МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект контрольно-оценочных средств

междисциплинарного курса

МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка - 2024

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553, с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н.

Составитель:
Дешина И.А., преподаватель ОГАПОУ «Алексеевский колледж»

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1.2 Цели и задачи МДК – требования к результатам освоения МДК

С целью овладения указанным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК должен:

иметь практический опыт:

О1 установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

О2 администрирование автоматизированных систем в защищенном исполнении

О3 эксплуатация компонентов систем защиты информации автоматизированных систем

О4 диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

уметь:

У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;

У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

У6 обеспечивать работоспособность, обнаруживать и устранять неисправности

знать:

З1 состав и принципы работы автоматизированных систем, операционных систем и сред;

З2 принципы разработки алгоритмов программ, основных приемов программирования;

З3 модели баз данных;

З4 принципы построения, физические основы работы периферийных устройств

З5 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

З6 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

З7 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;

2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;

3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;

4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;

5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;

6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

7) знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз.

1.3. Планируемые личностные результаты освоения рабочей программы

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д.

Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

Результатом освоения МДК является овладение обучающимися видом деятельности - Эксплуатация автоматизированных (информационных) систем в защищенном исполнении в том числе профессиональными компетенциями (ПК):

Код	**Наименование результата обучения**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные

	компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.3 Результаты освоения междисциплинарного курса, подлежащие проверке

Наименование тем	Коды компетенций (ОК, ПК), личностных результатов (ЛР), умений (У), знаний (З), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения **в рамках текущей аттестации** (номер задания)	Средства контроля и оценки результатов обучения **в рамках промежуточной аттестации** (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1.1. Основы информационных систем как объекта защиты.	О1 У1 У3 З2 З3 ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 1 ЛР 5	ПЗ№ 1	КВ № 1-32 ЭБ № 1-12
Тема 1.2. Жизненный цикл автоматизированных систем	О4 У5 У3 З6 ОК 02 ОК 07 ПК 1.1 ПК 1.4	ПЗ№ 2	КВ № 1-32 ЭБ № 1-12

	ЛР 1 ЛР 4		
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 2 ЛР 3	ПЗ№ 5	КВ № 1-32 ЭБ № 1-12
Тема 1.4. Основные меры защиты информации в автоматизированных системах	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 1 ЛР 4	ТЗ № 1	КВ № 1-32 ЭБ № 1-12
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 2 ЛР 3	ТЗ № 2	КВ № 1-32 ЭБ № 1-12
Тема 1.6. Защита информации в распределенных автоматизированных системах	О2 У1 У5 З1 З3 ОК 03 ПК 1.2 ЛР 1 ЛР 5	ТЗ № 3	КВ № 1-32 ЭБ № 1-12
Тема 1.7. Особенности разработки	О4 У5	ПЗ№ 7	КВ № 1-32 ЭБ № 1-12

информационных систем персональных данных	У3 З6 ОК 02 ОК 07 ПК 1.1 ПК 1.4 ЛР 1 ЛР 11		
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	О2 У1 У5 З1 З3 ОК 03 ПК 1.2 ЛР 3	ТЗ № 4	КВ № 1-32 ЭБ № 1-12
Тема 2.2. Администрирование автоматизированных систем	О1 У1 У3 З2 З3 ОК 01 ОК 03 ПК 1.1 ПК 1.2 ЛР 5	ТЗ № 5	КВ № 1-32 ЭБ № 1-12
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 9	ТЗ № 6	КВ № 1-32 ЭБ № 1-12
Тема 2.4. Защита от несанкционированного доступа к информации	О3 У1 У6 З2 З5 ОК 04 ОК 06 ПК 1.2 ПК 1.3 ЛР 2	ТЗ № 7	КВ № 1-32 ЭБ № 1-12

	ЛР 3		
Тема 2.5. СЗИ от НСД	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 1	ПЗ № 13	КВ № 1-32 ЭБ № 1-12
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	О2 У2 У3 З4 З7 ОК 05 ПК 1.1 ПК 1.4 ЛР 5 ЛР 2	ПЗ № 16	КВ № 1-32 ЭБ № 1-12
Тема 2.7. Документация на защищаемую автоматизированную систему	О1 У2 У4 З3 З7 ОК 01 ОК 03 ПК 1.1 ПК 1.4 ЛР 3	ПЗ № 17	КВ № 1-32 ЭБ № 1-12

2. Комплект оценочных средств для текущей аттестации

2.1. Практические задания (ПЗ)

ПЗ№ 1

Задание 1. Проведите сравнение традиционных и автоматизированных информационных технологий:

Традиционная технология	Автоматизированные технологии

Задание 2. Соотнесите данные программы к своему классу программного обеспечения.

Запишите в таблице под каждой буквой необходимые программы и опишите их назначение. Paint,Windows Media Player,Калькулятор,Dr Web, Фортран, Си, Лисп, Windows Vista, Pascal, WinRar, Касперский, Ассемблер, Avast, Блокнот, Skype, Алгол, ISQ, Linux, MS Office Word, операционные системы, WinZip, Пролог, драйвера, C++, MS Office Excel, игры, переводчики, проигрыватели, Adobe PhotoShop, утилиты, Basic, WordPad, Linux, Autocad, CCleaner, Scandisk, Delphi, MS DOS, FineReader

А системное	Б прикладное	В системы программирования

Задание 3. Составьте описание АРМ, имеющего непосредственное отношение к вашей будущей профессии, на основе рисунка:

Задание 4. Приведите классификацию информационных систем:

Классификация информационных систем по охвату задач (масштабности)	
Классификация информационных систем в зависимости от характера информационных ресурсов	
Классификация информационных систем по технологии обработки данных	
Классификация информационных систем по способу доступа	

Классификация информационных систем в зависимости от организации системы	
Классификация информационных систем по характеру использования информации	
Классификация информационных систем по сфере применения	

Задание 5. Проанализируйте и опишите компонентную структуру известных Вам АИС в форме таблицы:

Наименование	Средства	Ресурсы	Подсистема нормативно-методического обеспечения	Подсистема управления и контроля качества	Технологические процессы	Входной поток	ИПУ

Задание 6. Изучите и опишите автоматизированную информационную систему ЕГАИС: назначение, системные требования, функциональные возможности, интерфейс приложения, работа с нормативно-справочной информацией.

ПЗ№ 2

Задание 1. Изучить документ «Единая система программной документации. Техническое задание, требования к содержанию и оформлению».

Задание 2. Разработать техническое задание на проектирование информационной системы, предназначенной для решения задач автоматизации деятельности организации.

1) В соответствии с назначенным преподавателем вариантом определить наименование информационной системы, подлежащей проектированию.

№ варианта	Наименование информационной системы
1	Информационная система медицинских организаций города
2	Информационная система автопредприятия города
3	Информационная система проектной организации
4	Информационная система ГИБДД
5	Информационная система строительной организации
6	Информационная система библиотечного фонда города
7	Информационная система спортивных организаций города

8	Информационная система аэропорта
9	Информационная система гостиничного комплекса
10	Информационная система торговой организации

2) Изучить описание предметной области информационной системы.

Вариант 1: Информационная система медицинских организаций города

Каждая больница города состоит из одного или нескольких корпусов, в каждом из которых размещается одно или несколько отделений, специализирующихся на лечении определенной группы болезней; каждое отделение имеет некоторое количество палат на определенное число коек. Поликлиники могут административно быть прикрепленными к больницам, а могут быть и нет. Как больницы, так и поликлиники обслуживаются врачебным (хирурги, терапевты, невропатологи, окулисты, стоматологи, рентгенологи, гинекологи и пр.) и обслуживающим персоналом (мед. сестры, санитары, уборщицы и пр.). Каждая категория врачебного персонала обладает характеристиками, присущими только специалистам этого профиля и по-разному участвует в связях: хирурги, стоматологии гинекологи могут проводить операции, они же имеют такие характеристики, как число проведенных операций, число операций с летальным исходом; рентгенологи и стоматологи имеют коэффициент к зарплате за вредные условия труда, у рентгенологов и невропатологов более длительный отпуск. Врачи любого профиля могут иметь степень кандидата или доктора медицинских наук. Степень доктора медицинских наук дает право на присвоение звания профессора, а степень кандидата медицинских наук на присвоение звания доцента. Разрешено совместительство, так что каждый врач может работать либо в больнице, либо в поликлинике, либо и в одной больнице и в одной поликлинике. Врачи со званием доцента или профессора могут консультировать в нескольких больницах или поликлиниках.

Лаборатории, выполняющие те или иные медицинские анализы, могут обслуживать различные больницы и поликлиники, при условии наличия договора на обслуживание с соответствующим лечебным заведением. При этом каждая лаборатория имеет один или несколько профилей: биохимические, физиологические, химические исследования.

Пациенты амбулаторно лечатся в одной из поликлиник, и по направлению из них могут стационарно лечиться либо в больнице, к которой относится поликлиника, либо в любой другой, если специализация больницы, к которой приписана поликлиника не позволяет провести требуемое лечение. Как в больнице, так и в поликлинике ведется персонифицированный учет пациентов, полная история их болезней, все назначения, операции и т.д. В больнице пациент имеет в каждый данный момент одного лечащего врача, в поликлинике - несколько.

Вариант 2: Информационная система автопредприятия города

Автопредприятие города занимается организацией пассажирских и грузовых перевозок внутри города. В ведении предприятия находится автотранспорт различного назначения: автобусы, такси, маршрутные такси, прочий легковой транспорт, грузовой транспорт, транспорт вспомогательного характера, представленный различными марками. Каждая из перечисленных категорий транспорта имеет характеристики, свойственные только этой категории: например, к характеристикам только грузового транспорта относится грузоподъемность, пассажирский транспорт характеризуется вместимостью и т.д. С течением времени, с одной стороны, транспорт стареет и списывается (возможно, продается), а с другой, - предприятие пополняется новым автотранспортом.

Предприятие имеет штат водителей, закрепленных за автомобилями (за одним автомобилем может быть закреплено более одного водителя). Обслуживающий персонал (техники, сварщики, слесари, сборщики и др.) занимается техническим обслуживанием автомобильной техники, при этом различные вышеперечисленные категории также могут иметь уникальные для данной категории атрибуты. Обслуживающий персонал и водители объединяется в бригады, которыми руководят бригадиры, далее следуют мастера, затем начальники участков и цехов. Введении предприятия находятся объекты гаражного хозяйства (цеха, гаражи, боксы и пр.), где содержится и ремонтируется автомобильная техника.

Пассажирский автотранспорт (автобусы, маршрутные такси) перевозит пассажиров по определенным маршрутам, за каждым из них закреплены отдельные единицы автотранспорта. Ведется учет числа перевозимых пассажиров, на основании чего производится перераспределением транспорта с одного маршрута на другой. Учитывается также пробег, число ремонтов и затраты на ремонт по всему автотранспорту, объем грузоперевозок для грузового транспорта, интенсивность использования транспорта вспомогательного назначения. Учитывается интенсивность работы бригад по ремонту (число ремонтов, объем выполненных работ), число замененных и отремонтированных узлов и агрегатов (двигателей, КП, мосты, шасси и т.д.) по каждой автомашине, и суммарно по участку, цеху, предприятию.

Вариант 3: Информационная система проектной организации

Проектная организация представлена следующими категориями сотрудников: конструкторы, инженеры, техники, лаборанты, прочий обслуживающий персонал, каждая из которых может иметь свойственные только ей атрибуты. Например, конструктор характеризуется числом авторских свидетельств, техники -оборудованием, которое они могут обслуживать, инженер или конструктор может руководить договором или проектом и т.д. Сотрудники разделены на отделы, руководимые начальником так, что каждый сотрудник числится только в одном отделе.

В рамках заключаемых проектной организацией договоров с заказчиками выполняются различного рода проекты, причем по одному договору может выполняться более одного проекта, и один проект может выполняться для нескольких договоров. Суммарная стоимость договора определяется стоимостью всех проектных работ, выполняемых для этого договора. Каждый договор и проект имеет руководителя и группу сотрудников, выполняющих этот договор или проект, причем это могут быть сотрудники не только одного отдела. Проекты выполняются с использованием различного оборудования, часть которого приписано отдельным отделам, а часть является коллективной собственностью проектной организации, при этом в процессе работы оборудование может передаваться из отдела в отдел. Для выполнения проекта оборудование придается группе, работающей над проектом, если это оборудование не используется в другом проекте.

Для выполнения ряда проектов подрядная организация может привлекать субподрядные организации, передавая им объемы работ.

Ведется учет кадров, учет выполнения договоров и проектов, стоимостной учет всех выполненных работ.

Вариант 4: Информационная система ГИБДД

У ГИБДД есть три наиболее важные функциональные задачи: регистрация автотранспортных средств при совершении сделки купли-продажи; разработка мер, повышающих безопасность дорожного движения и выполнение всех мер при совершении ДТП (дорожно-транспортное происшествие) на улицах города (регистрация, разбор, выявление виновных, автоэкспертиза и т.п.); борьба с угоном автотранспортных средств, оперативный поиск угнанных машин и

задержание преступников.

ГИБДД занимается выделением и учетом номерных знаков на автотранспорт. К автотранспортным средствам относятся легковые, грузовые автомобили, прицепы, полуприцепы, мотоциклы, тракторы, автобусы, микроавтобусы. На разные виды транспорта выдаются разные виды номеров и в базу данных заносятся разные характеристики. Номера могут выделяться как частным владельцам, так и организациям. В справочнике номеров, выданных частным владельцам, фиксируется: номер, ФИО владельца, его адрес, марка автомобиля, дата выпуска, объем двигателя, номера двигателя, шасси и кузова, цвет и т.п. В справочнике номеров, выданных организации, дополнительно фиксируется: название организации, район, адрес, руководитель. Существует справочник свободных номеров (серия, диапазон номеров). ГИБДД периодически проводит технический осмотр (ТО) машин. Для прохождения техосмотра необходима квитанция об оплате налогов, сумма оплаты зависит от объема двигателя. Периодичность прохождения зависит от года выпуска и вида транспортного средства. Технические характеристики, проверяемые на ТО и допуски также зависят от вида транспортного средства.

ГИБДД занимается учетом и анализом ДТП (дорожно-транспортное происшествие). При регистрации ДТП фиксируется: дата, тип происшествия (наездна пешехода, наезд на ограждение либо столб, лобовое столкновение, наезд на впереди стоящий транспорт, боковое столкновение на перекрестке и т.п.), место происшествия, марки пострадавших автомобилей, государственный номер, тип машины (легковая, грузовая, специальная), краткое содержание, число пострадавших, сумма ущерба, причина, дорожные условия и т.п. Анализ накопленной по ДТП статистике поможет правильно расставить запрещающие и предупреждающие знаки на улицах города, а так же спланировать местонахождение постов патрульных.

Угон либо исчезновение виновника ДТП с места происшествия требует оперативного вмешательства всех постов ГИБДД и патрульных машин. Для информирования о разыскиваемой машине ее данные (включая номера двигателя и кузова) извлекаются из базы зарегистрированных номеров и передаются по рации всем постам. Ведение статистики угонов, ее анализ и опубликование результатов в СМИ поможет снизить количество угонов, а хозяевам машин принять необходимые меры (самые угоняемые марки, самый популярный способ вскрытия, самые надежные сигнализации и т. п.).

Вариант 5: Информационная система строительной организации

Строительная организация занимается строительством различного рода объектов: жилых домов, больниц, школ, мостов, дорог и т.д. по договорам с заказчиками (городская администрация, ведомства, частные фирмы и т.д.). Каждая из перечисленных категорий объектов имеет характеристики, свойственные только этой или нескольким категориям: например, к характеристикам жилых домов относится этажность, тип строительного материала, число квартир, для мостов уникальными характеристиками являются тип пролетного строения, ширина, количество полос для движения.

Структурно строительная организация состоит из строительных управлений, каждое строительное управление ведет работы на одном или нескольких участках, возглавляемых начальниками участков, которым подчиняется группа прорабов, мастеров и техников. Каждой категории инженерно-технического персонала(инженеры, технологи, техники) и рабочих (каменщики, бетонщики, отделочники, сварщики, электрики, шофера, слесари, и пр.) также свойственны характерные только для этой группы атрибуты. Рабочие объединяется в бригады, которыми руководят бригадиры. Бригадиры выбираются из числа рабочих, мастера, прорабы, начальники участков и управлений назначаются из числа инженерно-технического персонала.

На каждом участке возводится один или несколько объектов, на каждом объекте работу ведут одна или несколько бригад. Закончив работу, бригада переходит к другому объекту на этом или другом участке. Строительному управлению придается строительная техника (подъемные краны, экскаваторы, бульдозеры и т.д.), которая распределяется по объектам.

Технология строительства того или иного объекта предполагает выполнение определенного набора видов работ, необходимых для сооружения данного типа объекта. Например, для жилого дома - это возведение фундамента, кирпичные работы, прокладка водоснабжения и т.д. Каждый вид работ на объекте выполняется одной бригадой. Для организации работ на объекте составляется графики работ, указывающие в каком порядке и в какие сроки выполняются те или иные работы, а также смета, определяющая какие строительные материалы и в каких количествах необходимы для сооружения объекта. По результатам выполнения работ составляется отчет с указанием сроков выполнения работ и фактических расходов материалов.

Вариант 6: Информационная система библиотечного фонда города

Библиотечный фонд города составляют библиотеки, расположенные на территории города. Каждая библиотека включает в себя абонементы и читальные залы. Пользователями библиотек являются различные категории читателей: студенты, научные работники, преподаватели, школьники, рабочие, пенсионеры и другие жители города. Каждая категория читателей может обладать непересекающимися характеристиками-атрибутами: для студентов это название учебного заведения, факультет, курс, номер группы, для научного работника -название организации, научная тема и т. д. Каждый читатель, будучи зарегистрированным в одной из библиотек, имеет доступ ко всему библиотечному фонду города.

Библиотечный фонд (книги, журналы, газеты, сборники статей, сборники стихов, диссертации, рефераты, сборники докладов и тезисов докладов и пр.)размещен в залах-хранилищах различных библиотек на определенных местах хранения (номер зала, стеллажа, полки) и идентифицируется номенклатурными номерами. При этом существуют различные правила относительно тех или иных изданий: какие- то подлежат только чтению в читальных залах библиотек, для тех, что выдаются, может быть установлен различный срок выдачи и т.д. С одной стороны, библиотечный фонд может пополняться, с другой, - с течением времени происходит его списание.

Произведения авторов, составляющие библиотечный фонд, также можно разделить на различные категории, характеризующиеся собственным набором атрибутов: учебники, повести, романы, статьи, стихи, диссертации, рефераты, тезисы докладов и т.д.

Сотрудники библиотеки, работающие в различных залах различных библиотек, ведут учет читателей, а также учет размещения и выдачи литературы.

Вариант 7: Информационная система спортивных организаций города

Спортивная инфраструктура города представлена спортивными сооружениями различного типа: спортивные залы, манежи, стадионы, корты и т.д. Каждая из категорий спортивных сооружений обладает атрибутами, специфичными только для нее: стадион характеризуется вместимостью, корт - типом покрытия.

Спортсмены под руководством тренеров занимаются отдельными видами спорта, при этом один и тот же спортсмен может заниматься несколькими видами спорта, и в рамках одного и того же вида спорта может тренироваться у нескольких тренеров. Все спортсмены объединяются в спортивные клубы, при этом каждый из них может выступать только за один клуб.

Организаторы соревнований проводят состязания по отдельным видам спорта на спортивных сооружениях города. По результатам участия спортсменов в соревнованиях производится награждение.

Вариант 8: Информационная система аэропорта

Работников аэропорта можно подразделить на пилотов, диспетчеров, техников, кассиров, работников службы безопасности, сплавочной службы и других, которые административно относятся каждый к своему отделу. Каждая из перечисленных категорий работников имеет уникальные атрибуты-характеристики, определяемые профессиональной направленностью. В отделах существует разбиение работников на бригады. Отделы возглавляются начальниками, которые представляют собой администрацию аэропорта. В функции администрации входит планирование рейсов, составление расписаний, формирование кадрового состава аэропорта. За каждым самолетом закрепляется бригада пилотов, техников и обслуживающего персонала. Пилоты обязаны проходить каждый год медосмотр, не прошедших медосмотр необходимо перевести на другую работу. Самолет должен своевременно осматриваться техниками и при необходимости ремонтироваться. Подготовка к рейсу включает в себя техническую часть (техосмотр, заправка необходимого количества топлива) и обслуживающую часть (уборка салона, запас продуктов питания и т.п.).

В расписании указывается тип самолета, рейс, дни вылета, время вылета и прилета, маршрут (начальный и конечный пункты назначения, пункт пересадки),стоимость билета. Билеты на авиарейсы можно приобрести заранее или забронировать в авиакассах. Цена билета зависит не только от маршрута, но и от времени вылета (в неудобное время - ночь, раннее утро - цена билета ниже). До отправления рейса, если в этом есть необходимость, билет можно вернуть. Авиарейсы могут быть задержаны из-за погодных условий, технических неполадок, а также могут быть отменены, если не продано меньше установленного минимума билетов.

Авиарейсы можно разделить на следующие категории: внутренние, международные, чартерные, грузоперевозки, специальные рейсы. Пассажир при посадке в самолет должен предъявить билет, паспорт, а для международного рейса обязан также предъявить заграничный паспорт и пройти таможенный досмотр. Пассажиры могут сдавать свои вещи в багажное отделение. На рейсы грузоперевозок и специальные рейсы билеты не продаются. Для спец. рейсов не существует расписания. Билеты на чартерные рейсы распространяет то агентство, которое его организовало.

Вариант 9: Информационная система гостиничного комплекса

Гостиничный комплекс состоит из нескольких зданий-гостиниц (корпусов).Каждый корпус имеет ряд характеристик, таких, как класс отеля (двух-, пятизвездочные), количество этажей в здании, общее количество комнат, комнат на этаже, местность номеров (одно-, двух-, трехместные и т.д.), наличие служб быта: ежедневная уборка номера, прачечная, химчистка, питание (рестораны, бары) и развлечения (бассейн, сауна, бильярд и пр.). От типа корпуса и местности номера зависит сумма оплаты за него. Химчистка, стирка, дополнительное питание, все развлечения производятся за отдельную плату.

С крупными организациями (туристические фирмы, организации, занимающиеся проведением международных симпозиумов, конгрессов, семинаров, карнавалов и т.д.) заключаются договора, позволяющие организациям бронировать номера с большими скидками на определенное время вперед не для одного человека, а для группы людей. Каждая из перечисленных групп организаций обладает характеристиками, свойственными только этой группе. Желательно группы людей от одной организации не расселять по разным этажам. В брони указывается класс отеля, этаж, количество комнат и общее количество людей. Броня может быть отменена за неделю до заселения. На основе маркетинговых работ расширяется рынок гостиничных услуг, в результате чего заключаются договора с новыми фирмами. Также исследуется мнение жильцов о ценах

и сервисе. Жалобы фиксируются и исследуются. Изучается статистика популярности номеров. Ведется учет долгов постояльца гостинице за все дополнительные услуги.

Новые жильцы пополняют перечень клиентов гостиницы. Ведется учет свободных номеров, дополнительных затрат постояльцев гостиницы и учет расходов и доходов гостиничного комплекса.

Вариант 10: Информационная система торговой организации

Торговая организация ведет торговлю в торговых точках разных типов: универмаги, магазины, киоски, лотки и т.д.), в штате которых работают продавцы. Универмаги разделены на отдельные секции, руководимые управляющими секций и расположенные, возможно, на разных этажах здания. Как универмаги, так и магазины могут иметь несколько залов, в которых работает определенное число продавцов, универмаги, магазины, киоски могут иметь такие характеристики, как размер торговой точки, платежи за аренду, коммунальные услуги, количество прилавков и т.д. Кроме того, в универмагах и магазинах учет проданных товаров ведется персонифицировано с фиксацией имен и характеристик покупателя, чего в киосках и на лотках сделать не представляется возможным.

Заказы поставщику составляются на основе заявок, поступающих из торговых точек. На основе заявок менеджеры торговой организации выбирают поставщика, формируют заказы, в которых перечисляются наименования товаров и количество, которое может отличаться от запроса из торговой точки. Если указанное наименование товара ранее не поставлялось, оно пополняет справочник номенклатуры товаров. На основе маркетинговых работ постоянно изучается рынок поставщиков, в результате чего могут появляться новые поставщики и исчезать старые. При этом одни и те же товары торговая организация может получать от разных поставщиков и, естественно, по различным ценам.

Поступившие товары распределяются по торговым точкам и в любой момент можно получить такое распределение.

Продавцы торговых точек ведут продажу товаров, учитывая все сделанные продажи, фиксируя номенклатуру и количество проданного товара, а продавцы универмагов и магазинов дополнительно фиксируют имена и характеристики покупателей, что позволяет вести учет покупателей и сделанных ими покупок. В процессе торговли торговые точки вправе менять цены на товары в зависимости от спроса и предложения товаров, а также по согласованию передавать товары в другую торговую точку.

3) На основании анализа описания предметной области и запросов к будущей информационной системе сформулировать основные требования к ее функциям.

4) Выполнить поиск прототипа проектируемой информационной системы с применением Интернет.

5) Используя сформулированные требования к информационной системе, а также документацию пользователя на прототип найденного программного средства, разработать техническое задание на проектирование информационной системы в соответствии с ГОСТ
19.201- 78.

ПЗ№ 5

Задание 1. Охарактеризуйте виды угроз информационной безопасности. Приведите примеры:

Нарушение физической целостности	
Нарушение логической целостности	
Нарушение содержания информации	
Нарушение конфиденциальности	

Нарушение прав собственности на информации	

Задание 2. Заполните таблицу «Характер происхождения угроз информационной безопасности»:

Умышленные факторы	Естественные факторы

Задание 3. Заполните таблицу «Предпосылки появления угроз информационной безопасности»:

Объективные предпосылки	Субъективные предпосылки

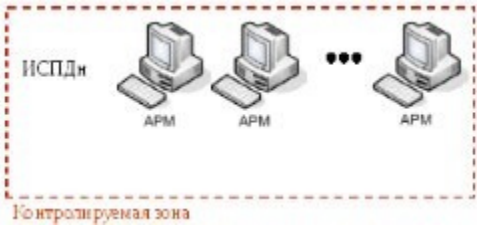
Задание 4. Проведите анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Класс защищенности автоматизированной системы

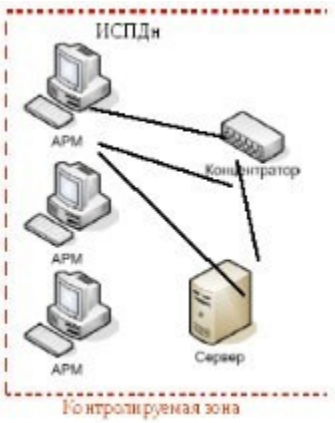
Приоритет	Виды угроз	Субъекты угроз			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудование, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

ПЗ№ 7

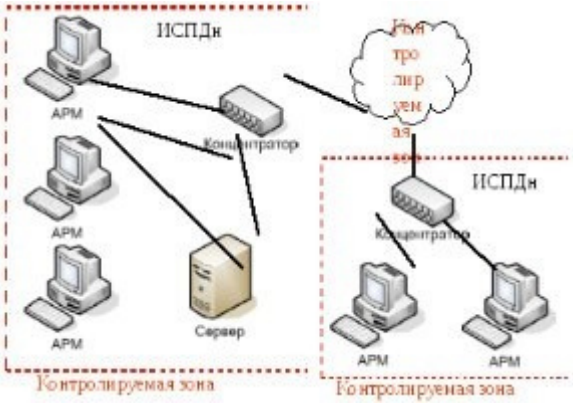
Задание 1. Оцените характеристики ИСПДн, обусловливающие возникновение угроз безопасности ПДн: 1) структура ИСПДн: автономные ИСПДн АРМ:



локальные ИСПДн:



распределенные ИСПДн):



2) категория обрабатываемых в ИСПДн персональных данных:

ИСПДн-С - информационная система, обрабатывающая специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

ИСПДн–Б - информационная система, обрабатывающая биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют

физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

ИСПДн-И - информационная система, обрабатывающая иные категории персональных данных, если в ней не обрабатываются персональные данные специальные, общедоступные и биометрические;

ИСПДн-О - информационная система, обрабатывающая общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

3) Объем обрабатываемых в ИСПДн персональных данных:

менее чем 100 000 субъектов;

более чем 100 000 субъектов.

4) наличие подключений ИСПДн к сетям связи общего пользования/сетям МИО: не имеющие подключение; имеющие подключение.

5) характеристики подсистемы безопасности ИСПДн; 6) режимы обработки персональных данных: однопользовательские ИСПДн; многопользовательские ИСПДН.

7) режимы разграничения прав доступа пользователей ИСПДн:

с разграничением доступа; без разграничения

доступа; 8) условия размещения технических

средств ИСПДн: в пределах контролируемой зоны;

вне контролируемой зоны.

9) по территориальному размещению:

распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий; локальная ИСПДн, развернутая в пределах

одного здания.

Задание 2. Изучите документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». ФСТЭК России от

15.02.2008 г.

Задание 3. Изучите категории нарушителей, описанные в документе ФСТЭК России «Базовая модель». Для конкретной информационной системы определите перечень вероятных нарушителей ИСПДн с учетом всех исключений.

Категория нарушителя	Перечень лиц	Описание категории нарушителя
1	Работники предприятия, не имеющие санкционированного доступа к ИСПДн	• имеет доступ к фрагментам информации, содержащей ПДн и распространяющейся по внутренним каналам связи ИСПДн; • располагает фрагментами информации о топологии ИСПДн (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах; • располагает именами и возможностью выявления паролей зарегистрированных пользователей; • изменяет конфигурацию технических средств ИСПДн, вносит в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИСПДн.
2	Пользователи ИСПДн	• обладает всеми возможностями лиц первой категории; • знает, по меньшей мере, одно легальное имя доступа; • обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; • располагает конфиденциальными данными, к которым имеет доступ.
3	Администраторы ППО ИСПДн	• Обладает всеми возможностями лиц первой и второй категорий; • располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИСПДн; • имеет возможность прямого (физического) доступа к фрагментам технических средств ИСПДн.

4	Администраторы локальной сети	• Обладает всеми возможностями лиц предыдущих категорий; • обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИСПДн; • обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИСПДн; • имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИСПДн; • имеет доступ ко всем техническим средствам сегмента (фрагмента) ИСПДн; • обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИСПДн.
5	Зарегистрированные пользователи с полномочиями системного администратора ИСПДн Администраторы информационной безопасности	• Обладает всеми возможностями лиц предыдущих категорий; • обладает полной информацией о системном и прикладном программном обеспечении ИСПДн; • обладает полной информацией о технических средствах и конфигурации ИСПДн; • имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн; • обладает правами конфигурирования и административной настройки технических средств ИСПДн
6	Работники сторонних организаций, обеспечивающие поставку, сопровождение и ремонт технических средств ИСПДн	• обладает всеми возможностями лиц предыдущих категорий; • обладает полной информацией об ИСПДн; • имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн; • не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
7	Программистыразработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его	• обладает информацией об алгоритмах и программах обработки информации на ИСПДн; • обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки,

	сопровождение на защищаемом объекте	внедрения и сопровождения; • может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.
8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств на ИСПДн	• обладает возможностями внесения закладок в технические средства ИСПДн на стадии их разработки, внедрения и сопровождения; • может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты информации в ИСПДн.

Задание 4. Изучите модели безопасности, описанные в документе ФСТЭК России «Базовая модель». Составьте перечень всех возможных угроз по документу ФСТЭК России «Базовая модель».

Перечень всех возможных угроз безопасности ПДн

Возможные угрозы безопасности ПДн
1. Угрозы от утечки по техническим каналам
1.1. Угрозы утечки акустической информации
1.2. Угрозы утечки видовой информации
1.3. Угрозы утечки информации по каналам ПЭМИН
2. Угрозы несанкционированного доступа к информации
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн
2.1.1. Кража ПЭВМ
2.1.2. Кража носителей информации
2.1.3. Кража ключей и атрибутов доступа
2.1.4. Кражи, модификации, уничтожения информации
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
2.1.7. Несанкционированное отключение средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
2.2.1. Действия вредоносных программ (вирусов)

2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера
2.3.1. Утрата ключей и атрибутов доступа
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками
2.3.3. Непреднамеренное отключение средств защиты
2.3.4. Выход из строя аппаратно-программных средств
2.3.5. Сбой системы электроснабжения
2.3.6. Стихийное бедствие
2.4. Угрозы преднамеренных действий внутренних нарушителей
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке
2.5.Угрозы несанкционированного доступа по каналам связи
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
2.5.3.Угрозы выявления паролей по сети
2.5.4.Угрозы навязывание ложного маршрута сети
2.5.5.Угрозы подмены доверенного объекта в сети
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
2.5.7.Угрозы типа «Отказ в обслуживании»
2.5.8.Угрозы удаленного запуска приложений
2.5.9.Угрозы внедрения по сети вредоносных программ

ПЗ № 13

1. Произвести настройку *аудита локальной системы* на своем ПК.
2. Просмотреть события, происходящие в Вашей системе.
3. Проанализировать текущие параметры Вашей системы.
4. Просмотреть состояние сетевых соединений в Вашей системы.

ПЗ № 16

1. Постройте кривую интенсивности отказов невосстанавливаемого элемента
2. Рассчитайте показатели надежности восстанавливаемого элемента

ПЗ № 17

Предлагается разработать следующую эксплуатационную документацию с соблюдением требований ЕСПД по их структуре и содержанию:

- руководство системного программиста;
- руководство программиста;
- руководство оператора;
- руководство по техническому обслуживанию.

В зависимости от предметной области и вида ПС, выданного в качестве задания, возможно изменение преподавателем состава и содержания технологической документации. Например, возможна разработка руководства пользователя, которое может рассматриваться как документ, объединяющий руководства системного программиста, программиста и оператора.

В документации обязательно должны быть приведены таблицы, схемы, иллюстрации, копии экранов, поясняющие положения документов.

2.2. Тестовые задания (ТЗ)

ТЗ № 1

1. Выберите правильный ответ

Основным источником права в области обеспечения информационной безопасности в России является

а) Уголовный кодекс
б) Конституция
в) государственные и отраслевые стандарты
г) Документы Гостехкомиссии

2. Выберите правильный ответ

В статье 42 Конституции РФ говорится о том, что

а) каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

б) сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются

в) каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом

г) каждый имеет право на достоверную информацию о состоянии окружающей среды

3. Дополните предложение

Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и доступа.

4. Выберите правильный ответ

В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет коллегиальный орган

а) ФАПСИ

б) ФСБ

в) Гостехкомиссия

г) Головная научно-исследовательская организация по защите информации

5. Выберите правильный ответ

Совокупность норм гражданского права, регулирующих отношения по признанию авторства и охране имущественных и неимущественных прав авторов и правообладателей - это определение

а) сертификата

б) авторского права

в) патента

г) товарного знака

6. Дополните предложение

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения_____.

7. Выберите правильный ответ

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, использовать знак охраны авторского права

а) ©
б) ®
в) ™
г) ∀

8. Выберите правильный ответ

Символ ® означает

а) патент
б) охраняемый знак
в) торговую марку
г) авторское право

9. Выберите правильный ответ

Программы для ЭВМ и базы данных к объектам авторского права

а) относятся
б) относятся в исключительных случаях
в) не относятся

10. Дополните предложение

Основной принцип компьютерной стеганографии предполагает использование двух типов файлов – файл-_____, которое должно быть скрыто, и файл-контейнер

Ответы
1. б
2. г
3. ограниченного
4. в
5. б
6. литературы
7. а
8. б
9. а
10. *сообщение*

ТЗ № 2

1. Под информационной безопасностью понимается…

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.**

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности.**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?
А) **от компьютеров**
Б) от поддерживающей инфраструктуры
В) от информации

4. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

5. Доступность – это…
А) **возможность за приемлемое время получить требуемую информационную услугу.**
Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..
А) **целостность информации**
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..
А) **защита от несанкционированного доступа к информации**
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) **получения определенных информационных услуг**
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) **статическую**
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) **анализе потока финансовых сообщений**
Б) обработке данных
В) **при выявлении кражи, дублирования отдельных сообщений**

11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) **все ответы правильные**

12. Угроза – это…
А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа

15. Окно опасности – это…
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?
А) **должно стать известно о средствах использования пробелов в защите.**
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:
А) **по спектру И.Б.**
Б) по способу осуществления
В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:
А) **отказ пользователей**
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) **все ответы правильные**

20. Основными источниками внутренних отказов являются:
А) **ошибки при конфигурировании системы**
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?
А) **вредоносная функция**
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) **все ответы правильные**

24. Вирус – это…
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:
А**) предметную**
Б) служебную
В) глобальную

27. Природа происхождения угроз:
А) **случайные**
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:
А) **объективные**
Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда

30. Отказ, ошибки, сбой – это:
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы

ТЗ № 3

1«МАСКИ» ВИРУСОВ ИСПОЛЬЗУЮТСЯ
+для поиска известных вирусов
- для поиска неизвестных вирусов
- для уничтожения известных вирусов
- для размножения вирусов
- для создания известных вирусов

2 IP-АДРЕС ИМЕЕТ ДЛИНУ
+4 байта
- 8 байт
- 1 бит
- 8 бит
- 16 байт

3 SECURITY UPDATES (ОБНОВЛЕНИЯ БЕЗОПАСНОСТИ) НЕОБХОДИМЫ
+для устранения обнаруженных недочетов в установленном ПО в операционных системах, установки патчей для предотвращения возможности эксплуатации уязвимостей, для поддержания внутренней самозащиты программ
- для поддержания внутренней самозащиты программ
- для обогащения вендоров, т.к. за дополнительные данные нужно платить
- для обновления внутренних модулей программ, чтобы приложения работали быстрее
- для облегчения работы с программами и улучшения восприятия интерфейса

4 АЛГОРИТМ DES ИСПОЛЬЗУЕТ ДЛИНУ БЛОКА:
+ 64 бит
- 256 бит
- 128 6ит
- 8 бит
- 16 бит

5 АЛГОРИТМ DES ИСПОЛЬЗУЕТ ДЛИНУ КЛЮЧА
+ 56 бит
- 256 бит
- 128 6ит
- 8 бит
- 16 бит

6 АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА ИСПОЛЬЗУЕТСЯ ДЛЯ
+ открытого распределения ключей

- вычисления хэш-функции
- генерации простых чисел
- генерации случайных чисел
- безопастного хранения ключей

7 АЛГОРИТМ ДИФФИ-ХЕЛМАНА ПОЗВОЛЯЕТ

+использовать незащищенный от прослушивания, но защищённый от подмены, канал связи
- генерировать новые простые числа
- вычислить хэш функцию
- генерировать случайные числа
- безопасно хранить ключи

8 АЛГОРИТМ ШИФРОВАНИЯ SHA ПРЕДНАЗНАЧЕН ДЛЯ ИСПОЛЬЗОВАНИЯ СОВМЕСТНО С АЛГОРИТМОМ ЦИФРОВОЙ ПОДПИСИ

+ DSA
- DOS
- DES
- EGS
- RSA

9 ОБЪЕКТ «А» ЗАЯВЛЯЕТ, ЧТО ОН НЕ ПОСЫЛАЛ СООБЩЕНИЕ ОБЪЕКТУ «Б», ХОТЯ НА САМОМ ДЕЛЕ ОН ВСЕ-ТАКИ ПОСЫЛАЛ:

+отказ (ренегатство)
- подделка
- модификация (переделка)
- маскировка
- активный перехват

10 АНТИВИРУС – ЭТО ПРОГРАММА, КОТОРАЯ

+ удаляет некоторые категории вредоносных программ, достигая успеха менее чем в 100 процентах случаев
- удаляет все виды вредоносного ПО с вашего компьютера
- может быть обновлена средствами «Автоматического обновления Windows» для получения новых сигнатур
- позволяет «откатить» все изменения, произведенные с момента активации враждебной программы, либо воспрепятствует ее активации в первую очередь
- удаляет все виды вредоносного ПО с компьютера

11АСПЕКТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЯВЛЯЮТСЯ

+ конфиденциальность, доступность, целостность
- неизменность, доступность, целостность
- неизменность , конфиденциальность
- конфиденциальность, целостность
- доступность, конфиденциальность

12АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОЛЖЕН ВКЛЮЧАТЬ В СЕБЯ

+ анализ информационных рисков с целью оценки вероятного ущерба и инструментальной проверки защищенности для определения возможности реализации угроз
- оценку угроз
- анализ и классификацию угроз безопасности согласно модели нарушителя
- оценку стоимости ресурсов и информации.
- оценку зависимости компании от внешних связей и тесты на проникновение

13 БЕЗОПАСНОСТЬ ДАННЫХ В ИНФОРМАЦИОННОЙ БАЗЕ ОБЕСПЕЧИВАЕТСЯ
+ конфиденциальностью, целостностью и доступностью информации
- периодичностью обновления информации
- шифрованием информации
- идентификацией абонентов
- определением полномочий

14АБОНЕНТ «А» ИЗМЕНЯЕТ СООБЩЕНИЕ И УТВЕРЖДАЕТ, ЧТО ДАННОЕ (ИЗМЕНЕННОЕ) СООБЩЕНИЕ ПОСЛАЛ ЕМУ АБОНЕНТ «Б»
+ модификация (переделка)
- маскировка
- активный перехват
- отказ
- подделка

15АБОНЕНТ «А» ФОРМИРУЕТ СООБЩЕНИЕ И УТВЕРЖДАЕТ, ЧТО ДАННОЕ (ИЗМЕНЕННОЕ) СООБЩЕНИЕ ПОСЛАЛ ЕМУ АБОНЕНТ «Б»
+ подделка
- активный перехват
- отказ
- модификация
- маскировка

16БОЛЕЕ УСОВЕРШЕНСТВОВАННЫЙ ВИД МНЕМОКОДОВ
+ автокоды
- RSS-коды
- штрихкоды
- чит-коды
- отладочный код

17В КАКОМ ГОДУ БЫЛ ПРЕДСТАВЛЕН АЛГОРИТМ ДИФФИ-ХЕЛМАНА:
+ 1975г
- 1974г
- 1978г
- 1977г
- 1976г

18В КАКОМ ГОДУ И ГДЕ БЫЛ РАЗРАБОТАН АЛГОРИТМ SHA
+ 1993 году в США

- 1991 году в США
- 1995 году в США
- 1992 году в США
- 1994 году в США

19В ВЕРСИЯХ MS OFFICE 2007 \ 2010 КОМПАНИЯ MICROSOFT ИСПОЛЬЗУЕТ АЛГОРИТМ ШИФРОВАНИЯ

+ AES с 128-битным ключом
- AES с 256-битным ключом
- AES с 16-битным ключом
- AES с 32-битным ключом
- AES с 8 -битным ключом

20В ПРОЦЕДУРЕ ПОСТАНОВКИ ПОДПИСИ ИСПОЛЬЗУЕТСЯ

+секретный ключ отправителя сообщения
- закрытый ключ отправителя сообщения
- открытый ключ отправителя сообщения
- чит-код
- хеш-функция

21В ПРОЦЕДУРЕ ПРОВЕРКИ ПОДПИСИ ИСПОЛЬЗУЕТСЯ:

+открытый ключ отправителя
- генерация пары ключей
- секретный ключ отправителя
- хеш-функция
- аудит подписи

22В ПРОЦЕДУРЕ ФОРМИРОВАНИЯ ПОДПИСИ ИСПОЛЬЗУЕТСЯ

+секретный ключ отправителя
- открытый ключ отправителя
- генерация пары ключей
- идентификация субъекта
- идентификация объекта

ТЗ № 4

1) Возможность за приемлемое время получить требуемую информационную услугу называется:
   1. Конфиденциальность
   2. Доступность
   3. Целостность
   4. Непрерывность

Эталон ответа: b

2) К аспектам информационной безопасности не относится:
   1. Доступность
   2. Целостность
   3. Конфиденциальность
   4. Защищенность

Эталон ответа: d

3) По каким критериям нельзя классифицировать угрозы:
   1. по расположению источника угроз
   2. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
   3. по способу предотвращения
   4. по компонентам информационных систем, на которые угрозы нацелены

Эталон ответа: c

4) Главное достоинство парольной аутентификации – …
   1. простота
   2. надежность
   3. секретность
   4. запоминаемость

Эталон ответа: a

5) Сколько уровней включает в себя сетевая модель OSI?
   1. 5
   2. 7
   3. 6
   4. 8

Эталон ответа: b

6) Межсетевой экран (Брандмауэр, firewall) – это…
   1. Комплекс аппаратных средств
   2. Комплекс программных средств
   3. Комплекс аппаратных или программных средств
   4. Комплекс аппаратных и программных средств

Эталон ответа: c

7) На каком уровне сетевой модели OSI не работает межсетевой экран:
   1. Физический
   2. Сеансовый
   3. Сетевой
   4. Транспортный

Эталон ответа: a

8) Межсетевого экрана какого класса не существует:
   1. экранирующий маршрутизатор
   2. экранирующий коммутатор
   3. экранирующий транспорт
   4. экранирующий шлюз

Эталон ответа: b

9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
   1. Подсистема сканирования
   2. Подсистема управления
   3. Подсистема обнаружения вирусной активности
   4. Подсистема устранения вирусной активности

Эталон ответа: d

10) На каком этапе заканчивается жизненный цикл автоматизированной системы?

1. Бета-тестирование системы
2. Внедрение финальной версии системы в эксплуатацию
3. Прекращение сопровождения и технической поддержки системы
4. Альфа-тестирование системы

Эталон ответа: c

11) Какие задачи выполняет теория защиты информации:

1. предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
2. аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
3. формировать научно обоснованные перспективные направления развития теории и практики защиты информации
4. выполняет все вышеперечисленные

Эталон ответа: d

12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

1. SSL
2. SET
3. HTTP
4. IPSec

Эталон ответа: c

13) Какого метода разграничения доступа не существует:

1. разграничение доступа по спискам
2. разграничение доступа по уровням секретности и категориям
3. локальное разграничение доступа
4. парольное разграничение доступа

Эталон ответа: c

14) К основным функциям подсистемы защиты операционной системы относятся:

1. идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
2. криптографические функции
3. сетевые функции
4. все вышеперечисленные

Эталон ответа: d

15) Риск – это…

1. вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки
2. фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки

3. действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
4. реализованная угроза

Эталон ответа: а

ТЗ № 5

1. С помощью какой сетевой службы выполняется преобразование доменного имени компьютера в ip-адрес?

A) LDAP B) NetBIOS
+C) DHCP D) DNS

2. С помощью какой сетевой службы, может быть организовано автоматическое выделение ip-адреса?

A) LDAP B) NetBIOS
C) DHCP +D) DNS

3. Какая команда позволяет проверить наличие соединения между хостами?

A) netstat B) nbtstat
+C) ping D) ipconfig

4. Какая команда позволяет отобразить активные сетевые подключения и порты соединений?

+A) netstat B) nbtstat
C) ping +D) ipconfig

5. Какая команда позволяет отображать и изменять таблицу маршрутизации?

A) netstat +B) nbtstat
C) ping D) ipconfig

6. Какая команда позволяет отобразить список существующих сетевых адаптеров?

A) netstat B) nbtstat
C) ping +D) ipconfig

7. Какая команда позволяет сделать общим сетевым ресурсом с именем MyCommonName локальную папку D:\USERS\MyFolder?

A) net share MyCommonName=D:\USERS\MyFolder
+B) net use MyCommonName=D:\USERS\MyFolder
C) net config MyCommonName=D:\USERS\MyFolder
D) net name MyCommonName disk=D:\USERS\MyFolder

8. Запишите команду, позволяющую подключить в качестве сетевого диска J: общую папку CommonDir на компьютере US112-SRV.

A) net share J: \\US112-SRV\CommonDir
+B) net use J: \\US112-SRV\CommonDir
C) net config J: \\US112-SRV folder=CommonDir
D) net name disk=J: server=US112-SRV folder=CommonDir

9. Какая служба Windows позволяет использовать общие ресурсы сети (папки и принтеры)?
+A) SERVER B) WORKSTATION
C) NetBIOS D) CONNECTION

10. Какая команда позволяет вывести список запущенных процессов на компьютере \\admin-is?
A) tasklist /s \\admin-is B) taskenum \\admin-is
C) commandlist /computer \\admin-is +D) processid /s \\admin-is

11. Какая команда позволяет принудительно завершить процесс с номер 1403 на компьютере \\admin-is?
+A) taskkill /s \\admin-is /pid 1403 B) taskkill /process 1403 \\admin-is
C) taskdeletete .зшв 1403 \\admin-is D) processkill /id 1403 \\admin-is

12. Запишите команду, добавляющую пользователя **Мой пользователь** с учетной записью NewUser в подразделение MyOU домена tc.rosnou.ru.
A) dsadd user “OU=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU” –samid NewUSER
+B) dsadd user “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU” –samid NewUSER
C) dsadd user “CN=Мой пользователь,CN=MyOU, DC=TC, DC=ROSNOU, DC=RU” –upn NewUSER
D) dsadd user “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU” –fn NewUSER

13. Запишите команду, создающую группу MyOwnGroup с одноименной учетной записью в качестве локальной группы в домене tc.rosnou.ru.
+A) dsadd group “OU=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU” –samid MyOwnGroup –scope l
B) dsadd group “CN=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU” –samid MyOwnGroup –scope l
C) dsadd group “OU= MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU” –samid MyOwnGroup –localgroup
D) dsadd group “CN= MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU” –samid MyOwnGroup –group=local

14. Запишите команду, добавляющую пользователя **Мой пользователь** из подразделения MyOU домена tc.rosnou.ru в группу MyOwnGroup.

A) dsmod group “OU=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU”
–addmbr “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU”
B) dsadd group “OU=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU”
–adduser “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU”
+C) dsmod group “CN=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU”
–addmbr “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU”
D) dsvar group “CN=MyOwnGroup, DC=TC, DC=ROSNOU, DC=RU”
–adduser “CN=Мой пользователь,OU=MyOU, DC=TC, DC=ROSNOU, DC=RU”

15. Какая команда позволяет изменить свойства объекта в Active Directory?
A) dschange B) dsmod
+C) dsadd D) dsvar

16. Какая команда позволяет, установить пароль p@ssw0rd для пользователя с учетной записью NewUSER в домене TC.
A) NET PASSWORD p@ssw0rd /USER NewUSER /DOMAIN
+B) NET USER NewUSER /PASSWORD p@ssw0rd /DOMAIN TC
C) NET USER NewUSER p@ssw0rd /DOMAIN
D) NET /USER NewUSER p@ssw0rd /DOMAIN TC

ТЗ № 6

1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:
1. **Информация**
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:
1. Информация
2. **Информационные технологии**
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:
1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. **Обладатель информации**

5. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:
1. База данных
2. Информационная технология
3. Информационная система
4. **Информационно-телекоммуникационная сеть**
5. Медицинская информационная система

6. ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:
1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. **Конфиденциальность информации**
5. Доступ к информации

7. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:
1. Уничтожение информации
2. **Распространение информации**
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

8. ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:
1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации

5. **Доступ к информации**

9. ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:
1. **Электронное сообщение**
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение

10. ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:
1. **Информационная система персональных данных**
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс
5. Сервер

11. К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:
1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. **Персональные данные**
5. Личная тайна

12. ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…
1. «Об информации, информационных технологиях»
2. «О защите информации»
3. **Федеральным законом «О персональных данных»**
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»

13. ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:
1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. **«Обработка персональных данных»**
5. «Изменение персональных данных»

14. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:
1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. **Деперсонификация**

15. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:
1. **Многопользовательские**
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений

16. ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:
1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. **Идентификация**

17. ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:
1. Авторизация
2. Обезличивание
3. Деперсонализация
4. **Аутентифика́ция**
5. Идентификация

18. ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ

1. **Авторизáция**
2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация

19. ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:

1. Токен
2. Password
3. Пароль
4. **Login**
5. Смарт-карта

20. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. **Шифрование**

21. ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

1. WWW
2. DICOM
3. **VPN**
4. FTP
5. XML

22. КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:
1. Антивирус
2. Замок
3. **Брандма́уэр**
4. Криптография
5. Экспертная система

23. ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:
1. Дисциплинарные взыскания
2. Административный штраф
3. Уголовная ответственность
4. Лишение свободы
5. **Смертная казнь**

24. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:
1. **Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально**
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя

25. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:
1. **Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу**
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

26. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
1. Выход в Интернет без разрешения администратора
2. При установке компьютерных игр

3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. **В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности**

27. МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:
1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. **Да**
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника

28. ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:
1. Идентификация
2. **Аутентификация**
3. Стратификация
4. Регистрация
5. Авторизация

29. НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:
1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. **Рядовые сотрудники предприятия**
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

30. ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:
1. **Нет, не при каких обстоятельствах**
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера

4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

31. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. **Конфиденциальная информация**
5. Документированная информация

32. ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:
1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. **Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)**
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК

33. ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН
1. **Содержать цифры и буквы, знаки препинания и быть сложным для угадывания**
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

34. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…
1. Блокирование информации
2. Искажение информации
3. **Сохранность информации**
4. Утрату информации
5. Подделку информации

35. ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:
1. 1982

2. 1985
3. 1988
4. **1993**
5. 2005

ТЗ № 7

Задание # 1

Вопрос:

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

Выберите один из 4 вариантов ответа:

1) пароли
2) анкеты
3) коды
4) ярлыки

Задание # 2

Вопрос:

От несанкционированного доступа может быть защищён:

Выберите несколько из 4 вариантов ответа:

1) каждый диск
2) папка
3) файл
4) ярлык

Задание # 3

Вопрос:

К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько из 9 вариантов ответа:

1) отпечаткам пальцев
2) характеристикам речи
3) радужной оболочке глаза
4) изображению лица
5) геометрии ладони руки
6) росту
7) весу
8) цвету глаз
9) цвету волос

Задание # 4

Вопрос:

Какие существуют массивы дисков RAID?

Выберите несколько из 4 вариантов ответа:

1) RAID 0
2) RAID 1
3) RAID 10

4) RAID 20

Задание # 5

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Для создания массива этого уровня понадобится как минимум два диска одинакового размера. Запись осуществляется по принципу чередования: данные делятся на порции одинакового размера (A1, A2, A3 и т.д.), и поочерёдно распределяются по всем дискам, входящим в массив.

2) Массивы этого уровня построены по принципу зеркалирования, при котором все порции данных (A1, A2, A3 и т.д.), записанные на одном диске, дублируются на другом.

__ RAID 0

__ RAID 1

Задание # 6

Вопрос:

Выберите типы вредоносных программ:

Выберите несколько из 6 вариантов ответа:

1) Вирусы, черви, троянские и хакерские программы
2) Шпионское, рекламное программное обеспечение
3) Потенциально опасное программное обеспечение
4) Операционная система Linux
5) Операционная система Windows
6) Microsoft Office

Задание # 7

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) сигнатуры. Сигнатура - это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы.

2) алгоритмы эвристического сканирования, т.е.анализа последовательности команд в проверяемом объекте.

__ Для поиска известных вредоносных программ используются

__ Для поиска новых вирусов используются

Задание # 8

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

__ Антивирусный монитор запускается
__ Антивирусный сканер запускается

Задание # 9

Вопрос:

Компьютерные вирусы -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание # 10

Вопрос:

По "среде обитания" вирусы можно разделить на:

Выберите несколько из 6 вариантов ответа:

1) загрузочные
2) файловые
3) макровирусы
4) очень опасные
5) не опасные
6) опасные

Задание # 11

Вопрос:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) заражают загрузочный сектор гибкого или жёсткого диска.
2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.
3) существуют для интегрированного офисного приложения Microsoft Office.

__ загрузочные вирусы
__ файловые вирусы
__ макровирусы

Задание # 12

Вопрос:

Сетевые черви -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание # 13

Вопрос:

Сетевые черви бывают:

Выберите несколько из 4 вариантов ответа:

1) Web-черви
2) почтовые черви
3) черви операционной системы
4) черви MS Office

Задание # 14

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.
2) Профилактическая защита от таких червей состоит в том, что не рекомендуется открывать вложенные в сообщения файлы, полученные от сомнительных источников. А также рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

__ Web-черви
__ почтовые черви

Задание # 15

Вопрос:

Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:

Выберите несколько из 3 вариантов ответа:

1) межсетевой экран

2) модуль проверки скриптов
3) антивирусный сканер

Задание # 16

Вопрос:

Межсетевой экран (брандмауэр) -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание # 17

Вопрос:

Троянская программа, троянец -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание # 18

Вопрос:

Троянские программы бывают:

Выберите несколько из 4 вариантов ответа:

1) утилиты удалённого администрирования
2) программы - шпионы

3) рекламные программы
4) программы удаления данных на локальном компьютере

Задание # 19
Вопрос:
Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:
1) троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи кофиденциальной информации.
2) троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.
3) эти программы встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Эти программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять её злоумышленнику.

__ Троянские утилиты удалённого администрирования
__ Троянские программы - шпионы
__ Рекламные программы

Задание # 20
Вопрос:
Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:
1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.
2) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров.

__ DoS - программы
__ DDos - программы

Ответы:

1) Верный ответ: 1;
2) Верные ответы: 1; 2; 3;
3) Верные ответы: 1; 2; 3; 4; 5;
4) Верные ответы: 1; 2;
5) Верные ответы: 1; 2;
6) Верные ответы: 1; 2; 3;
7) Верные ответы: 1; 2;
8) Верные ответы: 1; 2;
9) Верный ответы: 1;
10) Верные ответы: 1; 2; 3;
11) Верные ответы: 1; 2; 3;
12) Верный ответ: 2;
13) Верные ответы: 1; 2;
14) Верные ответы: 1; 2;

15) Верные ответы: 1; 2;
16) Верный ответ: 4;
17) Верный ответ: 3;
18) Верные ответы: 1; 2; 3;
19) Верные ответы: 1; 2; 3;
20) Верные ответы: 1; 2;

3. Комплект оценочных средств для промежуточной аттестации

3.1. Контрольные вопросы (КВ)

КВ №1. Понятие автоматизированной (информационной) системы

КВ №2. Отличительные черты АИС

КВ №3. Примеры областей применения АИС.

КВ №4. Процессы в АИС

КВ №5. Требования к АИС: гибкость, надежность, эффективность, безопасность.

КВ №6. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС

КВ №7. Модели жизненного цикла АИС.

КВ №8. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении.

КВ №9. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.

КВ №10. Требования к автоматизированной системе в защищенном исполнении.

КВ №11. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.

КВ №12. Требования по защите сведений о создаваемой автоматизированной системе.

КВ №13. Потенциальные угрозы безопасности в автоматизированных системах.

КВ №14. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз.

КВ №15. Методы оценки опасности угроз. Банк данных угроз безопасности информации

КВ №16. Понятие уязвимости угрозы. Классификация уязвимостей.

КВ №17. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.

КВ №18. Ограничение программной среды. Защита машинных

носителей информации. Регистрация событий безопасности

КВ №19. Антивирусная защита. Реализация антивирусной защиты.

КВ №20. Обновление баз данных признаков вредоносных компьютерных программ.

КВ №21. Обнаружение (предотвращение) вторжений

КВ №22. Защита технических средств.

КВ №23. Защита информационной системы, ее средств, систем связи и передачи данных

КВ №24. Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.

КВ №25. Требования по защите персональных данных, в соответствии с уровнем защищенности.

КВ №26. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.

КВ №27. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.

КВ №28. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении

КВ №29. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД.

КВ №30. Классификация автоматизированных систем. Требования по защите информации от НСД для АС

КВ №31. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

КВ №32. Основные эксплуатационные документы защищенных автоматизированных систем.

3.2. Экзаменационные билеты (ЭБ)

ЭБ № 1

1. Основные определения и понятия информационной системы (ИС). Классификация ИС, примеры.
2. Стадии разработки АИС в соответствие с ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».
3. Определить конфигурацию информационной системы по приведенной модели.

ЭБ № 2

1. Методы анализа ИС. Функциональный и информационный анализ.
2. Объектно-ориентированный подход при моделировании ИС. Модель «Совокупность – связь».
3. Разработать модель базы данных для конкретной информационной системы.

ЭБ № 3

1. Типовой метод проектирования ИС, его характеристика, недостатки, достоинства.
2. Базы данных как машинная часть информационного обеспечения автоматизированной системы.
3. Найти перечень документов, используя информационную систему «Консультант Плюс».

ЭБ № 4

1. Стадии создания ИС. Содержание этапов создания ИС на различных стадиях.
2. Приведите и поясните примеры моделей различных информационных процессов.
3. Составить структурную схему АИС предприятия.

ЭБ № 5

1. Классификация АИС по характеру представления и логической организации хранимой информации (фактографические, документальные, геоинформационные).
2. Типовые средства АИС. Информационное обеспечение: общий состав информационного обеспечения.
3. Произвести расчет качественных показателей работы ИПС.

ЭБ № 6

1. Классификация АИС по функциям и решаемым задачам (технологические, расчетные, поисковые, справочные).
2. Объектно-ориентированная методология: сущность, достоинства и недостатки. Основные понятия объектно-ориентированной методологии (объект, класс, атрибут, метод).
3. Осуществить поиск документов по разным поисковым признакам.

ЭБ № 7

1. Классификация методов проектирования. Выделение жизненных циклов проектирования ИС для решения конкретных задач в профессиональной деятельности.
2. Структура информационных систем: подсистемы и функциональные группы.

3. Разработать ИС по определенной методологии.

ЭБ № 8

1. Основные определения и понятия информационной системы (ИС).
2. Классификация ИС, примеры. Этапы проектирования АИС с применением языка универсального моделирования (UML). Особенности языка и его применение.
3. Определить конфигурацию информационной системы по приведенной модели.

ЭБ № 9

1. Стадии разработки АИС в соответствие с ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».
2. Объектно-ориентированный подход при моделировании ИС. Модель «Совокупность – связь». 3. По данному условию задачи создать разные варианты АИС и выбора оптимального.

ЭБ № 10

1. Типовой метод проектирования ИС, его характеристика, недостатки, достоинства.
2. Базы данных как машинная часть информационного обеспечения автоматизированной системы.
3. Составить техническое задание на разработку АИС.

ЭБ № 11

1. Классификация АИС по функциям и решаемым задачам (технологические, расчетные, поисковые, справочные).
2. Типовые средства АИС. Информационное обеспечение: общий состав информационного обеспечения.
3. Произвести расчет качественных показателей работы ИПС.

ЭБ № 12

1. Классификация АИС по характеру представления и логической организации хранимой информации (фактографические, документальные, геоинформационные).
2. Объектно-ориентированная методология: сущность, достоинства и недостатки. Основные понятия объектно-ориентированной методологии (объект, класс, атрибут, метод).
3. Осуществить поиск документов по разным поисковым признакам.

Критерии оценивания

«5» «отлично» или «зачтено» – студент показывает глубокое и полное овладение содержанием программного материала по МДК, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» или «зачтено» – студент в полном объеме освоил программный материал по МДК, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» или «зачтено» – студент обнаруживает знание и понимание основных положений программного материала по МДК но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» или «не зачтено» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по МДК, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им,

используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Эксплуатация автоматизированных (информационных) систем в защищённом исполнении (1-е изд.) учебное пособие/Кравченко В.Б.
М.: ИЦ Академия,2018-304 с

Дополнительные источники:

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.

3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.

4. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2015.

6. Синицын С.В. , Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2013.

7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2013.

Электронные издания (электронные ресурсы):

Цифровая образовательная среда СПО PROFобразование:

- Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. — Саратов : Профобразование, 2019. — 136 c. — ISBN 978-5-4488-0355-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/86210 (дата обращения: 07.09.2020). — Режим доступа: для авторизир. Пользователей

Электронно-библиотечная система:

IPR BOOKS - https://www.iprbookshop.ru/102192.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/