МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»

Методические рекомендации
по практическим занятиям
междисциплинарного курса: МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Нормативный срок обучения: 3 года 10 месяцев

Форма обучения: Очная

2021

Методические указания по практическим занятиям междисциплинарного курса: МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении разработаны на основе федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.15 Обеспечение информационной безопасности автоматизированных систем Утвержденным приказом Минобрнауки России от 09.12.2016г. №1553
дата утверждения и №)

Методические указания рассмотрены на заседании методического совета СПК и рекомендованы к использованию

«19» 02. 2020 года Протокол № __1__
Председатель методического совета СПК
Сергеева Светлана Ивановна _____

Методические указания утверждены на заседании педагогического совета СПК «28» 02. 2020 года Протокол № _6__
Председатель педагогического совета СПК
Облиенко Алексей Владимирович _____

Организация-разработчик: ФГБОУ ВО «ВГТУ»

Разработчики:
__ Парецких Елена Викторовна_____
(Ф.И.О., ученая степень, звание, должность

_____
(Ф.И.О., ученая степень, звание, должность)

_____
(Ф.И.О., ученая степень, звание, должность)

_____
(Ф.И.О., ученая степень, звание, должность)

ПРАКТИЧЕСКАЯ РАБОТА № 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.

ПРАКТИЧЕСКАЯ РАБОТА № 2, 3

Разработка технического задания на проектирование автоматизированной системы. Разработка концепции защиты автоматизированной (информационной) 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 (наездна пешехода, наезд на ограждение либо столб, лобовое столкновение, наезд на впереди стоящий транспорт, боковое столкновение на перекрестке и т.п.), место происшествия, марки пострадавших автомобилей, государственный номер, тип машины (легковая, грузовая, специальная), краткое содержание, число пострадавших, сумма ущерба, причина, дорожные условия и т.п. Анализ накопленной по ДТП статистике поможет правильно расставить запрещающие и предупреждающие знаки на улицах города, а так же спланировать местонахождение постов патрульных.

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

Вариант 5: Информационная система строительной организации

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

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

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

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

количествах необходимы для сооружения объекта. По результатам выполнения работ составляется отчет с указанием сроков выполнения работ и фактических расходов материалов.

Вариант 6: Информационная система библиотечного фонда города

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

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

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

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

Вариант 7: Информационная система спортивных организаций города

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

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

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

Вариант 8: Информационная система аэропорта

Работников аэропорта можно подразделить на пилотов, диспетчеров, техников, кассиров, работников службы безопасности, сплавочной службы и других, которые административно

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

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

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

Вариант 9: Информационная система гостиничного комплекса

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

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

рынок гостиничных услуг, в результате чего заключаются договора с новыми фирмами. Также исследуется мнение жильцов о ценах и сервисе. Жалобы фиксируются и исследуются. Изучается статистика популярности номеров. Ведется учет долгов постояльца гостинице за все дополнительные услуги.

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

Вариант 10: Информационная система торговой организации

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

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

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

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

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

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

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

ПРАКТИЧЕСКАЯ РАБОТА № 4
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 конфиден-циальности (В/Н/-) и вид тайны (БТ/КТ/ДСП)	Категория целостности (В/Н/-)	Размещение ресурса (АРМ, устройство, каталог, файл)	Ответствен-ный за определение требований к защищен-ности ресурса
1				
2				
3				
4				
…				
…				

ПРАКТИЧЕСКАЯ РАБОТА № 5

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

ПРАКТИЧЕСКАЯ РАБОТА № 6
Построение модели угроз

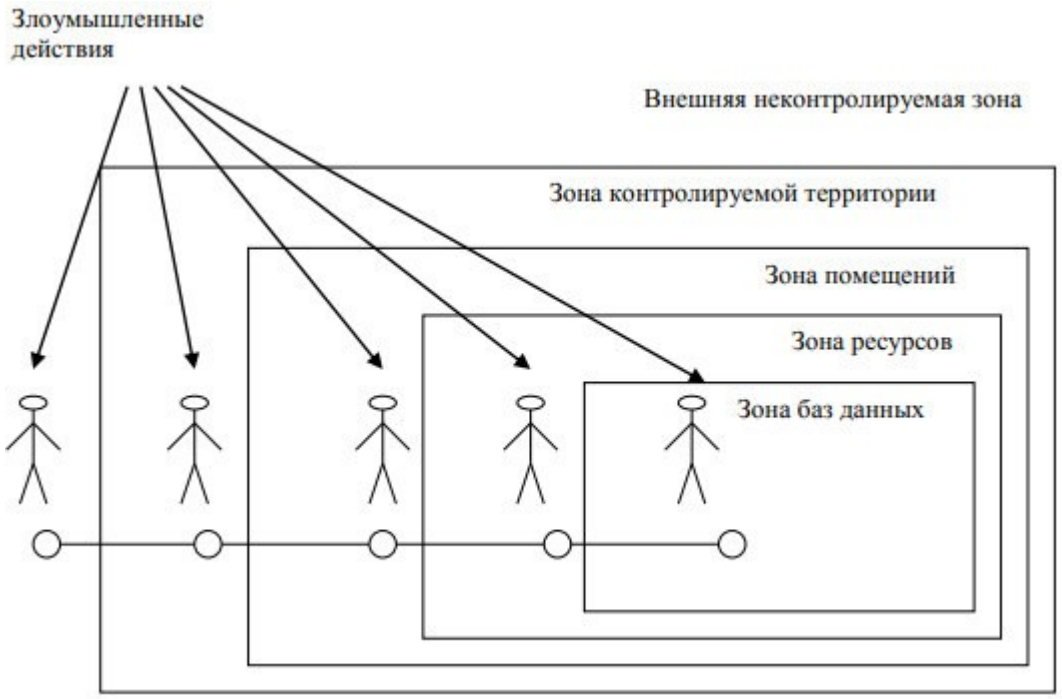
Цель: анализ и построение модели информационной безопасности.

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.	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
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

ПРАКТИЧЕСКАЯ РАБОТА № 7

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.

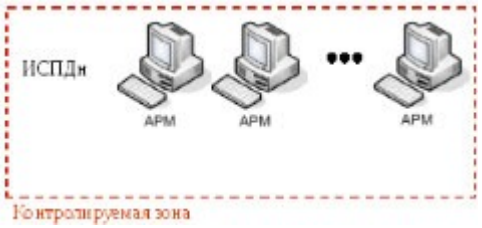
Теоретические вопросы

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.

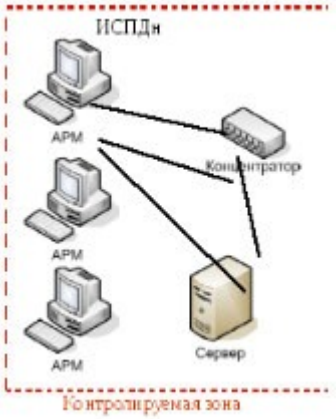
Задание 1. Оцените характеристики ИСПДн, обусловливающие возникновение угроз безопасности ПДн:

1) структура ИСПДн:

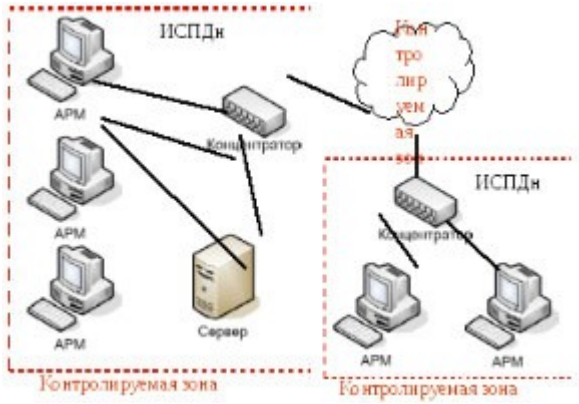
автономные ИСПДн АРМ:



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	Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его	• обладает информацией об алгоритмах и программах обработки информации на ИСПДн; • обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки,

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

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

Перечень всех возможных угроз безопасности ПДн

Возможные угрозы безопасности ПДн
1. Угрозы от утечки по техническим каналам
1.1. Угрозы утечки акустической информации
1.2. Угрозы утечки видовой информации
1.3. Угрозы утечки информации по каналам ПЭМИН
2. Угрозы несанкционированного доступа к информации
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн
2.1.1. Кража ПЭВМ
2.1.2. Кража носителей информации
2.1.3. Кража ключей и атрибутов доступа
2.1.4. Кражи, модификации, уничтожения информации
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
2.1.7. Несанкционированное отключение средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)
2.2.1. Действия вредоносных программ (вирусов)
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера
2.3.1. Утрата ключей и атрибутов доступа
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками
2.3.3. Непреднамеренное отключение средств защиты

2.3.4. Выход из строя аппаратно-программных средств
2.3.5. Сбой системы электроснабжения
2.3.6. Стихийное бедствие
2.4. Угрозы преднамеренных действий внутренних нарушителей
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке
2.5.Угрозы несанкционированного доступа по каналам связи
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
2.5.3.Угрозы выявления паролей по сети
2.5.4.Угрозы навязывание ложного маршрута сети
2.5.5.Угрозы подмены доверенного объекта в сети
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях
2.5.7.Угрозы типа «Отказ в обслуживании»
2.5.8.Угрозы удаленного запуска приложений
2.5.9.Угрозы внедрения по сети вредоносных программ

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	–	–	+

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
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. 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
2.2.1. Действия вредоносных программ (вирусов)	VI. Антивирусная защита (АВЗ)	АВЗ.1-2
2.2.2. Недекларированные 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

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)	

ПРАКТИЧЕСКАЯ РАБОТА № 8

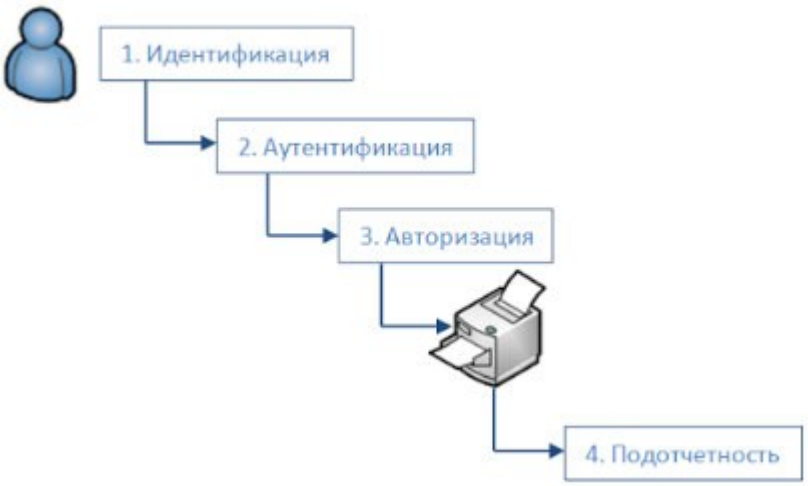
Анализ политик безопасности информационного объекта

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.

б) 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.

ЛИТЕРАТУРА

Основная литература:

1 Шишмарёв В.Ю. Автоматика : учебник для среднего профессионального образования / В. Ю. Шишмарёв. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 280 с. — (Профессиональное образование). — ISBN 978-5-534-09343-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/473405

Дополнительная литература:

1 Рогов Владимир Александрович. Технические средства автоматизации и управления : Учебник Для СПО / Рогов В. А., Чудаков А. Д. - 2-е изд. ; испр. и доп. - Москва : Издательство Юрайт, 2019. - 352. - (Профессиональное образование). - ISBN 978-5-534-09807-5 : 839.00. URL: https://www.urait.ru