1. Основные понятия и терминология защиты информации

Термин **информационная безопасность** в разных контекстах может иметь различное значение.

В Доктрине информационной безопасности РФ он используется в широком смысле и означает состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В рамках изучаемой дисциплины основное внимание уделяется информационным процессам хранения, обработки и передачи информации вне зависимости от того, на каком языке она закодирована, кто или что является ее источником, и какое психологическое воздействие на человека она оказывает. Поэтому в данной дисциплине термин информационная безопасность будет рассматриваться в узком смысле и означать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [3].

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов,

связанных с использованием информационных систем. Следовательно, угроза информационной безопасности – это оборотная сторона использования информационных технологий. Из этого положением можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно отличаться.
2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие (например: поломка системы, приведшая к перерыву в работе).

К поддерживающей инфраструктуре следует отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций, а также обслуживающий персонал.

Информационная безопасность – многогранная, многомерная область деятельности, в которой успех может принести только системный, комплексный подход. Спектр интересов субъектов, связанных с использование информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Доступность – это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Целостность – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. То есть целостность предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником

информации. Целостность можно подразделить на статическую (неизменность информационных объектов) и динамическую (корректное выполнение сложных действий – транзакций). Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и т.д. Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Конфиденциальность – это защита от несанкционированного доступа к информации. Основным средством обеспечения конфиденциальности является шифрование информации. Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе. Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности

приводит к отказу в доступе к информации, нарушение целостности - к фальсификации информации и, наконец, нарушение конфиденциальности - к раскрытию информации.

2. Классификация угроз информационной безопасности

Под **угрозой информационной безопасности объекта** будем понимать возможные воздействия на него, приводящие к ущербу. К настоящему времени известно большое количество угроз. Приведем упрощенную их классификацию. Угрозы делятся по свойству информации, против которого они направлены:

– физической и логической целостности (уничтожение или искажение информации);

– конфиденциальности информации;

– доступности (работоспособности);

– праву собственности.

По происхождению:

– случайные (отказы, сбои, ошибки, стихийные явления);

– преднамеренные (злоумышленные действия людей).

По источникам:

– люди (персонал, посторонние);

– технические устройства;

– модели, алгоритмы, программы;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Рассмотрим более подробно перечисленные угрозы.

Случайные угрозы обусловлены недост точной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибок персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории над жности, программировании, инженерной пси-хологии и т. д.).

Преднамеренные угрзы связаны с действиями людей. Это и работники спецслужб, хакеры, самого объекта. Огромное количество разнообразных ИО дает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов.

Например, для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если нет никаких мер защиты:

– через терминалы пользователей;

– через терминал администратора системы;

– через удаленные терминалы.

И через нештатные каналы:

– побочное электромагнитное излучение информации с аппаратуры системы;

– побочные наводки информации по сети электропитания и заземления;

– побочные наводки информации на вспомогательных коммуникациях;

– подключение к внешним каналам связи.

Классификация методов защиты информации

Все методы защиты информации по характеру проводимых действий можно разделить на: **законодательные (правовые); организационные; технические; комплексные.**

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнением законов, и собственниками информации. К таким мерам относятся и издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Правовое обеспечение включает в себя:

1) нормотворческую деятельность по созданию законодательства, регулирующего общественные отношения в области защиты информации;

2) исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации, защиты информации органами государственной власти и управления организациями (юридическими лицами), гражданами

Нормотворческая деятельность:

– оценка состояния действующего законодательства и разработка программы его совершенствования;

– создание организационно-правовых механизмов обеспечения защиты информации;

– формирование правового статуса всех субъектов в системе защиты информации и определение их ответственности за обеспечение информационной безопасности;

– разработка организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех категорий информации;

– разработка законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановление права и ресурсов, реализации компенсационных мер

Исполнительная и правоприменительная деятельность:

– разработка процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией; Библиотека БГУИР 18

– разработка составов правонарушений с учетом специфики уголовной, гражданской, административной и дисциплинарной ответственности.

Деятельность по правовому обеспечению информационной безопасности строится на трех фундаментальных положениях:

1) соблюдение законности (предполагает наличие законов и иных нормативных документов, их применение и исполнение субъектами права в области информационной безопасности);

2) обеспечение баланса интересов отдельных субъектов и государства (предусматривает приоритет государственных интересов как общих интересов всех субъектов). Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности);

3) неотвратимость наказания (выполняет роль важнейшего профилактического инструмента в решении вопросов правового обеспечения).

5.Государственное регулирование в сфере защиты информации

Государственная политика обеспечения информационной безопасности исходит из положений Концепции

национальной безопасности Республики Беларусь.

Система информационной безопасности является составной частью общей системы национальной безопасности

страны и представляет собой совокупность взаимодействующих субъектов обеспечения национальной безопасности и средств, используемых ими для осуществления деятельности по защите

и реализации национальных интересов Республики Беларусь и обеспечению

безопасности личности, общества и государства.

В систему входят:

– органы государственной власти и управления

– государственные и межведомственные комиссии и советы

структурные и межотраслевые подразделения по защите информации

органов государственной власти и управления

– научно-исследовательские, проектные и конструкторские организации,

выполняющие работы по обеспечению информационной безопасности;

– учебные заведения, осуществляющие подготовку и переподготовку

кадров для работы в системе обеспечения информационной безопасности.

Государственную систему защиты информации Республики Беларусь составляют:

– Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ);

– структурные подразделения по защите информации органов государственного управления, предприятий, организаций и учреждений;

– головные предприятия по направлениям защиты информации;

– сертификационные и испытательные центры, предприятия, учреждения и организации различных форм собственности по оказанию услуг в области защиты информации.

Основными функциями системы информационной безопасности страны являются:

– разработка и реализация стратегии обеспечения информационной безопасности;

– оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности

– координация и контроль деятельности субъектов системы информационной безопасности.

Первоочередные мероприятия по реализации государственной политики информационной безопасности должны включать:

– создание нормативно-правовой базы реализации государственной политики в области информационной безопасности

– анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

– формирование государственной научно-технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах

– создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств информатизации, используемых в государственных органах власти и управления.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных компьютерных системах и сетях являются:

– лицензирование деятельности предприятий в области защиты информации;

– аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

– сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в отношении защищенности информации от утечки по техническим каналам;

– введение территориальных, частотных, пространственных и временных

ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем

управления в защищенном исполнении.

6.ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. классификация

Технический канал утечки информации – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации

Источники конфиденциальной информации:

– человек;

– электронная аппаратура;

– документы (содержание);

– здания и сооружения (внешний вид).

Среда распространения конфиденциальной информации:

– воздушная;

– твердые вещества (строительные конструкции);

– электрические цепи.

Средства технической разведки:

– визуально-оптические (оптические увеличительные приборы);

– оптоэлектронные (телевизионные, приборы ночного видения, тепловизоры и т. д.);

– акустические (закладные устройства, направленные микрофоны, электронные стетоскопы и т. д.);

– радиоперехвата (перехвата сообщений радио-, сотовой связи и т. д.);

– фотографические;

– электронные (для перехвата сигналов в проводных коммуникациях).

По физическим принципам возникновения каналы утечки информации

можно разделить на следующие группы :

– акустический;

– материально-вещественный;

– визуально-оптический;

– электромагнитный.

7. Акустические каналы утечки информации. Закладные устройства.

Области спектра звука, в которых сосредоточивается основная мощность акустического сигнала, называются формантами

Закладное устройство (ЗУ) – автономное устройство для перехвата речевой информации, конструктивно объединяющее микрофон и передатчик

Направленный микрофон – электронное устройство, обладающее высокими чувствительностью и помехоустойчивостью за счет его узкой диаграммы направленности

Перехват информации средствами технической разведки в данном случае может реализовываться за счет применения закладных устройств,

устанавливаемых внутри помещения или при помощи направленных микрофонов, путем перехвата акустических сигналов через открытые окна, двери. В данном случае акустическая волна без существенного ослабления попадает в средство технической разведки. Таким образом, образуется прямой акустический канал утечки информации.

8. Электромагнитные каналы утечки информации.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные электромагнитные излучения (ПЭМИ), которые в той или иной степени связаны с обрабатываемой информацией (электромагнитный канал)

Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой «побочной системе связи», образованной источником излучения, средой и средством перехвата информации.

Электрический канал утечки информации (рис. 3.16) возникает за счет наводок ПЭМИ технических средств обработки информации (ТСОИ) на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны (сеть электропитания, цепи охранной и пожарной сигнализации и т. д.)

Параметрический электромагнитный канал может возникать в процессе облучения ТСОИ побочными электромагнитными излучениями ВТСС,

вследствие чего может произойти переизлучение электромагнитной волны, которое будет содержать информацию, обрабатываемую в ТСОИ.

Утечка информации по цепям заземления и электропитания

Заземлением называется преднамеренное соединение объекта с заземляющим устройством, осуществляемое путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.
Одной из причин попадания опасного (информационного) сигнала в систему заземления является наличие ПЭМИ(побочное элекмагнти излуч) – носителя информационного сиг- нала. Это ПЭМИ будет наводить в расположенной поблизости системе заземления ток опасного сигнала. провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля. На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания

Перехват информации в телефонных каналах связи

Телефонную линию можно разбить на зоны
1) телефонный аппарат. 2)распределительная коробка 3) магистральный кабель
4)автоматическая телефонная станция
В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, практически не отличается
Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «1», «2(наибольшая вероят)» и «3» Непосредственное подключение к линии – это самый простой и распространенный способ подслушивания телефонных разговоров. Подключение может быть: контактным; бесконтактным.
Шунт подслушивающего устройства в зонах «1» и «2» может быть установлен в любом месте, где есть доступ к телефонным проводам или телефонному аппарату: в телефонной розетке или любом другом месте телефонной линии на всем ее протяжении вплоть до распределительной коробки.

В зоне «В» при использовании магистрального кабеля подключение подслушивающего устройства маловероятно. Это связано с тем, что для этого необходимо проникнуть в систему телефонной канализации, т. е. в систему подземных сооружений, состоящую из одной или нескольких объединенных в блоки труб и смотровых устройств (колодцев)

Способы и устройства для перехвата информации в зоне «А»:

внедрение в телефонный аппарат передающих устройств, использую- щих для передачи голоса радиоканал или проводные линии. Такие устройства могут передавать как телефонные разговоры, так и речь в помещении и иметь как автономное питание, так и использовать напряжение телефонной линии;

прослушивание акустических сигналов в помещении при помощи высо- кочувствительных приборов за счет паразитных акустоэлектрических преобра- зований в телефонном аппарате;

прослушивание помещения при помощи «высокочастотного навязыва- ния» телефонного аппарата, когда он сам становится модулятором навязывае- мого сигнала.

Вопрос 11. Пассивные методы защиты информации – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня сигнала.

виды:

1. Экранирование электромагнитных полей,
2. Фильтрация,
3. Заземление технических стредств,
4. Звукоизоляция помещений.

Вопрос 12 .Экранирование электромагнитных полей.

На границе раздела двух сред с различными электрофизическими характеристиками (воздух–металл и металл–воздух) волна претерпевает отражение и преломление, а в толще экрана ввиду его проводящих свойств происходит частичное поглощение энергии электромагнитного поля. Таким образом, электромагнитная волна при взаимодействии с экраном отражается

от его поверхности, частично проникает в стенку экрана, претерпевает поглощение в материале экрана, многократно отражается от стенок экрана и, в конечном счете, частично проникает в экранируемую область.

Конструкции экранов электромагнитного излучения. Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней ПЭМИ средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.

13 Заземление технических средств

Основные требования, предъявляемые к системе заземления, заключаются в следующем:

– система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;

– сопротивления заземляющих проводников, а также земляных шин должны быть незначительными;

– каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления. Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;

– в системе заземления должны, по возможности, отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;

– следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;

– качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и механических нагрузок;

– контактные соединения е должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;

– контактные соединения должны исключать возможность образования игальванических пар для предотвращения коррозии в цепях заземления;

– запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, трубы систем отопления, водоснабжения, канализации и т. д.

Комплексные сопротивления заземляющих проводников должны обладать минимальными активным сопротивлением и собственной индуктивностью. Поэтому заземляющие проводники должны иметь

минимально возможную длину lз, которая значительно меньше длины волны электромагнитного поля λ – источника наводки. На практике должно выполняться условие lз < 0,02 Для уменьшения сопротивления форма и размеры поперечного сечения заземляющих проводников должны выбираться таким образом, чтобы на частоте наводки обеспечивались малые активное и реактивное сопротивления. Сопротивление заземления этих средств не должно превышать 4 Ом.

В целях исключения использования общих проводников в системах различных заземлений можно изолировать друг от друга цепи возврата сигнальных токов, цепи возврата постоянных токов питания и цепи возврата переменных токов питания. В этом случае необходимо построить систему заземления, состоящую из трех независимых контуров, сходящихся в одной точке. Такой подход позволяет оптимизировать каждую заземляющую цепь в отдельности. Например, цепи заземления схем распространения сигналов в диапазоне частот до нескольких мегагерц должны иметь низкое сопротивление и по ним должен течь маленький ток. Заземляющая цепь источников питания постоянного тока должна быть рассчитана на низкое сопротивление, но на значительно больший ток, а заземления источников питания по сети переменного тока должны иметь низкое сопротивление и выдерживать токи в сотни ампер.

14 Звукоизоляция помещений

Защита речевой информации от утечки по акустическим каналам может быть реализована за счет создания защищенных методом звукоизоляции помещений.

Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. У Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам.

Для сплошных, однородных, строительных конструкций ослабление акустического сигнала, характеризующее е качество звукоизоляции на

$$K = 20\lg\ q_{\text{ог}} f\ - 45,7,$$

где $q_{\text{ог}}$ – масса 1 м^2 ограждения, кг;

f – частота звука, Гц.

средних частотах, рассчитывается по формуле

При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:

– в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;

– в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;

– потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;

– в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т. п.).

Прохождение волн через препятствия осуществляется различными путями:

– через поры, окна, щели, двери и т. д. (путем воздушного переноса);

– через материал стен, по трубам тепло-, водо- и газоснабжения и т. д. За счет их продольных колебаний (путем материального переноса);

– через материал стен и перегородок помещения за счет их поперечных колебаний (путем мембранного переноса).

Звукоизоляция помещений обеспечивается за счет использования звукопоглощающих материалов – имеющих сквозную пористость и относительно высокий коэффициент звукопоглощения (более 0,2) и обладающих динамическим модулем упругости не более 150 кгс/см2.

По форме звукопоглощающие материалы разделяют на штучные (блоки, плиты), рулонные (маты, полосовые е прокладки, холсты), рыхлые и сыпучие (вата минеральная, стеклянная, керамзит, шлак).

По величине относительного сжатия (жесткости) звукопоглощающие и звукоизоляционные строительные материалы подразделяются на мягкие, полужесткие и твердые.

Мягкие звукопоглощающие материалы изготавливают на основе минеральной ваты или стекловолокна с минимальным объемом (до 3 % по массе) связующего или без него. К ним относятся маты или рулонные полотна с объёмной массой до 70 кг/м3 , которые обычно применяются в сочетании с защитными перфорированными листовыми экранами (алюминий,

гипсокартон, жесткий ПВХ) или с покрытием пористой плёнкой. Коэффициент звукопоглощения этих материалов на средних частотах (250...1000 Гц) достигает значений 0,7...0,95.

Полужесткие материалы включают в себя минераловатные или стекловолокнистые плиты с объёмной массой 80...130 кг/м3 при содержании синтетического связующего 10...15 % по массе , а также древесноволокнистые плиты с объёмной массой 180...300 кг/м3. У Поверхность плит покрывается пористой краской или плёнкой. Коэффициент звукопоглощения полужёстких материалов на средних частотах Б составляет 0,5...0,75. Сюда входят звукопоглощающие материалы с ячеистым строением – пенополиуретан, полистирол, а также базальтовые звукопоглощающие маты, получаемые из очень тонкого базальтового волокна с покрытием из стеклоткани.

У **твердых материалов** объемная масса составляет 300...400 кг/м3 и коэффициент звукопоглощения порядка 0,5. Их производят на основе гранулированной или суспензированной минеральной ваты и коллоидного связующего. К ним относятся материалы, в состав которых входят пористые заполнители (вспученный перлит, вермикулит, пемза).

Звукопоглощающая способность материалов обусловлена их пористой структурой и наличием большого числа открытых сообщающихся между собой пор, максимальный диаметр которых обычно не превышает 2 мм (общая пористость должна составлять не менее 75 % по объёму). Большая удельная поверхность материалов, создаваемая стенками открытых пор, способствует активному преобразованию энергии звуковых колебаний в тепловую энергию вследствие потерь на трение.

Обычно пористые материалы используют в сочетании со сплошными. Один из распространенных видов пористых материалов – облицовочные звукопоглощающие материалы. Их изготавливают в виде плоских плит или рельефных конструкций (пирамид, клиньев и т. Б д.), располагаемых или вплотную или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т. п.).

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются е на мембранные и резонаторные. **Мембранные поглотители** представляют собой натянутый холст (ткань), тонкий фанерный (картонный) лист, под которым располагают хорошо демпфирующий материал (материал с большой вязкостью — например поролон, губчатую реизину, строительный войлок и т. д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Перфорированные **резонаторные поглотители** представляют собой систему воздушных резонаторов, в устье которых расположен демпфирующий материал.

Наиболее распространенными являются перфорированные плиты, которые монтируются на некотором расстоянии от твердой стены.

Повышение звукоизоляции стен и перегородок помещений достигается применением слоистых или раздельных их конструкций. В многослойных перегородках и стенах целесообразно подбирать материалы слоев с резко отличающимися акустическими сопротивлениями (например бетон–поролон).

Основными конструктивными параметрами, определяющими звукоизолирующую способность многослойных конструкций, являются

материал толщина обшивок, вид каркаса и способ крепления к нему обшивок, толщина

промежутка между слоями, вид звукопоглощающего материала и степень заполнения им промежутка.

Звукоизолирующая способность сложных стен, имеющих дверные и оконные проемы, зависит от звукоизоляции дверей и окон. Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна дверей к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т. д. При недостаточной звукоизоляции однослойных дверей используются двойные двери с тамбуром, облицованные звукопоглощающим материалом.

Звукопоглощающая способность окон, так же как и дверей, зависит главным образом от поверхностной плотности стекла и прижатия притворов. Обычные окна с двойными переплетами обладают более высокой (на 4...5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улучшает звукоизоляционные качества окон. В случаях когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (например, двойное окно с заполнением оконного проема органическим стеклом толщиной 20...40 мм и с воздушным зазором между стеклами не менее 100 мм). Повышенное звукопоглощение обеспечивается применением конструкции окон на основе стеклопакетов с герметизацией и заполнением зазора между стеклами различными газовыми смесями. Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы

тепло-, газо-, водоснабжения и канализации, кабельная сеть энергоснабжения, вентиляционные короба и т. д.). Для них в стенах и перекрытиях сооружений делают соответствующие отверстия и проемы. Их надежная звукоизоляция обеспечивается применением У специальных гильз, прокладок, глушителей, вязкоупругих заполнителей и т. д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается использованием акустических фильтров и глушителей.

Во временно используемых помещениях используют складные экраны. Применение звукопоглощающих материалов, преобразующих кинетическую энергию звуковой волны в е тепловую, имеет некоторые особенности, связанные с необходимостью создания оптимального соотношения прямого и отраженного от преграды акустических сигналов. Чрезмерное звукопоглощение снижает уровень сигнала, большое время реверберации приводит к ухудшению разборчивости речи.

15. АКТИВНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Активные методы защиты информации – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня шума

16. АКУСТИЧЕСКАЯ МАСКИРОВКА

Мероприятия акустической маскировки позволяют обеспечить:

– неузнаваемость голоса диктора;

– существенное снижение неразборчивости речи диктора;

– скрыть факт передачи речевой информации.

Широко применяются методы компьютерной стеганографии, основанные на использовании естественных шумов, которые содержат цифровые массивы, полученные стандартными способами преобразования из аналоговых акустических и видеосигналов.

Стеганография – это наука о тайной передаче информации путем сокрытия самого факта передачи.

Для защиты информации от утечки используют метод микширования речевого сигнала с различными шумовыми сигналами. Технически это реализуется за счет использования автоматических генераторов шума. акустическую маскировку часто называют акустическим зашумлением.

Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются полупроводниковые и другие электронные приборы и элементы.

Виды акустических помех, создаваемых средствами защиты:

– «белый» шум – имеет равномерный спектр в полосе частот речевого сигнала;

– «окрашенный» шум – формируется из «белого» в соответствии с огибающей амплитудного спектра скрываемого речевого сигнала;

– «речеподобные» помехи – формируются путем микширования в различных сочетаниях отрезков речевых сигналов, музыкальных фрагментов и шумовых помех или формируется из фрагментов скрываемого речевого сигнала при многократном наложении с различными уровнями.

«Речеподобные» помехи:

– «речеподобная» помеха-1 – формируется из фрагментов речи трех дикторов радиовещательных станций при равных уровнях сигналов;

– «речеподобная» помеха-2 – формируется из одного доминирующего речевого сигнала или музыкального фрагмента и смеси фрагментов радиопередач с шумом;

– «речеподобная» помеха-3 – формируется из фрагментов скрываемого речевого сигнала при многократном их наложении с различными уровнями.

17. Электромагнитная маскировка

5.2. 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.

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.

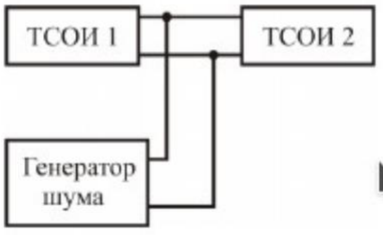

Рис. 5.3. Схема включения системы генератора шумового сигнала

Системы пространственного зашумления применяют для создания маскирующих помех в окружающем пространстве (рис. 5.5). В состав системы входят:

18. Обнаружение закладных устройств

5.3. 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 расстояния (20…400 м). Рабочую частоту для повы-

Наиболее информативными признаками проводной микрофонной системы являются:

– тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;

– наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

Демаскирующие признаки автономных некамуфлированных акустических закладок включают:

– признаки внешнего вида – малогабаритный предмет неизвестного назначения;

– одно или несколько отверстий малого диаметра в корпусе;

– наличие автономных источников питания (например аккумуляторных батарей);

– наличие полупроводниковых элементов, выявляемых при облучении

К основным методам поиска закладных устройств можно отнести:

– специальное обследование выделенных помещений;

– поиск ЗУ с использованием технических средств;

– измерение параметров линий электропитания, телефонных линий связи и т. д.;

2. По глубине проводимых проверок:

а) ***первый уровень.*** В результате проверки могут быть обнаружены радиоизлучающие изделия, установленные непосредственно в проверяемом или

смежных с ним помещениях. При этом если устройства в момент проверки находятся в пассивном состоянии, то они могут быть не выявлены;

б) ***второй уровень.*** Могут быть обнаружены все устройства первого уровня плюс сетевые передатчики, использующие в качестве канала передачи сеть питания 220 В 50 Гц;

в) ***третий уровень.*** Могут быть выявлены все изделия второго уровня плюс все типы кабельных микрофонных систем, а также оргтехника, работающая в режиме передачи за границы зоны охраны сигнала, содержащего полезную информацию.

г) ***четвертый уровень.*** Могут быть выявлены все типы заносных и закладных электронных устройств перехвата информации и естественные каналы утечки информации.

21.Категорирование объектов

Категория охраняемого объекта – комплексная оценка состояния объекта, учитывающая его экономическую или иную, например культурную, значимость в зависимости от концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны.

Классификация:

К категории А(особо важные) следует отнести особо важные объекты, на которых возможный ущерб в случае реализации основных угроз безопасности максимален по характеру и по масштабам. Характер ущерба заключается в создании угрозы для жизни и здоровья персонала и населения, а также в негативном воздействии на природную среду.

К категории Б(важные) предлагается отнести важные объекты, на которых характер возможного ущерба заключается в угрозе для жизни и здоровья персонала объекта, а его последствия не выходят за пределы территории объекта и могут быть локализованы путем принятия ликвидационных мер.

Категория В(прочие) характеризуются тем, что возможный ущерб носит локальный и в основном материальный характер и по масштабу может иметь как региональное, так и международное значение.

Например, особо важные объекты предлагается дополнительно разделить на три группы безопасности (№1, 2, 3). Номер группы определяет масштаб возможного ущерба, который может иметь последствия, соответственно, трансграничного, государственного, регионального значений.

Принадлежность объекта к соответствующей категории и группе необходимо определять на начальной стадии проектирования системы информационной безопасности (СИБ), т. к. от этого зависит не только уровень его защищенности, но и планируемая тактика действий сил охраны. От этой тактики зависят общие затраты на создание СИБ.

22.Классификация помещений и территории объекта

Классификация:

1. Свободная зона – помещения и прилегающая территория, доступ в которые свободен для любой категории лиц. Ведётся наблюдение.

2. Наблюдаемая зона – помещения и территория, доступ в которые также не ограничен, но за ними ведется систематическое наблюдение силами службы безопасности или охраны.

3. Регистрационная зона – зона, вход в которую свободен для любого желающего при условии, что он предъявит для регистрации документ, удостоверяющий его личность.

4. Режимная зона – зона, на входе в которую находится пост охраны. Проход допускается либо по пропускам установленной формы, либо по именным заявкам лиц, имеющих соответствующее право.

5. Зона усиленной защиты – это, как правило, помещения, куда допускаются только сотрудники предприятия, а для посторонних лиц доступ туда возможен только по специальным пропускам или в сопровождении уполномоченных лиц.

6. Зона высшей защиты – зона, вход в которую ограничен не только для клиентов и

посетителей, но и для собственных сотрудников, не имеющих прямого отношения к данным помещениям.

Отметим факторы, регламентирующие помещение по одной из вышеуказанных категорий:

– условия доступа сотрудников предприятия;

– условия доступа клиентов и посторонних лиц;

– наличие и вид физической охраны;

– виды использования технических средств наблюдения и охраны;

Наиболее оптимальным способом распределения помещений является компактное размещение в одном месте помещений одной и той же категории. При этом желательно, чтобы между собой соседствовали зоны одинаковых или не слишком различающихся категорий. Например попасть в помещение IV зоны можно только из помещения III или V зоны. Это позволит наиболее экономным способом разместить средства инженерного усиления строительных конструкций и технические средства безопасности.

23.Инженерные заграждения

Заграждение в составе системы охраны периметра объекта выполняет роль преграды, изменяющей условия передвижения нарушителя по направлению к охраняемому объекту.

Характеризуется временем сопротивления – время, необходимое на преодоление данного заграждения.

По назначению ограждения делятся на следующие виды:

–основные – препятствуют свободному входу нарушителя на территорию объекта;

–дополнительные – предназначены для повышения укрепленности основных ограждений;

– предупредительные – устанавливаются с внутренней или внешней стороны основного ограждения с вывешиванием на них запрещающих надписей («Стой», «Запретная зона», «Не подходить» и т.д.) и предназначены для ограничения доступа к нему людей.

Для защиты верхней части капитальных заборов применяется также армированная колючая лента (АКЛ «Егоза»), изготавливаемая путем армирования колючей ленты стальной оцинкованной проволокой диаметром 2,5 мм. Колючая лента заградительная представляет собой оцинкованную ленту толщиной 0,5 мм, имеющую обоюдоострые, симметрично расположенные шипы (рис. 6.1).

Рис. 6.1. Внешний вид АКЛ «Егоза»

Все заграждения в зависимости от назначения можно разделить на четыре типа: сигнализационные, сигнализационно-электризуемые (электрошоковые), строительные (технические) и строительно-сигнализационные.

Сигнализационные ограждения образовывают проводящие металлические конструкции, являющиеся чувствительным элементом периметрового средства обнаружения, которое называется заградительным (перемежающиеся линии колючей проволоки, закрепленные на деревянных или бетонных столбах и включенные в два активных шлейфа, чувствительных к обрыву и короткому замыканию смежных линий).

Сигнализационно-электризуемые заграждения представляют собой систему токонесущих проводов (изолированных от опор), по которой распространяются импульсы высокого напряжения (3…10 кВ), вызывающие болевой шок у нарушителя при касании.

Строительные заграждения весьма разнообразны, их классификация дана на рис. 6.2.

24. Технич. Средства охраны периметры объекта

Техническое средство охраны – вид техники, предназначенный для использования силами охраны с целью повышения эффективности обнаружения нарушителя и обеспечения контроля доступа на объект охраны.

Любая периметральная система охраны должна отвечать определенному набору критериев, некоторые из которых перечислены ниже:

– возможность раннего обнаружения нарушителя – еще до его проникновения на объект;

– точное следование контурам периметра, отсутствие «мертвых» зон;

– скрытая установка датчиков системы;

– независимость параметров системы от сезона (зима, лето) и погодных

– независимость параметров системы от сезона (зима, лето) и погодных
условий (дождь, ветер, град и т. д.);

– невосприимчивость к внешним факторам «нетревожного» характера – индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы;

– устойчивость к электромагнитным помехам – грозовые разряды, источники мощных электромагнитных излучений и т. п.

Каждое средство обнаружения строится на определенном физическом принципе, на основе которого действует его чувствительный элемент.

Чувствительный элемент – первичный преобразователь, реагирующий на воздействие на него (прямое или косвенное) объекта обнаружения и воспринимающий изменение состояния окружающей среды.

Средство обнаружения (СО) – устройство, предназначенное для автоматического формирования сигнала с заданными параметрами (сигнала тревоги) вследствие вторжения или преодоления объектом обнаружения чувствительной зоны (зоны обнаружения) данного устройства

Чувствительная зона СО (зона чувствительности) – участок, положение в котором объекта обнаружения вызывает возникновение полезного сигнала с уровнем, превышающим уровень шума или помехи.

Внутри зоны чувствительности располагается Зона обнаружения С-зона, где СО обеспечивает заданную вероятность обнаружения.

Различие между радиоволновыми средствами обнаружения (РВСО) и радиолучевыми (РЛСО) состоит в способе формирования чувствительной зоны:

РВСО использует ближнюю зону распространения радиоволн (менее 10 длин волн), а РЛСО – дальнюю зону (более 100 длин волн)

В зависимости от принципа действия различают:

– **пассивные РВСО и РЛСО** используют собственное излучение объекта обнаружения или вызываемое им изменение электромагнитных полей (ЭМП) внешних источников (как правило, вещательных телестанций и радиостанций).

– **активные РВСО и РЛСО** используют собственный источник ЭМП для формирования чувствительной зоны.

По конструкционному исполнению:

– **однопозиционные** имеют общий блок приемопередатчика (пассивные РВСО и РЛСО всегда являются однопозиционными);

– **двухпозиционные** имеют разнесенные блоки передатчика и приемника.

Форма чувствительной зоны для пассивных РВСО определяется формой диаграммы направленности антенны (рис. 6.8).

В первом случае она, как правило, круговая, а используемый диапазон 10 кГц…10 ГГц.

Во втором случае, как правило, чувствительная зона имеет лучевую форму и используются метровый и дециметровый диапазоны.

В РВСО в качестве чувствительных элементов используются кабели. На некотором расстоянии параллельно друг другу прокладываются два кабеля (две антенны) специальной конструкции (рис. 6.9). Зазоры между разреженными проводами «экрана» своеобразного коаксиального кабеля образуют щелевую антенну.

Рис. 6.9. Конструкция кабеля радиоволновой системы

Один из кабелей служит передающей антенной, другой – приемной антенной. При возбуждении первой антенны высокочастотными колебаниями она начинает излучать электромагнитное поле, воспринимаемое второй антенной. При этом приемник, подключенный к приемной антенне, принимает сигнал.

Если в окрестности двух антенн появляется тело определенного объема с диэлектрической и/или магнитной проницаемостью, отличной от проницаемости свободного пространства, электромагнитное поле, воспринимаемое приемной антенной, искажается (изменяются его амплитуда и фаза). Это изменение детектируется и анализируется приемником-анализатором. Если анализируемый сигнал превышает пороговое значение, формируется сигнал тревоги.

Во избежание образования мертвых зон кабели смежных зон охраны размещают с некоторым перекрытием (2…5 м) в продольном направлении.

РЛСО содержат передатчики и приемники с узконаправленными антеннами. Используемый диапазон частот обычно лежит в пределах 10…40 ГГц. Сечение радиолуча в горизонтальной (а) и вертикальной (б) плоскостях показано на рис. 6.10. Рабочей зоной радиолучевых систем считают зону на участке BC. На участке AB луч слишком узкий, и его можно обойти. На участке CD площадь поперечного сечения луча слишком велика по сравнению с площадью потенциального нарушителя, и обнаруживающая способность системы оказывается пониженной. В то же время наличие луча на достаточно протяженном участке CD за пределами рабочей зоны накладывает серьезные ограничения на минимальные размеры зоны отчуждения. При использовании одиночных совмещенных приемопередатчиков типа радиолокаторов зона отчуждения должна превышать размеры участка CD.

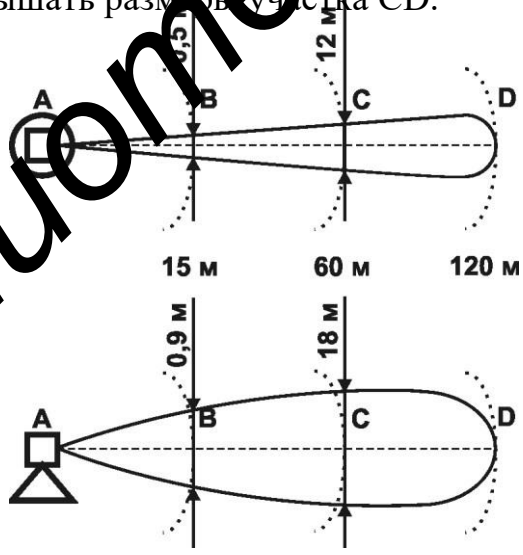

Рис. 6.10. Схематичное изображение зоны обнаружения радиолучевой системы

РЛСО чаще всего используют для контроля протяженных прямолинейных участков, когда имеется достаточно свободного пространства для вынесения приемников и передатчиков за пределы охраняемых зон. РЛСО,

как правило, применяются одновременно с другими средствами, которые позволяют закрыть присущие РЛСО мертвые зоны.

25 Охранное телевидение

Упрощенно функции охранного телевидения можно свести к двум основным:

– обнаружение;

– идентификация.

Обнаружение на охраняемой территории объектов сводится к предоставлению оператору визуальной информации либо выработке автоматическим устройством сигнала тревоги при обработке соответствующих видеосигналов. Это позволяет с определенной достоверностью вырабатывать суждение о наличии в данный момент тревожной ситуации (а в случае анализа видеозаписей – о том, что тревожная ситуация имела место). Второй задачей является идентификация объектов (людей, автомобилей и т. д.). Идентификация наиболее важна при анализе видеозаписей, т. е. при расследовании происшествий. Для выполнения идентификации требуется значительно больший по сравнению с обнаружением объем визуальной информации, и здесь на первое место выходит достоверность, а скорость реакции охраны уходит на второй план. Библиотека

Способы представления визуальной информации оператору.

Параллельный способ. Используется несколько видеомониторов, ко входу каждого из которых подключена видеокамера – при этом образуются независимые параллельные каналы.

Достоинства: – простота; – стоимость ниже, чем с использованием разделителя экрана или видеомультиплексора; – нет потери информации от оцифровки видеосигналов и переключения видеокамер; – высокая живучесть

системы (замена оборудования из одного канала на оборудование из другого канала). Недостатки: – из требований эргономики следует, что количество видеомониторов (каналов) в расчете на одного оператора не должно превышать 6…8; – при наличии одного устройства видеорегистрации невозможно осуществлять видеозапись по всем каналам одновременно; – при увеличении числа каналов возрастает занимаемая видеомониторами площадь.

Последовательный способ. Реализуется за счет использования видеокоммутаторов, которые осуществляют коммутацию видеокамер с низкой частотой (секунды или десятки секунд на канал). Видеокоммутаторы являются простейшими и самыми экономичными устройствами обработки видеосигналов

Достоинства: – простота обслуживания; – отсутствие потери качества изображения, вызванного оцифровкой; – возможность использования видеомониторов небольшого размера. Недостатки: – наличие неконтролируемого времени; – быстрое утомление оператора при непрерывном переключении каналов; – невозможность осуществления видеозаписи по всем каналам одновременно с помощью одного видеомагнитофона.

Разделители экрана (квадраторы) позволяют одновременного отображать на экране видеомонитора изображения от четырех видеокамер

Достоинства

практически отсутствует потеря информации на время переключения видеокамер;– последовательное отображение на видеомониторе полноэкранных изображений (в ручном или автоматическом режимах). Четырем сегментам на экране видеомонитора соответствует четыре области памяти разделителя экрана, обновление которых может осуществляться либо последовательно, либо параллельно. Библиотека БГУИР

При необходимости получения изображений с помощью одного разделителя экрана более чем от 4 видеокамер может использоваться двухстраничный разделитель экрана (8 видеовходов, коммутируемых группами по 4

Недостатки: – наличие неконтролируемого время для видеокамер; – не позволяют получить видеозапись приемлемого качества (выходной сигнал подвергается цифровой обработке, что снижает разрешающую способность).

Видеомультиплексор– устройство для организация видеозаписи с минимальными потерями сигналов от нескольких видеокамер на один охранный видеомагнитофон. Видеомультиплексор формирует на своем выходе мультиплексированный видеосигнал, получаемый переключением видеокамер с частотой полей.

Достоинство – на видеомагнитофон поступают с частотой полей видеосигналы, соответствующие полноэкранному отображению.

26 Системы контроля и управления доступом

Под системой контроля и управления доступом (СКУД) (рис. 6.29) понимают объединенные в комплексы технические средства, обеспечивающие возможность доступа определенных лиц в определенные зоны (территория, здание, помещение) или к определенной аппаратуре, техническим средствам и предметам (ПЭВМ, автомобиль, сейф и т. д.) и ограничивающие доступ лиц, не имеющих такого права.

Состав СКУД: – устройства ввода идентификационных признаков – устройства управления; – исполнительные устройства (управляемые преграждающие устройства). Идентификация – процедура распознавания субъекта по его идентификатору. Идентификатор – уникальный признак субъекта доступа. В процессе идентификации субъект предъявляет системе свой идентификатор и она проверяет его наличие в своей базе данных. Субъекты с известными системе идентификаторами считаются легальными

(законными), остальные субъекты относятся к нелегальным. Способы ввода идентификатора: – ручной, осуществляемый путем нажатия клавиш, поворота переключателей и т. д.; – контактный в результате непосредственного контакта между считывателем и идентификатором; – дистанционный (бесконтактный) при поднесении идентификатора к считывателю на определенное расстояние. Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

Автономные системы – предназначены для обеспечения контроля и управления доступом в отдельное помещение.

Состав автономных СКУД: – автономный контроллер – хранит базу данных идентификаторов и управляет работой остальных элементов системы; – электромагнитный замок – используется в качестве исполнительного устройства; – датчик положения двери – обеспечивает правильность работы всей системы; – считыватель для устройств идентификации; – кнопка открывания двери изнутри. Для идентификации пользователя используются различные типы карт с соответствующими считывателями (магнитные, Proximity, Touch Memory и т. д.).

Сетевые системы предназначены для обеспечения контроля и управления доступом на крупных объектах (банки, учреждения, предприятия и т. п.)

27 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографическая защита информации – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности

информации с использованием средств криптографической защиты информации.

К средствам криптографической защиты информации относятся технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации.

28 Основы построения криптосистем

Криптография – наука о методах, алгоритмах, программных и аппаратных средствах преобразования информации в целях сокрытия ее содержания, предотвращения видоизменения или несанкционированного использования

Доступность информационных технологий широкому кругу коммерческих компаний и частным лицам породила потребность, во-первых, обеспечивать конфиденциальность той информации, которая циркулирует в телекоммуникационных системах (ТКС), во-вторых, обеспечивать ряд функций, таких, как аутентификация субъектов системы, целостность сообщений, истинность документов и т. д. Оказалось, что все это можно обеспечить, используя принципы криптографии

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 составляют науку криптологию

28,1 Общие принципы криптографической защиты информации

Отправитель генерирует открытый текст исходного сообщения M, которое должно передаваться по открытому каналу. Отправитель шифрует текст с помощью обратимого преобразования E и ключа K: Ek и получает шифротекст C = Ek(M), который отправляет получателю. Получатель, приняв шифротекст C , расшифровывает его с помощью обратного преобразования 1 D EK и получает исходное сообщение в виде открытого текста M : 1 K K M D C E E M ( ) (( )).

Преобразование Ek выбирается из семейства криптографических преобразований, называемых криптоалгоритмами. Параметр, с помощью которого выбирается конкретное преобразование, называется криптографическим

Существует четыре основных типа криптоаналитических атак. Конечно, все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и шифротексты сообщений. Перечислим эти криптоаналитические атаки

1. Криптоаналитическая атака при наличии только известного шифротекста. Криптоаналитик имеет только шифротексты 1 2 , ,..., C C Ci нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования EK

2. Криптоаналитическая атака при наличии известного открытого текста. Криптоаналитик имеет доступ не только к шифротекстам 1 2 , ,..., C C Ci нескольких сообщений, но также к открытым текстам 1 2 , ,..., M M Mi этих сообщений.

3. Криптоаналитическая атака при возможности выбора открытого текста. Криптоаналитик не только имеет доступ к шифротекстам 1 2 , ,..., C C Ci и связанным с ними открытым текстам 1 2 , ,..., M M Mi нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде.

4. Криптоаналитическая атака с адаптивным выбором открытого текста. Это особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования.

28,2 Блочные и поточные шифры

Можно выделить следующие характерные признаки методов шифрования данных:

– выполнение операций с отдельными битами или блоками;

– зависимость или независимость функции шифрования от результатов шифрования предыдущих частей сообщения;

– зависимость или независимость шифрования отдельных знаков от их положения в тексте.

В соответствии с этим различают три основных способа шифрования:

– поточные шифры;

– блочные шифры;

– блочные шифры с обратной связью

1. Поточное шифрование. Состоит в том, что каждый бит открытого текста и соответствующий бит ключа преобразовываются по определенному алгоритму

2. Блочное шифрование. При блочном шифровании открытый текст сначала разбивается на равные по длине блоки, затем применяется зависящая от ключа функция шифрования для преобразования блока открытого текста длиной m бит в блок шифротекста такой же длины

3. Блочное шифрование с обратной связью. Как и при блочном шифровании, сообщения разбивают на ряд блоков, состоящих из m бит

29 Симметричные криптосистемы

Ключ – это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Основной характеристикой шифра является криптостойкость, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

– достаточная криптостойкость (надежность закрытия данных);

– простота процедур шифрования и расшифровывания;

– незначительная избыточность информации за счет шифрования; – нечувствительность к небольшим ошибкам шифрования и др.

В той или иной мере этим требованиям отвечают:

– шифры перестановок;

– шифры замены;

– шифры гаммирования;

– шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Например, можно использовать правило умножения вектора на матрицу, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны храниться в секрете), а символами умножаемого вектора последовательно служат символы шифруемого текста.

Процессы зашифровывания и расшифровывания осуществляются в рамках некоторой криптосистемы. Характерной особенностью симметричной криптосистемы является применение одного секретного ключа как при зашифровывании, так и при расшифровывании сообщений.

30 Асимметричные криптосистемы

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с открыто вычислительно неразрешимой задачей.

Характерные особенности асимметричных криптосистем:

– открытый ключ $К_0$ и криптограмма C могут быть отправлены по незащищенному каналу, т. е. могут быть известны противнику;

– алгоритмы шифрования $E_{К0}(M) \rightarrow C$ и расшифрования $D_{КС}(C) \rightarrow M$

являются открытыми;

– защита информации в асимметричной криптосистеме основана на секретности ключа $К_с$.

У. Диффи и М. Хелман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

– вычисление пары ключей ($К_0$, $К_с$) получателем *B* на основе начального условия должно быть простым;

– отправитель *A*, зная открытый ключ $К_0$ и сообщение *M*, может легко вычислить криптограмму $C\,E_{К0}\,M$;

– получатель *B*, используя секретный ключ $К_с$ и криптограмму *C*, может легко восстановить исходное сообщение $M\,D_{КС}\,C\,D_{КС}\,E_{К0}\,M$;

– противник, зная открытый ключ $К_с$, при попытке вычислить секретный ключ $К_с$ наталкивается на непреодолимую вычислительную проблему;

– противник, зная пару ($К_0$, С), при попытке вычислить исходное сообщение *M*, наталкивается на непреодолимую вычислительную проблему.

Политика безопасности

Политика безопасности – набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе.

Политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной АСОИ осуществляется при помощи средств управления механизмами защиты

Избирательная политика безопасности

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

– все субъекты и объекты системы должны быть идентифицированы;

– права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Полномочная политика безопасности

Основу полномочной политики безопасности составляет полномочное управление доступом (Mandatory Access Control; MAC), которое подразумевает следующее:

– все субъекты и объекты системы должны быть однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ

32) Обеспечение безопасности в системах электронной коммерции

Безопасность — это состояние, при котором отсутствует возможность причинения ущерба потребностям и интересам субъектов отношений.

Угроза безопасности — это совокупность условий и факторов, создающих опасность жизненно важным интересам, т. е. угроза представляется некой совокупностью обстоятельств (условий) и причин (факторов).

С юридической точки зрения понятие «угроза» определяется, как намерение нанести зло (ущерб).

Понятие защита (защищенность) означает ограждение субъекта отношений от угроз.

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 существующим видам угроз.

Система безопасности предназначена для выявления угроз интересам, поддержания в готовности сил и средств обеспечения безопасности и управления ими, организации нормального функционирования объектов безопасности.

Применительно к электронной коммерции определение безопасности можно сформулировать как состояние защищенности интересов субъектов отношений, совершающих коммерческие операции (сделки) с помощью технологий электронной коммерции, от угроз материальных и иных потерь. понятие «безопасность» любого предприятия или организации включает:

- физическую безопасность, под которой понимается обеспечение защиты от посягательств на жизнь и личные интересы сотрудников;
- экономическую безопасность, под которой понимается защита экономических интересов субъектов отношений. В рамках экономической безопасности рассматриваются также вопросы обеспечения защиты материальных ценностей от пожара, стихийных бедствий, краж и других посягательств;
- информационную безопасность, под которой понимается защита информации от модификации (искажения, уничтожения) и несанкционированного использования.

К общим принципам обеспечения защиты относятся:

1) принцип неопределенности. Обусловлен тем, что при обеспечении защиты неизвестно, кто, когда, где и каким образом попытается нарушить безопасность объекта защиты;

2) принцип невозможности создания идеальной системы защиты. Этот принцип следует из принципа неопределенности и ограниченности ресурсов, которыми, как правило, располагает система безопасности;

3) 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;

4) принцип защиты всех от всех. Данный принцип предполагает необходимость защиты всех субъектов отношений против всех видов угроз.

33) Противодействие атакам в информационных системах

- Физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу.
- Базовые средства защиты электронной информации. Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.
- Анти-DDoS. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик.

При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.

- Резервное копирование данных. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в случае чрезвычайной ситуации, например, при изъятии сервера органами власти. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке.
- План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты
- защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки, тем устойчивее положение компании на рынке.после восстановления данных. Сам процесс восстановления следует максимально отработать с учетом всех изменений системы.

• Шифрование данных при передаче информации в электронном формате (end-to-end protection). Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования.

Электронная цифровая подпись Общие сведения

При обмене сообщениями через ТКС возникает задача подтверждения их подлинности (подтверждения авторства и целостности). Такая же проблема существует и при переходе от юридически значимых бумажных документов к электронным. Сообщения, для которых эта проблема актуальна, будем в дальнейшем называть электронными документами. В обычной (бумажной) информатике эти проблемы решаются за счет того, что информация в документе и рукописная подпись автора жестко связаны с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет. Естественно, что для электронных документов традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе совершенно непригодны, поэтому для подтверждения подлинности документа используется специфическая криптографическая процедура, называемая электронной цифровой подписью (ЭЦП). ЭЦП функционально аналогична обычной рукописной подписи и обладает ее основными достоинствами: удостоверяет, что подписанный текст исходит от лица, поставившего подпись; не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом; гарантирует целостность подписанного текста ЭЦП представляет собой относительно небольшое количество дополнительной цифровой

информации, передаваемой вместе с подписываемым текстом. Технология ЭЦП включает две процедуры: 1) процедуру постановки подписи; 2) процедуру проверки подписи. В процедуре постановки подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя. При формировании ЭЦП отправитель прежде всего вычисляет хэш-функцию h M подписываемого документа M. Вычисленное значение хэш-функции h M представляет собой один короткий блок информации m , характеризующий весь документ M в целом. Затем число m «шифруется» секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного документа M. В принципе можно обойтись без предварительного хэширования документа, а «шифровать» весь документ, однако в этом случае придется иметь дело с гораздо большим по размерам файлом. Употребление слова «шифровать» здесь весьма условное и справедливо при использовании алгоритма RSA, для других алгоритмов точнее говорить «преобразовывать».

Варик 1

Интеллектуа́льная со́бственность — в широком понимании термин означает закреплённое законом временное исключительное право,
а также личные неимущественные права авторов на результат интеллектуальной деятельности или средства индивидуализации

интеллектуальная собственность является категорией невещественной, неосязаемой, что приносит определенную специфику в порядок обращения с такой собственностью. Это вызвано тем, что интеллектуальная собственность связана с идеями, которые можно воплощать в осязаемые объекты неограниченное число раз (книги, картины, машины и пр.). Называется она

интеллектуальной потому, что заключается не в этих вещественных воплощениях, а в реализованной в них информации.
В понятие «интеллектуальная собственность» входят в качестве ее составляющих промышленная собственность и произведения, охраныемые авторском правом.

Варик 2
Объекты интеллектуальной собственности – это находящиеся под охраной нормативными правовыми актами результаты деятельности интеллекта. Классификация их очень разнообразна, в зависимости от состава, степени применения во время производственного процесса, по характеру влияния на финансовое благополучие юридических, физических лиц или отдельных предприятий.

По ряду факторов распределить данные объекты можно на такие группы:

по степени производственного использования активы нематериального характера разделяются на работающие (те функционирующие объекты, которые в обиходе предприятия в данный момент времени и приносят ему доход) и неработающие (те функционалы, которые в данный период не работают, а находятся в запасе на будущее);

по характеру влияния на доход предприятия – нематериальные активы, прямо приносящие финансовую прибыль за счет своей включенности в процесс эксплуатации, и активы, которые влияют на результат опосредованно;

по направленности получения результата интеллектуальной работы – научные, гуманитарные, технические объекты;

по степени юридической защиты бывают охранными государством объектами авторских прав, неохраняемые (незащищенные) объекты авторского права.

К группе активов собственности, принадлежащей и используемой в промышленности, можно отнести:

промышленные образцы;
товарные знаки;
изобретения;
знаки обслуживания;
полезные модели;
наименование мест производства продукции.

Авторское право и смежные права

2.1. Объекты авторского права

Законодательством большинства стран охраняются права творческих работников на результаты их труда. Основная цель охраны авторских прав — это содействие обогащению и распространению национального культурного наследия.

Авторское право на произведения науки, литературы и искусства возникает в силу факта их создания.

Объектами охраны могут быть как хорошие произведения литературы или музыки, так и плохие (дело вкуса). Заложенные в произведении идеи необязательно должны быть новыми (например, тема любви), однако форма их выражения должна быть оригинальной.

Объектами авторского права являются.

1. Литературные произведения, к которым относятся романы,

поэмы, рассказы, драматургические и другие произведения независимо от их содержания и формы (книга, брошюра, статья в журнале, газета), письма, дневники, лекции, доклады и т. п., перевод произведения на другой язык.

2. Научные произведения — это любые оригинальные произведения научного характера (монографии, книги, брошюры, диссертации, отчеты и т. д.).

3. Драматические (пьесы), музыкально-драматические (мюзиклы) и сценарные произведения.

Сценарные произведения — это сценарии, по которым ставятся фильмы, балетные спектакли и другие массовые представления.

4. Хореографические произведения (танец) и пантомимы (театр

«Лицедеи»). Правовая охрана хореографических произведений наступает с момента обнародования, т. е. произведение необязательно фиксировать письменно с помощью рисунка.

5. Музыкальные произведения, к которым относятся классическая или популярная музыка, песни, хоровые произведения, симфонии, оратории и т. п.

6. Аудиовизуальные произведения охватывают широкий круг кино-, теле- и видеопроизведений, рассчитанных на зрительное и слуховое восприятие. Авторами аудиовизуального произведения являются режиссер-постановщик, автор сценария.

7. Произведения живописи, графики, скульптуры и другие произведения изобразительного искусства, особенностью которых является их неразрывная связь с материальными носителями, где они воплощены. Воспроизведение репродукций, слайдов, фотографий и других произведений изобразительного искусства может осуществ-ляться только с согласия автора.

7. Произведения декоративно-прикладного искусства — это ху-

дожественные изделия, имеющие практическое назначение в быту (утварь, мебель, ткани, одежда, украшения, игрушки и др.). В декора-тивно-прикладном искусстве используются литье, ковка, чеканка, гравировка, резьба.

8. Произведения архитектуры, градостроительства и садово-

паркового искусства (здания, сооружения, парки, сады, кварталы, за-стройки и др.).

9. Фотографические произведения — это портреты, пейзажи, изображения текущих событий, произведения голографии.

10. Компьютерные программы (программы для ЭВМ), охраняе-мые как литературные произведения, и базы данных.

Объектами авторского права не являются:

- официальные документы (законы);

- государственные символы (герб, флаг, гимн, денежные знаки, ордена);

- произведения народного творчества, авторы которых неизвестны.

2.2. Субъекты авторского права. Авторский договор

Субъектами авторского права являются лица, которым по за-кону как создателям произведений принадлежит авторское право в отношении того или иного произведения (автор, соавторы).

Автором произведения считается лицо, указанное в качестве ав-тора на оригинале или экземпляре произведения, если не доказано иное. Авторское право на произведение, созданное совместным твор-ческим трудом двух или более лиц (соавторство), принадлежит авто-рам совместно, как и право на использование произведения в целом принадлежит авторам совместно.

Необходимым условием признания тех или иных лиц соавтора-ми является наличие соглашения между ними о соавторстве («Автор-ский договор»). Авторский договор является добровольным и может быть выражен в любой форме, однако конкретные условия возникновения соавторства законом не оговорены. В спорных случаях этот вопрос решается судом.

Субъектами авторского права после смерти автора становятся его наследники.

2.3. Неимущественные права авторов

Действующее законодательство закрепляет за автором в отношении его произведения следующие личные неимущественные права:

• право авторства — право признаваться автором произведения;

• право на имя — право использовать или разрешать использовать произведение под подлинным именем автора;

• право на защиту репутации — это право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора, т. е. за автором закреплено право сохранения своей творческой индивидуальности и без его согласия невозможно вносить любые изменения (сокращать объем, изменять содержание отдельных частей в целях их улучшения, нарушать целостность произведения и др.);

- право на обнародование — право обнародовать или разрешать обнародовать произведение в любой форме, оно отнесено

к одному из существенных неимущественных прав и обеспечивает автору возможность довести произведение до всеобщего сведения, т. е. осуществить публичное оглашение произведения.

2.4. Имущественные права авторов

Имущественное право — это право осуществлять или разрешать осуществлять следующие действия:

- воспроизведение произведения;

- распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;

- прокат оригиналов или экземпляров;
- импорт экземпляров произведения;
- публичный показ оригинала или экземпляра произведения;
- публичное исполнение произведения;
- передачу произведения в эфир;
- иное сообщение произведения для всеобщего сведения;

- перевод произведения на другой язык;
- переделку или иную переработку произведения.

Одним из способов использования произведения является его распространение. Право автора на распространение тесно связано с правом на воспроизведение, поскольку, прежде чем произведение распространять, необходимо его изготовить в определенном количестве экземпляров. Распространением является продажа или введение в гражданский оборот иным способом ограниченного числа копий произведения.

Право на публичный показ и право на публичное исполнение произведения законодательно отнесены к числу важных имуществен-ных прав. Публичный показ означает представление произведения (преимущественно произведений изобразительного искусства) пуб-лике непосредственно или с помощью технических средств (напри-мер, телевидение, изображение на экране с помощью проекционного аппарата и др.).

Публичным исполнением является представление широкой пуб-лике произведения посредством игры, декламации, танца в живом исполнении или с помощью технических средств. Право на публичное исполнение относится преимущественно к музыкальным, драматическим, хореографическим и литературным произведениям.

Закон закрепляет за автором право разрешать или запрещать пе-редачу в эфир (Интернет) своего произведения для всеобщего сведе-ния.

Автор или его правопреемник имеет право осуществлять или разрешать перевод произведения на другой язык.

2.5. Охрана смежных прав авторов

К смежным правам относятся права исполнителей на исполняе-мые произведения, права производителей фонограмм на их фоно-граммы и права организаций эфирного или кабельного вещания. Смежные права предусматривают охрану прав тех, кто оказывает по-мощь творцам произведений в доведении творческого замысла автора до сведения широкой аудитории, и в этом смысле они производны и зависимы от прав создателей произведения. В связи с этим, Законом Республики Беларусь «Об авторском праве и смежных правах» (ст.

29) четко оговорено, что как субъект авторского права исполнитель осуществляет свои права при условии соблюдения прав автора исполняемого произведения: производитель фонограммы, организация эфирного или кабельного вещания в свою очередь осуществляют свои права в пределах прав, полученных по договору с исполнителем и автором записанного или передаваемого в эфир произведения. Охрана прав исполнителей означает защиту интересов актеров,

певцов, музыкантов, танцоров и иных лиц, которые играют на сцене, выступают в концертах, декламируют или иными способами испол-няют литературные и художественные произведения.

Охрана прав производителей фонограмм подразумевает защиту интересов физических или юридических лиц, осуществивших первую звуковую запись какого-либо исполнения или иных звуков.

Под правами организации эфирного или кабельного вещания понимаются организации, ведущие радио- и телевещание, в том числе посредством кабельного и спутникового телевидения.

Для возникновения и осуществления прав, предусмотренных законом, не требуется соблюдения каких-либо формальностей. Положения закона также применяются к исполнителям, производителям фонограмм и организациям эфирного или кабельного вещания, кото-рым охрана прав на территории Республики Беларусь предоставляется в соответствии с международными договорами Республики Беларусь.

Промышленная собственность

3.1. Патенты и объекты патентования

Наиболее важной с точки зрения экономики является патентная форма охраны объектов промышленной собственности (изобретения, полезные модели, промышленные образцы), которая получила рас-пространение в всем мире.

Патент — это выдаваемый патентным органом от имени госу-дарства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование.

В Беларуси патентным органом является Национальный центр интеллектуальной собственности (г. Минск).

Патент имеет территориальное действие (при выдаче указыва-ется, на территории каких стран действует).

Патент имеет временное действие (срок действия ограничен):

• патент на изобретение действует в течение 20 лет (до 25 лет); • патент на полезную модель действует в течение 5 лет (до 8

лет);

• патент на промышленный образец действует в течение 10 лет

(до 15 лет).

В соответствии со ст. 6 Закона Республики Беларусь патент вы-

дается:

• автору (соавторам) объекта промышленной собственности;

• физическому и (или) юридическому лицу (лицам), являющемуся нанимателем автора;

• физическому и (или) юридическому лицу или нескольким физическим и (или) юридическим лицам, которые указаны автором (соавторами) в заявке на выдачу патента;

• правопреемнику (правопреемникам) лиц, указанных выше. Изобретение, полезная модель, промышленный образец являют-

ся служебными, если они относятся к области деятельности нанима-теля, при условии что деятельность, которая привела к их созданию, относится к служебным обязанностям работника, либо созданы в свя-зи с выполнением работником конкретного задания, полученного от нанимателя.

Действие патента может быть прекращено досрочно:

- на основании заявления патентообладателя, поданного в патентный орган;

- при неуплате в установленный срок годовой пошлины за поддержание патента в силе;

- при признании патента недействительным.

Важное значение при определении патентоспособности объекта промышленной собственности имеет его приоритет (первенство).

Приоритет изобретения, полезной модели, промышленного образца устанавливается по дате подачи заявки в патентный орган.

3.2. Критерии патентоспособности

6 декабря 2002 г. издан Закон Республики Беларусь «О патентах на изобретения, полезные модели и промышленные образцы», воплотивший последние достижения мировой системы охраны прав на объекты промышленной собственности и положения международных договоров.

Закон устанавливает действия по приему и рассмотрению заявок на изобретения, полезные модели и промышленные образцы, определяет права авторов и патентообладателей, устанавливает критерии патентоспособности, правила и процедуры экспертизы, публикации и выдачи патента.

Для получения автором патента на свой объект промышленной собственности необходимо провести его экспертизу на соответствие критериям патентоспособности.

Критерии патентоспособности:

1. Новизна.

Изобретение признается новым, если оно не является частью уровня техники. При оценке новизны технического решения ему могут быть противопоставлены лишь источники, существовавшие до даты приоритета. Если до даты подачи заявки (приоритета) сущность заявленного или тождественного ему решения не была раскрыта настолько, что стало возможным его осуществление, решение признается новым.

2. Технический (изобретательский) уровень.

Критерий изобретательский уровень означает, что

предложенное решение является результатом творческой деятельности, т. е. оно характеризуется новой совокупностью заяв-ленных признаков. Решение должно не просто быть очевидным, исходя из существующего уровня знаний, а представлять качественное развитие знания, превышать уровень обычного проектирования. Сравнение с предшествующим уровнем проводят по сумме отличий, которыми обладает новое решение по отношению к известным.

3. Промышленная применимость.

Это определение предполагает оценку принципиальной пригодности изобретения для использования в какой-либо из отраслей экономики (промышленность, сельское хозяйство, здраво-охранение) по указанному в материалах заявки назначению. При этом не должен возникать вопрос о возможных масштабах его использова-ния. Такому требованию соответствуют и изобретения, реализуемые лишь однократно в специфических, неповторимых условиях. Для признания изобретения промышленно применимым необходимо под-тверждение возможности его осуществления с помощью средств и методов, описанных в материалах заявки или источниках, ставших общедоступными до даты приоритета.

В соответствии с Законом «О патентах на изобретения, полез-ные модели, промышленные образцы» объектом изобретения являет-ся продукт, т. е. предмет как результат человеческого труда, и способ-процесс, прием или метод выполнения взаимосвязанных действий над объектом, а также применение процесса, приема, метода или про-дукта по определенному назначению.

3.3. Две мировые системы выдачи патентов

Правовая охрана объектов промышленной собственности осу-ществляется на основе национального законодательства и междуна-родных соглашений.

В мире существует две основные системы выдачи патентов:

- явочная;
- проверочная.

В связи со значительным ростом количества подаваемых заявок, увеличением сроков проведения экспертизы в ряде стран (Нидерлан-ды, ФРГ, Япония, Австралия, Россия, Беларусь и др.) введена отло-женная (отсроченная) система, как модификация проверочной.

Явочная система принята в ряде стран Африки, Азии, Южной Америки, а также в Италии, Испании, Греции и других странах.

Достоинство этой системы состоит в том, что заявитель срав-нительно быстро получает патент, а общественность также быстро получает информацию об изобретении
Недостатки явочной системы:

- определенное число патентов не имеет ценности из-за отсутствия новизны и технического уровня;

- могут регистрироваться заведомо бесполезные решения, вводящие в заблуждение общественность;

- теряется доверие промышленности к действительной значимости патентов;

- велика вероятность аннулирования патентов решением суда со всеми вытекающими экономическими последствиями.

Проверочная (исследовательская) система предусматривает проведение как формальной, так и патентной экспертизы заявок на соответствие критериям: новизна, изобретательский уровень, про-мышленная применимость. Патент,

выданный по проверочной систе-ме, удостоверяет наличие отличий предмета изобретения от извест-ных решений в данной области техники. Проверочная система приня-та в США, Швеции, Индии и других странах.

Достоинства: патент гарантирует новизну, способствует конку-рентоспособности продукции.

Недостатки: данная система требует достаточного количества высококвалифицированных экспертов, является более дорогостоящей по сравнению с явочной и отличается более длительной процедурой рассмотрения — от подачи заявки до выдачи патента.

Отложенная (отсроченная) система предусматривает проведе-ние формальной экспертизы и обязательную публикацию (выкладку) заявки не более чем через 18 месяцев после даты ее подачи. Патент-ная экспертиза проводится по ходатайству заявителя или другого за-интересованного лица в установленные сроки (в ФРГ, Нидерландах

— 7 лет, в Австрии — 5 лет, в России, Беларуси — 3 года).

Сохраняя все преимущества проверочной, отложенная система предоставляет возможность заявителю оценить практическую значи-мость предполагаемого изобретения, перспективы его коммерческой реализации и в любые разумные, в пределах возможных, сроки по-дать ходатайство на проведение экспертизы по признакам патенто-способности.

В Республике Беларусь, например, более 90 % ходатайств о про-ведении патентной экспертизы подаются сразу же после проведения формальной экспертизы и получения уведомления о приеме заявок патентным органом

С даты публикации сведений о заявке на изобретение до даты публикации сведений о патенте заявленному изобретению предостав-ляется временная правовая охрана. После опубликования выложен-ной заявки любое лицо может подать возражения против выдачи па-тента.

3.4. Изобретение как объект промышленной собственности

Изобретения относятся к объектам промышленной собственно-сти и защищаются патентами.

Для патентования изобретения необходимо его соответствие трем критериям патентоспособности:

- новизна,
- технический уровень,
- промышленная применимость.

Изобретение может быть представлено в одном из трех видов:

- устройство;
- способ;
- вещество.

Устройство как объект изобретения — это новое, обладающее изобретательским уровнем и промышленной применимостью соору-жение (изделие).

К ним относятся машины, приборы, аппараты, оборудование, инструмент, тара, транспортные средства, крепежные изделия, детали машин.

Способ как объект изобретения — это новый и обладающий су-щественными отличиями, изобретательским уровнем и промышленно применимый процесс выполнения взаимосвязанных действий над ма-териальным объектом и с помощью материальных объектов.

Это процессы выполнения действий (операций, приемов), при-водящие к созданию новых или изменению известных материальных объектов, или процессы исследования материальных объектов.

Вещество как объект изобретения — это новое, обладающее изобретательским уровнем и промышленной применимостью искусственно созданное материальное образование.

Это химические соединения, в том числе и высокомолекулярные соединения, композиции (составы, смеси), продукты ядерного превращения.

3.5. Полезная модель как объект промышленной собственности

Полезной моделью является конструктивное выполнение средств производства и предметов потребления. Ей предоставляется правовая охрана (выдается патент), если она соответствует только двум крите-риям патентоспособности:

- является новой;

- промышленно применимой (треугольная насадка на шланг пылесоса).

Не требуется высокого технического уровня!

Полезная модель является новой, если совокупность ее суще-ственных признаков не является частью уровня техники.

Полезная модель является промышленно применимой, если она может быть использована в промышленности, сельском хозяйстве, здравоохранении и других сферах деятельности.

3.6. Промышленный образец как объект промышленной собственности

Промышленным образцом, которому предоставляется правовая

охрана, признается дизайнерское или художественно-конструкторское решение промышленного изделия, определяющее его внешний вид и являющееся новым и оригинальным.

Промышленному образцу предоставляется правовая охрана (вы-дается патент), если он соответствует только двум критериям патен-тоспособности:

- является новым;
- промышленно применимым.

Не требуется высокого технического уровня!

Промышленные образцы реализуются в различных изделиях промышленного назначения (станках, приборах, транспортной техни-ке) и в других средствах и предметах потребления (мебели, бытовой технике, детских игрушках, ковровых изделиях и др.). Изящные и эс-тетичные формы машин и приборов оказывают положительное влия-ние на настроение и работоспособность человека, предметы домаш-него обихода воспитывают тонкий вкус, повышают культурный уро-вень.

Эстетичные и эргономичные формы и конфигурации изделий стали важнейшим фактором коммерческого успеха. Поэтому эффек-тивная правовая охрана новых и оригинальных художественных и художественно - конструкторских решений позволяет предотвратить экономический ущерб от подделок, других пиратских действий, и обеспечивает добросовестную конкуренцию на рынке.

Промышленный образец признается новым, если совокупность его существенных признаков неизвестна из сведений, ставших обще-доступными в мире до даты приоритета.

К существенным признакам относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида из-делия, его формы, конфигурации, орнамента и сочетания цветов.

Правовая охрана не предоставляется:

• объектам неустойчивой формы из жидких, газообразных, сыпучих и им подобных веществ;

• решениям, противоречащим общественным интересам.

3.7. Правовая охрана товарных знаков и знаков обслуживания

Товарные знаки широко используются во всем мире и играют важную экономическую роль в маркетинге и торговле. Ценность то-варного знака состоит в том, что он: 1) способствует завоеванию ре-путации производителя товара, 2) стимулирует спрос на соответ-ствующие товары, 3) позволяет конкурировать с аналогичными това-рами других производителей.

Одновременно с товарами в сфере торговли обращаются и услу-ги. Их предоставляют туристические фирмы, рекламные агентства, транспортные и страховые компании, гостиницы, рестораны, авиали-нии, прачечные, химчистки и др. В качестве отличительного знака эти предприятия используют знаки обслуживания.

В ст. 1 Закона Республики Беларусь «О товарных знаках и зна-ках обслуживания» дано следующее определение товарного знака и знака обслуживания: «Товарный знак и знак обслуживания — обо-значение, способствующее отличию товаров и услуг одних юридиче-ских или физических лиц от однородных товаров или услуг других юридических или физических лиц».

В качестве товарных знаков регистрируются обозначения, кото-рые могут быть представлены в графической форме: словесные, бук-венные,

цифровые, изобразительные, трехмерные, включая форму то-вара или его упаковку, другие обозначения и их комбинации.

Словесные знаки находят свое выражение в определенном сло-ве, например: «Элема», «Фея», «CASIO», «IBM».

Изобразительные товарные знаки представляют собой рисунки на самые разнообразные темы. Это различные символы, изображения животных, птиц, стилизованные изображения всевозможных предметов (например, изображение льва для автомобилей французской фир-мы «Пежо»).

Основные функции товарных знаков:

а) отличительная, служащая для обозначения производителя товара или организации по оказанию услуг;

б) средства индивидуализации товаров и услуг, т. е. с помощью товарного знака различают однородные товары, например, сигареты «ВТ» и «Орбита»;

в) стимулирующая, или качественная, когда товарный знак свидетельствует о качестве продукции, выпускаемой конкретным пред-приятием или фирмой. Так, мировой известностью пользуется спортивная одежда фирмы «ADIDAS», напитки фирмы «Coca-Co1a»;

г) рекламная, т. е. обеспечение прав на товарный знак позволяет осуществлять необходимую рекламную работу, поэтому не случайно фирмы платят крупные денежные суммы за изображения их товарных знаков в местах проведения спортивных и зрелищных мероприятий;

д) культурно-просветительной, способствующая эстетическому воспитанию, распространению знаний.

Право на товарный знак и знак обслуживания охраняется государством. На основании решения о регистрации товарного знака патентный орган производит его регистрацию в Государственном ре-естре товарных знаков и знаков обслуживания.

Приоритет товарного знака устанавливается по дате подачи за-явки в патентный орган.

Первым знаком, получившим охрану в Республике Беларусь в качестве общеизвестного, является комбинированный товарный знак «Мілавіца» по отношению к корсетным изделиям.

3.8. Недобросовестная конкуренция

Защита от недобросовестной конкуренции с 1900 г. считается частью системы охраны промышленной собственности.

Международным бюро Всемирной организации интеллектуаль-ной собственности (ВОИС) подготовлены типовые положения о за-щите от недобросовестной конкуренции.

Общие принципы сводятся к тому, что любой акт или обычай при осуществлении промышленной или коммерческой деятельности считается актом недобросовестной конкуренции, если он:

- а) противоречит честным обычаям;

- б) создает или может создать смешение в отношении предприятия, другого лица или его деятельности, в частности, продуктов или услуг;

- в) наносит или может нанести ущерб гудвиллу (деловой репутации) или репутации другого предприятия;

- г) вводит или может ввести в заблуждение в отношении предприятия или его деятельности;

- д) дискредитирует или может дискредитировать предприятие другого лица или его деятельность.

38. Патентные исследования

Патентные исследования - исследования технического уровня и тенденций развития ОТ, их патентоспособности и патентной чистоты на основе патентной и другой научно-технической информации.

Основной целью патентных исследований является получение исходных данных для обеспечения высокого технического уровня и конкурентоспособности ОТ, использование современных научных достижений и исключение неоправданного дублирования исследований и разработок.

Задачи патентных исследований определяются разработчиками на соответствующих стадиях жизненного цикла ОТ. Основные этапы патентных исследований:

1. анализ патентно-лицензионной ситуации;
2. анализ "ведущих в данном виде техники фирм";
3. тенденции развития техники;
4. технический уровень.

Патентные исследования включают в себя:

• разработку регламента поиска информации;
• поиск и отбор патентной и другой научно-технической документации;
• систематизацию и анализ отобранной документации;
• обобщение результатов и составление отчета.

Разработка регламента - важный этап, от которого зависит достоверность отчета в целом, так как регламент ограничивает область проведения поиска по фондам патентной, научно-технической и конъюнктурно-экономической информации. На этом этапе определяется предмет поиска, его классификация по МПК, НКИ, МКПО, УДК, определение стран поиска, фирм, определение ретроспективы или глубины поиска, выбор источников информации.

Патентные исследования проводят при:

· разработке научно-технических прогнозов;
· разработке планов развития науки и техники;
· создании объектов техники;
· освоении и производстве продукции;
· определении целесообразности экспорта промышленной продукции и экспонировании ее
· образцов на международных выставках и ярмарках;
· продаже и приобретении лицензий;

· при решении вопроса о патентовании созданных объектов промышленной собственности и

· в других целях.

Особенности патентных исследований

Содержание патентных исследований может включать:

- исследование технического уровня объектов техники, выявление тенденций и направлений их развития;
- исследование состояния рынков конкретной продукции, сложившейся патентной ситуации, выявление требований потребителей к товарам и услугам;
- исследование направлений научно-исследовательской и производственной деятельности предприятий и фирм, которые действуют или могут действовать на определенном рынке продукции;
- технико-экономический анализ и обоснование выбора технических, художественно-конструкторских решений, отвечающих требованиям создания новых объектов техники; выявление новых технических, художественно-конструкторских решений, определение их патентоспособности и обоснование целесообразности правовой охраны, выбор стран патентования;
- исследование патентной чистоты объектов техники;
- обоснование целесообразности и форм проведения за рубежом коммерческих мероприятий по реализации объектов техники, закупке и продаже лицензий, оборудования, комплектующих изделий и т.д.

Одной из важнейших частей патентного исследования является поиск патентной информации. Он включает процессы отбора соответствующих заданию документов или сведений из массива патентных документов.

Цели патентного поиска определяются задачами использования патентной информации на конкретной стадии создания, освоения и реализации новой техники или продукции. При планировании тематики патентный поиск проводится для того, чтобы выяснить, решалась ли поставленная техническая задача ранее, какие решения защищены патентами, какие фирмы работают в данной области техники, каковы перспективы разработки темы. Поиск проводится также с целью техникоэкономического анализа изобретений при прогнозировании тенденций развития техники.

39. Коммерческое использование объектов интеллектуальной собственности

Успешное использование объектов промышленной собственности, получивших правовую охрану, в производственной деятельности субъектов хозяйствования является важнейшим условием обеспечения конкурентоспособности производимых ими товаров и оказываемых услуг.

В каждом товаре заложены результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, ноу-хау, организационные и иные решения. Объекты промышленной собственности представляют собой научно-технические, художественно-конструкторские решения и взаимосвязанные с ними ноу-хау, обеспечивают новизну и высокий технический уровень продукции, эффективность использования всех видов производственных ресурсов.

Получение охранных документов, подтверждающих право собственности, позволяет контролировать рынок, пресекать деятельность недобросовестных конкурентов.

Порядок использования объектов промышленной собственности регулируется законодательством Республики Беларусь. Так, в соответствии с Законом Республики Беларусь «О патентах на изобретения, полезные модели, промышленные образцы» [8, Ст. 36] под использованием

изобретения признается введение в гражданский оборот продукта, изготовленного с применением запатентованного изобретения, а также способа, охраняемого патентом.

Востребованность объектов промышленной собственности предприятиями и организациями определяется способностью этих объектов приносить доход (прибыль) за счет: снижения себестоимости, материалоемкости и энергоемкости товарной продукции; повышения качественных показателей продукции; повышения экологичности продукции и т. д.

В то же время результаты практической реализации создаваемых в РБ объектов промышленной собственности пока нельзя признать удовлетворительными.

Ежегодно впервые осваивается не более 100 новых изобретений, что составляет около 10 % от количества регистрируемых патентов. Показатели по другим объектам (промышленные образцы, полезные модели) значительно ниже. Эти данные, безусловно, не соответствуют научно-техническому потенциалу и потребностям в обновлении и совершенствовании производственных фондов, применяемых технологий и материалов.

Очевидно, не все созданные объекты промышленной собственности могут найти практическое применение.

Определенная доля объектов промышленной собственности не получает коммерческого воплощения из-за высоких первоначальных затрат на доведение их до стадии практической реализации. Кроме того, часть принципиально новых решений не может быть осуществлена при имеющемся уровне технического развития конкретной отрасли и относится к категории неперспективных.

Данные о практической реализации объектов промышленной собственности показывают, что из всего количества создаваемых изобретений лишь 10–15

% приносят ощутимый доход патентообладателю. В то же время имеются примеры более успешной деятельности. Например, фирма IBM выделяется не только количеством получаемых патентов, но и значительной долей (около 50 %) их коммерческой реализации, что обеспечивает годовой поток поступлений в размере 1,2 млрд долларов. Часть этих средств вкладывается в проведение научных исследований и разработок, которые дают поток новых изобретений. Таким образом, реализуется классическая модель инновационного процесса: исследования — изобретения — патенты — новые изделия — прибыль — инвестирование в исследования — новые изобретения.

Управление интеллектуальной собственностью не ограничивается использованием ее в качестве нематериальных активов предприятий и организаций. Существенные доходы можно получить от реализации ОИС в качестве товара на внутреннем и внешних рынках по лицензионным договорам.

Основной целью использования объектов промышленной собственности (изобретений, полезных моделей, промышленных образцов) является производство продукции более высокого технического уровня и качества, получение большей нормы прибыли на вложенный капитал благодаря новизне и оригинальности решений.

40. Защита прав авторов и правообладателей

Защита авторских прав

Объектами авторского права являются: музыкальные и литературные произведения, скульптурные произведения, произведения живописи, программы ЭВМ и т. д.

Закон РБ «Об авторском праве и смежных правах» как закон гражданско-правовой не содержит норм об уголовной и административной ответственности за нарушение авторских и смежных прав.

В общей форме в Законе установлено, что за нарушение авторских и смежных прав наступает либо гражданская, либо уголовная и административная ответственность.

Соответствующие нормы внесены в Уголовный кодекс РБ и РБ об административных правонарушениях, Гражданский кодекс.

Гражданская ответственность за нарушение авторских прав

1. Автор, обладатель смежных прав или иной обладатель исключительных прав вправе защитить свои права способами, предусмотренными Гражданским кодексом РБ.

2. Обладатели исключительных прав вправе требовать по своему выбору от нарушителя, вместо возмещения убытков, выплаты компенсации:

• в размере от 10 до 50 минимальных заработных плат, определяемом по усмотрению суда;

• в двукратном размере стоимости экземпляров произведений или объектов.

Компенсация подлежит взысканию при доказанности факта правонарушения независимо от наличия или отсутствия убытков.

3. Авторы и исполнители в случае нарушения их личных неимущественных прав или имущественных прав также вправе требовать от нарушителя возмещения морального вреда.

4. Автор, обладатель смежных прав или иной обладатель исключительных прав в установленном законом порядке вправе обратиться для защиты своих прав в суд, арбитражный суд, органы прокуратуры, органы дознания, органы предварительного следствия в соответствии с их компетенцией.

Уголовная ответственность за нарушение авторских и смежных прав

Уголовным преступлением в соответствии с Законом признается незаконное использование объектов авторского права, а равно присвоение авторства, если эти действия причинили крупный ущерб.

Объектом данного преступления являются не все охраняемые законом авторские и смежные с ними права, а лишь право авторства, а также право на использование, т. е. вся совокупность принадлежащих обладателям авторских и смежных прав правомочий имущественного характера.

Нарушение иных прав авторов, в частности, права на имя, права на обнародование, право на защиту репутаций и так далее уголовно наказуемого деяния не образуют.

Защита патентных прав

Защита прав и законных интересов изобретателей и патентообладателей — это предусмотренные законом меры по их признанию и восстановлению, пресечению их нарушений, применением к нарушителям мер ответственности, а также механизм практической реализации этих мер.

Субъектами прав на защиту прав авторов и патентообладателей являются: авторы разработок; патентообладатели; владельцы лицензий; правопреемники перечисленных лиц.

Формы защиты прав:

• юрисдикционная форма защиты охватывает судебный и административный порядок реализации предусмотренных законом мер защиты, при этом общим является судебный порядок;

• неюрисдикционная форма — принятие потерпевшим мер по самозащите нарушенных прав; эта форма защиты встречается редко и в основном сводится к отказу от совершения каких-либо действий.

Различают следующие способы защиты прав авторов и патентообладателей.

Гражданская ответственность за нарушение патентных прав

Включает в себя предусмотренные законом меры принудительного характера, с помощью которого осуществляется восстановление (признание) нарушенных прав и интересов создателей изобретений, полезных моделей и промышленных образцов, пресечение нарушений, а также имущественное воздействие на нарушителей.

Нарушения исключительных прав авторов и патентообладателей, попадающие под гражданско-правовые способы защиты:

• присвоение результатов чужого творческого труда и попытка выдать их за собственную разработку;

• неуказание имени действительного разработчика в официальных и неофициальных публикациях;

• несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью продукта, содержащего запатентованное изобретение, полезную модель.

Пострадавший составляет иск в соответствии с общими правилами по месту жительства ответчика или по месту нахождения органа или имущества юридического лица.

Уголовная ответственность за нарушение патентных прав

Уголовно-правовые — это действия, отнесенные УК РБ к числу уголовно-правовых нарушений в сфере патентного права (если эти действия причинили крупный ущерб). К ним относятся:

• незаконное использование изобретений;

• разглашение без согласия автора сущности изобретения;

• присвоение авторства;

• принуждение к соавторству.

Введение уголовной ответственности за нарушение патента в целом усиливает ответственность в данной области, хотя, судя по зарубежному

опыту, патентообладатель стремится в первую очередь добиться полного возмещения причиненных ему убытков.

Нарушение изобретательских и патентных прав наказывается штрафом либо обязательными общественными работами, либо лишением свободы на срок до двух лет.