**1Основные понятия и термин. защ. Информ**

Защита информации — это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информацииЦель защ.-предотвр. утраты, искажениия, утечки, копир., блокир.и иных форм незакон. вмешат.в ИС. Инф-это сведения о лицах, предм., фактах,и процес.Инф-это снятие необпределенности.Инф может сущ. в виде документов, сигналов, физ и биолог полей (память человека)Инф объект (ИО)-это среда в кот.либо создается, либо хранится, либо обрабатывается.Виды воздействия на ИО: непреднамеренное, преднамеренноеУщерб: наруш. конф-ти, целосн-ти, доступ-ти.Уязвимость- св-ва объекта, делающ воз-ть возникн угрозы.Атака-целенапр. действиев поиске уязвимости.Политика без-ти- совокупность норм, правил, рекомендаций, регламентир. работу ср-в защиты от заданного множества угроз безопасности

**2Классификация угроз инф. Безопасности**

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.- по свойствам информации- по физ. и лог. целостности - по доступности- по праву собственности-по происхождению (случайные и преднамеренные)-по источникам (люди, технческие устр-ва, алгоритмы, внешняя среда )По аспекту информационной безопасности, на который направлены угрозы:- Угрозы конфиденциальности- Угрозы целостности- Угрозы доступностиПо расположению источника угроз:Внутренние (источники угроз располагаются внутри системы);Внешние (источники угроз находятся вне системы).По размерам наносимого ущерба:Общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);Локальные (причинение вреда отдельным частям объекта безопасности);Частные (причинение вреда отдельным свойствам элементов объекта безопасности).По степени воздействия на информационную систему:Пассивные (структура и содержание системы не изменяются);Активные (структура и содержание системы подвергается изменениям).По природе возникновения:Естественные (объективные) — вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;Искусственные (субъективные) — вызванные воздействием на информационную сферу человека. Среди искусственных угроз в свою очередь выделяют: Непреднамеренные (случайные), Преднамеренные (умышленные) угрозыВсе источники угроз информационной безопасности можно разделить на три основные группы:Обусловленные действиями субъекта (антропогенные источники) Обусловленные техническими средствами (техногенные источники)Стихийные источники

**3Классификация методов защ. Инф**

- законодательные (правовые)-организационные-технические-комплексныеСегодня используется шесть основных способов защиты: препятствие, маскировка, регламентация, управление, принуждение, побуждение.

Маскировка – способы защиты информации, предусматр преобраз данных в форму, не пригодную для восприятия посторонними лицамиПрепятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.Управление – способы защиты инф, при которых осуществ управ над всеми компонентами информ сист.Регламентация – важнейший метод защиты инф систем, предполагающий введение особых инструкций, согласно которым должны осущест все манипуляции с охран данными. Управление - оказание управляющих воздействий на элементы защищаемой системыПринуждение – методы защиты инф, тесно связанные с регламентацией, предполаг введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям, то речь идет о побуждении.

Средства защиты информации:Физические средства Аппаратные средства Программные средства Законодательные средства

**4 Правовые и организ методы защ инф**

Правов обеспеч защ инф: нормотворческое и исполнительное (право-ая деятельность)Фундаментальные правила: эл. оборудование, внешний вид сооруженийПравовое обеспечение включает в себя:Нормотворческую деятельность по созданию законодательства, регулирующего общественные отношения в области информационной безопасности;Исполнительную и правоприменит деят-ть по исполнению законодат в обл инф, информатизации, защиты информации органами государственной власти и управления, организация (юридическими лицами), гражданами.Общегосударственные документы:Законы, кодексы; Указы Президента РБ;Постановления Совета Министров.Ведомственные документы: Межведомственные; Внутриведомственные.Основные правовые акты, регламентирующие защиту информации в Республике Беларусь: закон РБ “Об информатизации”; закон РБ “О государственных секретах”, закон “Об органах государственной безопасности Республики Беларусь”;

**5Государственное регулирование в области защи-ты информации. /**

Государство занимает важное место в системе защи-ты информации в любой стране, в том числе и в Рес-публике Беларусь. Государственная политика обеспе-чения информационной безопасности исходит из по-ложений Концепции национальной безопасности Рес-публики Беларусь.Гос секреты- такие сведения, не-санкц распр-е которых мажет нанести ущерб нац без-опасности, оборонос-и, и жизненно важным вопросам РБНосители сведений: люди, знающие эти секреты; материальные объекты.Гос. Тайна-гос секреты, раз-глашение которых может повлечь тяжкие после-я для нац без-ти,а также соз угрозу для прав и свобод граж-дан.Служебная тайна- может нанести ущерб без-ти, обороно-ти и тд3 степени секретности: особой важно-сти, совершенно секретно, секретно.3 формы допуска: 1(особой важности),2, (совершенно секретно), 3(секретно)сновные правовые акты:- “Концепция национальной без-ти РБ”-‘Закон РБ об информации, информатизации и защите информации’-‘Закон РБ об электронной цифровой подписи’-‘ Закон РБ о гос секретах’-Закон РБ об органах гос. без-ти.-ОАЦ при президенте РБ

**6Технические каналы утечки информации**

Информация передается полем или веществом. Это может быть либо акустическая волна, либо электро-магнитное излучение, либо лист бумаги с текстом и т.п. Другими словами, используя те или иные физи-ческие поля, человек создает систему передачи ин-формации или систему связи.Утечка - бесконтроль-ный выход конфиденциальной информации за пре-делы организации или круга лиц, которым она была доверена.Утечка (информации) по техническому каналу - неконтролируемое распространение инфор-мации от носителя защищаемой информации через физическую среду до технического средства, осу-ществляющего перехват информации Техн канал-совокупность источников конф-ой инф, среды распр-я и средства разведки.Источники конф-ой информа-ции: человек, эл. оборудование, внешний вид соору-женийСредства распространения …. инф-воздушная среда-здания, сооружения-электрические цепиСред-ства тех. разведки-визуально-оптические (бинокль) -опто-электронные-акустические-радиоперехвата (ра-дио, сотовая связь)-фотографические -электронные (для перехвата сигнала …..)По физическим принци-пам возникновения, каналы связи делятся на 4 типа: акустические, мат-вещественные, визуально-оптические, электромагнитные

**7Акустические каналы утечки инф. Закладные устройства.**

Звук - механические колебания частиц упругой сре-ды, субъективно воспринимаемые органом слуха. Так как звук, по сути, является волной, его основными ха-рактеристиками являются амплитуда и спектр ча-стотЗвуковое давление - это переменное давление в среде, обусловленное распространением в ней звуко-вых волн.Делятся на типы: прямой акустич, вибро-акустические, акусто-электрические, акусто-оптические, параметрическиеВ акустическом канале утечки носителем инф от источника к несанкционир получателю явл акустическая волна в атмосфере, во-де и твердой среде. Источниками ее могут быть: го-ворящий человек, речь которого подслушивается в ре-альном масштабе времени или озвучивается звуко-воспроизводящим устройством; механические узлы механизмов и машин, которые при работе издают акустические волны.Закладные устройства создают-ся специально для подслушивания речевой информа-ции и обеспечивают повышения дальности составного акустического канала до единиц км и возможность съема информации злоумышленником за пределами контролируемой зоны. Закладное устройство как ретранслятор является более надежным элементом канала утечки, чем источник опасного сигнала, так как процесс образования канала утечки информации на основе закладки управляем злоумышленником.

**8Электромагнитные каналы утечки инф.**

Делятся на группы: электрические, индукционные, параметрическиеВ электромагнитных каналах утечки информации носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами.**Параметрические каналы**Перехват инф возможен путем «высокочастотного облучения» ТСПИ. При взаимодействии облучающего э/м поля с эл-ми ТСПИ происходит переизлучение э/м поля. В ряде случаев это вторичное излучение имеет модуляцию, обусловленную воздействием инф сигнала.Для перехвата инф по данному каналу необх спец высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства.**Электрические каналы**Электрические каналы утечки информации возникают за счет:- наводок э/м излучений ТСПИ на соединит линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;- просачивания инф сигналов в линии электропитания и цепи заземления ТСПИ;- использования закладных устройств.**Индукционные**Спецслужбы наиболее часто используют индуктивный канал перехвата инф, т.к. он не требует контактного подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи э/м поля при прохождении по нему инф электрических сигналов, которые перехват спец индукционными датчиками Индукц датчики испол в основном для съема инф с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществ частотное разделение каналов, и инф, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на спец магнитофон. Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные низкочастотные усилители, снабженные магнитными антеннами. Некоторые средства бесконтактного съема информации, передаваемой по каналам связи, могут комплексироваться с радиопередатчиками для ретрансляции в центр ее обработки.

9**Утечка инф по цепям заземления электропитания**

Циркулирующая в тех или иных технических средствах конфиденциальная информация может попасть в цепи и сети электрического питания и через них выйти за пределы контролируемой зоны. Например, в линию электропитания высокая частота может передаваться за счет паразитных емкостей трансформаторов блоков питания.Цепи заземления выходят за пределы помещений и зданий и по этой причине могут служить причиной утечки инф. Опасные сигналы в цепях заземления возникают за счет наводок ЭДС полями побочных ЭМИ, а также за счет протекания тока по контуру заземления. Опасный сигнал может быть снят с цепи заземления индуктивным способом или с сопротивления, включенного в цепь заземления.Для предотвращения утечки инф по цепям заземления применяются меры, направленные: на уменьшение сопротивления заземления; на уменьшение площади магнитных рамок, образуемых цепями заземления; При выборе схемы заземления следует помнить, что лучшие результаты дает многоточечное заземление. Последовательное заземление, напротив, дает наибольший коэффициент гальванической паразитной связи.Цепи электропитанияСуществует 4 причины появления опасных сигналов в цепях электропитания.1 причиной является наведение в них ЭДС полями НЧ и ВЧ побочных излучений отдельными техническими средствами связи.Учитывая, что в современных зданиях кабели питания и линии высокочастотной передачи прокладываются в специальных каналах, их близкое расположение делает проблему устранения наводок весьма актуальной.2 причина обусловлена модуляцией тока электропитания токами радиоэлектронного средства.3 причина: опасный сигнал может попасть в цепи электропитания через паразитные индуктивные и емкостные связи, например, силового трансформатора питания, практически без ослабления.4 причина связана с применением импульсных блоков питания. В таких блоках выпрямленное напряжение 220 В с помощью электронного ключа (релаксационного генератора) преобразуется в импульсы, частота которых может составлять сотни килогерц. Спектральные составляющие этих импульсов могут являться переносчиками опасных сигналов.

**10Перехват инф в телеф каналах связи**

К зоне «А» относится телефонный аппарат (ТА) абонента. Сигнал с аппарата по телефонному проводу попадает в распределительную коробку (РК) (зона «Б») и оттуда в магистральный кабель (зона «В»). После коммутации на автоматической телефонной станции (АТС) (зона «Г») сигнал распространяется по многоканальным кабелям (зона “Д”) до следующей автоматической телефонной станции (АТС).Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «А», «Б» и «В(первые три на рисунке)Методы: непостредств. подкл-е к линии связи, бесконтактное подкл-е-внедрение в ТА подслу-х утр-ви передающих утр-в (могут распоз-ть голоса и непосредст-о подкл-ся к тлф линии)-прослушивание активных каналов непосредственно в помещении-высокочастотное навязываниеМетоды борьбы: метод выжигания ………..

**11.Пассив. м-д защиты инф. от утечки по тех. кан.**

Пассивн. мд защиты инф. предначены для предотвр или сущ-ого затруднения перехвата инф по тех каналам за счет снижения соотношения с/ш на вх ср-ва тех разветки путем уменьшения ур-ня сигнала. Пассивные методы защиты информации направлены на:ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, беспечивающих невозможность их выделения средством разведки на фоне естественных шумов;исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

**12.Экранирование элекрмагнт. полей. Конструкция экранов электромагнт излучения**

Экранирование электрического поля металлическим заземленным экраном достигается за счет нейтрализации зарядов в экране, вызванных этим полем. В результате этого напряженность электрического поля за экраном уменьшается. Для стекания зарядов с экрана, наводимых электрическим полем, необходимо обеспечить заземление экрана с малым (менее 4 Ом) сопротивлением.При выборе толщины и материала экрана следует руководствоваться также соображениями:- механической прочности, жесткости, стойкости против коррозии,- удобства стыковки отдельных деталей и осуществления между ними переходных контактов с малым сопротивлением,- удобства пайки, сварки и пр.При экранировании магнитного поля заземление экрана не изменяет величины возбуждаемых в экране токов и, следовательно, на эффективность магнитного экранирования не влияет.

**13.Заземление технических средств**

Необходимо помнить, что экранирование ТСПИ и соединительных линий эффективно только при правильном их заземлении. Поэтому одним из важнейших условий по защите ТСПИ является правильное заземление этих устройств.   
     В настоящее время существуют различные типы заземлений. Наиболее часто используются одноточечные, многоточечные и комбинированные (гибридные) схемыОсн. требования1)Система заз включ:общ заземлитель, заземл кабель, шины, провода2) Сопр-е заземл пр-ов д б минимальным3) Каждый прибор д б соединен с заземл магистрлью с помощью отдельного контура4) В цепи должны отсутствовать замкн контуры5)Послед-оеподкл уос-в к заземл маг-ми запрещено6)тдлина пр-ов не должна превышать 0,02, L<0,02, f=50гц ,

**14. Звукоизоляция технических средств**

**Звукоизоляция –**это процесс снижения уровня шума как исходящего из помещения, так и поступающего из вне. Уровень шума измеряется в децибелах.**По характеру спектра шум следует подразделять на:**широкополосный с непрерывным спектром шириной более одной октавы; тональный, в спектре которого имеются выраженные дискретные тона. Методы:- В качестве перекрытий нужно использовать. акуст-неоднородные конструкции**-** В качестве полов жел-но исп констр. на упругом основании или констр, утсановл на виброизолятр- потолки жел-но сдел-ть подвесными- В качестве стен исп. многослойные акуст-неоднород конструкции с упругими прокладкамиМеханизм прохож-я волн через препядствия-окна, двери, щели и др(воздушный перенос)-через мат-л стен, по трубам (путем матер переноса)-через мат-л стен и перегородок (путем мембранного переноса) Общ св-ва звукопоглощающих мат-ов:-явл пористыми-имеют малую удельную массуИсп-е многосл-е мат-лов с защитными св-миПо форме бвают:-штучные (блоки, плиты)-рулонные (прокладки, холсты)-рыхлые и сыпучие (шлак)По вел-не относительного сжатия-мягкие (Б70 кг/м^3)-полужесткие-жесткие (300-400 кг/м^3)Отдельную группу составл резонансные поглотителиСкладные акустические экраны

**15.Активные мд защ инф по тех каналам**

Предназначены для предотвращения или сущ-го затруд-я передав инф по тлф каналам за счет снижения соотношонеия с/ш навх ср-ва техн разведки путем увеличения уровня шума Активные методы защиты информации направлены на:создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.

**16.Акустическая маскировка**

Акуст маскировка обеспечивает: неузнаваемость голоса диктатора, сущ-ное снижение разборч. речи диктора, скрытность самого факта передачи реч инфКлассификация:-Изменение голоса: сохранение естественности звучания на основе хар-к голоса говорящих, сохр ест-ти звуч-я на основе хар-к заданного голоса образца, без сох-ти ест-ти звучания-технич закрытие: микширование реч сигнала с помехой , модификация фонет ф-ции, комбинир мд-Скрытая передача и маскировка: в аналог сигнале разл природы, в массивах данных, в форматах дан.Стенография- сп-б передачи инф с учетомскрытия самого факта передачи информацииБелый шум-шум, который по частоте расположен равномернобелый” шум — имеет равномерный спектр в полосе частот речевого сигнала;Виды акустических помех: белый шум, “окрашенный ”шум, “ речеподобные” сигналыокрашенный” шум — формируется из “белого” в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала“речеподобные” помехи — формируются путем микширования в различных сочетаниях отрезков речевых сигналов и музыкальных фрагментов, а также шумовых помех, или формируется из фрагментов скрываемого речевого сигнала при многократном наложении с различными уровнями.Основные требования: -временные, спектр, корреляционные хар-ки помех д.б. близки соотв хар-ками полезного согнала-ср-ва созд помех должны обеспеч тебуемое превыш над полезным сигналами-эл-ты крепления мех преобразователей не должны сущ искажать помехи сигнала.

**17.Электромагнитная маскировка**

Этот метод основан на создании активных маскирующих помех (как правило, шумовых) в заданном диапазоне частот и реализуется с помощью систем активной защиты. Такие системы подразделяются на системы линейного и пространственного зашумления.- линейного зашумления (провода, кабели )-пространственного зашумления *Системы линейного зашумления* применяются для маскировки опасных сигналов в проводах, кабелях, различных токоведущих линиях и конструкциях, выходящих за пределы контролируемой территории. Объектами линейного зашумления являются, например, провода, цепи и устройства технических средств, подверженные воздействию низкочастотных электромагнитных полей, возникающих при работе ТСОИ, а также элементы и устройства, обладающие свойствами электроакустических преобразователей.*Системы пространственного зашумления* применяют для создания маскирующих помех в окружающем пространстве .В состав системы входят:– генераторы шумового сигнала;– усилители, обеспечивающие необходимую мощность шумового сигнала в заданном диапазоне частот;– антенны;– устройства коммутации и контроля.Цель зашумления считается достигнутой в том случае, когда отношение опасный сигнал/шум на границе контролируемой территории в окружающем пространстве или в токоведущей линии уменьшается до требуемого уровня, не позволяющего средствам перехвата качественно решать задачи обнаружения и анализа опасного сигнала. Способы размещения и подключения систем линейного и пространственного зашумления определяются особенностями схемного решения, расположения и монтажа защищаемых объектов и средств зашумления.

**18.Обнаружение закладных устройств**

Речевая информация, циркулирующая в помещении, может негласно транслироваться за его пределы при помощи ЗУ.Закладные устройства занимают ведущее место среди средств технического шпионажа. Для повышения скрытности работы мощность передатчика ЗУ делается небольшой, но достаточной для перехвата высокочувствительным приемником с небольшого расстоянияВиды ЗУ: Радиомикрофоны-С автономным питанием- с питанием от тлф линии-с пит от сети 220В-с дистанционным управлением- с автоспуском- полуактивные -с накоплением информации2) Электронные уши проводные микрофоны - микр стетоскопы-с остр диаграммой напряженности3) Лазерные микрофоны 4)Гидроакустические микрофоныУст-ва перехвата: посредственные и непосредственные,подкл через индукт датчики, встраиваемые, микровидеосистемы Иногда рабочую частотц располагают вблизи мощн местной радиостанцМикрофоны камуфл-ся спец оразом и имеют дистанционные включателиМикрофоны: встроенные и выносныеПит-е: от сети электроп, от тлф кабеля, по радиоканалОсновные методы поиска ЗУ- поиск с использованием техн ср-в-изменение пар-ов линий электропитания-проведение тестового разгона тлф аппаратовКлассификация работ по поиску ЗУПо хар-ру выполненных работ-разовая проверка (перед провед важн переговор.)-профилактическая-конспиративная (в случ явн утечки данных)-послепроверочная консультация2) по глубине проверки (4 уровня): слабый, …, высокий

**19.Техниеские ср-ва обнаружения закладных ус-в**

Индикаторы э/м излучений сост из: антенна, микрополосный усилитель, амплитудный детекторИндикаторы частотомеры -)Низкая чувствительность3) нелинейные локаторы (могут нах-ся в выкл сост)Используются для физического обнаружения и определения местоположения скрытно размещенных электронных устройств, которые могут находиться в выключенном состоянии4)Анализаторы спектра5)Сканирующие радиоприёмникиСовременные сканеры могут автоматически перестраиваться в диапазоне до нескольких ГГц и обнаруживать сигналы с различными видами модуляции (рис. 5.11). Эти изделия можно разделить на две группы. Первые обладают уникальными параметрами, однако их размеры, масса и, главное, стоимость весьма высоки.**Компьютерные программы управления сканерами.** Большинство современных сканеров можно подключить к компьютеру, который значительно расширяет возможности управления, отображения и хранения информации об исследуемых сигналах7) ТепловизорыТехническое средство, обеспечивающее преобразование электромагнитного излучения (теплового), излучаемого различными объектами в видимое изображение

**20.Инж-тех защ объектов от несанкцион доступа**

Инженерно-техническая защита (ИТЗ) по определению -это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.По функциональному назначению средства инженерно-технической защиты делятся на следующие группы: физические средства, аппаратные средства, программные средства, криптографические средства*Аппаратные средства* и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы.*Программные средства* и методы защиты: надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных.*Криптографические методы* занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды.

**21. Категорирование объектов.**

*Категория охр. объекта* – комплексная оценка состояния объекта, учитывающая его экономическую или иную (например, культурную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны.Категории:*А* – особо важные объекты (ущерб – особо крупный или невосполнимый: экологическая катастрофа, гибель большого числа людей, полит. последствия, утечка государственных секретов и т.д.). Выход за пределы территории и не м.б. локализированы (хр-ща банков, пред-я по хранению или произ-ву токс-ых, взрыв-ых и других опасных веществ, пред-ие оборонного профиля).*Б* – важные объекты (значительный материальный ущерб, угроза здоровью или жизни людей, утечка гос-ых секретов). Не выходит за пределы территории (касс. залы банка, инкассаторские машины, крупные торговые центры).*В* – прочие (материальный или финансовый ущерб, информационный ущерб). Носит локальный характер (магазин, служ-ые пом-я, жилые пом-я и др.).Категорирование объектов позволяет систематизировать разнообразные требования к объектам физической защиты и сформулировать их в виде нормативов. По этому, это должно стать одной из первоначальных задач, которые предшествуют процессу построения комплексной защиты объектов.

**23. Инженерные заграждения.**

Заграждение в составе системы охраны периметра объекта выполняет роль преграды, изменяющей условия передвижения нарушителя по направлению к охраняемому объекту.*Инжен. загражд.* – переграда, изменяющая условия передвижения нарушителя по направлению к охраняемому объекту.По назначению:Основные (препятствующие свободному входу нарушителя на территорию).Дополнительные. предназначены для повышения укрепленности основных огражденийПредупредительные (устанавливаются с внутренней стороны с вывеской запрещающих надписей).Виды:сигнализациисигн. - электриз. (электрошок)строительныестроительно – сигнализационные*Сигнализац.* – провод. металлич. конструкции, два провода которых являются чувствительными элементами.Важным звеном явл-ся зона отчуждения – полоса грунта шириной 3 метра, предназначенная для системной охраны, в том числе и в грунте.Часть зон отчуждения может оборудоваться контр. – след. полосой.

**24. Технические средства охраны периметра объекта.**

**Техническое средство охраны**– вид техники, предназначенный для использования силами охраны с целью повышения эффективности обнаружения наруштеля и обеспечения контроля доступа на объект охраны.Предназначение:Для эффективного обнаружения объекта- эффективность обнаружения- контроль доступаКритерии:Возможность раннего обнаружения.Точное следование контурам периметра.Отсутствие мертвых зон.Скрытая установка датчиков системы.Независимость параметров системы от сезона и погодных условий.Невосприимчивость к внешним факторам «нетревожного» помехоприема.Устойчивость к мощным магнитным полям.*Чувствительный эл-т* – часть управляющего устройства, предназначенная для восприятия воздействующей величины, на которую реагирует чувствительное управляющее устройство.*Чувствительная зона* – участок, появление которого на объекте обнаружения вызывает повышенный сигнал.- РВСО (рад. – волн. ср-ва обнаружения)- РЛСО (радиолуч. ср-ва обнаружения)От зависимости принципа действия:ПассивныеАктивныеПо констр. исполнению:Однопозиционные средства обнаружения.Двухпозиционные средства обнаружения.Имеют круговую диаграмму напряженности.Оптические средства обнаружения (исп-ся для блокирования помещений, коридоров и др.). Исп-ся в ИКСО.Пассивн. ИКСО:Обладает высоким качеством обнаружения и помехоустойчивостью.Удобны в эксплуатации.Экономичны.Экологически безопасны.Не создают помех другим средствам эл. техн.*Сейсмические ср. обнар*. – эти средства регистрируют колебания, возникающие в грунте. Предназначены для блокировки протяж. участков объекта.

**25. Охранное телеидение**

**.** Сист. *охранного телевидения* или видеонаблюд. – совок-ть элект-ых уст-тв, предназнач. для ведения непрерывного наблюд. и записи видеоинф-ии об обстановке в той или иной части объекта, что необход. для обеспеч. безоп-ти и осущ-ния контроля за деят-тью сотрудников. Функции: обнаружение. и идентификация.Обнаружение на охраняемой территории объектов сводится к предоставлению оператору визуальной информации, либо выработке автоматическим устройством сигнала тревоги при обработке соответствующих видеосигналов.*Идентификация* – установление тождественности неизвестного объекта, достоверность.Если в качестве РУ выступает человек, то на выходе анализ устройства должно присутствовать изображение.Идентификация наиболее важна при анализе видеозаписейСпособы представления визуальной информации:ПараллельныйПлюсы: простота, низкая ст-ть выс. жив-ть системы.Минусы: невозможно осуществить видеозапись со всех камер.Последовательный.Плюсы: стоимость ниже, простота, относит. потери качества изображения вызваны оцифровкой.Минусы: работа только одного канала.*Неконтр. время* – промежуток времени, в котором сигнал с данной видеокамеры не поступает на экран монитора.Использ квадраторов:Плюсы: практ. отс. потеря инф-ии, возможность изобр. с одной видеокам. выв. на всю площадь монитора.*Видеомультиплексер* – одновременная запись сигнала от нескольких видеокамер.

**26. Системы контроля и управления доступом.**

*СКУД* – это объед в компл техн ср-ва, обесп воз-ть дост опр лиц в опред зоны (террит здания, помещения или к опред аппаратуре) к техн ср-вам, огранич доступ лиц, не имеющего такого права.— совокупность программно-аппаратных технических средств [безопасности](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C), имеющих целью ограничение и регистрацию входа-выхода объектов (людей, [транспорта](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82)) на заданной территории через «точки прох да»: [двери](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%B5%D1%80%D1%8C), [ворота](https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D1%80%D0%BE%D1%82%D0%B0), [КПП](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C%D0%BD%D0%BE-%D0%BF%D1%80%D0%BE%D0%BF%D1%83%D1%81%D0%BA%D0%BD%D0%BE%D0%B9_%D0%BF%D1%83%D0%BD%D0%BA%D1%82" \o "Контрольно-пропускной пункт).Состав:Устройство ввода идент пр-ков.Устройство упр.Исполн устройства.Способы ввода идент-ра:Ручной.Контактный.Бесконтактный.*Аутентификация* – проверка подлинности субъекта.По способу упр прегражд устройства:- автономные (локальные)- централизованные (сетевые)- универсальные*Автономия* – обеспечение контроля и доступа в конкреном помещении.Сост:- авт контроллер (хр базу данных авт индефикаторов)- э/м замок- датчики положения двери- счит-ль для устр-ва идентифик- кнопка откр двери изнутриСетевые: для упр дост прим турникеты и шлюзовые кабины.

**27. Криптографическая защита информации.**

*Криптография* – наука о методах, алгоритмах, прогр и апп ср-вах преобраз инф-ции в целях сокрытия ее содерж, предотвр изм или несанкц использования.*Криптология* – наука об иссл стойкости исп криптопреобраз.*Криптографическая защита инф-ции* – деят-сть, направл. на обеспеч. конфиденциальности, контроля целостности и подлинности инф-ии с использ. [средств криптографической защитыинф-ии](https://ru.wikipedia.org/wiki/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F).К ср-вам криптографической защиты инф-ии относ. технич., программные, программно-аппаратные ср-ва защиты инф-ии, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также ф-ции управл. криптографическими ключами, мех-мы идентификации и аутентификации.

**28. Основы построения криптосистем.**

Под *шифром* понимают совок-ть процедур и правил криптографических преобраз., использ. для зашифровывания и расшифровывания инф-ии по ключу шифрования. Под *зашифровыванием информации* понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования наз. *расшифровыванием* (дешифрованием).

Исходный текст передаваемого сообщения (или хранимой информации) М зашифровывается с помощью криптографического преобразования *Е*с получением в результате *шифр-текста* С.Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифровывания. Соответственно различают два класса криптосистем:  
• симметричные криптосистемы (с единым ключом);  
• асимметричные криптосистемы (с двумя ключами).

**Криптография** – наука о методах, алгоритмах, про/граммных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования.Исторически сложилось так, что криптография длительное время использовалась исключительно как средство обеспечения конфиденциальности сообщений. Областью применения криптографии была область защиты государственной тайны: в военной, дипломатической и разведывательной сферах. Поэтому естественно, что криптография находилась в руках спецслужб. Всякие упоминания об этой науке в открытой печати были запрещены, хотя работы велись полным ходом, огромное число специалистов трудилось в этой области: математики, инженеры, разведчики. Наряду с решением задач обеспечения конфиденциальности, целостности и доступности информации существует задача анализа стойкости используемых криптопреобразований. Эта задача решается наукой, называемой *криптоанализ*. *Криптография* и *криптоанализ* составл. науку: **криптологию**.

**29. Симметричные криптосистемы.**

*Шифр* – совокупность обратимых преобразований множества откр данных на мн-во зашифр данных, задаваемых ключом и алгоритмом преобразования.

*Ключ* – конкр секр состояние некоторых пар-ов алгоритма, обеспечивающих выбор одного варианта из всех возможных.

*Симметричные криптосистемы* — способ шифрования, в котором для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [расшифровывания](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BA%D0%B0) применяется один и тот же криптографический [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)). До изобретения [схемы асимметричного шифрования](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC) единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Основная хар-ка шифра – крипкостойкость.Требования к шифрам:Достаточная крипкостойкость.Простота шифрования и расш.Незнач избыт инф за счет шифрования.Нечувстительность к небольшим ошибкам шифрования.

В той или иной мере данным требованиям удовлетворяют некоторые шифры: - шифры перестановки- шифры замены- гаммирования- основаны на аналитических преобразованиях данных

*Шифр подстановки* – символы текста заменяются другими символами из данного алфавита.

*Шифрование гаммированием* заключается в том, что символы шифру-емого текста складываются с символами некоторой случайной последова-тельности, именуемой гаммой шифра*.*

Стойкость шифрования определяется в основном длиной (периодом) непо-вторяющейся части гаммы шифра

Шеннон утверждал, что в практ шифровании исп 2 принципа: рассеивания и перемеш.

*Рассеивание* представляет собой распр влияния одного символа открытого текста на много символов шифротекста, что позволяет скрыть стаиистические свойства открытого текста.

*Перемешивание* предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статист свойств открытого и шифрованного текста.

**30. Асимметричные криптосистемы.**

Асимметричные криптографические системы были разработаны в 1970-х гг. Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последующего расшифровывания используются различные ключи:• *открытый ключ К* используется для шифрования информации, вычисляется из секретного ключа *к*;•

*секретный ключ к* используется для расшифровывания информации, зашифрованной с помощью парного ему открытого ключа *К*

.Эти ключи различаются таким образом, что с помощью вычислений нельзя вывести секретный ключ *к* из открытого ключа *К*. Поэтому открытый ключ *К* может свободно передаваться по каналам связи.Асимметричные системы называют также *двухключевыми криптографическими системами*, или *криптосистемами с открытым ключом*.Для криптографического закрытия и последующего расшифровывания передаваемой информации используются открытый и секретный ключи получателя *В* сообщения.В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровывания — его секретный ключ.Секретный и открытый ключи генерируются попарно. Секретный ключ должен оставаться у его владельца и быть надежно защищен от НСД). Копия открытого ключа должна находиться у каждого абонента криптографической сети, с которым обменивается информацией владелец секретного ключа.

**31. Политика безопасности.**

Это набор законов, правил и практ рекомендаций, на основе которых стр упр, защита и распространение критичной информации в системе.Реализуется при помощи орг мер и прогр-техн ср-в, опред арх-ру в системе защиты.Политика безпасности для каждой организации индивидуальна. Зависит от исп прогр и техн ср-в, назн-я орг и т д.*Сист* – нек сов-ть субъектов и объектов.*Субъект* – акт компонент системы, кот может явиться прич потока информации к субъекту или изм сост системы.**Объект** – пассивный компонент системы, хранящий, принимающий или передающий информацию.*Доступ к объекту* – дост к содерж в нем информации.Основой политики безопасности составляет способ управления доступом.Сущ 2 вида политики без-ти:- *избирательная* (основой явл избирательное управление, кот подразумевает, что: все субъекты и объекты системы должны быть идентифицированы; права доступа субъекта к объекту сист опред на основ некот правила)- *полномочная* (или мандатная, основу сост полномочное управление доступом, кот подраз, что: все субъеты и объекты сист должны быть однозначно идентиф; каждому объекту сист присвоена метка критичности, опред ценность сожерж в нем инф-ии; каждому субъекту сист присвоен уровень прозрачности, опред максимальное знач метки критичности объектов, к кот субъект имеет доступ).

**32. Обеспечение безопасности в системах электронной коммерции.**

*Угроза безопасности* – это совокупность условий и факторов, создающих опасность жизненно важным интересам, то есть угроза представляется некой совокупностью обстоятельств (условий) и причин (факторов). С юридической точки зрения, понятие «угроза» определяется как намерение нанести зло (ущерб). Поэтому для их ослабления, нейтрализации и парирования создается система обеспечения безопасности.*Обеспечение безопасности* – это особым образом организованная деятельность, направленная на сохранение внутренней устойчивости объекта, его способности противостоять разрушительному, агрессивному воздействию различных факторов, а также на активное противодействие существующимвидам угроз.Принципы создания и функционирования системы обеспечения безопасности можно разбить на три основные блока:- общие принципы обеспечения защиты;- организационные принципы;- принципы реализации системы защиты**Общие принципы обеспечения защиты:***Принцип неопределенности*обусловлен тем, что при обеспечении защиты неизвестно, кто, когда, где и каким образом попытается нарушить безопасность объекта защиты.*Принцип невозможности создания идеальной системы защиты* следует из принципа неопределенности и ограниченности ресурсов, которыми, как правило, располагает система безопасности.*Принцип минимального риска*заключается в том, что при создании системы защиты необходимо выбирать минимальную степень риска, исходя из особенностей угроз безопасности доступных ресурсов и конкретных условий, в которых находится объект защиты в любой момент времени.*Принцип защиты всех от всех*предполагает необходимость защиты всех субъектов отношений против всех видов угроз.**Организационные принципы:***Принцип законности,* важность которого трудно переоценить в условиях возникновения новых правоотношений в российском законодательстве – «частная собственность», «интеллектуальная собственность», «коммерческая тайна» и др. Однако нормативная правовая база, регламентирующая вопросы обеспечения безопасности, пока несовершенна.*Принцип персональной ответственности* предполагает ответственность каждого сотрудника фирмы за обеспечение режима безопасности в рамках своих полномочий. Ответственность за нарушение режима безопасности должна быть заранее конкретизирована и персонифицирована.*Принцип разграничения полномочий*позволяет снизить вероятность нарушения коммерческой тайны или нормального функционирования предприятия, так как она прямо пропорциональна количеству осведомленных лиц, обладающих информацией. Поэтому никого не следует знакомить с конфиденциальной информацией, если этого не требуется для выполнения его должностных обязанностей.*Принцип взаимодействия и сотрудничества*предполагает наличия на предприятии доверительных отношений между сотрудниками на основе понимания всеми необходимости выполнения мероприятий обеспечения безопасности информации в своих же собственных интересах.**Принципы реализации системы защиты:***Принцип комплексности и индивидуальности* предполагает обеспечение безопасности совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям.*Принцип последовательности рубежей*позволяет своевременно обнаружить и посягательство на безопасность и организовать последовательное противодействие угрозе в соответствии со степенью опасности.*Принцип защиты средств защиты*является логическим продолжением принципа защиты всех от всех. Иначе говоря, любое мероприятие по защите само должно быть соответственно защищено. Например, средство защиты от попыток внести изменения в БД должно быть защищено программным обеспечением, реализующим разграничение прав доступа

**33. Противодействие атакам в информационных системах.**

В последние годы частота несанкционированных воздействий на информационные системы (ИС) постоянно увеличивается, что неминуемо приводит к огромным финансовым и материальным потерям. Известно, что в последние несколько лет защита ИС от внутренних нарушителей преимущественно обеспечивается специализированными средствами разграничения доступа пользователей к информационным ресурсам. При помощи этих средств каждому пользователю назначаются определённые права, в соответствии с которыми ему разрешается (или запрещается) локальный доступ к информации, хранящейся в его компьютере, или же удалённый доступ по каналам связи к информации, имеющейся на других компьютерах.И всё же приходится констатировать, что этот подход не решает всей проблемы защиты информационных ресурсов от злоумышленников, действующих изнутри ИС.Таким образом, обеспечение эффективной защиты от внутренних нарушителей информационной безопасности требует использования дополнительных средств защиты, таких как системы активного мониторинга рабочих станций, а так же системы обнаружения атак. Рассмотрим эти типы средств защиты более подробно.Системы обнаружения атак предназначены для выявления и противодействия сетевым атакам злоумышленников. Системы обнаружения атак представляют собой специализированное программно-аппаратное обеспечение с типовой архитектурой, включающей в себя следующие компоненты:модули-датчики для сбора необходимой информации о сетевом трафике ИС;модуль выявления атак, выполняющий обработку данных, собранных датчиками, с целью обнаружения информационных атак;модуль реагирования на обнаруженные атаки;модуль хранения конфигурационной информации, а также информации об обнаруженных атаках;модуль управления компонентами системы обнаружения атак.Учитывая тот факт, что на протяжении длительного времени эта задача решалась лишь при помощи средств разграничения доступа, поэтому полностью обеспечить защиту ИС от внутренних нарушителей не представлялось возможным. Это связано с тем, что функциональные возможности этих средств не позволяют защитить ИС от внутренних сетевых атак, а также тех действий внутренних пользователей ИС, которые напрямую не связаны с нарушением правил разграничения доступа к информационным ресурсам ИС. Совместное использование систем обнаружения атак и систем активного мониторинга позволит комплексно подойти к вопросу защиты от внутренних атак и значительно повысить уровень информационной безопасности ИС.

**34. Электронная цифровая подпись.**

Электронная цифровая подпись для электронных документов играет ту же роль, что и подпись, поставленная от руки в документах на бумаге: это данные, присоединяемые к передаваемому сообщению, подтверждающие, что владелец подписи составил или заверил это сообщение. Получатель сообщения с помощью цифровой подписи может проверить, что автором сообщения является именно владелец подписи и что в процессе передачи не была нарушена целостность полученных данных. При разработке механизма цифровой подписи возникают следующие задачи: - формирование подписи таким образом, чтобы её невозможно было подделать; - обеспечение возможности проверки того, что подпись действительно принадлежит указанному субъекту; - предотвращение отказа субъекта от **сво**ей подписиПри создании цифровой подписи по классической схеме отправительдолжен выполнить следующие действия.1. Вычислить хеш-образ m исходного сообщения M при помощи хеш-функции h.2. Вычислить цифровую подпись S по хеш-образу сообщения с использованием секретного ключа Kс создания подписи.3. Cформировать новое сообщение (M, S), состоящее из исходного сообщения и добавленной к нему цифровой подписи.Получив подписанное сообщение (M’, S), получатель должен выполнить следующие действия (принятое сообщение обозначено как M’ по причине того, что оно могло быть преднамеренно либо случайно искажено в процессе передачи по каналу связи и может не совпадать с отправленным).Вычислить хеш-образ m’ сообщения M’ при помощи хеш-функции h.С использованием открытого ключа проверки подписи (Kо ) извлечь хеш-образ m сообщения из цифровой подписи S.18Сравнить вычисленное значение m’ с извлеченным из цифровой подписи значением хеш-образа m. Если хеш-образы совпадают, то подпись признается подлинной

**35. Интеллектуальная собственность. Основные понятия. Классификация.**

*Интеллект собственность* – термин, опис произв-я арх-ры, лит-ры, кот явл немат при их созд, но потом становятся ценностями в материальной форме.*Объект мат собст* – охраноспособный результат интеллектуальной деятельности.*Инт товар* – продукт инт собств, кот может продаваться за деньги.*Инт потенциал* – способность накапл новые знания.1623 год – первый патент.1790 год – патентный закон в США.1812 год – патент в России.1830 год – патент в Беларуси.Классификация:- промышл собственность- авторские праваОбъекты авт права охраняются законом РБ (произведения науки, лит-ры и искусства, произведения архитектуры и декоративно прикладного искусства, программы ЭВМ), объекты смежных прав (права использования фоногр, передачи каб телевидения)Объекты пром собст охраняются законом РБ о патентах на изобрет полезн модели, пром образцы (изобр, к кот относ устр-ва, пром образцы, селекц достиж, топология ИМС, секреты пр-ва, фирм наименования, тов знаки и зн обслуж, геогр ук-я).

**36. Авторское право и смежные права.**

*Основная цель охр авторского права* – содействие обогащению и распространению нац.-культурного наследия.В соответствии с законодательством Республики Беларусь авторское право распространяется на обнародованные или необнародованные произведения **науки**, **литературы** и **искусства**, являющиеся **результатом творческой деятельности**, существующие в какой-либо объективной форме.Авт права возн на произведения науки, искусства и лит-ры, возн в силу факта их создания.Объектами охраны могут быть как хорошие произведения, так и плохие. Залож в пр идеи не обяз должно быть новыми, но ф-ма их выраж должна быть оригинальной.Лит пр-я независ от их ф-мы.Научн пр-я – люоые ориг пр-я научн хар-ра.Монография – пр-е на заданную тему (коллективн).Драм и сцен произвед.Хореография.Музык проивед.Аудио/видео прои-яПр-я живописи, грфики, скульптуры.Пр-я дек прикл ис-ва (мебель, одежда, ткани, украшения, игрушки и тд)Пр-я арх-ры, градостр-ва и садово-парк сооружения (квартиры, застройки).Фотогр сооруж.Базы данных.Объектами авт права не явл офиц док-ты, гос символы, произв нар-го творчества, авт кот неизвестно.*Субъектами* авт права явл лица, которые по з-ну принад авт право на то, или иное пр-е.Авт пр-я счит лицо, указ в кач-ве автора на оригинале или экемпляре пр-я, если не док иное.Авт право на совм пр-е принадл авторам совместно.Необход усл признания тех или иных лиц соавторами явл налич соглашения между ними об авторстве. М б выражено в любой форме.Неимущ авт права: - право авт-ва- право на имя (исп-ть пр-е под подлинным именем автора)- на защиту репутации- на обнародованиеИмущ права авторов. Право осущ или разреш след действия:Воспр-е пр-я.Распр ориг или экзепл посредством продажи илиной перед пр-я собств.Прокат оригинала.Импорт.Публ показ оригинала.Публ исп произв.Перед пр-я в эфир.Иное сообщ пр-я для всеобщ сведения.Перевод произв на др язык.Переделка или переработка пр-я.Смежные права – права исп на фонограммы и кабельное вещание.Объекты авт права охраняются законом РБ (произведения науки, лит-ры и искусства, произведения архитектуры и декоративно прикладного искусства, программы ЭВМ), объекты смежных прав (права использования фоногр, передачи каб телевидения)

**37. Промышленная собственность.**

разновидность [интеллектуальной собственности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D0%BB%D0%BB%D0%B5%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BE%D0%B1%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C)Под пром собственность понимают изобретение полезной модели и образца.Объектами охраны промышленной собственности являются: [патенты](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D0%B5%D0%BD%D1%82) на [изобретения](https://ru.wikipedia.org/wiki/%D0%98%D0%B7%D0%BE%D0%B1%D1%80%D0%B5%D1%82%D0%B5%D0%BD%D0%B8%D0%B5), [полезные модели](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B5%D0%B7%D0%BD%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C), [промышленные образцы](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%B5%D1%86), [товарные знаки](https://ru.wikipedia.org/wiki/%D0%A2%D0%BE%D0%B2%D0%B0%D1%80%D0%BD%D1%8B%D0%B9_%D0%B7%D0%BD%D0%B0%D0%BA) и знаки обслуживания, [наименования места происхождения товаров](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D0%B8%D0%BC%D0%B5%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BC%D0%B5%D1%81%D1%82%D0%B0_%D0%BF%D1%80%D0%BE%D0%B8%D1%81%D1%85%D0%BE%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F_%D1%82%D0%BE%D0%B2%D0%B0%D1%80%D0%B0), фирменные наименования, коммерческие обозначения, пресечение недобросовестной конкуренции, топология интегральных схем, селекционное достижение. С 1970-х годов к понятию «Промышленная собственность» относят также «[ноу-хау](https://ru.wikipedia.org/wiki/%D0%9D%D0%BE%D1%83-%D1%85%D0%B0%D1%83)» (секреты производства, производственный опыт).Субъектами права промышленной собственности являются граждане и юридические лица.К их числу относятся:авторыпатентообладателипатентные поверенныеНациональный патентно-информационный центр

**38. Патентные исследования.**

*Патент* – выдаваемый патентным органом от имени гос-ва док-т, кот удостов авт-во, приоритет на объект собств. И прво на его исп-е.*Патентные исследования* – это исследования технического уровня и тенденций развития объектов техники, их патентоспособности, патентной чистоты, конкурентоспособности на основе патентной и иной информации. По своему характеру и содержанию патентные исследования относятся к прикладным научно-исследовательским работам.По своему характеру и содержанию патентные исследования относятся к прикладным научно-исследовательским работам. Патентные исследования проводятся как в виде самостоятельной научно-исследовательской работы, так и в составе работ субъекта хозяйствования.

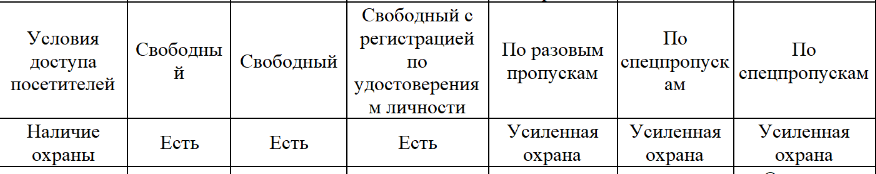
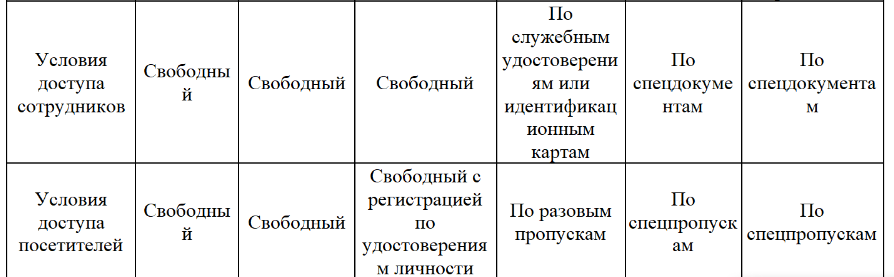
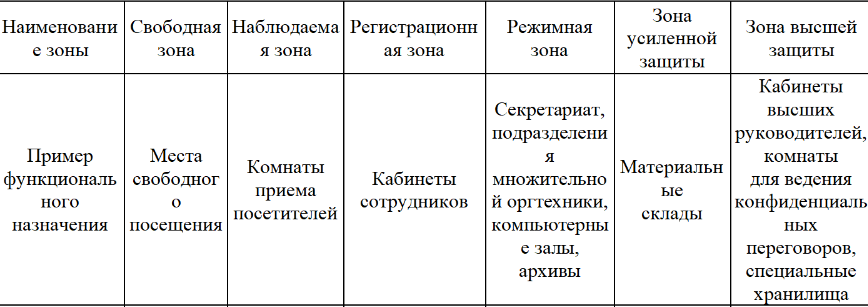
**39. Коммерческое использование объектов интеллектуальной собственности.**

Интеллектуальной собственностью могут владеть юриди­ческие лица, индивидуальные предприниматели, физические лица, причем способы фиксации их прав бывают самые раз­личные. Законодательство Республики Беларусь предусматривает такие способы коммерческого использования объектов интеллектуальной собственности как лицензионный договор, франчайзинговый дого­вор, инжиниринговое соглашение и другие.*Лицензионный договор (лицензия)*– это гражданско-правовое со­глашение (разрешение) о передаче правообладателем (лицензиаром) права на использование объекта интеллектуальной собственности другому лицу (лицензиату) за определенное вознаграждение. Договор имеет юридическую силу после регистрации в Национальном центре интеллектуальной собственности.Лицензионный договор имеет определенную структуру, соблюде­ние которой необходимо для правильного оформления прав на пере­даваемый объект, а также защиты своих прав в процессе использова­ния предмета договора. К существенным условиям лицензионного договора относят: определение терминов, предоставление техниче­ской документации, регулирование улучшений и усовершенствова­ний, распределение гарантий и ответственности, оказание техниче­ской помощи, платежи, обеспечение конфиденциальности, защита передаваемых прав, разрешение споров, арбитраж, применяемое пра­во, срок действия договора и условия его расторжения и прочие. *Франчайзинг (договор комплексной предпринимательской лицен­зии)*определяется Гражданским кодексом Республики Беларусь как договор, в соответствие с которым одна сторона (правообла­датель) обязуется предоставить другой стороне (пользователю) за вознаграждение комплекс исключительных прав (лицензионный комплекс), включающий право использования фирменного наимено­вания правообладателя и охраняемой коммерческой информации, а также других объектов исключительных прав (товарного знака, знака обслуживания и др.), предусмотренных договором, для предпринима­тельской деятельности. Целью франчайзинга является открытие сети одинаковых предприятий по всему миру, которые используют общие подходы, одинаковые способы организации бизнеса, единые техноло­гии. Сторонами договора комплексной предпринимательской лицен­зии могут быть как юридические лица, так и индивидуальные пред­приниматели. Для заключения договора предусматривается письмен­ная форма. Договор подлежит обязательной регистрации.Предметом *договора на оказание инжиниринговой услуг* является предоставление комплекса или отдельных видов услуг инженерно-технического характера (исследование, проектирование, строитель­ство, разработка и освоение новых технологических процессов, по­ставка комплектного оборудования и проч.).

**40. Защита прав авторов и правообладателей.**

Законодательство предоставляет правообладателям возможность подачи апелляций на решения государственных органов, осуществления действий против лиц, нарушающих их права, с тем, чтобы предотвратить дальнейшие нарушения и компенсировать потери, причиненные нарушением. *Субъекты, обладающие правами на защиту*прав - носители этих прав, т. е. сами авторы, их наследники, правопреемники, работодатели авторов в силу создания служебных произведений.*Нарушители прав* - физические или юридические лица, которые не выполняют требования зак-ва. Чаще всего нарушителями оказываются лица, допускающие незаконное использование произведений.Система борьбы с нарушениями авторских состоит из двух элементов:собственно защита, содержанием которой является признание оспариваемого права, восстановление нарушенного права или предоставление денежной компенсации правообладателю. Таким образом, собственно защита может быть осуществлена только методами гражданского права.борьба с нарушениями методами публичного права (административного и уголовного), которая в основном направлена на общую и частную превенцию предусмотренных авторским договором, либо от исполнения договора в целом, скажем, в случае его недействительности.*Форма защиты* - комплекс внутренне согласованных организационных мероприятии по защите субъективных прав и охраняемых законом интересов. Формы защиты подразделяют на:судебные (защита в судах различных уровней)Средством защиты при использовании адм. формы является жалоба или заявление. Содержание жалобы, возражения или заявления на отказ в регистрации объекта промышленной собственности.неюрисдикционные(самозащита).Примером средств самозащиты являются действия, совершаемые в порядке необходимой обороны и крайней необходимости, рассматриваемой области спектр средств самозащиты достаточно узок и сводится в основном к возможности отказа совершать определенные действия интересах неисправного контрагента, например отказаться от внесения в произведение изменений и дополнений. Наряду с правовыми, выделяют технические средства защиты авт. права и смежных прав, введенные в Закон об авторском праве в 2004 г.

**22. Классификация помещений и территории объекта.** К вопросу классификации служебных помещений с точки зрения их безопасности существует несколько подходов. Учитывая, что степень безопасности от перечисленных выше угроз тесно связана прежде всего с режимом пребывания в помещениях сотрудников и посетителей, целесообразно проводить классификацию по степени режимных ограничений и возможности доступа в них. Предлагается все помещения и территорию разбить на шесть категорий или зон.

****