Рабочая программа

Дисциплина:	Информационная безопасность в профессиональной деятельности
Наименование кафедры	Экономико-математических методов и информационных технологий (ЭММиИТ)

Специальность: 380501 «Экономическая безопасность» (степень – специалист)

Специализация «Экономико-правовое обеспечение экономической безопасности»

Сведения о разработчиках:

ФИО	Аббревиатура кафедры	Ученая степень, звание
Козлова Любовь Александровна	ЭММиИТ	к.т.н.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Целью изучения дисциплины является обучение современным технологиям в области информационных систем, создания и эксплуатации систем защиты информации.

Задачами освоения дисциплины являются:

- усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;
- ознакомление с угрозами информационной безопасности, создаваемыми компьютерными вирусами

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП,ОПОП:

Дисциплина входит в цикл дисциплин по выбору рабочего учебного плана и имеет код Б1.В.ДВ.3.

До начала ее изучения студент должен освоить содержание учебных дисциплин: «Информационные системы в экономике» (ОК-12), «Эконометрика» (ОПК-1, ОПК-2, ПК-30, ПК-31), «Бухгалтерский учет» (ПК-6, ПК-33), и иметь представление о том, на каких участках своей будущей профессиональной деятельности он сможет использовать полученные знания в рамках компетенций, обусловленных спецификой его предстоящей работы.

Знания, навыки и умения, приобретенные в результате прохождения курса, могут быть востребованы при выполнении курсовых и дипломных работ, связанных как с применением информационных систем готовых пакетов и информационных структур, так и с темой о принятии решений об использовании развивающихся перспективных направлений в сфере информационных технологий и информационной безопасности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСНОВЕНИЯ ДИСЦИПЛИНЫ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ✓ ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
- ✓ ПК-29 способностью выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор.

В результате освоения дисциплины студенты должны:

знать: предпосылки формирования сферы знаний по информационной безопасности; законодательную и нормативную базу ИБ; основные меры, направленные на обеспечение ИБ на различных уровнях деятельности современного предприятия; иметь полное представление о значение информационной безопасности для современного бизнеса, о перспективах развития технологий обеспечения информационной безопасности.

уметь: анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ. Использовать знания о современной методологии управления ИБ для разработки

реальных методов формирования защиты информационной инфраструктуры. Применять эти методы для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ. Ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ.;

- ***владеть:*** способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации ИБ. Способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; использовать современные инструментальные средства анализа рисков и разработки политики ИБ.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) – 3

4.2. По видам учебной работы (в часах)

Вид учебной работы	Количество часов (форма обучения – **очная**)	
	Всего по плану	в т.ч. по семестрам
		4
1	2	3
Контактная работа обучающихся с преподавателем	54	54
Аудиторные занятия:	54	54
лекции	18	18
лабораторные работы	36	36
Самостоятельная работа	54	54
Всего часов по дисциплине	108	108
Текущий контроль	нет	нет
Курсовая работа	нет	нет
Виды промежуточной аттестации	зачет	зачет

4.3. Распределение часов по темам и видам учебной работы: Форма обучения: очная

Название и разделов и тем	Всего	Виды учебных занятий			
		Аудиторные занятия		Занятия в интерактивной форме	Самостоятельная работа
		лекции	практические занятия, семинар		
1	2	3	4	5	6
Тема 1. Информационная	12	2	4	4	6

безопасность и уровни ее обеспечения.					
Тема 2. Компьютерные вирусы и защита от них.	24	4	8	8	12
Тема 3. Информационная безопасность вычислительных сетей.	24	4	8	8	12
Тема 4. Механизмы обеспечения "информационной безопасности".	12	2	4	4	6
Тема 5. Информационная безопасность при использовании Internet.	12	2	4	4	6
Тема 6. Безопасность операционных систем.	24	4	8	8	12
Итого:	108	18	36	36	54

5. СОДЕРЖАНИЕ КУРСА

Тема 1. Информационная безопасность и уровни ее обеспечения. Понятие "информационная безопасность". Проблема информационной безопасности общества. Определение понятия "информационная безопасность". Составляющие информационной безопасности. Доступность информации. Целостность информации. Конфиденциальность информации. Система формирования режима информационной безопасности. Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности.

Тема 2. Компьютерные вирусы и защита от них. Вирусы как угроза информационной безопасности. Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивным возможностям. Характеристика "вирусоподобных" программ. Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Антивирусные программы. Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ. Профилактика компьютерных вирусов. Характеристика путей проникновения вирусов в компьютеры. Правила защиты от компьютерных вирусов. Обнаружение неизвестного вируса. Обнаружение загрузочного вируса. Обнаружение резидентного вируса. Обнаружение макровируса. Общий алгоритм обнаружения вируса.

Тема 3. Информационная безопасность вычислительных сетей. Особенности обеспечения информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей.

Тема 4. Механизмы обеспечения "информационной безопасности". Идентификация и аутентификация. Определение понятий "идентификация" и "аутентификация". Механизм идентификация и аутентификация пользователей. Криптография и шифрование. Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи. Методы разграничение доступа. Методы разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита информационных систем. Этапы регистрации и методы аудита событий информационной системы. Межсетевое экранирование. Классификация межсетевых экранов. Характеристика межсетевых экранов. Технология виртуальных частных сетей (VPN). Сущность и содержание технологии виртуальных частных сетей. Понятие "туннеля" при передаче данных в сетях.

Тема 5. Информационная безопасность при использовании Internet.

Тема 6. Безопасность операционных систем.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Практическая работа по данному курсу проводится в виде ролевой деловой игры «Разработка элементов информационной защиты современного высокотехнологичного предприятия».

Группы студентов строят модель информационной безопасности для своих компаний. Модель ИБ включает в себя концепцию, программу и политику ИБ, модель угроз, модель защиты данных и информации. В результате должна быть разработана модель комплексной защиты информационной инфраструктуры компании.

Темы семинарских занятий включают:

Тема 1. Подготовка предварительного варианта концепции информационной безопасности компании. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 2. Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 3. Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели информационной безопасности. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 4. Разработка параметров защищенности программных и информационных систем компании и программы ИБ. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 5. Разработка модели общей и частных политик информационной безопасности компании. Подготовка нормативного документа для введения в действия политики ИБ. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 6. Описание структуры информационных рисков, построение модели процесса оценки рисков, составление списка мероприятий для уменьшения рисков. Обзор программных продуктов для оценки информационных рисков. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 7. Формирование опорной системы стандартов для реализации информационной безопасности предприятия. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 8. Подготовка базовой совокупности сервисов информационной защиты. Выбор и внедрение средств криптографической защиты информации. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Тема 9. Формирование программно-аппаратных и технических средств защиты информационных ресурсов от внешних атак и вирусной опасности. Построение комплексной

системы информационной защиты. Трудоемкость – 4 часа, в том числе в интерактивной форме – 4 часа.

Отчётным материалом является сайт компании, на котором представлены результаты деловой игры. На каждом практическом занятии (семинаре) заслушиваются доклады всех групп, сопровождаемые презентациями о пошаговой реализации модели ИБ.

7. ЛАБОРАТОРНЫЕ РАБОТЫ

Не предусмотрены.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

ВОПРОСЫ К ЗАЧЕТУ

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура
    требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России.
13. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
14. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
15. Единые критерии безопасности информационных технологий. Проект защиты.
16. Требования безопасности (функциональные требования и требования адекватности).
17. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
18. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
19. Идентификация и аутентификация при входе в информационную систему.
20. Использование парольных схем. Недостатки парольных схем.
21. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
22. Биометрические средства идентификации и аутентификации пользователей.

23. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
24. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
25. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
26. Законодательный уровень применения цифровой подписи.
27. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
28. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
29. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
30. Средства обеспечения информационной безопасности в ОС Windows 2000.
31. Разграничение доступа к данным. Групповая политика.

9. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

К самостоятельной работе студентов по дисциплине «Информационная безопасность в профессиональной деятельности» относятся их подготовка к практическим занятиям и написание докладов по изучаемым темам:

1. Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности.
2. Информационные, программно-математические, физические и организационные угрозы. Методы и средства продиводействия им.
3. Криптографическая защита.
4. Проблема вирусного заражения программ.
5. Безопасность в компьютерных сетях.
6. Защита от несанкционированного доступа, модели и основные принципы защиты информации.
7. Программно-аппаратные средства защиты информации.
8. Безопасность операционных систем.

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. : ДМК Пресс, 2010. - 544 с. : ил. - http://www.book.ru
2. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft/ СА. Нестеров - М.: Национальный Открытый Университет "ИНТУИТ", 2009, 375 с. - http://www.knigafund.ru/books/173009
3. Гончарук С.В. Администрирование ОС Linux/ С.В. Гончарук - М.: Национальный Открытый Университет "ИНТУИТ", 2011, 170 с. -http://www.knigafund.ru/books/173018
4. Перетолчин А.С. Защита Windows от сбоев [Текст] / А. С. Перетолчин. — Новосибирск: Сиб. унив. изд-во, 2008. — 108 с. - http://www.knigafund.ru/books/17225
5. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - http://znanium.com/bookread2.php?book=495249

Дополнительная литература

6. Расторгуев С. П. Основы информационной безопасности: учеб. пособие. М.: Академия, 2009. – 187 с.

7. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
8. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2009. - 256 с.
9. Мао В. Современная криптография: теория и практика. :Пер. с англ. – М.: Издательский дом "Вильямс", 2005. –768 с.
10. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. – М.: Издательский Дом ДМК-пресс, 2006. – 288 с.: ил.
11. Смит Р.Э. Аутентификация: от паролей до открытых ключей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. –432 с.: ил.
12. Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 527 с.: ил.
13. Алферов А.П., Зубов А.Ю, Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. – М.:Гелиос АРВ, 2002. – 380 с.: ил.
14. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие для студентов образоват. учреждений сред. проф. образования, обуч. по спец. "Информатика и вычислит. техника" / В. Ф. Шаньгин. - М. : ФОРУМ : ИНФРА-М, 2016. - 416 с.
15. Васильков А.В. Информационные системы и их безопасность: учеб. пособие [для студентов образоват. учреждений сред. проф. образования] / А. В. Васильков, А. А. Васильков, И. А. Васильков. - М. : ФОРУМ, 2015. - 528 с. : ил. - (Профессиональное образование)

Сайты Интернет:

1. Интернет-библиотека русскоязычных СМИ Public.ru http://www. public.ru/
2. Научная электронная библиотека (НЭБ) http://elibrary.ru/
3. Университетская библиотека online http://www.biblioclub.ru/
4. ЭБС znanium.com издательства «ИНФРА-М» http://www.znanium.com/
5. Электронно-библиотечная система РУКОНТ http://rucont.ru/
6. Электронно-библиотечная система BOOK.ru http://www.book.ru/
7. Электронно-библиотечная система IPRbooks http://www.iprbookshop.ru/

Программное обеспечение

1. Операционная система Windows;
2. Пакет прикладных программ Microsoft Office;
3. Инструментальная среда разработки Visual Studio.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Аудитории для проведения лекционных занятий, оснащенные проектором, ноутбуком (актовый зал, 703, 709 и др. аудитории).
2. Компьютерные классы с доступом в сеть Интернет.

Приложение к рабочей программе

Фонды оценочных средств
по дисциплине «Автоматизация обработки учетной информации»

1. Перечень компетенций, которые формируются в процессе изучения дисциплины:

- ✓ ОК-12 способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
- ✓ ПК-29 способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор.

Этапы формирования компетенций по дисциплине для студентов специальности «Экономическая безопасность»

№ семестра	Дисциплины (модули)	Код компетенции				
		ОК-12	ПК-29			
1,2	Информационные системы в экономике	+				
4	Автоматизация обработки учетной информации	+	+			
4	Информационная безопасность в профессиональной деятельности	+	+			
8	Производственная практика		+			
10	Преддипломная практика		+			
10	Государственная итоговая аттестация	+	+			

2. Показатели и критерии оценивания, шкала оценивания

В основе оценки знаний по предмету лежат следующие основные требования:

- освоение всех разделов теоретического курса Программы;
- умение применять полученные знания к решению конкретных задач.

Ответ заслуживает оценки ***зачтено***, если он глубоко усвоил программный материал, логически стройно его излагает, не испытывает затруднений с иными формулировками задаваемого вопроса; умеет увязать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, правильно обосновывает принятое решение.

Оценка ***незачтено*** выставляется студенту, который не знает значительной части программного материала, не умеет даже с помощью преподавателя сформулировать правильные ответы на вопросы.

3. Тесты для оценивания компетенций

1) Концепция и структура защиты информации не включает в себя
a) арсенал технических средств защиты информации предприятия, специализирующиеся на решении вопросов защиты информации
b) четко очерченная система взглядов на эту проблему
c) **значительное число антивирусных средств**

2) Защита информации должна быть
a) **непрерывной**
b) неплановой
c) пассивной

d) выборочной

3) Система защиты информации должна удовлетворять требованиям
a) охватывать весь технологический комплекс информационной деятельности
b) быть разнообразной по используемым средствам
c) быть открытой для изменения и дополнения мер
d) быть нестандартной, разнообразной
e) быть надежной
f) **все из перечисленного**
g) ничего из перечисленного

4) К системе безопасности информации предъявляется требование
a) предоставление пользователю максимальных полномочий, необходимых ему для выполнения порученной работы
b) предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы
c) игнорирование попыток несанкционированного доступа
d) периодическое реагирование на выход из строя средств защиты

5) Система защиты информации может иметь
a) правовое обеспечение
b) организационное обеспечение
c) аппаратно-программное обеспечение
d) информационное обеспечение
e) математическое обеспечение
f) лингвистическое обеспечение
g) методическое обеспечение
h) все из перечисленного
i) ничего из перечисленного

6) Угрозами конфиденциальной информации не являются
a) ознакомление без нарушения ее целостности
b) модификация информации
c) разрушение информации
d) создание и распространение вирусов

7) Источниками внешних угроз не являются
a) недобросовестные конкуренты
b) преступные группировки и формирования
c) лица административно-управленческого аппарата
d) компьютерные сети

8) Способствует неправомерному овладению конфиденциальной информацией
a) применение нелицензионного ПО
b) несанкционированный доступ
c) приобретение недорогих технических средств
d) доступ сотрудников к сети Интернет

9) Соединения удаленного доступа могут использоваться
a) для получения несанкционированного доступа к организациям
b) для передачи своих персональных данных
c) для проверки имени и пароля
d) все из перечисленного

10) Механизм аутентификации
a) Модем обратного вызова
b) Проверка отпечатков пальцев
c) Генератор случайных чисел
d) Брандмауэр

11) Вредоносный код проникает в организации способами

a) Файлы с общим доступом с домашних и рабочих компьютеров
b) Файлы, загружаемые с сайтов интернета
c) Файлы, поступающие в организацию в виде вложений электронной почты
d) Файлы, внедряемые в системы посредством использования уязвимостей
e) Все из перечисленного
f) Ничего из перечисленного

12) Эффективная антивирусная программ программа осуществляет контроль
a) За серверами и рабочими станциями
b) За пользователем
c) За дисководом
d) За модемом

13) При использовании паролей следует руководствоваться
a) Длинной пароля
b) Частотой смены пароля
c) Историей пароля
d) Содержимым пароля
e) Все из перечисленного
f) Ничего из перечисленного

14) Физическая безопасность обеспечивает защиту информационных систем
a) Защиту от пожара
b) Защиту от вирусов
c) Защиту от сбоев
d) Защиту от кражи

15) ISO 17799 не охватывает
a) Политику безопасности
b) Организационная безопасность
c) Классификация и контроль имущества
d) Безопасность персонала
e) Физическая безопасность и безопасность среды
f) Управление коммуникациями и операциями
g) Контроль доступа
h) Разработка и поддержка систем
i) Поддержка непрерывности деловых процессов
j) Соответствие политике
k) Охватывает все

16) Интернет-политика организации не позволяет внутренним пользователям использовать службу
a) HTTP
b) HTTPS
c) FTP
d) Telnet
e) TCP

17) Виртуальные частные сети обладают характеристикой
a) Время службы
b) Обеспечивают поддержку множества протоколов
c) Число одновременных подключений
d) Способ создания

18) Виртуальные частные сети обозначают
a) VPN
b) SSN
c) DLL
d) ЛВС

19) К числу сервисов безопасности нельзя отнести
a) Идентификация и аутентификация

b) Управление доступом
c) Протоколирование и аудит
d) Шифрование
e) Контроль целостности
f) Экранирование
g) Все можно

20) Меры безопасности на основе сервисов безопасности
a) Превентивные
b) Первичные
c) Локальные
d) Вторичные

21) Подсистемы системы информационной безопасности
a) Подсистема поддержки доверенной информационной среды
b) Подсистема аутентификации и идентификации
c) Подсистема контроля доступа
d) Подсистема защиты потоков
e) Подсистема аудита и регистрации
f) Подсистема управления
g) Все
h) Ни одна

22) Парольная аутентификация имеет достоинство
a) Простота и удобства для человека
b) Наложение технических ограничений (длина пароля, алфавит пароля)
c) Управление сроком действия пароля, их периодическая смена
d) Ограничение доступа к файлу паролей
e) Ограничение числа неудачных попыток входа в систему
f) Обучение пользователей

23) Ролевое управление предполагает
a) Опрос пользователя
b) Для каждого пользователя активны несколько ролей
c) Проверку отпечатков пальцев
d) Проверку геометрии руки и лица

24) Ролевое управление не определяется понятием
a) Пользователь
b) Сеанс работы пользователя
c) Роль (определяемая организационной структурой)
d) Должность
e) Объект (сущность, доступ к которой разграничивается)
f) Операция (выполняемая над объектом)
g) Право доступа

25) Протоколирование – это
a) Сбор и накопление информации о событиях ИС
b) Ведение документов
c) Все из перечисленного
d) Ничего из перечисленного

26) События для протоколирования
a) Запуск программы
b) Операции с файлами
c) Вывод на печать
d) Изменение настроек рабочего стола

27) Задача активного аудита
a) Проверка имени и пароля
b) Выявление подозрительной активности и управление средствами реагирования

c) Ограничение доступа в Интернет
d) Проверка электронной почты

28) Программные закладки могут выполнять действия
a) вносить произвольные искажения в коды программ
b) переносить фрагменты информации
c) искажать выводимую информацию
d) Все из перечисленного
e) Ничего из перечисленного

29) Конфигурация системы Windows 2000 не включает в себя
a) Настройку файловой системы
b) Настройку параметров сети
c) Настройку учетных записей
d) Проверку на вирусы