МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

ФИЛИАЛ ФГБОУ ВО «ЮГУ»
НЕФТЯНОЙ
ИНСТИТУТ

МДК 01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий
для обучающихся 2 курса всех форм обучения
образовательных организаций
среднего профессионального образования

Часть 1

Нижневартовск, 2022

ББК 32.973.202
Э 41

РАССМОТРЕНО
На заседании ПЦК «МиЕНД»
Протокол № 9 от 15.10.2022
Председатель Бойко Я.С.

УТВЕРЖДЕНО
Председателем методического совета
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Хайбулина Р.И.
« 10 » ноября 2022 г.

Методические указания к выполнению практических занятий для обучающихся 2 курса всех форм обучения образовательных организаций среднего профессионального образования по МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ), часть 1, разработаны в соответствии с:

1. Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденным МИНОБРНАУКИ от 09.12.2016 №1553.
2. Рабочей программой профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении, утвержденной на методическом совете НефтИн (филиал) ФГБОУ ВО «ЮГУ» протоколом № 4 от 31.08.2022.

Разработчики:
1. Бойко Яна Сергеевна, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ»;
2. Винник Анна Валентиновна, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».

Рецензенты:
1. Валиева Л.Ф., методист НефтИн (филиал) ФГБОУ ВО «ЮГУ».
2. Фазылова Е.Х., преподаватель БУ «Нижневартовский строительный колледж».

Замечания, предложения и пожелания направлять в Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет» по адресу: 628615, Тюменская обл., Ханты-Мансийский автономный округ, г. Нижневартовск, ул. Мира, 37.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания к практическим занятиям по МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении для обучающихся всех форм обучения разработаны в соответствии с требованиями Федерального государственного стандарта (ФГОС) по специальности по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем и рабочей программы профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

Цель методических указаний: оказание помощи обучающимся в выполнении практических занятий по МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Настоящие методические указания содержат первую часть практических занятий, которые позволят обучающимся закрепить теорию и направлены на формирование следующих профессиональных (ПК) и общих (ОК) компетенций:

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.

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.

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.

В результате выполнения практических занятий по МДК 01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении обучающиеся должны уметь обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем.

Правила выполнения практических работ:

В ходе выполнения практических работ обучающийся должен:

- выполнять требования по охране труда
- соблюдать инструкцию по правилам и мерам безопасности в лаборатории информационных технологий
- строго выполнять весь объем работы, указанный в задании
- соблюдать требования эксплуатации компьютерной техники (правила включения и выключения)
- изучить теоретические вопросы, используя лекционный материал к теме
- предоставить отчет о проделанной работе по окончании выполненной работы.

Рекомендации по оформлению практической работы:

✓ при выполнении практической работы в программе MS Word необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы в соответствии с заданием;

✓ при выполнении в программе MS Word практической работы содержащей таблицы соблюдать структуру и выравнивание ячеек таблиц, цвет границы и заливки фигур;

✓ при выполнении практической работы в программе в MS Excel соблюдать формат и выравнивание ячеек, название листов, точность вычислений в соответствии с заданием.

✓ при выполнении практической работы в программе MS Power Point необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы, макеты оформления, графические объекты, анимацию и переходы в соответствии с заданием;

✓ при выполнении практической работы в программе MS Access (создание базы) в таблицы добавлять не менее 10 записей, таблицы переименовывать в соответствии с заданием, отчеты формировать в табличной форме, кнопочная форма обязательна.

Работы проводятся согласно календарно-тематическому планированию, в соответствии с учебной программой. Пропущенные практические работы выполняются обучающимися самостоятельно и сдаются в отведенные на изучение дисциплины сроки.

Критерии оценивания:

Оценка «Отлично» - полно раскрыто содержание материала в объеме, предусмотренном программой, практическая работа выполнена правильно, в полном объеме и защищена.

«Хорошо» - в изложении материала допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; в выполненной практической работе допущены в ответах отдельные неточности, исправленные с помощью преподавателя.

«Удовлетворительно» - неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии; практическая работа выполнена частично, допущены ошибки и неточности, которые не всегда исправляются с помощью преподавателя.

«Неудовлетворительно» - не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; практическая работа носит трафаретный характер, выполнена неправильно или не выполнена вовсе.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№ темы	Номер и наименование работы (занятия)	Кол-во аудиторных часов	Формируемые компетенции
1	2	3	4
1.1	Практическое занятие № 1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.4
1.2	Практическое занятие № 2. Разработка технического задания на проектирование автоматизированной системы	2	ОК4, ОК5, ОК6, ОК8, ОК9, ПК1.2, ПК1.4

1	2	3	4
1.3.	Практическое занятие № 3. Категорирование информационных ресурсов	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.4
	Практическое занятие № 4. Анализ угроз безопасности информации	2	ОК2, ОК4, ОК6, ОК8, ОК9, ПК1.1, ПК1.2, ПК1.4
	Практическое занятие № 5. Построение модели угроз	2	ОК4, ОК5, ОК6, ОК8, ОК9, ПК1.2, ПК1.4
1.7	Практическое занятие № 6. Определение уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн	2	ОК4, ОК6, ОК8, ОК9, ПК1.1, ПК1.2, ПК1.4
2.5.	Практическое занятие № 7. Установка и настройка СЗИ от НСД	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.4
	Практическое занятие № 8. Защита входа в систему (идентификация и аутентификация пользователей)	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.4
	Практическое занятие № 9. Разграничение доступа к устройствам	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
	Практическое занятие № 10. Управление доступом	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
	Практическое занятие № 11. Использование принтеров для печати конфиденциальных документов. Контроль печати	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
	Практическое занятие № 12. Настройка системы для задач аудита	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
	Практическое занятие № 13. Настройка контроля целостности и замкнутой программной среды	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
	Практическое занятие № 14. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
2.6	Практическое занятие № 15. Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	2	ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК1.3, ПК1.4
2.7	Практическое занятие № 16. Оформление основных эксплуатационных документов на автоматизированную систему	2	ОК1, ОК4, ОК6, ОК8, ОК9, ПК1.2, ПК 1.3, ПК1.4

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1

РАССМОТРЕНИЕ ПРИМЕРОВ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ (ЕГАИС, РОССИЙСКАЯ ТОРГОВАЯ СИСТЕМА, АВТОМАТИЗИРОВАННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА КОМПАНИИ)

Цели: ознакомиться с современными информационными системами.

Теоретические вопросы:

1. Понятие автоматизированной (информационной) системы
2. Классификация АИС.
3. Примеры областей применения АИС.
4. Процессы в АИС: ввод, обработка, вывод, обратная связь.
5. Требования к АИС: гибкость, надежность, эффективность, безопасность.

Задание 1. Проведите сравнение традиционных и автоматизированных информационных технологий:

Традиционная технология	Автоматизированные технологии

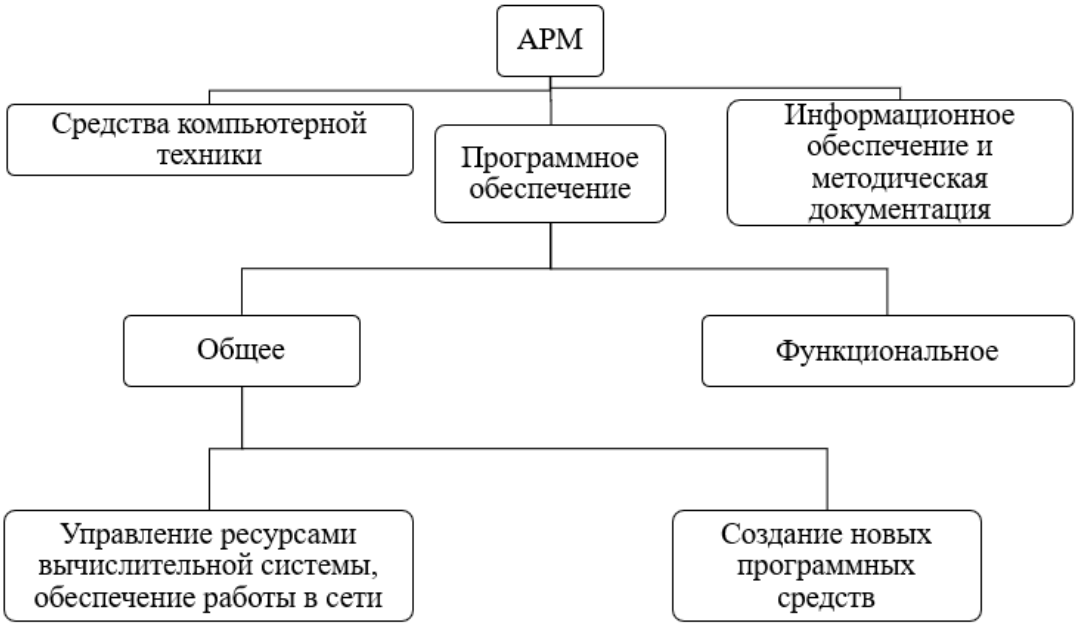
Задание 2. Соотнесите данные программы к своему классу программного обеспечения. Запишите в таблице под каждой буквой необходимые программы и опишите их назначение.

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.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2

РАЗРАБОТКА ТЕХНИЧЕСКОГО ЗАДАНИЯ НА ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Цели: научиться разрабатывать техническое задание на проектирование автоматизированной системы.

Теоретические вопросы:

1. Понятие «программная документация».
2. Внешняя и внутренняя программная документация.
3. Единая система программной документации.
4. Содержание технического задания.
5. Понятие «документация пользователя».

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 (наезда 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 19.20178.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3

КАТЕГОРИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Цели: изучить правила категорирования информационных ресурсов.

Теоретические вопросы:

1. Категорирование защищаемых ресурсов.
2. Упрощенный алгоритм оценки защищенности объекта информатизации.
3. Правила категорирования критичности информационного ресурса.
4. Цели категорирования информационных ресурсов.
5. Категории конфиденциальности защищаемой информации.
6. Требуемые степени доступности функциональных задач.

Задание 1. Изучите предложенную классификацию информационных ресурсов:

Государственные (национальные) информационные ресурсы Государственные информационные ресурсы - информационные ресурсы, полученные и оплаченные из федерального бюджета	1) федеральные ресурсы; 2) информационные ресурсы; находящиеся в совместном ведении Российской Федерации и субъектов РФ; • библиотечная сеть России; • архивный фонд Российской Федерации; • государственная система статистики • государственная система научно-технической информации 3) информационные ресурсы субъектов РФ.
Информационные ресурсы организаций и предприятий Информационные ресурсы предприятий- информационные ресурсы, созданные или накопленные в организациях и на предприятиях.	• центры- генераторы; • центры распределения; • информационные агентства; • базы данных.
Персональные информационные ресурсы Персональные информационные ресурсы- информационные ресурсы, созданные и управляемые каким- либо человеком и содержащие данные, относящиеся к его личной деятельности.	

Определите вид следующих информационных ресурсов в соответствии с данной классификацией:

1. http://portal.gersen.ru
2. http://school-collection.edu.ru
3. http://fcior.edu.ru
4. http://e-lib.gasu.ru
5. http://books.ifmo.ru
6. http://window.edu.ru
7. http://ivanurgant.com/

8. http://www.schwarzenegger.com/
9. http://zim-angel.ucoz.ru/
10. http://www.educom.ru/ru/works/

Задание 2. Раскройте суть основных параметров информационного ресурса:

№	Параметр информационного ресурса	Характеристика параметра
1.	Содержание	
2.	Охват	
3.	Время	
4.	Источник	
5.	Качество	
6.	Соответствие потребностям	
7.	Способ фиксации	
8.	Язык	
9.	Стоимость	

Задание 3. Опишите правила категорирования критичности информационного ресурса.

Задание 4. Приведите категории конфиденциальности, целостности и доступности информационных ресурсов.

Задание 5. Охарактеризуйте информационные ресурсы заданного предприятия. Заполните таблицу:

Наименование информационного ресурса (информации)	Категория конфиденциальности (В/Н-) и вид тайны (БТ/КТ/ДСП)	Категория целостности (В/Н/-)	Размещение ресурса (АРМ, устройство, каталог, файл)	Ответственный за определение требований к защищенности ресурса
1.				
2.				
3.				
…				

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Цель: научиться анализировать угрозы безопасности информации.

Теоретические вопросы:

1. Понятие угрозы безопасности информации.
2. Виды угроз безопасности информации.
3. Источники угроз безопасности информации.
4. Предпосылки появления угроз безопасности информации.

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	Вид угроз	Субъект угроз			
		Стихия	Нарушитель	Злоумышленник	
				на территории	вне территории
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудования, 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		+	+	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5

ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ

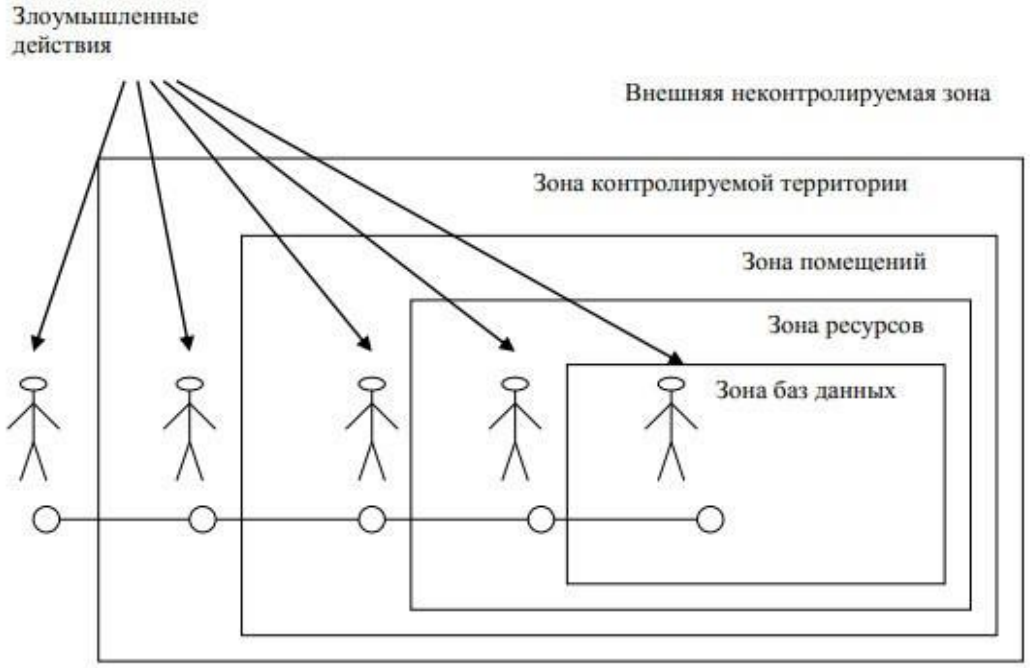
Цель: анализ и построение модели информационной безопасности.

Теоретические вопросы:

1. Классы каналов несанкционированного получения информации.
2. Моделирование угроз безопасности информации.
3. Модель нарушителя информационной безопасности.

Задание 1. Приведите примеры каналов несанкционированного получения информации.

Задание 2. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных:



Определите выделенные зоны для заданного объекта.

Задание 3. Проведите анализ потенциальных каналов утечки на указанном объекте. Составьте перечень каналов утечки информации на защищаемом объекте с указанием места расположения по образцу:

Каналы утечки информации с объекта защиты			Место расположения
1			2
11	Оптический канал	Окно со стороны проспекта	Каб. №1
		Окно со стороны проспекта	Каб. №2
		Окно со стороны проспекта	Каб. №3
2.	Радиоэлектронный канал	Стоянка автотранспорта на просп.	указать
		Система часофикации	указать
		телефон	указать
		Розетки	указать
		ПЭВМ	указать
		Воздушная линия электропередачи	указать
		Система оповещения	указать
		Система пожарной сигнализации	указать

1			2
3.	Акустический канал	Теплопровод подземный	указать
		Водопровод подземный	указать
		Стены помещения	указать
		Батареи	указать
		Окна контролируемого помещения	указать
4.	Материально-вещественный канал	Документы на бумажных носителях	указать
		Персонал предприятия	указать
		Производственные отходы	указать

Задание 4. Постройте модель угроз защищаемого объекта:

№ элемента	Цена информации	Путь проникновения	Оценка реальности	Величина угрозы	Ранг угрозы

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6

ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДН И ВЫБОР МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Цели: научиться определять уровень защищенности информационных систем персональных данных и выбирать меры по обеспечению безопасности персональных данных.

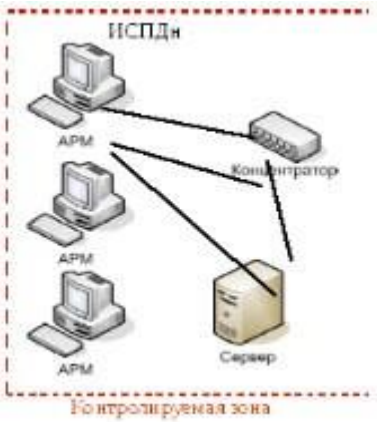
Теоретические вопросы:

1. Общие требования по защите персональных данных.
2. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
3. Порядок выбора мер по обеспечению безопасности персональных данных.
4. Требования по защите персональных данных, в соответствии с уровнем защищенности.

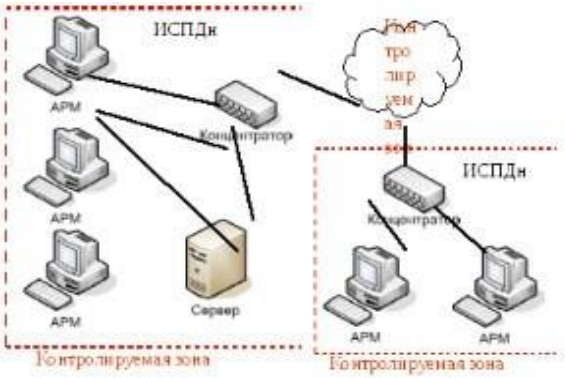
Задание 1. Оцените характеристики ИСПДн, обусловливающие возникновение угроз безопасности ПДн: 1) структура ИСПДн:

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,	• 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, внедрения и сопровождения; • может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и

	обеспечивающие его сопровождение на защищаемом объекте	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

Задание 5. Изучите документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», разработанный ФСТЭК России.

Задание 6. Заполните таблицу, проставив в виде «+» показатели высокого, среднего и низкого уровня защищённости для всех технических и эксплуатационных характеристик ИСПДн. Например:

Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. 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	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+

ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
Количество «+» в колонках	5	5	7
РЕЗУЛЬТАТ (*Y_1*)	5		

Задание 7. Изучите документ Приказ ФСТЭК России от 18.02.2013 № 21"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Задание 8. Составьте модель защиты, заключающаяся в выборе мер, закрывающих актуальные угрозы безопасности. Модель защиты, в соответствии с пунктом 9 Приказа ФСТЭК России от 18.02.2013 № 21, составляется по следующему алгоритму:

1) определяется базовый набор мер, а именно составляется перечень тех мер, которые отмечены плюсами для соответствующего УЗ в приложении к Приказу ФСТЭК России от 18.02.2013 № 21;

2) адаптация базового набора мер. На этом этапе из базового набора мер

исключаются те, которые не актуальны из-за особенностей конкретной ИСПДн (например, исключаются меры по защите виртуализации, если виртуализация не используется);

3) уточнение адаптированного базового набора мер. На этом этапе добавляются ранее не выбранные меры, если в соответствии с частной моделью угроз какие-либо из актуальных угроз остались незакрытыми.

Для адаптации мер необходимо соотнести возможные угрозы безопасности ПДн к мерам по приложению Приказа №21 ФСТЭК. Для этого необходимо воспользоваться таблицей:

Соответствие угроз безопасности ПДн мерам по обеспечению безопасности ПДн.

Возможные угрозы безопасности ПДн	**Меры по Приказу №21 ФСТЭК**	
1	**2**	
1. Угрозы от утечки по техническим каналам	XII. Защита технических средств (ЗТС)	
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		ЗТС.4
1.3. Угрозы утечки информации по каналам ПЭМИН		ЗТС.1
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		ЗТС.3
2.1.2. Кража носителей информации	IV. Защита машинных носителей персональных данных (ЗНИ)	ЗНИ.1ЗНИ.2
2.1.3. Кража ключей и атрибутов доступа		ЗНИ.5
2.1.4. Кражи, модификации, уничтожения информации		ЗНИ.8
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	V. Регистрация событий безопасности (РСБ) II. Управление доступом субъектов доступа к объектам доступа (УПД)	РСБ.1-3
2.1.7. Несанкционированное отключение средств защиты		ЗТС.3
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)	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3

1	2	
2.2.1. Действия вредоносных программ (вирусов)	VI. Антивирусная защита (АВЗ)	АВЗ.1-2
2.2.2. Не декларированные возможности системного ПО и ПО для обработки персональных данных	III. Ограничение программной среды (ОПС)	ОПС.2
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей		ОПС.3
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	X. Обеспечение доступности персональных данных (ОДТ)	ОДТ.4
2.3.1. Утрата ключей и атрибутов доступа	I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	ИАФ.4
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	V. Регистрация событий безопасности (РСБ)	РСБ.7
2.3.3. Непреднамеренное отключение средств защиты	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.3
2.3.4. Выход из строя аппаратно-программных средств	IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	ОЦЛ.1
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	X. Обеспечение доступности персональных данных (ОДТ)	ОЦЛ.2
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке		ОЦЛ.2
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:	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
2.5.1.1. Перехват за переделами контролируемой зоны		ОЦЛ.4

1	2	
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями		ОЦЛ.1
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.		ОЦЛ.1
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.	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.1-2
2.5.3. Угрозы выявления паролей по сети	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	АНЗ.3
2.5.4. Угрозы навязывание ложного маршрута сети		ЗИС.3
2.5.5. Угрозы подмены доверенного объекта в сети		ЗИС.11
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	VI. Антивирусная защита (АВЗ)	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7

УСТАНОВКА И НАСТРОЙКА СЗИ ОТ НСД

Цель: познакомиться с системами защиты информации от несанкционированного доступа.

Теоретические вопросы:

1. Меры противодействия несанкционированному доступу.
2. Идентификация и аутентификация пользователей.
3. Ограничение доступа на вход в систему.
4. Разграничение доступа.
5. Регистрация событий (аудит).
6. Модель защищенной компьютерной системы.
7. Системы защиты информации от несанкционированного доступа.

Задание 1. Изучите возможности системы защиты информации от несанкционированного доступа «Страж NT»:

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,

- контроль целостности,
- организация учета съемных носителей информации,
- регистрация событий,
- гарантированное удаление данных.

Задание 2. Установка автономной версии СЗИ от НСД Dallas Lock 8.0.

Инсталлировать автономную версию системы защиты Dallas Lock 8.0 на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь. Если пользователь доменный, то важно, чтобы он был добавлен в группу «Администраторы» или «Администраторы домена».

Пользователь, установивший систему защиты, автоматически становится суперадминистратором, на которого не распространяются ограничительные действия Dallas Lock 8.0. Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять имя (переименовывать) суперадминистратора средствами Windows нельзя.

Имя и пароль пользователя для входа в операционную систему, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленной системой защиты Dallas Lock 8.0 пользователем в качестве суперадминистратора. Для установки автономно работающего СЗИ от НСД Dallas Lock 8.0 необходимо запустить приложение «Dallas Lock 8.0.msi».

После запуска программы установки следует выполнять действия, указанные в подсказках инсталлятора. На каждом шаге установки предоставляется возможность полной отмены инсталляции с возвратом всех сделанных изменений. Для этого служит кнопка «Отмена».

Переход на следующий этап установки выполняется с помощью кнопки «Далее». Во время установки клиента Dallas Lock 8.0 выполняется автоматическая настройка Брандмауэра Windows.

При запуске инсталлятора Dallas Lock 8.0 на компьютере с установленной операционной системой Windows 7, если включен механизм контроля учетных записей, после запуска приложения «Dallas Lock 8.0.msi» на экране будет выведено диалоговое окно для подтверждения операции.

SКонтроль учетных записей пользователей

Разрешить следующей программе установить программное обеспечение на этом компьютере?

Имя программы: Dallas Lock 8.0

Проверенный издатель: Confident

Источник файла: Жесткий диск компьютера

Показать подробности Да/Нет

Для продолжения установки следует ответить «Да», после чего запустится инсталлятор системы Dallas Lock 8.0.

Dalias Lock 8.0

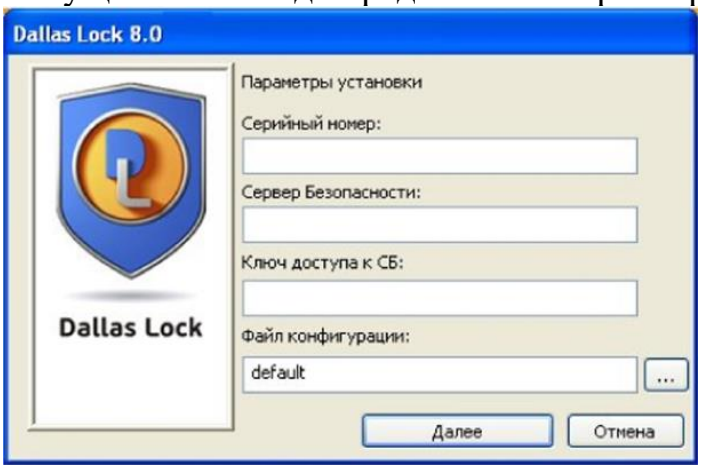
СЗИ НСД Dallas Lock 8.0 Данная программа выполнит установку системы защиты информации от несанкционированного доступа Dallas Lock 8.0-К на вашем компьютере. Для установки необходимо:

- Обладать правами администратора
- Отключить антивирусную защиту в BIOS компьютера и программные антивирусные средства.
- Наличие не менее 30 Мб свободного дискового пространства на системном разделе жёсткого диска
- Операционная система должна быть установлена на диск С.

Путь установки: C:DLLOCK80

Начать установку/ Отмена

Для установки необходимо нажать кнопку «Начать установку», после чего программа приступит к инсталляции продукта. На данном этапе программа попросит осуществить ввод определенных параметров.



Для защиты от нелегального использования продукта необходимо ввести серийный номер лицензии Dallas Lock 8.0, который указан на компакт-диске с дистрибутивом в поле «Код» и в формуляре комплекта поставки.

Если требуется ввести компьютер в Домен безопасности в процессе установки системы, то в соответствующие поля необходимо ввести имя Сервера безопасности и его ключ доступа. Для установки автономно

работающей версии никаких данных в полях «Сервер безопасности» и «Ключ досту па к СБ» вводить не надо. Добавить компьютер в Домен безопасности можно и позже, в процессе работы автономной версии Dallas Lock 8.0. После нажатия кнопки «Далее» процесс установки системы будет завершен.

Dallas Lock 8.0

Установка...

Проверка прав текущего пользователя.

Текущий пользователь является Администратор- Копирование Файлов...

Копирование Файлов успешно завершено.

Создание ярлыков...

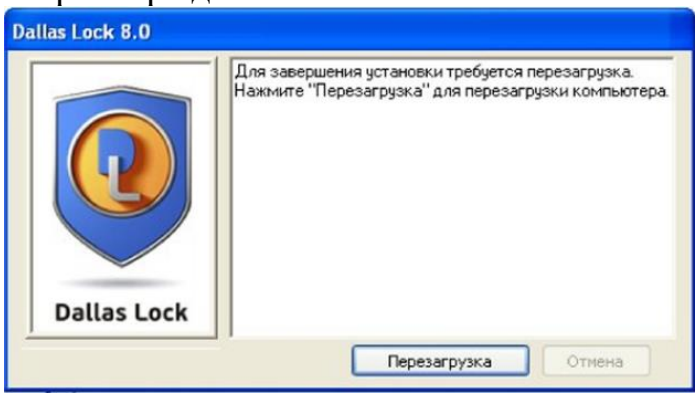
Ярлыки успешно созданы.

Установка драйвера системы защиты...

Драйвер безопасности успешно установлен. Регистрация компонентов и настройка системы. Настройка системы успешно завершена Администратором системы безопасности HasnaMet otzi

Далее система потребует перезагрузки компьютера.

Первый вход на защищенный компьютер сможет осуществить пользователь, под учетной записью которого выполнялась инсталляция системы защиты Dallas Lock 8.0, либо доменный пользовать, если компьютер является клиентом контроллера домена.

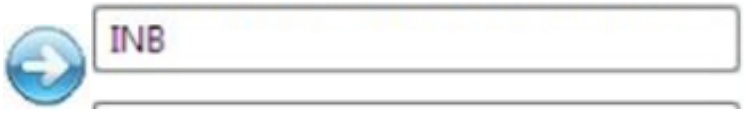


После установки системы защиты и перезагрузки компьютера па рабочем столе пользователя и в меню «Пуск» появятся иконки оболочки администратора системы защиты Dallas Lock 8.0.

Задание 3. Вход на защищенный компьютер.

При загрузке компьютера, защищенного системой Dallas Lock 8.0, появляется экран приветствия (приглашение на вход в систему).

Вход пользователя



Домен. Не заполняйте для локального

Аппаратные идентификаторы 0 Ann. идентификатор не выбран Уровень мандатного доступа 0 (Открытые данные)

Пароль

Для входа на защищенный СЗИ от НСД Dallas Lock 8.0 компьютер каждому пользователю надо выполнить последовательность шагов:

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе. В зависимости от настроек системы защиты в этом поле может оставаться имя пользователя, выполнившего вход последним.

2. Заполнить поле имени домена. Если пользователь доменный, то указывается имя домена, если пользователь локальный, то в этом поле оставляется имя компьютера или оставляется пустое значение.

3. Если пользователю назначен аппаратный идентификатор, то его необходимо предъявить. В зависимости от типа устройства предъявить идентификатор можно, вставив его в соответствующий usb- или com-порт, или прикоснувшись к считывателю.

4. Указать уровень мандатного доступа. Этот параметр актуален только для модификации Dallas Lock 8.0-«С». Первый вход любому пользователю в Dallas Lock 8.0-«С» следует выполнять в режиме «Открытые данные».

5. Ввести пароль. При вводе пароля поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой кла више, появляется символ «•» (точка). При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.

6. Нажать кнопку «Enter». После нажатия кнопки «Enter» осуществляется проверка наличия в системе зарегистрированного пользователя с указанным именем. После чего проверяется соответствие с именем пользователя номера аппаратного идентификатора, зарегистрированного в системе защиты, и правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход в систему, иначе вход в систему пользователю запрещается.

Задание 4. Изучите возможности системы защиты информации от несанкционированного доступа «Secret NET 5.0-С»:

- назначение,
- запуск и регистрация системы защиты,
- создание пользователей,
- реализация мандатной модели разграничения доступа,
- реализация дискреционной модели разграничения доступа,
- обеспечение замкнутости программной среды,
- контроль целостности,
- регистрация событий,
- гарантированное удаление данных,
- печать штампа,
- настройка механизма шифрования.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8

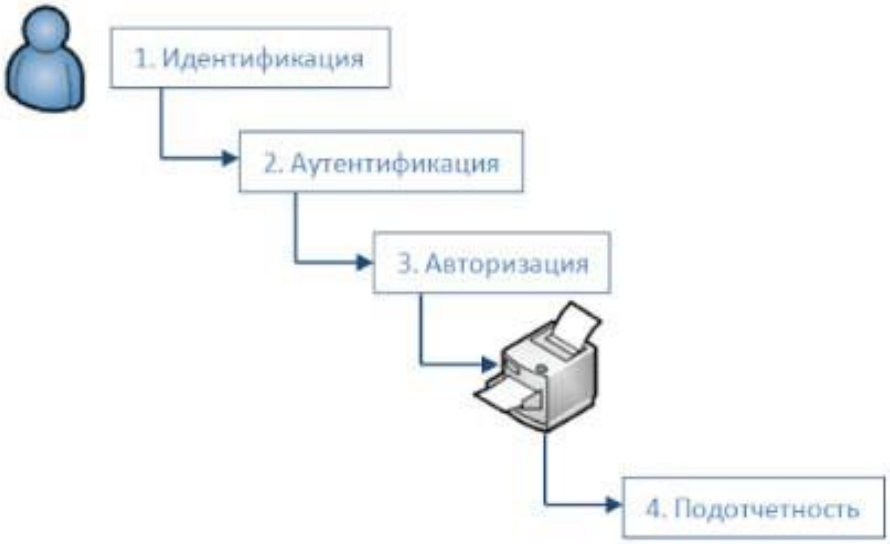
ЗАЩИТА ВХОДА В СИСТЕМУ (ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ)

Цели: изучить методы, применяемые для установления подлинности различных объектов и своевременного обнаружения несанкционированных действий пользователя; правила составления пароля; расчета среднего времени безопасности пароля.

Теоретические вопросы:

1. Понятия идентификации, аутентификации, авторизации.
2. Логическое управление доступом.
3. Методы идентификации и аутентификации.

Задание 1. Опишите четыре шага, которые необходимо пройти субъекту для получения доступа к объекту:



Задание 2. Опишите правила выбора и использования пароля.

Задание 3. Поясните формулу:

Среднее время безопасности пароля определяется по формуле:

$$T = \left(d + \frac{m}{n}\right) \cdot \frac{S}{2},$$

где d - **промежуток времени между двумя неудачными попытками несанкционированного входа в систему;**

m - **количество символов в пароле;**

n - **скорость набора пароля (количество символов, набираемых в единицу времени);**

S - **количество всевозможных паролей указанной длины.**

Задание 4. С использованием одного из языков программирования составить программу, которая выполняет действия.

а) Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard». Составить

программу, которая записывает пароль следующим образом:

1. В строку <результат> в качестве первого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26.

2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z».

3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z».

4. в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a».

5. Вывести полученную строку.

Дополнить полученную программу средствами аутентификации:

1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*».

2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ.

3. Вывести результат аутентификации: пароль верен или неверен?

Задание 5. Определите степень защиты информации организации, защищенной с применением пароля, а также исследуйте методы противодействия атакам на пароль.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9

РАЗГРАНИЧЕНИЕ ДОСТУПА К УСТРОЙСТВАМ

Цели: Изучить способы разграничения доступа. Научиться распределять права доступа сотрудникам предприятия в зависимости от их должностных обязанностей.

Теоретические вопросы:

1. Технические средства разграничения доступа к устройствам.
2. Механизмы разграничения доступа к устройствам.

Ход работы:

1. Запустите виртуальную машину «Secret Net Client». Для настройки конфигурации виртуальной машины VMware задаст вопрос о том была ли она скопирована или перемещена (рис. 1), выберите вариант «I Moved It» (виртуальная машина перемещена). После загрузки операционной системы войдите под локальной учетной записью «Администратор» (рис. 2). Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». После этого будет выведено сообщение об изменении аппаратной конфигурации. Снимите блокировку рабочей станции (Да) и выполните следующее:

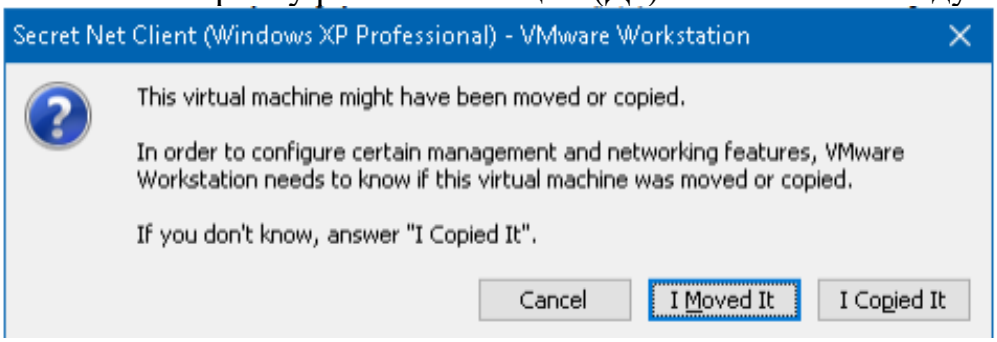


Рисунок 1 – Запрос конфигурации при запуске виртуальной машины

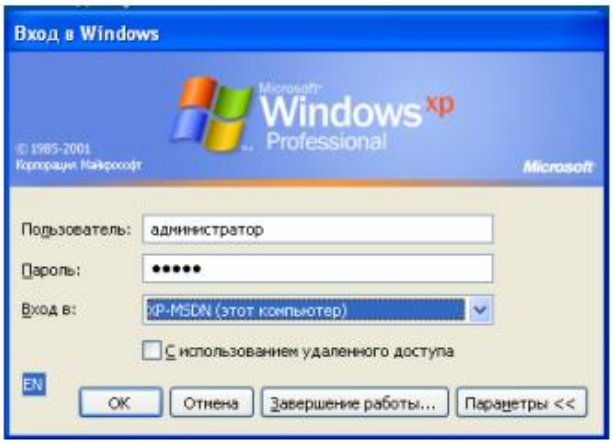


Рисунок 2 – Вход в систему под локальной учетной записью

Откройте свойства учетной записи Администратор (Мой компьютер-Управление - Локальные пользователи- Пользователи - Администратор). Измените уровень допуска на строго конфиденциально (Вкладка Secret Net

7 - Доступ), разрешите управление категориями конфиденциальности, вывод и печать конфиденциальных документов (рис. 3). Создайте учетные записи user и conf. Настройте пользователю conf категорию доступа конфиденциально и добавьте возможность печати конфиденциальных документов (рис. 4). Для пользователя user по умолчанию задан уровень допуска «Неконфиденциально».

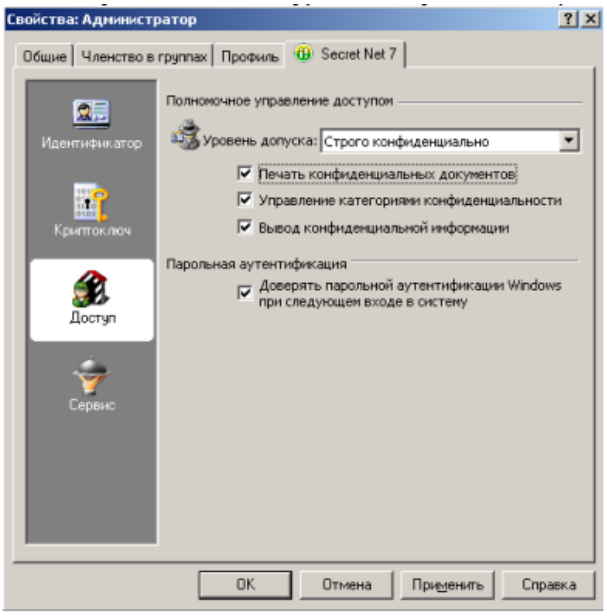


Рисунок 3– Параметры управления полномочным доступом для пользователя Администратор

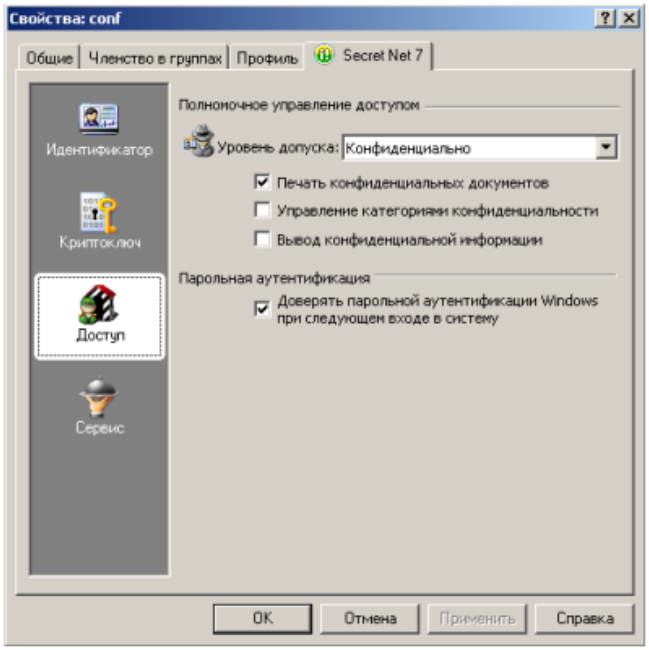


Рисунок 4– Параметры управления полномочным доступом для пользователя conf

2. Вызовите оснастку для управления параметрами объектов групповой политики (Пуск-Программы-Код безопасности- Secret Net – Локальная политика безопасности) и перейдите к разделу «Параметры безопасности |

Параметры Secret Net» - выберите папку «Устройства». Утвердите изменения. В правой части окна появится общий список устройств. - выберите в списке оптический диск «VMWare IDE CDR» (или другой CDдисковод, который будет предоставлен средством виртуализации VMware), вызовите контекстное меню и выберите команду «Свойства». В группе настройки выберите «Подключение устройства разрешено» (рис. 5). В группе «полномочный доступ» выберете параметр доступа «Для устройств задана категория конфиденциальности» и выберете категорию конфиденциальности «Строго конфиденциально» (рис. 6).

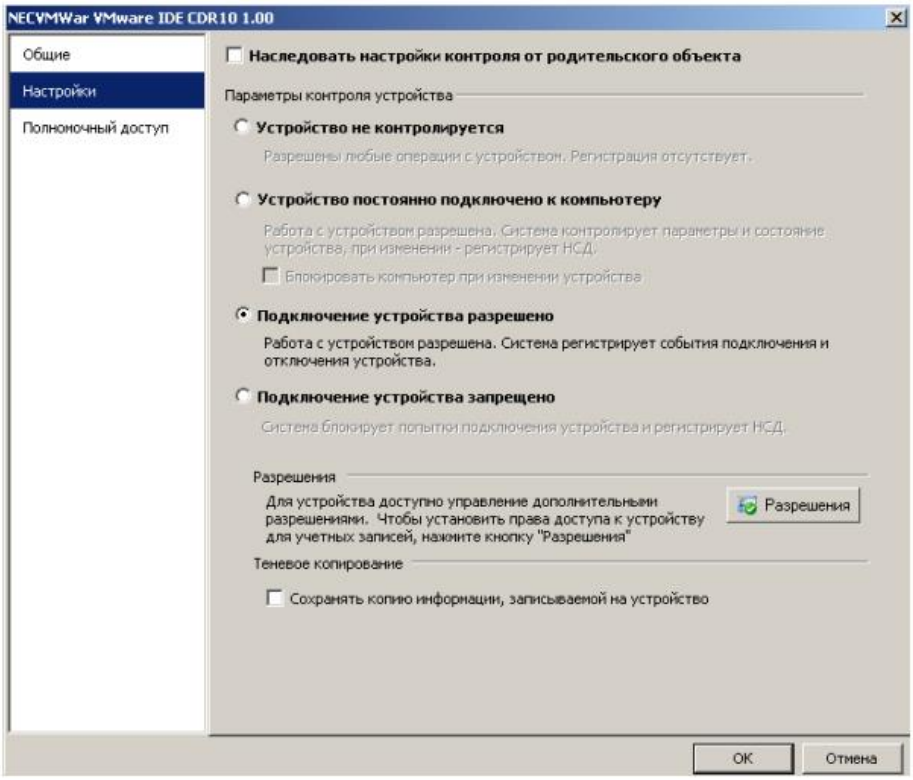


Рисунок 5- Настройки виртуального CD- привода
в групповых политиках Secret Net

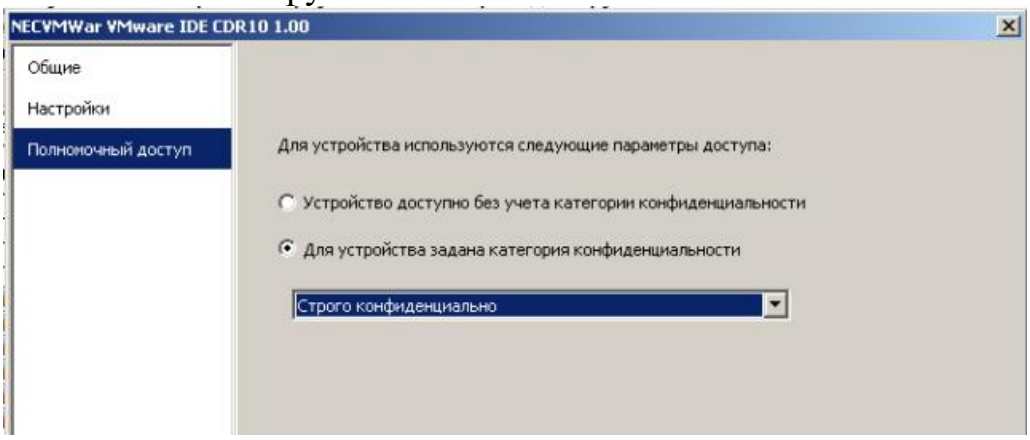


Рисунок 6 – Настройки конфиденциальности виртуального CD-привода
в групповых политиках Secret Net

- войдите под учетной записью «user» и убедитесь, что вход в систему,

при наличии устройства с категорией конфиденциальности выше, чем у пользователя, недоступен. Приведите результат в отчете.

3. Войдите под учетной записью «Администратор», измените назад параметры конфиденциальности оптического диска на «Устройство доступно без учета категории конфиденциальности», запретите использование оптических дисков для пользователя 8 «user» следующим образом: откройте разрешения в свойствах CD-дисковода (НастройкиРазрешения), добавьте пользователя user и запретите всех разрешения к данному CDприводу (рис. 7) - галочки «запретить».

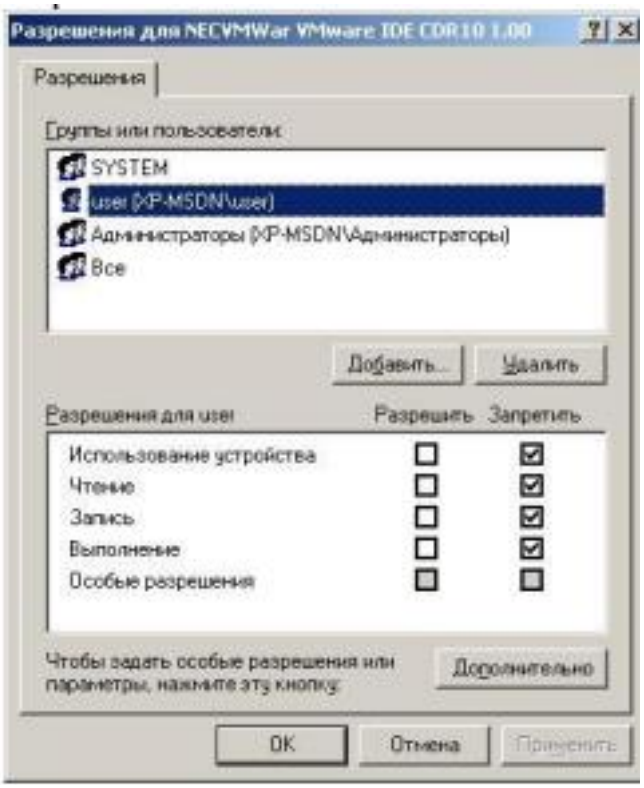


Рисунок 7 – Изменение прав доступа к CD-приводу для пользователя user.

- Войдите под учетной записью user и убедитесь в запрете доступа, попытавшись открыть CD-привод в проводнике.

4. Настройку политик контроля устройств можно выполнить индивидуально для каждого устройства (отдельной модели), класса или группы устройств с использованием принципа наследования параметров. Для настройки политики контроля устройств выполнить следующее:

- Войдите под учетной записью Администратор. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности | Параметры Secret Net»

- выберите папку «Устройства». В правой части окна появится общий список устройств. - выберите в списке объект «Устройства USB», вызовите контекстное меню и выберите команду «Свойства».

На экране появится диалог для настройки параметров объекта. По умолчанию в диалоге отображаются параметры группы «Общие» (рис. 8), представляющие основные сведения об объекте.

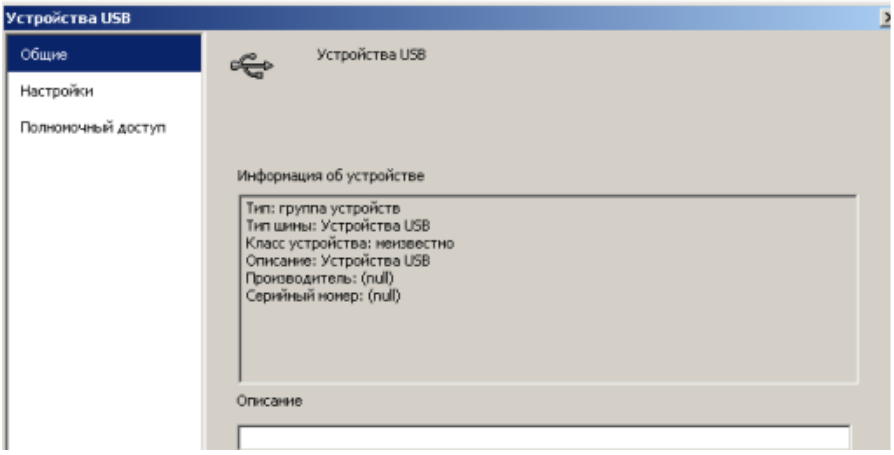


Рисунок 8 – Вкладка общие для группы устройства USB 9

- перейдите к группе параметров «настройки» и поставьте значения параметров в соответствии с рис. 9. Примените настройки ко всем дочерним объектам.

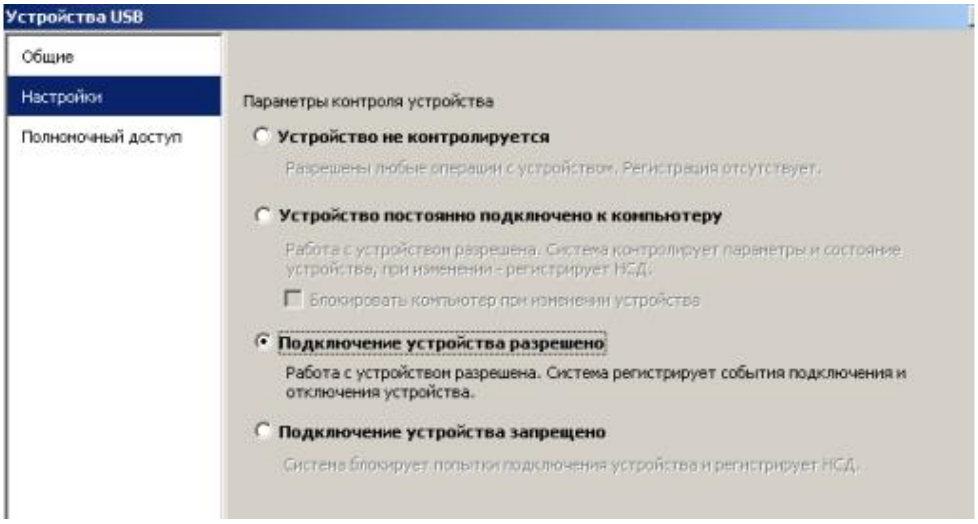


Рисунок 9 – Вкладка «Настройки» для группы устройства USB

При этом для подключенных устройств можно задать следующие параметры:

– Поле «Устройство не контролируется». Если в поле установлена отметка — для объекта отключен режим контроля.

– Поле «Устройство постоянно подключено к компьютеру». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру. В случае изменения состояния устройства в журнале регистрируются события несанкционированного доступа (НСД), и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности. Для усиления защиты можно дополнительно включить режим автоматического блокирования компьютера при изменении состояния устройства: для этого установите отметку в поле «Блокировать компьютер при изменении

устройства». Возможность разблокировки компьютера будет иметь только администратор безопасности.

– Поле «Подключение устройства разрешено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование.

– Поле «Подключение устройства запрещено». Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. Попытки подключения устройства регистрируются в журнале как события НСД. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 10

УПРАВЛЕНИЕ ДОСТУПОМ

Цели: изучить механизмы управления доступом.

Теоретические вопросы:

1. Модели управления доступом.
2. Выбор модели управления доступом.
3. Дискреционное управление доступом.
4. Мандатное управление доступом.
5. Списки управления доступом.
6. Ролевое управление доступом.

Задание 1. Поясните фрагмент матрицы доступа:

	Файл	Программа	Линия связяи	Реляционная таблица
Пользователь 1	orw с системой консоли	e	Rw с 8.00 до 18.00	
Пользователь 2				

Задание 2. Заполните таблицу:

Разрешения доступа к общим папкам

Разрешение	Позволяет
Изменение	
(Чтение)	
(Полный доступ)	

Задание 3. Пусть пользователю User101 назначены разрешения для получения доступа к ресурсам как отдельному пользователю и как члену

группы. Определите, какие результирующие разрешения будут у User101 в следующих ситуациях:

1. User101 — член групп Group1, Group2 и Group3. Для папки ПапкаА у Group1 есть разрешение Read (Чтение), у Group3 — Full Control (Полный доступ), а для Group2 разрешений не назначено. Какими результирующими разрешениями будет обладать User101для ПапкиА?

2. User101 также является членом группы Sales, которой назначено разрешение Read для ПапкаВ. Для User101 как отдельного пользователя, отменено разрешение Full Control для ПапкаВ. Какие результирующие разрешения будет иметь User101 для ПапкаВ?

Задание 4. Определите результирующие разрешения пользователей, спланируйте совместное использование папок и разрешений доступа к ним, назначьте разрешения доступа к папке, подключитесь к ней, закройте к ней доступ и проверьте эффекты от сочетания разрешений доступа к общей папке и разрешений NTFS:

3. Открыт доступ к папке Data. Группа Sales имеет для нее разрешение read (Чтение), а для вложенной в нее папки ^ Sales — NTFS-разрешение Full Control (Полный доступ). Каким будет результирующее разрешение группы Sales для доступа к папке Sales при подключении по сети к папке Data?

4. Папка Users (Пользователи) содержит личные папки пользователей. Каждая личная папка содержит данные, доступные только пользователю, именем которого она названа. Папка Users доступна группе Users с разрешением Full Control (Полный доступ). Userl и User2 имеют разрешения NTFS Full Control только для своих личных папок: никаких разрешений NTFS для остальных. Эти пользователи — члены группы Users. ^ Какими разрешениями доступа к папке Userl будет обладать Userl при подключении к общей папке Users?

Какими будут его разрешения для папки User2?

Задание 5. Закройте доступ к заданной папке.

Задание 6. Назначьте разрешения NTFS папкам **Dostup**, **Public** и **Manuals** и откройте к ним доступ:

Путь	Группа	Разрешения NTFS
C:\Dostup	Администраторы	Полный доступ
	Users(Пользователи)	Чтение и выполнение
C:\Dostup\ Manuals	Администраторы	Полный доступ
	Users	Чтение и выполнение
C:\Dostup\ Public	Администраторы	Полный доступ
	Users	Полный доступ

ПРАКТИЧЕСКАЯ РАБОТА № 11

ИСПОЛЬЗОВАНИЕ ПРИНТЕРОВ ДЛЯ ПЕЧАТИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ. КОНТРОЛЬ ПЕЧАТИ

Цели: изучить особенности использования принтеров для печати конфиденциальных документов и возможности контроля печати.

Теоретические вопросы:

1. Использование функции блокированной печати, безопасной печати.
2. Программно-аппаратные средства контроля печати.
3. Политики печати и квоты.

Ход работы:

1. В список принтеров групповой политики можно добавлять элементы, соответствующие конкретным принтерам. По умолчанию ни один принтер в системе не контролируется. Добавление осуществляется с помощью специальной программы мастера. При необходимости принтер можно удалить из списка — для этого вызовите контекстное меню принтера и активируйте команду «Удалить». Добавьте принтер в групповую политику Secret Net. Для добавления принтера в список групповой политики необходимо выполнить следующее:

- Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу «Параметры безопасности \ Параметры Secret Net».

- Выберите папку «Принтеры». В правой части окна появится список принтеров.

- В меню оснастки выберите команду «Действие | Добавить принтер». На экране появится стартовый диалог мастера добавления принтеров.

- Выберите вариант добавления принтера (подключенный к компьютеру -> Microsoft XPS Document Writer) (рис.1)

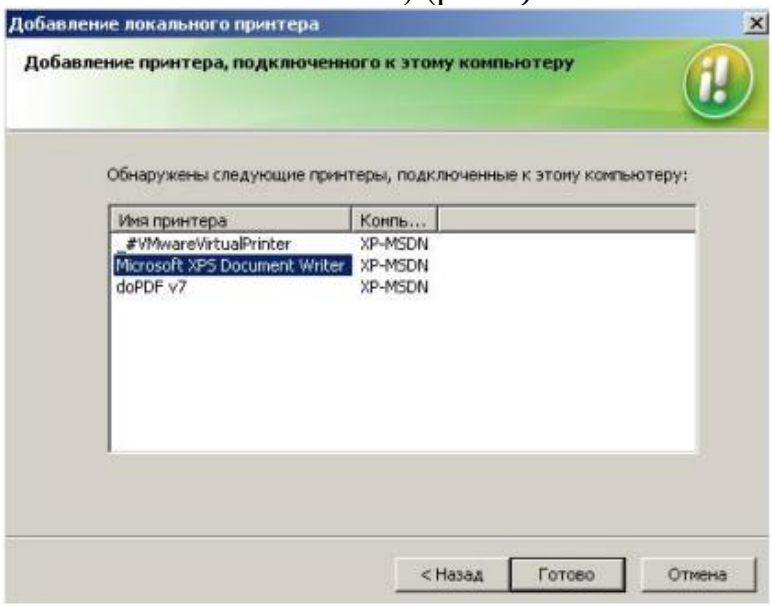


Рисунок 1 – Добавление принтера, контролируемого Secret Net

После того, как добавлен принтер, необходимо настроить права пользователей для печати. В оснастке для управления параметрами объектов групповой политики Secret Net («Параметры безопасности | Параметры Secret Net»), выберите папку «Принтеры» и вызовите контекстное меню принтера «Microsoft XPS Document Writer» - параметр «Свойства» (рис.2).

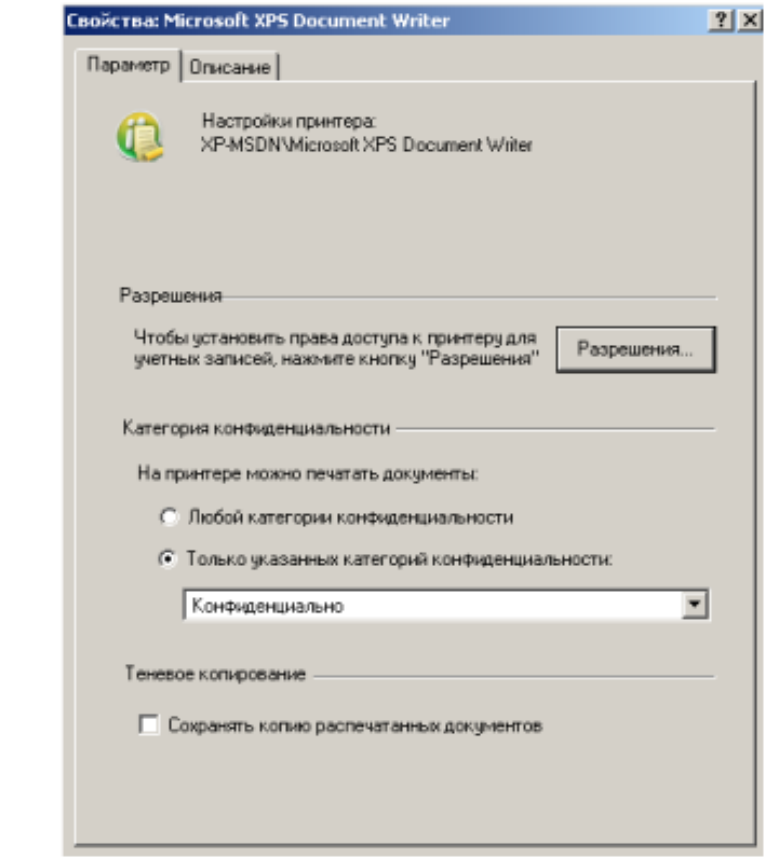


Рисунок 2 – Настройка разрешений печати
для принтера Microsoft XPS Document Writer

2. В окне свойств принтера выберите «Только указанных категорий конфиденциальности», а категорию – «Конфиденциально». Стоит отметить, что для печати документов соответствующей категории конфиденциальности пользователя должна быть включена возможность печати конфиденциальных документов (было выполнено ранее). Измените разрешения на доступ к диску «D:\» (Диск D – Свойства – Безопасность – Все – Полный доступ). Измените у папки «D:\temp» категорию конфиденциальности на «Конфиденциально», изменив категорию и у всех вложенных файлов (рис.3). Отдельно файлу «D:\temp\Неконф.txt» задайте категорию «Неконфиденциально».

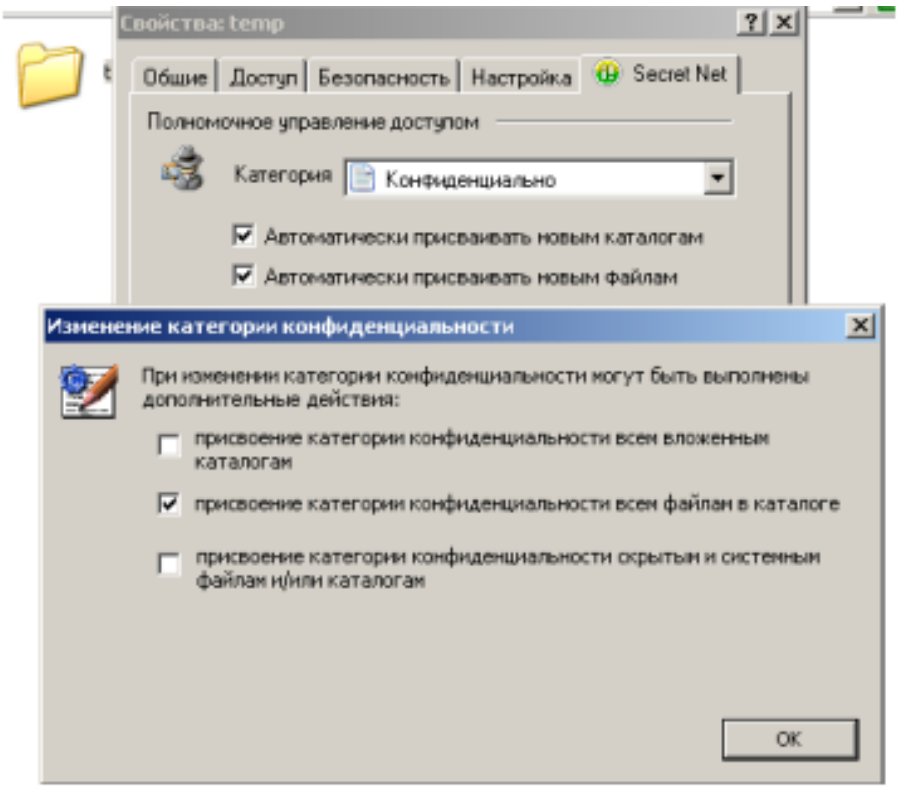


Рисунок 3 – Изменение уровня конфиденциальности папки temp

3. Зайдите под учетной записью conf и убедитесь в возможности печати документов «D:\temp\Конф.txt» с категорией «Конфиденциально» и документа «D:\temp\Неконф.txt» 12 «Неконфиденциально». В параметрах печати необходимо задать настройку «Печать в файл» (рис. 4). При наличии права на печать конфиденциального документа, будет предложено заполнить гриф, добавляемый в распечатываемый документ (рис. 5). Попробуйте распечатать данные документы с помощью принтеров «Microsoft XPS Document Writer» и «doPDF» (рис. 6). Проанализируйте полученные результаты, зафиксируйте их в отчете.

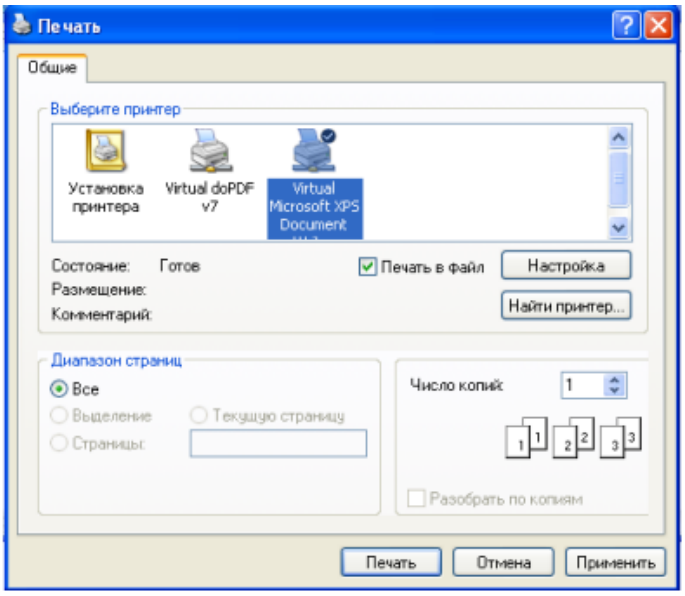


Рисунок 4 – Параметры печати конфиденциального документа

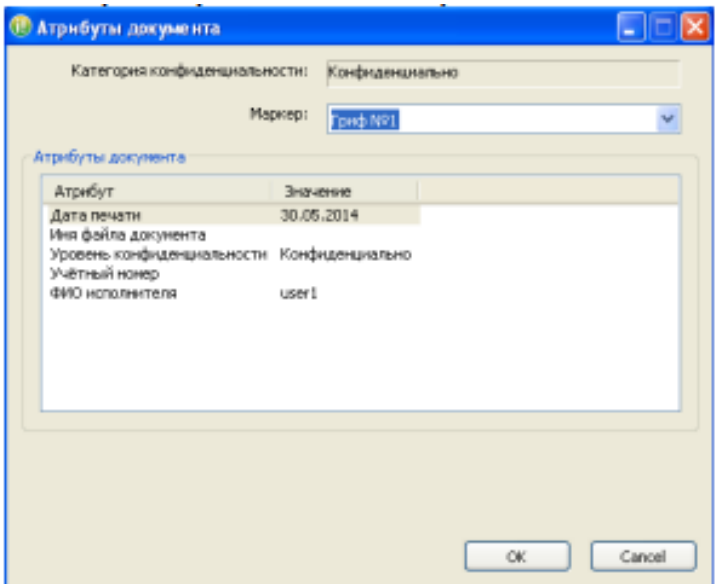


Рисунок 5 – Выбор и заполнение грифа для распечатываемого документа

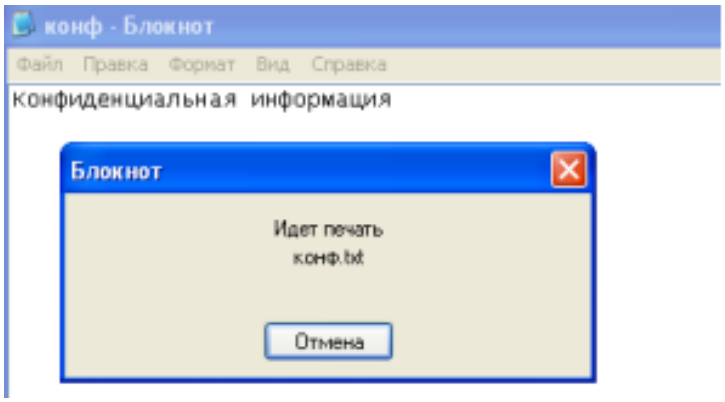


Рисунок 6 – Процесс печати конфиденциального документа

Задание: Проделайте ход работы, зафиксировав полученные результаты в отчете. Создайте учетную запись, соответствующую имени в факультетской сети (либо из ФИО). В зависимости от номера варианта задайте учетной записи пользователя категорию конфиденциальности и запретите подключение устройств:

Вариант	1	2	3	4	5	6	7	8	9	10
В зависимости от номера вариант задайте учетной записи пользователя категорию конфиденциальности										
Конфиденциально		+				+			+	
Строго конфиденциально			+		+		+			+
Не конфиденциально	+			+				+		
Запретить подключение устройств										
Усройства SD			+		+	+		+		+
Принтеры	+			+		+	+			
Электронные идентификаторы и считыватели		+				+		+	+	
Сетевые платы			+	+			+			
Оптические диски	+		+			+		+		+
USB устройства		+		+	+		+			

Примечание: “+” означает, что для данного устройства нужно запретить подключение.

Также для данной учетной записи и устройства проделайте следующие действия:

1. Для соответствующего класса устройств по варианту измените разрешения, для созданного пользователя, на запрет «чтения», «записи» и «выполнения». Проверьте, выполняются ли данные разрешения.

2. Для принтера разрешите вывод на печать документов с категорией «Строго конфиденциально». Попытайтесь из-под созданной учетной записи распечатать документ с категорией конфиденциальности «Конфиденциально» («D:\temp\Конф.txt») и документ с категорией конфиденциальности «Не конфиденциально» («D:\Неконф.txt»).

Задание 1. Распечатайте документ при помощи функции безопасной или блокированной печати.

Задание 2. Нарисуйте таблицу способов программно-аппаратные средств контроля печати.

Задание 3. Составьте список преимуществ использования программно-аппаратных средств контроля печати.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 12

НАСТРОЙКА СИСТЕМЫ ДЛЯ ЗАДАЧ АУДИТА

Цели: приобретение обучаемыми необходимого объёма знаний и практических навыков в области настройки системы для задач аудита.

Теоретические вопросы:

1. Аудит событий. Настройка аудита событий.
2. Просмотр событий.
3. Диспетчер задач и внутренние параметры системы.

Задание 1. Произведите настройку аудита системы на своем ПК.

Задание 2. Просмотреть события, происходящие в системе.

Задание 3. Проанализируйте текущие параметры системы.

Задание 4. Просмотрите состояние сетевых соединений в Вашей системы.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 13

НАСТРОЙКА КОНТРОЛЯ ЦЕЛОСТНОСТИ И ЗАМКНУТОЙ ПРОГРАММНОЙ СРЕДЫ

Цели: приобретение обучаемыми необходимого объёма знаний и практических навыков в области настройки контроля целостности и замкнутой программной среды.

Теоретические вопросы

1. Понятие замкнутой программной среды.
2. Механизм контроля подключения и изменения устройств
3. Механизм разграничения доступа к устройствам.
4. Иерархическая схема списка устройств.

Задание 1. Войдите под учетной записью «Администратор» и запретите использование оптических дисков для пользователя «user».

Задание 2. Запретите использование принтера всем пользователям, кроме администратора.

Задание 3. Запретите использование программы для просмотра видео всем пользователям, кроме администратора.

Задание 4. Настройте контроль целостности для диска «C:\».

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 14

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ, ОПЕРАТИВНЫЙ МОНИТОРИНГ И АУДИТ БЕЗОПАСНОСТИ

Цели: приобретение необходимого объёма знаний и практических навыков в области централизованного управления системой защиты, оперативного мониторинга и аудита безопасности.

Теоретические вопросы:

1. Понятие централизованного управления системой защиты.
2. Режимы централизованного управления.
3. Конфигурация структуры оперативного управления.
4. Объекты конфигурирования.

Задание 1. Перечислите типовые задачи администратора безопасности, для выполнения которых используется программа оперативного управления в режиме управления.

Задание 2. Включите политику устройств. Отредактируйте параметры:

- Сменные диски, оптические диски – подключение запрещено (необходимо также поставить галочку для включения политики).
- Устройства хранения – отключить наследование и запретить подключение устройства (необходимо также поставить галочку для включения политики).
- Сеть - запретить подключение устройств. Отключить наследование и разрешить подключение устройств для соединения Ethernet.

Задание 3. Просмотрите журнал событий НСД.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 15

УСТРАНЕНИЕ ОТКАЗОВ И ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ КОМПОНЕНТОВ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Цели: изучить механизмы устранения отказов и восстановления работоспособности компонентов систем защиты информации автоматизированных систем.

Теоретические вопросы:

1. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

2. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении.

3. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.

Задание 1. Опишите возможные сбои/отказы компонентов систем защиты информации и пути решения проблем. Заполните таблицу:

Некорректная работа операционной системы	
Неисправность оборудования, от персональных компьютеров и периферии для них до систем обеспечения безопасности как информационной, так и безопасности предприятия	
Взлом с попыткой хищения информации	
Потеря интернет-соединения	

Задание 2. Опишите инженерно-технические средства обеспечения безопасности информации:

WinMTR	
SNMPMAN	
SNMP	
Netguard	

Задание 3. Разработайте план обеспечения непрерывной работы и восстановления работоспособности подсистемы защиты информации автоматизированной системы.

Задание 4. Опишите средства обеспечения непрерывной работы и восстановления:

Наименование информационного ресурса	Где размещается ресурс в системе	Вид резервного копирования (период возобновляемого копирования)	Ответственный за резервное копирование и порядок создания резервной копии (используемые технические средства)	Где хранится резервная копия (ответственный, его телефон)	Порядок использования резервной копии (кто, в каких случаях)

Задание 5. Проверьте работу средства Восстановление системы путем создания контрольной точки и выполнения восстановления системы до более раннего состояния.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 16

ОФОРМЛЕНИЕ ОСНОВНЫХ ЭКСПЛУАТАЦИОННЫХ ДОКУМЕНТОВ НА АВТОМАТИЗИРОВАННУЮ СИСТЕМУ

Цели: изучить правила оформления основных эксплуатационных документов на автоматизированную систему.

Теоретические вопросы:

1. Основные эксплуатационные документы защищенных автоматизированных систем.
2. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем.
3. Акт ввода в эксплуатацию на автоматизированную систему.
4. Технический паспорт на защищаемую автоматизированную систему.

Задание 1. Изучите основные требования следующих стандартов, определяющие построение системы, структуру конструкторских документов, их номенклатуру (комплектность), а также правила выполнения текстовых конструкторских документов:

ГОСТ 2.001-70 “ЕСКД. Общие положения”.

ГОСТ 2.101-68 “ЕСКД. Виды изделий».

ГОСТ 2.102-68 “ЕСКД . Виды и комплектность конструкторских документов”. ГОСТ 2.103-68 “ЕСКД. Стадии разработки”.

ГОСТ 2.104-68 “ЕСКД. Основные надписи”.

ГОСТ 2.105-68 “ЕСКД. Общие требования к текстовым документам”.

ГОСТ 2.106-68 “ЕСКД. Текстовые документы».

ГОСТ 2.107-68 “ЕСКД. Спецификация”.

ГОСТ 2.108-68 “ЕСКД. Ведомость держателей подлинников».

ГОСТ 2.109-68 “ЕСКД. Техническое условие”.

Задание 2. Разработайте эксплуатационную документацию на автоматизированную систему.

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основные источники:

1. Е.К. Баранова, А.В. Бабаш Информационная безопасность и защита информации: учеб. пособие. - 4-е изд., перераб. и доп. - МИ.: ИнфраМ, 2019. - 336 с. ISBN 978-5-369-01761-6 (РИОР)

2. Нестеров С.А. Информационная безопасность. Учебник и практикум для СПО. ISBN 978-5534-07979-1 Юрайт 2019. - 321 с.

3. Батаев А.В., Н.Ю. Налютин, С.В. Синицин. Операционные системы и среды: учебник для студ. Учреждений сред.проф.образования - 2-е изд. - М.: Академия, 2018. - 272 с. ISBN 978-5-44686801-8

4. Внуков А.А. Основы информационной безопасности: защита информации: учеб.пособие для СПО SBN 978-5-534-10711-1 Юрайт 2019. - 240с.

5. Технические средства и методы защиты информации. Учебник для вузов. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков / Под ред.А.П. Зайцева, А.А. Шелупанова. - 7-е изд., испр. ISBN 9785-9912-0233-6. - Телеком 2018, - 442 с.

Дополнительные источники

1. Советов, Б. Я. Базы данных: учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2019. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/438438

2. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2019. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/438283

Интернет-ресурсы:

Автономная некоммерческая организация профессионального образования «Московский колледж информационных технологий»: официальный сайт. – Москва. – URL: https://mkit.online/eios/

СОДЕРЖАНИЕ

МДК 01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий для обучающихся 2 курса всех форм обучения образовательных организаций среднего профессионального образования

Часть 1

Методические указания
разработали преподаватели:
Бойко Яна Сергеевна, Винник Анна Валентиновна

Подписано к печати ***10.11.2022 г.*** Объем ***3,4*** п.л.
Формат 60х84/16 Заказ
Тираж ***1*** *экз.*

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
628615 Тюменская обл., Ханты-Мансийский автономный округ,
г. Нижневартовск, ул. Мира, 37.