и удачные попытки взлома последних двух лет. В лицах и фактах.
21. • Классификация вредоносных программ. Методы защиты, алгоритмы работы противоборствующих программ.
22. • Принцип работы программных и аппаратных межсетевых экранов (МЭ). Предлагаемые возможности.
23. • Решения по защите от несанкционированного использования мобильных устройств (мобильных телефонов, смартфонов, КПК и т.п.)
24. • Защита Web-сервера. Организация доступа к Web-серверу для просмотра информации.
25. • Возможность удаленного управления компьютером (УУК). Защита от несанкционированного УУК.
26. • Обзор локальных и сетевых программ-шпионов (клавиатурные, запуск программ, клавиатурные в окне конкретной программы и т.п.).
27. • Программные средства по контролю за действиями пользователей
28. • Защита от перехвата трафика, передаваемого по радиоканалам (wi-fi, bluetooth, и т.д.), защита точек доступа, построение беспроводных сетей.
29. • Организация и защита VPN-сетей.
30. • Безопасность VoIP.

Второй период контроля

1. Экзамен

Вопросы к экзамену:

1. • Понятие защищенной операционной системы.
2. • Подходы к организации защиты операционной системы.
3. • Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
4. • Применение типовых моделей управления доступом в операционных системах.
5. • Управление доступом в UNIX.
6. • Управление доступом в Windows.
7. • Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
8. • Средства минимизации полномочий пользователей в Windows.

9. • Управление средствами аутентификации в Linux и Windows.
10. • Управление средствами аудита в Linux и Windows.
11. • Управление доменами Windows.
12. • Групповая политика в доменах Windows.
13. • Сетевые атаки.
14. • Адаптивная безопасность в вычислительных сетях.
15. • Пакетные фильтры и межсетевые экраны, их классификация и особенности применения.
16. • Виртуальные частные сети.
17. • Угрозы безопасности баз данных: общие и специфичные.
18. • Модели безопасности СУБД.
19. • Средства и методы обеспечения целостности данных СУБД.
20. • Ролевое разграничение доступа к данным в современных СУБД.
21. • Понятие программной закладки.
22. • Модели взаимодействия программной закладки с атакуемой компьютерной системой.
23. • Предпосылки к внедрению программных закладок.
24. • Метод внедрения программных закладок.
25. • Основные принципы построения политики безопасности, повышающей защищенность от программных закладок.
26. • Сигнатурное и эвристическое сканирование как метод выявления программных закладок.
27. • Контроль целостности как метод выявления программных закладок.
28. • Антивирусный мониторинг как метод выявления программных закладок.
29. • Изолированная программная среда как метод выявления программных закладок.
30. • Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.
31. • Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.
32. • Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия Скриптовым вирусам.
33. • Стелс-технологии: назначение, методы противодействия.
34. • Основные компоненты подсистемы защиты Unix
35. • Файловая система – как основа подсистемы защиты.
36. o Права доступа к элементам файловой системы.
37. o Управление процессами. Создание и удаление бюджетов пользователей
38. • Основные компоненты подсистемы защиты ОС Windows
39. • Основы взаимодействия элементов гетерогенных сетей
40. • Методы и средства ограничения доступа к компонентам ЭВМ.

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно 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.

2. Практические

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий и семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

При подготовке к практическому занятию необходимо, ознакомиться с его планом; изучить соответствующие конспекты лекций, главы учебников и методических пособий, разобрать примеры, ознакомиться с дополнительной литературой (справочниками, энциклопедиями, словарями). К наиболее важным и сложным вопросам темы рекомендуется составлять конспекты ответов. Следует готовить все вопросы соответствующего занятия: необходимо уметь давать определения основным понятиям, знать основные положения теории, правила и формулы, предложенные для запоминания к каждой теме.

В ходе практического занятия надо давать конкретные, четкие ответы по существу вопросов, доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

3. Зачет

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

4. Экзамен

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой. Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы, также как и основные вопросы билета, требуют развернутого ответа.

Результат экзамена выражается оценкой «отлично», «хорошо», «удовлетворительно».

5. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);

− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.

− оставить время для проверки ответов, чтобы избежать механических ошибок.

6. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.

Подготовка к опросу включает в себя:

− изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;

− повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;

− изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;

− составление в мысленной форме ответов на поставленные вопросы.

7. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

8. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

9. Задача

Задачи позволяют оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей.

Алгоритм решения задач:

1.Внимательно прочитайте условие задания и уясните основной вопрос, представьте процессы и явления, описанные в условии.

2.Повторно прочтите условие для того, чтобы чётко представить основной вопрос, проблему, цель решения, заданные величины, опираясь на которые можно вести поиск решения.

3.Произведите краткую запись условия задания.

4.Если необходимо, составьте таблицу, схему, рисунок или чертёж.

5.Установите связь между искомыми величинами и данными; определите метод решения задания, составьте план решения.

6.Выполните план решения, обосновывая каждое действие.

7.Проверьте правильность решения задания.

8.Произведите оценку реальности полученного решения.

9.Запишите ответ.

10. Реферат

Реферат − теоретическое исследование определенной проблемы, включающее обзор соответствующих литературных и других источников.

Реферат обычно включает следующие части:

1. библиографическое описание первичного документа;
2. собственно реферативная часть (текст реферата);
3. справочный аппарат, т.е. дополнительные сведения и примечания (сведения, дополнительно характеризующие первичный документ: число иллюстраций и таблиц, имеющихся в документе, количество источников в списке использованной литературы).

Этапы написания реферата

1. выбрать тему, если она не определена преподавателем;
2. определить источники, с которыми придется работать;
3. изучить, систематизировать и обработать выбранный материал из источников;
4. составить план;
5. написать реферат:

− обосновать актуальность выбранной темы;

− указать исходные данные реферируемого текста (название, где опубликован, в каком году), сведения об авторе (Ф. И. О., специальность, ученая степень, ученое звание);

− сформулировать проблематику выбранной темы;

− привести основные тезисы реферируемого текста и их аргументацию;

− сделать общий вывод по проблеме, заявленной в реферате.

При оформлении реферата следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

11. Ситуационные задачи

Ситуационная задача представляет собой задание, которое включает в себя характеристику ситуации из которой нужно выйти, или предложить ее исправить; охарактеризовать условия, в которых может возникнуть та или иная ситуация и предложить найти выход из нее и т.д.

При выполнении ситуационной задачи необходимо соблюдать следующие указания:

1. Внимательно прочитать текст предложенной задачи и вопросы к ней.
2. Все вопросы логично связаны с самой предложенной задачей, поэтому необходимо работать с каждым из вопросов отдельно.
3. Вопросы к задаче расположены по мере усложнения, поэтому желательно работать с ними в том порядке, в котором они поставлены.

12. Эссе

Эссе - это прозаическое сочинение небольшого объема и свободной композиции, выражающее индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендующее на определяющую или исчерпывающую трактовку предмета.

Структура эссе определяется предъявляемыми к нему требованиями: мысли автора эссе по проблеме излагаются в форме кратких тезисов; мысль должна быть подкреплена доказательствами - поэтому за тезисом следуют аргументы . При написании эссе важно также учитывать следующие моменты:

Вступление и заключение должны фокусировать внимание на проблеме (во вступлении она ставится, в заключении - резюмируется мнение автора).

Необходимо выделение абзацев, красных строк, установление логической связи абзацев: так достигается целостность работы.

Стиль изложения: эссе присущи эмоциональность, экспрессивность, художественность. Должный эффект обеспечивают короткие, простые, разнообразные по интонации предложения, умелое использование "самого современного" знака препинания - тире.

Этапы написания эссе:

1. написать вступление (2–3 предложения, которые служат для последующей формулировки проблемы).
2. сформулировать проблему, которая должна быть важна не только для автора, но и для других;
3. дать комментарии к проблеме;
4. сформулировать авторское мнение и привести аргументацию;
5. написать заключение (вывод, обобщение сказанного).

При оформлении эссе следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Цифровые технологии обучения
2. Кейс-технологии

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. учебная аудитория для семинарских, практических занятий
3. лаборатория
4. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC