**Конспект ОЗИ Насоновой**

**РАЗДЕЛ 1 МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

* 1. **Основные понятия и определения в сфере защиты информации**

**Целью обеспечения национальной безопасности** является достижение и поддержание такого уровня защищенности личности, общества и государства от внутренних и внешних угроз, который гарантирует устойчивое развитие Республики Беларусь и реализацию ее национальных интересов.

**Основными задачами** обеспечения национальной безопасности выступают:

- разработка и реализация государственной политики обеспечения национальной безопасности;

- определение и поддержание необходимого баланса интересов личности, общества и государства;

- нейтрализация источников внутренних угроз и защита от внешних угроз национальной безопасности;

- обеспечение реализации национальных интересов и устойчивого развития Республики Беларусь;

- создание системы обеспечения национальной безопасности и организация ее эффективного функционирования.

Принципами обеспечения национальной безопасности являются:

- законность, соблюдение конституционных прав и свобод человека;

- гуманизм и социальная справедливость;

- гласность;

- соблюдение баланса интересов личности, общества и государства, их взаимная ответственность;

- комплексный подход к решению задач обеспечения национальной безопасности;

- единство и взаимосвязь видов и направлений обеспечения национальной безопасности;

- участие в системах международной и региональной коллективной безопасности;

- разграничение сфер ответственности и полномочий государственных органов в решении задач обеспечения национальной безопасности;

- приоритетность правовых, политических, экономических и информационных мер обеспечения национальной безопасности;

оперативность, своевременность, превентивность и соразмерность мер по нейтрализации источников внутренних угроз и защите от внешних угроз.

**Целями защиты информации** являются: предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы.

**Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах не зависимо от формы их предоставления.

Информация может существовать в виде документа (бумажного), в виде физических полей и сигналов (электромагнитных, акустических, тепловых и т. д.), в виде биологических полей (память человека).

В дальнейшем будем рассматривать информацию в документированной (на бумаге, дискете и т. д.) форме, в форме физических полей (радиосигналы, акустические сигналы). Среду, в которой информация либо создается, либо передается, обрабатывается, хранится, будем называть **информационным объектом**.

Под **безопасностью информационного объекта (ИО)** будем понимать его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

Природа воздействия на ИО может быть двух видов: непреднамеренной (стихийные бедствия, отказы, ошибки персонала и т. д.); преднамеренной (действия злоумышленников). Все воздействия могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности; нарушению целостности; нарушению доступности.

Информация делится на следующие виды:

1. Общедоступная - о правах, свободах и законных интересах физических и юридических лиц и о порядке реализации прав, свобод и законных интересов и т.д.

2. Ограниченного распространения - о частной жизни физического лица и персональные данные, сведения, составляющие государственные секреты, информация, составляющая коммерческую и профессиональную тайнуи т. д.

* 1. **Охраняемые сведения и их демаскирующие признаки**

**Охраняемые сведения** - сведения, содержащие государственные секреты или отнесенные к другой информации ограниченного распространения.

**Демаскирующие признаки (ДП)** — характеристики любого рода, поддающиеся обнаружению и анализу с помощью специальных технических средств негласного получения информации (СТСНПИ) и являющиеся источниками информации об охраняемых сведениях. Классификация ДП представлена на рисунке 1.1.

**Первичные ДП** - представляют собой физические характеристики объектов и среды, непосредственно регистрируемые СТСНПИ и содержащие информацию об охраняемых сведениях (амплитуда, частота и фаза переменного электрического тока, уровень радиационного излучения, процентное содержание химического вещества в среде и т.д.).

**Вторичные ДП** - признаки, которые могут быть получены путем накопления и обработки первичных ДП.

|  |
| --- |
| Безымянный  Рисунок 1.1. – Классификация демаскирующих признаков |

Опознавательные признаки описывают объекты в статическом состоянии: его внешний вид, излучения, физические и химические свойства и др. Признаки деятельности объектов характеризуют этапы и режимы функционирования объектов. Например, этапы создания новой продукции включают: научные исследования, подготовку к производству, изготовление новой продукции, ее испытания и т.д. Признаки деятельности представляют собой последовательность во времени событий или действий составных элементов рассматриваемого объекта и взаимодействующих с ним объектов, а также значения статистических характеристик событий и действий. Например, по активности посещения студентами библиотек и их количеству в читальном зале можно спрогнозировать время сдачи курсового проекта, зачета или экзамена. По активности работы средств радиосвязи войсковой части можно определить вид их деятельности: повседневная деятельность в местах постоянной дислокации, подготовка к передислокации, перемещение, развертывание в месте новой дислокации.

Демаскирующие признаки объекта можно разделить на три группы:

• видовые признаки;

• признаки сигналов;

• признаки веществ.

К видовым признакам относятся форма объекта, его размеры,  
детали объекта, тон, цвет и структура его поверхности и др.

Признаки сигналов описывают параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т.д.

Признаки веществ определяют физический и химический состав, структуру и свойства веществ материального объекта.

Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет собой модель объекта, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.

Важнейшим показателем признака является его информативность. Информативность признака оценивается мерой в интервале [0-1], характеризующей его индивидуальность. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен. Величину информативности можно определить как Ik = (N - Nk) / N, где Nk - количество объектов, содержащих признак k, из N рассматриваемых. Если признак принадлежит одному объекту, то информативность максимальная и приближается к 1; если признак принадлежит всем объектам выборки, то информативность нулевая. Информативность конкретного k-го признака можно характеризовать вероятностью Pt обнаружения конкретного объекта по этому признаку среди других рассматриваемых объектов.

Наиболее информативен именной признак, присущий одному конкретному объекту. Такими признаками являются фамилия, имя, отчество человека, папиллярный рисунок его пальцев, инвентарный номер прибора или образца мебели. Факты, например, о совпадении папиллярных узоров пальцев хотя бы двух разных людей не известны.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых прямыми, колеблется в пределах [0-1]. Признаки, непосредственно не принадлежащие объекту, но отражающие его свойства и состояние, называются косвенными. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Следы краски или характер деформации поверхности автомобиля в результате автодорожного происшествия позволяют находить автомобиль, скрывшийся с места происшествия. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако если в результате взаимодействия объектов на одном из них появляются именные признаки другого объекта, то информативность косвенного признака может приближаться к 1, например, четкие отпечатки пальцев на предметах, следы обуви, протектора шин машины и др.

По времени проявления признаки могут быть:

• постоянными, не изменяющимися или медленно меняющимися  
в течение жизненного цикла объекта;

• периодическими, например следы на снегу;

• эпизодическими, проявляющимися при определенных услови-  
ях, например случайно появившееся на поверхности объекта  
пятно краски.

По времени проявления признаки могут быть:

- постоянными, не изменяющимися или медленно меняющимися в течение жизненного цикла объекта;

- периодическими, например следы на снегу;

- эпизодическими, проявляющимися при определенных условиях, например случайно появившееся на поверхности объекта пятно краски.

**Государственные секреты** - защищаемые государством сведения, распространение которых может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам Республики Беларусь.

Государственная секреты являются собственностью Республики Беларусь.

Категории государственных секретов:

1. Служебная тайна - сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

2. Государственная тайна - сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Существуют следующие ограничительные грифы:

1. Особой важности.

2. Совершенно секретно.

3. Секретно.

Формы допуска к государственным секретам:

1. Форма 1.

2. Форма 2.

3. Форма 3.

**Носитель государственных секретов** - материальный объект, на котором государственные секреты содержатся в виде символов, образов, сигналов и (или) технических решений и процессов, позволяющих их распознать и идентифицировать.

**1.3 Классификация угроз информационной безопасности и методов защиты информации**

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 виду на:

– конфиденциальности информации - нарушение свойства информации быть известной только определенным субъектам;

– целостности - несанкционированное изменение, искажение, уничтожение информации;

– доступности (работоспособности) - нарушаются доступ к информации, работоспособность объекта, доступ к которому получил злоумышленник.

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).

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибок персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).

Преднамеренные угрозы связаны с действиями людей. Это и работники спецслужб, хакеры, работники самого объекта. Огромное количество разнообразных ИО делает 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.

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. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

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.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т. е. комплексно.

**РАЗДЕЛ 2 ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**2.1 Государственное регулирование в сфере 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:

1. Оценка состояния действующего законодательства и разработка программы его совершенствования.

2. Создание организационно правовых механизмов обеспечения защиты информации.

3. Формирование правового статуса всех субъектов в системе защиты информации и определение их ответственности за обеспечение информационной безопасности.

4. Разработку организационно правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех категорий информации.

5. Разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановление права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность:

1. Разработка процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией.

2. 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).

Нормативно-правовая база в области защиты информации основывается на общегосударственных документах и ведомственных документах.

Общегосударственные документы:

1) Законы, кодексы;

2) Указы Президента Республики Беларусь;

3) Постановления Совета Министров.

Ведомственные документы:

1) межведомственные;

2) внутриведомственные.

Основные правовые акты, регламентирующие защиту информации в Республике Беларусь:

Концепция национальной безопасности Республики Беларусь (9 ноября 2010 г.) представляет собой совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз и обеспечивает единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования.

Закон Республики Беларусь «Об информации, информатизации и защите информации» (9 октября 2008 г.) является основой для регулирования общественных отношений, возникающих при:

– поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

– создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

– организации и обеспечении защиты информации.

Постановление Совета Министров Республики Беларусь «О некоторых вопросах защиты информации» (26 мая 2009 г.) регламентирует порядок:

– защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено;

– аттестации систем защиты информации;

– проведения государственной экспертизы средств защиты информации.

Постановление Совета Министров Республики Беларусь «Об утверждении положения о лицензировании деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи» (20 октября 2003 г.) устанавливает порядок выдачи специальных разрешений (лицензий) на осуществление деятельности по технической защите информации, в том числе криптографическими методами, включая применение электронной цифровой подписи.

Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» (28 декабря 2009 г.) определяет правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе.

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасности компании. Это прежде всего международные и национальные стандарты управления информационной безопасностью ISO 15408, ISO 17799 (BS7799), BSI; стандарты аудита информационных систем и информационной безопасности COBIT, SAC, COSO, SAS 78/94 и некоторые другие, аналогичные им.

В соответствие с международными и национальными стандартами ISO 15408, ISO 17799 (BS7799), BSI; COBIT, SAC, COSO, SAS 78/94 обеспечение информационной безопасности в любой компании предполагает следующее. Во-первых, определение целей обеспечения информационной безопасности компьютерных систем. Во-вторых, создание эффективной системы управления информационной безопасностью. В третьих, расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям. В четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния. В пятых, использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации.

Международный стандарт ISO 15408

Следуя по пути интеграции, в 1990 г. Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (ТЕС) составили специализированную систему мировой стандартизации, a ISO начала создавать международные стандарты по критериям оценки безопасности информационных технологий для общего использования, названные Common Criteria for Information Technology Security Evaluation или просто Common Criteria. В их разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Нидерланды), Органы исполнения программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция).

В дальнейшем "Общие критерии" неоднократно редактировались. В результате 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием "Общие критерии оценки безопасности информационных технологий" (ОК).

Общие критерии обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии, и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК — полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Использование методик данного стандарта позволяет определить для компании те критерии, которые могут быть использованы в качестве основы для выработки оценок защитных свойств продуктов и систем информационной технологии. Кроме того, эти методики позволяют проводить наиболее полное сравнение результатов оценки защитных свойств корпоративных информационных систем с помощью общего перечня (набора) требований для функций защиты продуктов и систем, а также методов точных измерений, которые проводятся во время получения оценок защиты. Основываясь на этих требованиях, в процессе выработки оценки уровня защиты устанавливается уровень доверия.

Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Вместе с тем в ОК главное внимание уделено защите от несанкционированного доступа (НСД). Модификации или потери доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов информационной безопасности остался не рассмотренным. Например, оценка административных мер безопасности, оценка безопасности от побочных электромагнитных излучений, методики оценки различных средств и мер безопасности, критерии для оценки криптографических методов защиты информации.

Поэтому необходимо дополнять данный подход рядом своих собственных апробированных методик оценки важнейших элементов защиты. Дополненные таким образом ОК можно использовать как при задании требований к продуктам и системам информационных технологий, так и при оценке их безопасности на всех этапах жизненного цикла корпоративной информационной системы.

Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

Версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;

- основные понятия и определения информационной безопасности;

- политика информационной безопасности компании;

- организация информационной безопасности на предприятии;

- классификация и управление корпоративными информационными ресурсами;

- Кадровый менеджмент и информационная безопасность;

- физическая безопасность;

- администрирование безопасности корпоративных информационных систем;

- управление доступом;

- требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;

- управление бизнес-процессами компании с точки зрения информационной безопасности;

- внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799-2:2000 "Спецификации систем управления информационной безопасностью - Information security management – Part 2: Specification for information security management systems”, определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов - British Standards Institution(BSI) http://www.bsi-global.com/, изданные в период 1995-2003 в виде следующей серии:

1. Введение в проблему управления информационной безопасности -Information security managment: an introduction.

2. Возможности сертификации на требования стандарта BS 7799 -Preparing for BS 7799 sertification.

3. Руководство BS 7799 по оценке и управлению рисками -Guide to BS 7799 risk assessment and risk management.

4. Готовы ли вы к аудиту на требования стандарта BS 7799-Are you ready for a BS 7799 audit?

5. Руководство для проведения аудита на требования стандарта – BS 7799Guide to BS 7799 auditing.

6. Практические рекомендации по управлению безопасностью информационных технологий -Code of practice for IT management.

**2.2 Нормативно-правовое обеспечение защиты информации в организации**

Стандарт BS ISO/IEC 27001:2005 описывает модель системы управления информационной безопасностью (СМИБ) и предлагает набор требований к организации информационной безопасности (ИБ) на предприятии без привязки к способам реализации, которые выбираются исполнителями организации.

В стандарте предложено применение модели PDCA (Plan-Do-Check-Act) к жизненному циклу СМИБ, который включает разработку, внедрение, эксплуатацию, контроль, анализ, поддержку и совершенствование (рисунок 2.1).

|  |
| --- |
| 1  Рисунок 2.1. – Применение модели PDCA к процессам СМИБ |

Решение о создании (и последующей сертификации) СМИБ принимается высшим руководством организации. Это демонстрирует поддержку и подтверждение руководством ценности СМИБ для бизнеса. Руководство организации инициирует создание группы по планированию СМИБ.

Группа, ответственная за планирование СМИБ, должна включать:

- представителей высшего руководства организации;

- представителей бизнес-подразделений, охватываемых СМИБ;

- специалистов подразделений ИБ;

- сторонних консультантов (при необходимости).

Рассмотрим этапы создания СМИБ.

**1 этап. Планирование СМИБ.**

Установление политики, целей, процессов и процедур, относящихся к управлению рисками и защите информации, в соответствии с общей политикой и целями организации.

**a) Определение области применения и границ СМИБ:**

- описание вида деятельности и бизнес-целей организации;

- указание границ систем, охватываемых СМИБ;

- описание активов организации (виды информационных ресурсов, программно-технические средства, персонал и организационная структура);

- описание бизнес-процессов, использующих защищаемую информацию;

**б) Определение политики в отношении СМИБ организации (расширенная версия ПБ).**

- содержание политики СМИБ:

- цели, направления и принципы деятельности в отношении защиты информации;

- ссылки на законодательные, нормативные и деловые требования, а также договорные обязательства по ЗИ, определение на их основе основных требований и положений политики ИБ организации;

- описание стратегии (подходов) управления рисками в организации, структуризация контрмер по защите информации по видам (правовые, организационные, аппаратно-программные, инженерно-технические);

- описание критериев значимости риска;

- позиция руководства, определение периодичности проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядка обучения всех категорий пользователей информационной системы по вопросам ИБ.

**в) Определение подхода к оценке рисков в организации.**

Методология оценки риска выбирается в зависимости от СМИБ, установленных деловых требований защиты информации, законодательных и нормативных требований.

Выбор методологии оценки рисков зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер по защите информации. В частности различают базовые, а также повышенные или полные требования к режиму ИБ.

Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ. Такие требования применяются, как правило, к типовым проектным решениям. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как: вирусы, сбои оборудования, несанкционированный доступ и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно. Зарубежные стандарты в этой области ISO 27002, BSI, NIST и др.

В случаях, когда нарушения режима ИБ ведут к тяжелым последствиям, предъявляются дополнительно повышенные требования.

Для формулирования дополнительных повышенных требований, необходимо:

- определить ценность ресурсов;

- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

- оценить вероятности угроз;

- определить уязвимости ресурсов;

- оценить потенциальный ущерб от воздействий злоумышленников.

Необходимо подобрать такую методику оценки рисков, которую можно было бы использовать с минимальными изменениями на постоянной основе. Есть два пути: использовать существующие на рынке методики и инструментарий для оценки рисков или создать свою методику, адаптированную к специфике компании и охватываемой СМИБ области деятельности.

Последний вариант наиболее предпочтителен, поскольку пока большинство существующих на рынке продуктов, реализующих ту или иную методику анализа рисков, не отвечают требованиям Стандарта. Типичными недостатками таких методик являются:

- стандартный набор угроз и уязвимостей, который зачастую невозможно изменить;

- принятие в качестве активов только программно-технических и информационных ресурсов - без рассмотрения человеческих ресурсов, сервисов и других важных ресурсов;

- общая сложность методики с точки зрения ее устойчивого и повторяющегося использования.

Критерии принятия рисков и приемлемые уровни риска (должны базироваться на достижении стратегических, организационных и управленческих целей организации).

**в) Выявление рисков.**

Идентификация активов и их владельцев

Активы:

- информационные входные данные;

- информационные выходные данные;

- информационные записи;

- ресурсы: люди, инфраструктура, оборудование, программное обеспечение, инструменты, услуги.

Идентификация угроз (в стандартах по оценке рисков зачастую предлагаются классы угроз, которые можно дополнять и расширять).

Идентификация уязвимостей (также существуют списки наиболее распространенных уязвимостей, на которые можно опираться при анализе своей организации).

Определение ценности активов (возможные последствия от потери конфиденциальности, целостности и доступности активов). Информация о ценности актива может быть получена от его владельца или же от лица, которому владелец делегировал все полномочия по данному активу, включая обеспечение его безопасности.

**г) Оценка риска.**

- оценка ущерба, который может быть нанесен бизнесу от потери конфиденциальности, целостности и доступности активов.

- оценка вероятности реализации угроз через существующие уязвимости с учетом имеющихся средств управления ИБ и оценки возможного наносимого ущерба;

- определение уровня риска.

- применение критериев принятия риска (приемлемый/требующий обработки).

**д) Обработка рисков (в соответствии с выбранной стратегией управления рисками).**

Возможные действия:

- пассивные действия:

- принятие риска (решение о приемлемости полученного уровня риска);

- уклонение от риска (решение об изменении деятельности, вызывающей данный уровень риска – вынесение веб-сервера за границы локальной сети);

- активные действия:

- уменьшение риска (применением организационных и технических контрмер);

- передача риска (страхование (пожара, кражи, ошибок в ПО)).

Выбор возможных действий зависит от принятых критериев рисков (задается приемлемый уровень риска, уровни риска, которые могут быть понижены средствами управления ИБ, уровни риска, при которых рекомендуется отказаться или преобразовать вид деятельности, которая его вызывает, и риски, которые желательно передать другим сторонам).

**е) Выбор целей и средств управления для обработки риска.**

Цели и средства управления должны реализовывать стратегию управления рисками, учитывать критерии для принятия рисков и законодательные, нормативные и др. требования.

Стандарт ИСО 27001-2005 предлагает список целей и средств управления в качестве основы для построения плана обработки рисков (требований к СМИБ).

План обработки рисков содержит перечень первоочередных мероприятий по снижению уровней рисков с указанием:

- лиц, ответственных за реализацию данных мероприятий и средств;

- сроков реализации мероприятий и приоритетов их выполнения;

- ресурсов для реализации таких мероприятий;

- уровней остаточных рисков после внедрения мероприятий и средств управления.

Принятие плана обработки рисков и контроль за его выполнением осуществляет высшее руководство организации. Выполнение ключевых мероприятий плана является критерием, позволяющим принять решение о вводе СМИБ в эксплуатацию.

На данном этапе производится обоснование выбора различных контрмер по ЗИ, структурированных по нормативно-правовому, организационно-управленческому, технологическому и аппаратно-программному уровням обеспечения информационной безопасности. (Далее комплекс контрмер реализуется в соответствии с выбранной стратегией управления информационными рисками). При полном варианте анализа рисков, для каждого риска дополнительно оценивается эффективность контрмер.

**ж) Утверждение руководством предлагаемого остаточного риска.**

**з) Получение разрешения руководства на реализацию и ввод в эксплуатацию СМИБ.**

**и) Заявление о применимости (в соответствии с ИСО 27001-2005).**

Датой ввода СМИБ в эксплуатацию является дата утверждения высшим руководством компании Положения о применимости средств управления, которое описывает цели и средства, выбранные организацией для управления рисками:

- средства управления и контроля, выбранные на этапе обработки рисков;

- уже существующие в организации средства управления и контроля;

- средства, обеспечивающие выполнение требований законодательства и требований регулирующих организаций;

- средства, обеспечивающие выполнение требований заказчиков;

- средства, обеспечивающие выполнение общекорпоративных требований;

- любые другие соответствующие средства управления и контроля.

**2 этап. Реализация и эксплуатация СМИБ.**

Для внедрения и эксплуатации политики ИБ, средств управления, процессов и процедур в области ИБ выполняются следующие действия:

а) Разработка плана обработки рисков (описание запланированных средств управления, ресурсов (программные, аппаратные, персонал), которые требуются для их реализации, поддержки, контроля, и обязанностей руководства по управлению рисками ИБ (разработка документов на этапе планирования, поддержка целей ИБ, определение ролей и ответственности, обеспечение необходимыми ресурсами для создания СМИБ, аудит и анализ).

б) Распределение финансирования, ролей и ответственности по реализации плана обработки рисков.

в) Внедрение запланированных средств управления.

г) Определение контрольных показателей эффективности (метрик) средств управления, методов их измерения, которые обеспечат сравнимые и воспроизводимые результаты.

д) Повышение квалификации, осведомленности персонала в области ИБ в соответствии с их трудовыми обязанностями.

е) Управление эксплуатацией СМИБ, управление ресурсами для поддержки в рабочем состоянии, контроля и улучшения СМИБ.

з) Внедрение процедур и других средств управления для быстрого обнаружения и реагирования на инциденты ИБ.

**3 этап. Постоянный контроль и анализ функционирования СМИБ.**

Этап предполагает проведение оценки или измерений ключевых показателей эффективности процессов, анализ результатов и предоставление отчетов руководству для анализа и включает:

а) Проведение постоянного контроля и анализа (позволяет быстро обнаруживать ошибки функционирования СМИБ, быстро выявлять и реагировать на инциденты безопасности, разграничить роли персонала и автоматизированных систем в СМИБ, предотвращать инциденты безопасности за счет анализа необычного поведения, определять результативность обработки инцидентов безопасности).

б) Проведение регулярного анализа результативности СМИБ (анализируются соответствие политике и целям СМИБ, аудиты, ключевые показатели эффективности, предложения и реакция заинтересованных сторон).

в) Измерение эффективности средств управления для проверки выполнения требований защиты

г) Периодическая переоценка рисков, анализ остаточных рисков и определение приемлемых уровней риска при каких-либо изменениях в организации (бизнес-целей и процессов, выявленных угроз, новых выявленных уязвимостей и т.д.)

д) Периодическое проведение внутренних аудитов СМИБ.

**Аудит СМИБ** – проверка соответствия выбранных контрмер целям и задачам бизнеса, декларированным в ПБ организации, по его результатам проводится оценка остаточных рисков и, в случае необходимости, их оптимизация.

е) Регулярный анализ области применения и тенденции СМИБ руководством.

ж) Обновление планов управления рисками для учета результатов контроля и анализа.

з) Ведение журналов регистрации событий, оказавших негативное влияние на результативность или качество работы СМИБ.

**4 этап. Поддержка и улучшение СМИБ.**

По результатам внутреннего аудита СМИБ  и анализа со стороны руководства разрабатываются и внедряются корректирующие и предупреждающие действия, направленные на постоянное улучшение СМИБ:

а) Совершенствование политики ИБ, целей защиты информации, проведение аудита, анализ наблюдаемых событий.

б) Разработка и реализация корректирующих и предупреждающих действий для  устранения несоответствий СМИБ требованиям.

в) Контроль улучшений СМИБ.

**2.3 Коммерческая тайна**

Предпринимательская деятельность во всех сферах неразрывно связана с получением и использованием различного рода информации. Причем в современных условиях информация представляет собой особого рода товар, имеющий определенную ценность. Для предпринимателя зачастую наиболее ценной является информация, которую он использует для достижения целей фирмы и разглашение которой может лишить его возможностей реализовать эти цели, то есть создает угрозы безопасности предпринимательской деятельности. Конечно, не вся информация может, в случае ее разглашения, создавать эти угрозы, однако существует определенная ее часть, которая нуждается в защите.

Информация, используемая в предпринимательской деятельности весьма разнообразна. Ее можно разделить на два вида: промышленная и коммерческая. К промышленной относится: информация о технологии и способе производства, технических открытиях и изобретениях, “ноу-хау”, конструкторская документация, программное обеспечение и т. п. Коммерческая информация – о финансово-экономическом положении предприятия (бухгалтерская отчетность), кредитах и банковских операциях, о заключаемых договорах и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и пр.

Вся эта информация представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам экономической безопасности различной степени тяжести.

Поэтому информацию необходимо разделить на три группы:

а) информация для открытого пользования любым потребителем в любой форме;

б) информация ограниченного доступа – только для органов, имеющих соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура);

в) информация только для работников (либо руководителей) фирмы.

Информация относящаяся ко второй и третьей группам является конфиденциальной и имеет ограничения в распространении.

Коммерческая тайна предприятия - это не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами др., разглашение (передача, утечка) которых может нанести ущерб его интересам. Такова общая характеристика категории «коммерческая тайна» предприятия, определенная закодательно.

Обобщение различных точек зрения отечественных и зарубежных авторов позволяет дать расширенную трактовку этой весьма сложной категории. В наиболее общем виде она включает информацию:

- о торговых отношениях фирм;

- об организации и размерах оборота средств;

- о состоянии рынка сбыта;

- о банковских операциях;

- о поставщиках и потребителях;

- о содержании патентов;

- о структуре капиталов;

- о планах инвестиций;

- о заключенных контрактах;

- о формировании цены на товар;

- о размере прибыли и объеме производства.

Производственная тайна включает информацию:

- о способах производства и технологии;

- об организации труда;

- о технических открытиях и изобретениях;

- о целях и характере исследовательских работ.

Целесообразно также в общем объеме коммерческой информации выделять два основных блока. Согласно этому подходу, к категории научно-технической и технологической информации относятся сведения о конструкции машин и оборудования, используемых материалах, методах и способах производства, дизайне, программном обеспечении ЭВМ и др.

К категории деловой информации относятся:

- финансы предприятия (финансовая отчетность, состояние расчетов с клиентами, задолженность, кредиты, платежеспособность, прибыль, себестоимость продукции и др.);

- стратегические и тактические планы развития производства, в том числе с использованием новых технологий, изобретений, ноу-хау;

- планы и объемы реализации продукции (планы маркетинга, характер и объем торговых операций, уровень цен, складские запасы);

- анализ конкурентоспособности своей продукции, эффективности экспорта и импорта, предполагаемое время выхода на рынок;

- планы рекламной деятельности;

- списки торговых и других клиентов, конкурентов, сведения о взаимоотношениях с ними, их финансовом положение, условиях контрактов и др.;

- методы и организация управления;

- собственная оценка характера и репутации персонала и предприятия;

- система организации труда.

При отнесении той или иной информации к категории коммерческой тайны следует учитывать два обстоятельства.

Во-первых, на практике возможны случаи, когда под предлогом охраны коммерческой тайны могут скрывать сведения и документы, свидетельствующие о фактах злоупотреблений, бесхозяйственности и других нарушениях. Для исключения подобных ситуаций необходимо на общегосударственном уровне создать специальную систему регулирования взаимоотношений предприятия и контролирующих его органов.

Во-вторых, в условиях рынка засекречивать информацию становится невыгодно с экономической точки зрения. Информация все чаще выступает как рыночный товар, имеющий определенную цену и спрос. В отдельных промышленно развитых странах около половины валового национального продукта дают производство, распространение и переработка информации в различных видах.

Сведения, составляющие коммерческую тайну и подлежащие охране, должны удовлетворять следующим пяти критериям оценки:

а) их открытое использование связано с ущербом для предприятия;

б) они не являются общеизвестными или общедоступными на законных основаниях;

в) предприятие сможет осуществить надлежащие меры по сохранению их конфиденциальности по соображениям экономической и иной выгоды;

г) эти сведения нуждаются в защите, так как они не являются государственными секретами и не защищены авторским и патентным правом;

д) сокрытие этих сведений не наносит ущерба обществу.

Анализ законодательных актов промышленно развитых стран по вопросам защиты коммерческой тайны позволяет определить совокупность сведений, сокрытие которых противоречит интересам государства и общества. В наиболее общем виде это информация:

а) о нерациональном природопользовании;

б) о сверхнормативном загрязнении окружающей среды;

в) о несоблюдении техники безопасности в производстве, представляющем реальную угрозу здоровью и жизни людей;

г) о нарушении специального законодательства, регулирующего деятельность предпринимателей (например, законов о качестве продукции и защите прав потребителя);

д) о занятии деятельностью, не предусмотренной уставом данного предприятия или запрещенной законами данной страны;

е) о злоупотреблении и недобросовестности руководителей и работников фирмы;

ж) о фактах проявления недобросовестной конкуренции;

з) о возможностях и реальных случаях, уклонения от правильной уплаты налогов

и) о причинах и фактах невыполнения договоров и др.

**2.4 Политика информационной безопасности**

Процесс создания системы управления информационной безопасностью (СУИБ) в соответствии с рекомендациями большинства стандартов предполагает разработку следующих документов:

**‑ политика ИБ** (ПИБ) верхнего уровня, политика СУИБ;

**- частные (детальные) политики** в отдельных областях деятельности, охватываемых СУИБ;

**- процедуры** СУИБ.

Разрабатываемые политики и процедуры должны охватывать следующие ключевые процессы СУИБ:

**-**управление рисками;

**-**управление инцидентами;

**-**управление эффективностью системы;

**-**управление персоналом;

**-**управление документацией и записями системы управления ИБ;

**-**пересмотр и модернизация системы;

**-**управление непрерывностью бизнеса и восстановления после прерываний.

**Создание ПИБ позволяет:**

- снизить риски и повысить эффективность бизнеса;

- выполнить требования законодательства;

- выполнить требования клиентов и партнеров;

- осуществить подготовку к сертификации;

- повысить имидж компании.

В соответствии со стандартом ISO/IEC 27001 требуется, чтобы организации имели политику СУИБ и политику ИБ. Однако эти политики могут разрабатываться, как равноправные политики или являться расширенной версией другой (рисунок 2.2).

|  |
| --- |
| 1  Рисунок 2.2. – Иерархия политик организации |

Политика информационной безопасности (ПИБ) ‑ совокупность принципов, правил, процедур и практических приёмов в области безопасности, которые направлены на защиту информации.

Назначение ПИБ:

- формулирование целей и задач информационной безопасности организации с точки зрения бизнеса (позволяет определить это для руководства и продемонстрировать поддержку руководством значимости ИБ),

- определение правил организации работы в компании для минимизации рисков информационной безопасности и повышения эффективности бизнеса.

**Требования к ПИБ:**

- должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.) для демонстрации поддержки руководства;

- должна быть написана понятным языком для конечных пользователей и руководства компании и быть по возможности краткой;

- должна определять цели ИБ, способы их достижения и ответственность. Технические подробности реализации способов содержатся в инструкциях и регламентах, на которые даются ссылки в ПИБ;

- минимизация влияния ПИБ на производственный процесс

- непрерывность обучения сотрудников и руководства организации в вопросах обеспечения ИБ;

- непрерывный контроль выполнения правил ПИБ на этапе внедрения и в дальнейшем;

- постоянное совершенствование;

- согласованность во взглядах и создание корпоративной культуры безопасности.

**Предлагается следующая структура ПИБ:**

**Общие положения** (ссылки на законы, нормативные акты и др.руководящие документы, которым подчиняется деятельность организации),

Подтверждение значимости ИБ для организации и формулирование **целей защиты информации** с точки зрения бизнеса организации (выполнение требований законодательства и др. норм, удовлетворение ожиданий клиентов и партнеров, повышение конкурентоспособности, финансовой стабильности, имиджа организации).

Описание **стратегии** организации по обеспечению информационной безопасности (например, выполнение требований законодательства, оценка и управление рисками).

**Область применения** ПИБ (например, ПИБ обязательна для выполнения всеми сотрудниками и руководством организации, или отдельного филиала, или сотрудниками, использующими ноутбуки).

**Описание объекта защиты** (защищаемые ресурсы – информация различных категорий, информационная инфраструктура и т.д.).

**Цели и задачи** обеспечения информационной безопасности (например, снижение угроз ИБ до приемлемого уровня, выявление потенциальных угроз и уязвимостей ИБ, предотвращение инцидентов ИБ).

**Угрозы и модель нарушителя**, которые принимаются во внимание для данной организации (по источникам возникновения, по способам реализации, по направленности).

Краткое разъяснение **принципов политики** ИБ:

- подход к построению СУИБ;

- требования к подготовке и осведомленности персонала в области ИБ;

- последствия и ответственность за нарушение ПИБ;

- подход к управлению рисками;

- определение оргструктуры, общих и специальных обязанностей по управлению ИБ, включая отчеты об инцидентах;

- ссылки на документацию, которая может поддержать политику, например, частные политики и процедуры в области защиты для конкретных информационных систем или правила защиты, которым должны следовать пользователи;

- механизмы контроля за выполнением положений ПИБ;

- порядок пересмотра и принятия изменений в политике.

**После утверждения политики ИБ необходимо:**

1. Довести положения политики ИБ, процедур и инструкций под роспись до сведения рядовых сотрудников при их первоначальном и последующем периодическом обучении и информировании.

2. Разработать процедуры, инструкции и т.д., уточняющие и дополняющие политику (для специалистов отдела ИБ).

3. Периодически анализировать политику для поддержки ее адекватности и результативности.

4. Проводить периодический аудит на выполнение сотрудниками положений политики с предоставлением отчета Руководству организации.

Кроме того, в должностные инструкции ответственного персонала, положения о подразделениях, контрактные обязательства организации должны быть включены обязанности по обеспечению информационной безопасности.

Таким образом, в результате не только создается документальная база СУИБ, но и происходит реальное распределение обязанностей по обеспечению безопасности информации среди персонала организации.

**Жизненный цикл политики безопасности.**

**1. Планирование.**

Первоначальный аудит безопасности:

- проведение обследования;

- идентификация угроз безопасности;

- идентификация ресурсов, нуждающихся в защите;

- оценка рисков.

В ходе аудита производится анализ текущего состояния информационной безопасности, выявляются существующие уязвимости, наиболее критичные области функционирования и самые чувствительные к угрозам безопасности бизнес-процессы.

Разработка политики безопасности:

- определяются основные условия, требования и базовая система мер по обеспечению информационной безопасности в организации, позволяющие уменьшить риски до приемлемой величины;

- оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации.

**2. Внедрение ПИБ.**

Решение технических, организационных и дисциплинарных проблем.

**3. Проверка.**

Аудит и контроль.

**4. Корректировка.**

Периодические пересмотр и корректировка, а также при изменении исходных данных.

**2.5 Организационные меры по защите информации**

Организационно-административные методы защиты информации

Они регламентируют процессы создания и эксплуатации информационных объектов, а также взаимодействие пользователей и систем таким образом, чтобы несанкционированный доступ к информации становился либо невозможным, либо существенно затруднялся.

Организационно-административные методы защиты информации охватывают все компоненты автоматизированных информационных систем на всех этапах их жизненного цикла: проектирования систем, строительства зданий, помещений и сооружений, монтажа и наладки оборудования, эксплуатации и модернизации систем. К организационно-административным мероприятиям защиты информации относятся:

выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

выделение специальных ЭВМ для обработки конфиденциальной информации;

организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;

использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;

установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;

постоянный контроль за соблюдением установленных требований по защите информации.

Организационно-технические методы защиты информации.

Они охватывают все структурные элементы автоматизированных информационных систем на всех этапах их жизненного цикла. Организационно-техническая защита информации обеспечивается осуществлением следующих мероприятий:

ограничение доступа посторонних лиц внутрь корпуса оборудования за счет установки механических запорных устройств или замков;

отключение ЭВМ от локальной вычислительной сети или сети удаленного доступа (региональные и глобальные вычислительные сети) при обработке на ней конфиденциальной информации, кроме случаев передачи этой информации по каналам связи;

использование для отображения конфиденциальной информации жидкокристаллических, а для печати — струйных принтеров или термопечати с целью снижения утечки информации по электромагнитному каналу. При использовании обычных дисплеев и принтеров с этой же целью рекомендуется включать устройства, создающие дополнительный шумовой эффект (фон), — генераторы шума, кондиционер, вентилятор, или обрабатывать другую информацию на рядом стоящей ЭВМ;

установка клавиатуры и печатающих устройств на мягкие прокладки с целью снижения утечки информации по акустическому каналу;

размещение оборудования для обработки конфиденциальной информации на расстоянии не менее 2,5 м от устройств освещения, кондиционирования, связи, металлических труб, теле- и радиоаппаратуры;

организация электропитания ЭВМ от отдельного блока питания (с защитой от побочных электромагнитных излучений или от общей электросети через фильтр напряжения);

использование бесперебойных источников питания (БИП) персональных компьютеров для силовых электрических сетей с неустойчивым напряжением и плавающей частотой. Основное назначение бесперебойных источников питания — поддержание работы компьютера после исчезновения напряжения в электрической сети. Это обеспечивается за счет встроенных аккумуляторов, которые подзаряжаются во время нормальной работы. БИП мгновенно предупредит своего владельца об аварии электропитания и позволит ему в течение некоторого времени (от нескольких минут до нескольких часов) аккуратно закрыть файлы и закончить работу. Кроме обычных для БИП функций они могут выполнять функцию высококлассного стабилизатора напряжения и электрического фильтра. Важной особенностью устройства является возможность непосредственной связи между ним и сетевой операционной системой.

**2.6 Социальный инжиниринг**

**Социальная инженерия** - совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение организационных структур, определяющих человеческое поведение и обеспечивающих контроль за ним.

Социальная инженерия сегодня представляет собой комплекс практически ориентированных знаний в области управления социальными структурами и процессами, развивающийся по следующим направлениям:

- строительство социальных институтов, например, государственное строительство, реорганизация системы высшего образования и т.д. («социетальный» блок);

- региональное строительство (региональный блок);

- формирование местных сообществ (муниципальный блок);

- строительство организаций или «организационная инженерия» (организационный блок);

- формирование целевых групп и команд («групповая» инженерия). Избирательные технологии и другие способы продвижения лидеров или их команд являются составной частью всех блоков социоинженерной деятельности.

В образовательной практике идеи социальной инженерии реализуются путем применения современных образовательных технологий и активных методов обучения, а также посредством “насыщения” учебного процесса дисциплинами социоинженерного и организационного цикла, в том числе:

- теория и методы социальной инженерии;

- диагностика организаций;

- прогнозирование и моделирование развития организаций;

- организационное проектирование и программирование;

- социальное планирование;

- внедрение социальных новшеств в организации и т.д.;

- практикум по социальным технологиям;

- методы разрешения конфликтов.

Техники социальной инженерии:

1. **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание) - вид [интернет-мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE), целью которого является получение доступа к конфиденциальным данным пользователей — [логинам](https://ru.wikipedia.org/wiki/%D0%A3%D1%87%D1%91%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C) и [паролям](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C).

2. [**Троянская программа**](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) - вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях. Данная техника зачастую эксплуатирует любопытство, либо другие эмоции цели. Чаще всего злоумышленник отправляет жертве электронное сообщение, содержащее «интересный» контент, обновление антивируса, или другую информацию, способную ее заинтересовать. Открывая прикрепленный к письму файл, пользователь устанавливает себе на компьютер вредоносное программное обеспечение, позволяющее мошеннику получить доступ к конфиденциальной информации.

3. **Сбор информации** из открытых источников. Применение техник социальной инженерии требует не только знания [психологии](https://ru.wikipedia.org/wiki/%D0%9F%D1%81%D0%B8%D1%85%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F), но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из [социальных сетей](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C). К примеру, такие сайты как [livejournal](https://ru.wikipedia.org/wiki/%D0%96%D0%B8%D0%B2%D0%BE%D0%B9_%D0%96%D1%83%D1%80%D0%BD%D0%B0%D0%BB), «[Одноклассники](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%BD%D0%BE%D0%BA%D0%BB%D0%B0%D1%81%D1%81%D0%BD%D0%B8%D0%BA%D0%B8_%28%D1%81%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C%29)», «[ВКонтакте](https://ru.wikipedia.org/wiki/%D0%92%D0%9A%D0%BE%D0%BD%D1%82%D0%B0%D0%BA%D1%82%D0%B5" \o "ВКонтакте)», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

Для защиты крупных компаний и их сотрудников от мошенников, использующих техники социальной инженерии, часто применяются комплексные многоуровневые системы безопасности. Ниже перечислены некоторые особенности и обязанности таких систем.

**Физическая безопасность.** Барьеры, ограничивающие доступ в здания компании и к корпоративным ресурсам. Не стоит забывать, что ресурсы компании, например, мусорные контейнеры, расположенные вне территории компании, физически не защищены.

**Данные.** Деловая информация: учетные записи, почтовая корреспонденция и т. д. При анализе угроз и планировании мер по защите данных нужно определить принципы обращения с бумажными и электронными носителями данных.

**Приложения.** Программы, запускаемые пользователями. Для защиты среды необходимо учесть, как злоумышленники могут использовать в своих целях почтовые программы, службы мгновенной передачи сообщений и другие приложения.

**Компьютеры.** Серверы и клиентские системы, используемые в организации. Защита пользователей от прямых атак на их компьютеры, путем определения строгих принципов, указывающих, какие программы можно использовать на корпоративных компьютерах.

**Внутренняя сеть.** Сеть, посредством которой взаимодействуют корпоративные системы. Она может быть локальной, глобальной или беспроводной. В последние годы из-за роста популярности методов удаленной работы, границы внутренних сетей стали во многом условными. Сотрудникам компании нужно разъяснить, что они должны делать для организации безопасной работы в любой сетевой среде.

**Периметр сети.** Граница между внутренними сетями компании и внешними, такими как Интернет или сети партнерских организаций.

**РАЗДЕЛ 3 ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ**

**3.1 Классификация технических каналов утечки информации по физическим принципам возникновения**

**Технический канал утечки информаци**и – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации (рисунок 3.1).

|  |
| --- |
| 1  Рисунок 3.1 Технический канал утечки 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 (рисунок 3.2):

– акустический;

– материально-вещественный;

– визуально-оптический;

– электромагнитный.

|  |
| --- |
| 1  Рисунок 3.2. Классификация каналов утечки информации |

В случае когда источником информации является голосовой аппарат человека, информация называется **речевой**.

Области спектра звука, в которых сосредоточивается основная мощность акустического сигнала, называются **формантами**. Большинство звуков речи имеют одну или две форманты. Форманты звуков речи расположены в области частот от 150…200 до 8600 Гц. Основная энергия подавляющей части формант сосредоточена в диапазоне частот 300…3400 Гц, что позволило ограничить спектр речевого сигнала, передаваемого по стандартному телефонному каналу, этой полосой.

Психологическая (с учетом чувствительности уха на разных частотах) интенсивность акустических сигналов изменяется в широких пределах (0…130 дБ). Для человека как основного источника соотношение между уровнем громкости и его качественной оценкой характеризуется следующими данными: очень тихая речь (шепот) – 5…10 дБ, тихая речь – 30…40 дБ, речь умеренной громкости 50…60 дБ, громкая речь – 60…70 дБ, крик – 70…80 дБ и более. Для сравнения: звук сирены «скорой помощи» – 100 дБ, а шум реактивного двигателя на расстоянии 5 м – 120 дБ.

Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (рисунок 3.3).

|  |
| --- |
| Рис 3  Рисунок 3.3. Структурная схема прямого акустического канала утечки информации |

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.

**Закладное устройство (ЗУ)** – автономное устройство для перехвата речевой информации, конструктивно объединяющее микрофон и передатчик (рисунок 3.4).

|  |
| --- |
| Безымянный  Рисунок 3.4. Внешний вид закладного устройства типа «электронные уши» |

Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, телефонной линии, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот. Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

**Направленный микрофон** – электронное устройство, обладающее высокими чувствительностью и помехоустойчивостью за счет его узкой диаграммы направленности (рисунок 3.5).

|  |
| --- |
| Безымянный  Рисунок 3.5. Внешний вид направленного микрофона ТМ-341 |

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний. В данном случае строительные конструкции выполняют преобразование акустических колебаний в вибрационные и возникает виброакустический (вибрационный) канал утечки информации (рисунок 3.6).

|  |
| --- |
| Рис 3  Рисунок 3.6. Структурная схема виброакустического канала утечки информации |

Перехват информации в виброакустических каналах обеспечивается электронными стетоскопами (рисунок 3.7), выполняющими преобразование механических колебаний строительных конструкций (пол, потолок, стены) в электрические. В качестве преобразователей, подключаемых к электронному стетоскопу, используются акселерометры.

|  |  |
| --- | --- |
| 2  а) | 1  б) |
| Рисунок 3.7. Внешний вид электронного стетоскопа (а) и подключаемых к нему преобразователей (б) | |

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по инженерным коммуникациям (ультразвуковые колебания).

Акустоэлектрические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические.

Некоторые элементы вспомогательных технических средств и систем, в том числе трансформаторы, катушки индуктивности, электромагниты звонков телефонных аппаратов и т. п. обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы, либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.

Вспомогательные технические средства и системы (ВТСС), кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом».

Таким образом, речь воздействия на элементы электронной аппаратуры, содержащей в себе элементы, обладающие микрофонным эффектом, преобразуется ими в электрический сигнал. Если электронная аппаратура подключена к проводным коммуникациям, например к линии связи, то данный сигнал может быть перехвачен при подключении к такой линии, что обуславливает возникновение акустоэлектрического канала утечки информации (рисунок 3.8).

|  |
| --- |
| Рис 3  Рисунок 3.8. Структурная схема акустоэлектрического канала утечки информации |

Акустооптический канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием речевого сигнала отражающих поверхностей (отражатель-модулятор) помещений (оконных стекол, зеркал и т. д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация (рисунок 3.9).

|  |
| --- |
| Рис 3  Рисунок 3.9. Структурная схема акустооптического канала утечки информации |

Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.

На рисунке 3.10 приведен простейший вариант подобной системы: луч лазера падает на стекло окна под некоторым углом (например 45 градусов). На границе стекло–воздух происходит модуляция луча речевыми колебаниями. Отражённый луч принимается фотодетектором, расположенным с другой стороны окна под углом, равным углу падения луча лазера. Такая система требует тщательной юстировки.

|  |
| --- |
| Рисунок 3.11. Схема реализации лазерного микрофона |

Второй способ, использующий сплиттер (делитель пучка) и приведенный на рисунок 3.11, несколько сложнее, но он позволяет совместить лазер и детектор. Отпадает необходимость в тщательной юстировке системы. Применение сплиттера позволяет свести падающий и отражённый луч в одну точку.

|  |
| --- |
| Рисунок 3.11. Схема реализации лазерного микрофона с использованием сплиттера |

Лазерные акустические системы дистанционного зондирования имеют дальность действия при приеме диффузноотраженного излучения до 100 м, при нанесении на стекла специального покрытия – более 300 м, а при установке на оконных стеклах триппель-призм – более 500 м.

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.

Регистрация средством технической разведки ПЭМИ источника информации (персональный компьютер и др.) распространяющихся через воздушную среду обусловливает возникновение индукционного канала утечки информации (рис. 3.12).

Кроме того, в индукционном канале используется эффект возникновения вокруг кабеля связи ПЭМИ при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики применяются в основном для перехвата информации с симметричных высокочастотных кабелей.

|  |
| --- |
| Рис 3  Рис. 3.12. Структурная схема индукционного канала утечки информации |

Электрический канал утечки информации (рис. 3.13) 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.). В этом случае наводка обусловлена тем, что данные проводники выступают в качестве случайных антенн (цепь ВТСС или посторонние проводники, способные принимать ПЭМИ).

|  |
| --- |
| Рис 3  Рис. 3.13. Структурная схема электрического канала утечки информации |

Наводки электромагнитных излучений ТСОИ возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСОИ и посторонних проводников.

**3.2 Защита речевой информации**

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. 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 качество звукоизоляции на средних частотах, рассчитывается по формуле

|  |  |
| --- | --- |
|  | (3.1) |

где *q*ог, – масса 1 м2 ограждения, кг;

*f* – частота звука, Гц.

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 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 (рисунок 3.14). 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.

|  |
| --- |
| Рис 4  Рисунок 3.14. Внешний вид минераловатного мата М1-100 |

**Полужесткие материалы** включают в себя минераловатные или стекловолокнистые плиты с объёмной массой 80…130 кг/м3 при содержании синтетического связующего 10…15 % по массе (рисунок 3.15), а также древесноволокнистые плиты с объёмной массой 180…300 кг/м3. Поверхность плит покрывается пористой краской или плёнкой. Коэффициент звукопоглощения полужёстких материалов на средних частотах 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.

|  |
| --- |
| Рис 4  Рисунок 3.15. Внешний вид минераловатных плит П-75 |

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. 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 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 резину, 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 (рисунок 3.16), которые монтируются на некотором расстоянии от твердой стены.

|  |
| --- |
| Рис 4  Рисунок 3.16. Внешний вид фрагмента перфорированной плиты СМЛ-ППГЗ |

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 и 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 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 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.

Мероприятия акустической маскировки позволяют обеспечить (рисунок 3.17):

– неузнаваемость голоса диктора;

– существенное снижение неразборчивости речи диктора;

– скрыть факт передачи речевой информации.

Реализация первого направления позволяет обеспечить неузнаваемость голоса диктора, что затрудняет его идентификацию. Это достигается путем изменения или генерации тех или иных параметров речевого сигнала (характеристики четырех формантных областей (средняя частота, частотный диапазон, энергия), огибающая спектра и т. д.). Изменение голоса диктора в данном случае может обеспечиваться при сохранении естественности ее звучания за счет использования некоторых характеристик голоса диктора или заданного голосового образца. При отсутствии естественности звучания голос имеет механический оттенок.

Под техническим закрытием речи будем понимать технологии маскирования речи, относящиеся к методам и средствам смысловой защиты речевой информации и имеющие цель обеспечения неразборчивости защищаемого речевого сообщения. Их реализация на практике может быть выражена в микшировании речи шумами и помехами и/или в модификации речевого сигнала по вычисляемым из его описаний параметрам по заранее известному закону преобразования (закрытия–восстановления). При микшировании речевого сигнала с помехой необходимо обеспечить превышение ее уровнем уровня речи.

|  |
| --- |
| Рис 5  Рисунок 3.17. Классификация методов акустической маскировки |

Под модификацией речи будем понимать такое преобразование исходного речевого сигнала, прежде всего его фонетической функции, с целью достижения его неразборчивости и/или неузнаваемости по известному заданному закону, когда параметры этого преобразования на передающем конце канала связи либо известны заранее, либо выделяются из самого исходного сигнала и не изменяются в процессе всего сеанса связи. На приемном конце эти параметры преобразования либо также известны заранее, либо выделяются из принятого модифицированного сигнала с целью восстановления неразборчивого речевого сигнала по тому же заранее известному закону. Данный метод реализуется за счет использования маскираторов речи.

Особую популярность в последнее время получила стеганография, используемая в области сокрытия конфиденциальной информации в графических изображениях, передаваемых по телекоммуникационным сетям. В тоже время прогресс, достигнутый в области разработки устройств передачи речевых сообщений, а также в средствах вычислительной техники, открывает новые возможности как для скрытой передачи конфиденциальной информации в аналоговых и цифровых аудио сигналах и речи, так и для скрытой передачи в информационных контейнерах различного рода на основе использования динамично развивающихся технологий мультимедиа, компьютерной и сотовой телефонии.

В настоящее время широко применяются методы компьютерной стеганографии, основанные на использовании естественных шумов, которые содержат цифровые массивы, полученные стандартными способами преобразования из аналоговых акустических и видеосигналов. Эти шумы являются ошибками квантования и не могут быть полностью устранены. Использование шумовых бит для передачи дополнительной конфиденциальной информации позволяет создавать скрытый канал передачи данных. В качестве шумовых бит обычно рассматриваются младшие разряды значений отсчетов, которые являются шумом с точки зрения точности измерений и несут наименьшее количество информации, содержащейся в отсчете.

Для защиты информации от утечки по виброакустическому, акустооптическому каналам используют метод микширования речевого сигнала распространяющегося в виде механических колебаний в ограждающих конструкциях с различными шумовыми сигналами. Технически это реализуется за счет использования автоматических генераторов шума. Именно поэтому 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. Роль оконечных электроакустических преобразователей, осуществляющих преобразование электрических колебаний в акустические колебания речевого диапазона длин волн, обычно выполняют электромеханические, пьезоэлектрические преобразователи и малогабаритные широкополосные громкоговорители (рисунок 3.18).

|  |
| --- |
| Рис 5  Рисунок 3.18. Внешний вид устройства защиты речевой информации «Прибой‑Р» |

При закреплении электромеханических, пьезоэлектрических преобразователей, например на оконном стекле защищаемого помещения, виброколебания, создаваемые средством маскировки, вызывают интенсивные колебания стекла с амплитудой, существенно превышающей амплитуду его колебаний, вызванных речевым сигналом. Вследствие этого при лазерно-локационном зондировании оконного стекла отраженный от него акустический сигнал оказывается промодулированным не только речевым информационным сигналом, но и в значительной степени помеховым. Это приводит к существенному ухудшению условий приема и восстановления перехваченных речевых сообщений.

Аналогичное ухудшение условий перехвата будет иметь место и при наличии виброакустического канала утечки информации, например при перехвате речевого сигнала скрытно размещенным на оконном стекле или на стене защищаемого помещения электронным стетоскопом. Уровень маскирующего вибрационного шума должен превосходить уровень информационного сигнала на определенную нормами виброакустической защиты величину.

Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемых псевдослучайными.

Наряду с шумовыми помехами в целях активной акустической маскировки используют и другие помехи.

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 примерно равных уровнях смешиваемых 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.

Акустические колебания, создаваемые средствами активной акустической маскировки, могут отрицательно воздействовать на людей, находящихся в зашумленном помещении, и приводить к их быстрой и повышенной утомляемости.

Основные требования, которым должны удовлетворять современные средства акустического зашумления:

– временные, спектральные и корреляционные характеристики помех должны быть близки соответствующим характеристикам полезного сигнала;

– средства создания помех должны обеспечивать требуемое превышение помехи над полезным сигналом в каждой выделенной полосе частот, исключающее возможность выделения сигнала на фоне помехи;

– элементы крепления электромеханических преобразователей не должны существенно искажать помеховый сигнал;

– следует учитывать, что создаваемые средствами маскировки виброколебания могут раздражающе воздействовать на нервную систему человека, вызывая различные функциональные отклонения.

**3.3 Защита информации от утечки за счет побочных электромагнитных излучений и наводок**

Рассмотрим процесс экранирования электромагнитного поля при падении плоской волны на бесконечно протяженную металлическую пластину толщиной *d*, находящуюся в воздухе (рисунок 3.19).

|  |
| --- |
| 34  Рисунок 3.19. Схематичное изображение процесса взаимодействия электромагнитной волны с металлическим экраном |

В этом случае 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.

В результате общая эффективность экранирования (величина потерь энергии электромагнитной волны) металлической пластиной определяется суммой потерь за счет поглощения (затухания) энергии в толще материала *Апогл*, отражения энергии от границ раздела внешняя среда–металл и металл–экранируемая область *Аотр* и многократных внутренних отражений в стенках экрана *Амотр*:

|  |  |
| --- | --- |
|  | (3.2) |

Потери на поглощение связаны с поверхностным эффектом в проводниках, приводящим к экспоненциальному уменьшению амплитуды проникающих в металлический экран электрических и магнитных полей.

Это обусловлено тем, что токи, индуцируемые в металле, вызывают омические потери и, следовательно, нагрев экрана.

Глубина проникновения δ определяется как величина, обратная коэффициенту затухания, и зависит от частоты: чем больше частота, тем меньше глубина проникновения. В СВЧ–диапазоне глубина проникновения δ в металлах имеет малую величину и тем меньше, чем больше проводимость металла и его магнитная проницаемость.

|  |  |
| --- | --- |
|  | (3.3) |

где *μ* – абсолютная магнитная проницаемость материала экрана;

*f* – частота электромагнитного поля;

σ – удельная проводимость материала экрана.

Выражение для определения потерь на поглощение экраном толщиной *d* может быть представлено в следующем виде:

|  |  |
| --- | --- |
|  | (3.4) |

Таким образом, потери на поглощение растут пропорционально толщине экрана, магнитной проницаемости и удельной проводимости его материала, а также частоте электромагнитного поля.

Потери на отражение на границе раздела двух сред связаны с различными значениями полных характеристических сопротивлений этих сред. При прохождении волны через экран она встречает на своем пути две границы раздела: воздух–металл и металл–воздух.

Хотя электрическое и магнитное поля отражаются от каждой границы по-разному, суммарный эффект после прохождения обеих границ одинаков для обеих составляющих поля. При этом наибольшее отражение при входе волны в экран (на первой границе раздела) испытывает электрическая составляющая поля, а при выходе из экрана (на второй границе раздела) наибольшее отражение испытывает магнитная составляющая поля. Для металлических экранов потери на отражение определяются выражением

|  |  |
| --- | --- |
|  | (3.5) |

Откуда следует, что потери на отражение велики у экрана, изготовленного из материала с высокой проводимостью и малой магнитной проницаемостью.

Потери на многократные отражения в стенках экрана связаны с волновыми процессами в толще экрана и в основном определяются отражением от его границ. Для электрических полей почти вся энергия падающей волны отражается от первой границы (воздух–металл) и только небольшая ее часть проникает в экран. Поэтому многократными отражениями внутри экрана для электрических полей можно пренебречь.

Для магнитных полей большая часть падающей волны проходит в экран, в основном отражаясь только на второй границе (металл–воздух), тем самым создавая предпосылки к многократным отражениям между стенками экрана. Корректирующий коэффициент *Амотр* многократного отражения для магнитных полей в экране с толщиной стенки d при глубине проникновения δ равен

|  |  |
| --- | --- |
|  | (3.6) |

Величина *Амотр* имеет отрицательное значение, т. е. многократные отражения в толще экрана ухудшают эффективность экранирования. С уменьшением эффективности можно не считаться в случаях, когда на данной частоте выполняется условие *d*>δ, но им нельзя пренебрегать при применении тонких экранов, когда толщина экрана меньше глубины проникновения.

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.

Для изготовления экранов ЭМИ применяются различные материалы, объединяемые в единую конструкцию (рисунок 4.2).

Выбор материала экрана проводится исходя из обеспечения требуемой эффективности экранирования в заданном диапазоне частот при определенных ограничениях. Эти ограничения связаны с массогабаритными характерными экрана, его влиянием на экранируемый объект, с механической прочностью и устойчивостью экрана против коррозии, с технологичностью его конструкции и т. д.

Под эффективностью экранирования будем понимать отношение действующих значений напряженности электрического поля *Е1* (магнитного поля *Н1*) в данной точке при отсутствии экрана к напряженности электрического поля *Е2* (магнитного поля *H2*) в той же точке при наличии экрана:

|  |  |
| --- | --- |
|  | (3.7) |

|  |
| --- |
| Рис 1  Рисунок 3.20. Классификация конструкций экранов электромагнитного излучения |

Здесь эффективность выражается в относительных единицах (разах). На практике обычно данную величину представляют в логарифмических единицах – децибелах (дБ):

|  |  |
| --- | --- |
|  | (3.8) |

Однослойные конструкции экранов ЭМИ листовой формы и в виде сеток выполняются из разнообразных материалов (сталь, медь, алюминий, цинк, латунь), в том числе металлических. Металлические материалы удовлетворяют требованию устойчивости против коррозии при использовании соответствующих защитных покрытий.

Наиболее технологичными являются конструкции экранов из стали, так как при их изготовлении и монтаже можно широко использовать сварку. Толщина стали выбирается исходя из назначения конструкции экрана и условий его сборки, а также из возможности обеспечения сплошных сварных швов при изготовлении.

Использование сетчатых экранов ЭМИ обеспечивает снижение их материалоемкости. В случае когда расстояние между микропроводом сетчатого экрана соответствует λ/2, он по своим экранирующим свойствам эквивалентен сплошному металлическому листу.

Сетчатые экраны ЭМИ могут изготавливаться путем машинной вязки полотна, в процессе которой совместно с ассистирующей нитью (рисунок 3.21) в вязальное оборудование поступает микропровод, диаметр (рисунок 3.22) и материал (рисунок 3.23) которого влияет на экранирующие свойства формируемой таким образом конструкции. Эффективность экранирования данных материалов уменьшается с ростом частоты. Подобные конструкции характеризуются высоким коэффициентом отражения и обладают значительной стоимостью, вследствие использования металлов и их сплавов, что в значительной степени ограничивает их практическое использование.

|  |  |
| --- | --- |
| Петля  а) | 3  б) |
| Рисунок 3.21. Схема расположения ассистирующей нити и микропровода (а) и внешний вид сетчатого экрана ЭМИ (б) | |

|  |
| --- |
| Рисунок 3.22. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с различным диаметром микропровода |

|  |
| --- |
| Рисунок 3.23. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с микропроводом из различных материалов |

Пониженным значением коэффициента отражения обладают экраны ЭМИ, конструктивно выполненные в виде четвертьволнового поглотителя, в котором радиопоглощающий материал (РПМ) находится на некотором расстоянии от отражающей ЭМВ поверхности. Поглощение достигает максимального значения на частоте, соответствующей длине волны, четверть которой равна расстоянию между верхней поверхностью поглощающего материала и отражающей поверхностью, а также на всех ее высших нечетных гармониках (рисунок 3.24).

|  |
| --- |
| Рис 4  Рисунок 3.25. Схема взаимодействия с ЭМИ четвертьволнового экрана |

В настоящее время находят широкое применение четвертьволновые РПМ различного типа: резонансные, содержащие дипольные решетки, РПМ с плавно‑неоднородным изменением параметров с толщиной покрытия, например, диэлектрической проницаемости (рисунок 3.26).

|  |
| --- |
| 1  Рисунок 3.26. Схематичное изображение градиентного экрана ЭМИ |

Конструкции четвертьволновых экранов ЭМИ широко используются в технике. Они являются высокоэффективными с точки зрения подавления ЭМВ, но в узкой полосе частот, что обусловлено конструктивными их особенностями и представляется главным их недостатком.

Одной из важнейших задач, решаемых при создании РПМ, является уменьшение массы конструкции, что достигается путем использования порошкообразных материалов, в том числе магнитных.

Размер частиц и магнитная проницаемость порошкообразных материалов применяемых в конструкциях экранов ЭМИ, определяют их рабочий диапазон частот. Недостатком таких материалов, как и четвертьволновых РПМ, является их узкодиапазонность, а при использовании магнитных порошкообразных материалов – высокая стоимость.

Использование магнитных материалов в виде порошков, в том числе специальной формы, позволяет создавать эффективные экраны ЭМИ с граничной частотой до 10 ГГц, однако массовое практическое использование сдерживается их высокой стоимостью, обусловленной сложным технологическим процессом изготовления и дорогостоящим сырьем. Такие материалы, как правило, имеют значительную толщину, что является их недостатком.

Снижение толщины рабочего слоя РПМ достигается при совместном использовании проводящих и диэлектрических материалов, что приводит, как правило, к уменьшению механической прочности таких конструкций экранов ЭМИ. Устранение данного недостатка выполняется за счет применения композиционных материалов, получаемых путем закрепления вышеуказанных компонент (А) в связующем веществе (В) (рисунок 3.27). Однако данные материалы, как правило, узкополосные и обладают значительной стоимостью.

|  |
| --- |
| Рис 4  Рисунок 3.27 – Схематичное изображение экрана ЭМИ, выполненного на основе композиционного материала |

Для создания оптически прозрачных конструкций экранов ЭМИ используются стекла с токопроводящим покрытием. Такие экраны должны обеспечивать требуемую эффективность экранирования при ухудшении их оптических характеристик не ниже заданных граничных значений. Электрические и оптические свойства стекол с токопроводящим покрытием зависят от природы окислов, составляющих пленку, условий и методов ее нанесения и свойств самого стекла. Наибольшее распространение получили пленки на основе оксида олова, оксида индия – олова и золота, так как они обеспечивают наибольшую механическую прочность, химически устойчивы и плотно соединяются со стеклянной подложкой. Такие конструкции экранов используются для уменьшения уровня ЭМИ видеодисплейных терминалов (мониторов) (рисунок 3.28), которое распространяется в сторону пользователя. Такие материалы могут использоваться для экранирования оконных проемов защищаемых помещений.

|  |
| --- |
| Рис 4  Рисунок 3.28. Внешний вид экрана ЭМИ «Русский щит» для видеодисплейного терминала |

Создание широкодиапазонных экранов ЭМИ может быть также реализовано за счет выполнения их в виде многослойной конструкции, где каждый из слоев обладает определенным, отличным друг от друга комплексом свойств. Создание таких экранов ЭМИ в первую очередь приводит к увеличению толщины и веса конструкции, что не всегда оправдывается их эффективностью.

Формирование геометрических неоднородностей на поверхности экрана ЭМИ (пирамидальной, клиновидной формы) (рисунок 3.29) позволяет обеспечить широкодиапазонность характеристик отражения. Взаимодействие с ЭМВ в подобных конструкциях обусловлено не только параметрами материала, из которого она изготовлена, но и сложной формой волноведущей поверхности (рисунок 3.30). В таких конструкциях падающая ЭМВ преобразуется в поверхностную волну и по мере ее переотражения от неоднородностей поверхности ее энергия уменьшается.

|  |  |
| --- | --- |
| Рис 4  а) | Рис 4  б) |
| Рисунок 3.29. Внешний вид фрагментов конструкций экранов ЭМИ с геометрическими неоднородностями поверхности пирамидальной (а) и клиновидной (б) формы | |

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.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который подключается в зашумляемую токоведущую линию (рисунок 3.31).

|  |  |
| --- | --- |
| Рис 4 | Рис 4 |
| Рисунок 3.30. Внешний вид фрагментов конструкций экранов ЭМИ со сложной формой волноведущей поверхности | |

|  |
| --- |
| 37  Рисунок 3.31. Схема включения системы генератора шумового сигнала |

|  |
| --- |
| Рис 5  Рисунок 3.32. Внешний вид устройства линейного зашумления «SEL SP-44» |

**Системы пространственного зашумления** применяют для создания маскирующих помех в окружающем пространстве (рисунок 3.33). В состав системы входят:

– генераторы шумового сигнала;

– усилители, обеспечивающие необходимую мощность шумового сигнала в заданном диапазоне частот;

– антенны;

– устройства коммутации и контроля.

Цель зашумления считается достигнутой в том случае, когда отношение опасный сигнал/шум на границе контролируемой территории в окружающем пространстве или в токоведущей линии уменьшается до требуемого уровня, не позволяющего средствам перехвата качественно решать задачи обнаружения и анализа опасного сигнала. Способы размещения и подключения систем линейного и пространственного зашумления определяются особенностями схемного решения, расположения и монтажа защищаемых объектов и средств зашумления.

|  |
| --- |
| Рис 5  Рисунок 3.33. Внешний вид устройства пространственного зашумления «ПАЗК‑01» |

При применении систем активной зашиты необходимо учитывать их возможное влияние на качество работы защищаемых и других технических средств, расположенных в зоне действия электромагнитных полей, создаваемых ими.

Одним из методов локализации опасных сигналов, циркулирующих в технических средствах и системах обработки информации, является фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства – источника опасного сигнала. Фильтрация в устройствах – рецепторах электромагнитных полей и наводок – должна исключить их воздействие на рецептор.

В системах и средствах информатизации и связи фильтрация может осуществляться в:

– высокочастотных трактах передающих и приемных устройств для подавления нежелательных излучений – носителей опасных сигналов – и исключения возможности их нежелательного приема;

– различных сигнальных цепях технических средств для устранения нежелательных связей между устройствами и исключения прохождения сигналов, отличающихся по спектральному составу от полезных сигналов;

– цепях электропитания, управления, контроля, коммутации технических средств для исключения прохождения опасных сигналов по этим цепям;

– проводных и кабельных соединительных линиях для защиты от наводок;

– цепях пожарной и охранной сигнализации для исключения прохождения опасных сигналов и воздействия навязываемых высокочастотных колебаний.

Одна из возможных схем фильтрации опасных сигналов, создаваемых или воспринимаемых техническим средством по различным цепям, представлена на рисунок 3.34.

|  |
| --- |
| 35  Рисунок 3.34. Обобщенная схема фильтрации |

Фильтрация в различных цепях осуществляется с помощью фильтров, дросселей и трансформаторов.

В целях фильтрации в технических средствах систем информатизации и связи широко используют различные фильтры (нижних и верхних частот, полосовые, заграждающие и т. д.). Основное назначение фильтра – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе, и подавлять сигналы с частотами, лежащими за пределами этой полосы.

Количественно эффективность ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением

|  |  |
| --- | --- |
|  | (3.9) |

где *U1(P2)* – напряжение (мощность) опасного сигнала на входе фильтра;

*U2(P2)* – напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

– величины рабочих напряжения и тока фильтра должны соответствовать величинам напряжения и тока цепи, в которой фильтр установлен;

– эффективность ослабления нежелательных сигналов должна быть не меньше заданной в защищаемом диапазоне частот;

– ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным, не влияющим на качество функционирования системы;

– габариты и масса фильтров должны быть, по возможности, минимальными;

– фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление, удары, вибрация и т. д.);

– конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

– затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть незначительным (например 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 1010 Гц);

– сетевые фильтры должны эффективно работать при больших проходящих токах, высоких напряжениях и высоких уровнях мощности рабочих и подавляемых электромагнитных колебаний;

– ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

**Фильтры нижних частот.** Фильтр, у которого полоса прозрачности находится в пределах от ω=0 (постоянный ток) до некоторой граничной частоты ω*n*, называется фильтром нижних частот (ФНЧ) (рисунок 3.35, а).

**Полоса прозрачности (пропускания) фильтра** – полоса частот, в которой ослабление сигнала фильтром составляет не более 3 дБ.

**Фильтры верхних частот.** Фильтр, у которого полоса прозрачности занимает все частоты выше некоторой определенной граничной частоты ω*n*, называется фильтром верхних частот (ФВЧ). В таком фильтре постоянный ток и все колебания с частотами ниже определенной граничной частоты должны задерживаться, а колебания частот ω>ωn – пропускаться (рисунок 3.35, б).

**Полосовые фильтры.** Полосовые фильтры (ПФ) характеризуются тем, что обе частоты ω*n*1, и ω*n*2 ограничивающие полосу прозрачности, конечны и ни одна из них не равна нулю (рисунок 3.35, в).

В ряде случаев ставится задача задержания определенной полосы частот и в то же время пропускания всех остальных частот. Такая задача решается **заграждающим фильтром (ЗФ)** (рисунок 3.35, г).

С точки зрения конструктивного исполнения фильтры могут быть выполнены на элементах с сосредоточенными параметрами (фильтры, предназначенные для работы на частотах до 300 МГц) и на элементах с распределенными параметрами (коаксиальные, волноводные, полосковые, применяемые на частотах выше 1 ГГц). В диапазоне частот 300 МГц…1 ГГц могут использоваться фильтры, включающие элементы как с сосредоточенными, так и с распределенными параметрами.

**Разделительные трансформаторы.** Должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

|  |  |
| --- | --- |
| Безымянный  а) | Безымянный  б) |
| Безымянный  в) | Безымянный  г) |
| Рисунок 3.35. Амплитудно-частотные характеристики ФНЧ (а), ФВЧ (б), ПФ (в), ЗФ (г) | |

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

– разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;

– устранения асимметричных наводок;

– ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

**3.4. Выявление 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 повышения скрытности нередко выбирают вблизи несущей частоты мощной радиостанции. Микрофоны делают как встроенными, так и выносными. Они бывают двух типов: акустическими (чувствительнымик голосам людей) или вибрационными (преобразующими в электрические сигналы колебания, возникающие от человеческой речи в разнообразных жестких конструкциях). Для повышения скрытности они камуфлируются специальным образом и имеют дистанционное включение или выключение, например, по голосу человека (VOX-закладки). В качестве канала связи они обычно используют сеть электропитания, телефонные линии или радиоканал (рисунок 3.36).

|  |
| --- |
| Рис 5  Рисунок 3.36. Классификация закладных устройств |

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры.

Обнаружение закладных устройств, так же как и любых других объектов, производится по их демаскирующим признакам. Каждый вид электронных устройств перехвата информации имеет свои демаскирующие признаки, позволяющие обнаружить закладку.

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 обследуемого устройства нелинейным радиолокатором;

– наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.

Камуфлированные акустические закладки по внешнему виду на первый взгляд не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками ЗУ. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают.

Некоторые камуфлированные ЗУ не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

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.;

– проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов автоматических телефонных станций.

Поисковые работы ЗУ классифицируются в соответствии со следующими критериями:

По характеру выполняемых работ:

**Разовая проверка.** Разовые работы, которые обычно производятся перед проведением важных переговоров или после посещения защищаемого помещения определенными личностями.

**Профилактическая проверка.** Периодически проводимый комплекс мероприятий, направленных на поддержание на должном уровне информационной безопасности объекта. Обычно производится в совокупности с другими организационно-техническими видами информационного обеспечения.

**Конспиративная проверка.** Этот вид работ производится в случаях очевидной утечки информации, и является наиболее трудоемким видом проверок, требующим большой подготовительной работы как со стороны поисковиков, так и со стороны руководства предприятия заказчика. Основной задачей в данном виде работ является не только обнаружение канала утечки информации или средства перехвата, но и сохранение производимых мер в тайне.

**Послепроверочная консультация.** По результатам проведенного обследования объекта даются рекомендации по выбору и установке средств защиты информации, а также по реализации необходимых мер для устранения или предотвращения каналов утечки.

По глубине проводимых проверок:

**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.

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

**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.

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

**Технические средства обнаружения закладных устройств**

**Индикаторы электромагнитных излучений.** Простейший индикатор электромагнитного поля состоит из антенны, широкополосного усилителя, амплитудного детектора и порогового устройства, которое срабатывает, если сигнал на выходе детектора превысит регулируемый пороговый уровень. Порог устанавливается так, чтобы индикатор не реагировал на внешние излучения (фон). В результате подслушивающее устройство обнаруживается только в тех точках помещения, где уровень его поля превосходит фоновый на 15…20 дБ (рисунок 3.37).

Для повышения чувствительности используются режекторные фильтры, настроенные на частоты мощных внешних источников данного региона (телевизионные и радиовещательные станции), или пространственная компенсация внешних электромагнитных полей.

Некоторые устройства оснащаются простейшими средствами идентификации: звуковой выход позволяет прослушивать демодулированный сигнал и выявлять радиомикрофоны методом так называемой «акустической обратной связи», вызывающей самовозбуждение в тракте радиомикрофон – индикатор.

|  |
| --- |
| Рис 5  Рисунок 3.37. Внешний вид широкополосного индикатора «Редут» |

Индикаторы поля отличаются небольшими размерами и массой, простотой, быстродействием и низкой стоимостью. Однако из-за недостаточной чувствительности и избирательности они не обеспечивают требуемой достоверности обнаружения. Поэтому эти устройства рекомендуются лишь для предварительного обследования помещения или ручной локализации радиомикрофонов, обнаруженных более совершенными системами.

**Индикаторы-частотомеры.** Отличаются от индикаторов электромагнитных излучений встроенным счетчиком – частотомером, который измеряет частоту радиосигнала, превысившего установленный порог, и помогает оператору идентифицировать сигнал подслушивающего устройства (рисунок 3.38).

Кроме того, некоторые индикаторы можно подключать к компьютеру и сканирующему радиоприемнику. В этой конфигурации индикатору поручается предварительный анализ электромагнитной обстановки с последующей проверкой результатов сканером. Индикаторы-частотомеры сохраняют основной недостаток индикаторов поля: достоверно обнаружить источник излучения они могут только в непосредственной близости от него.

**Нелинейные локаторы.** Используются для физического обнаружения и определения местоположения скрытно размещенных электронных устройств, которые могут находиться в выключенном состоянии (рисунок 3.39). Нелинейный локатор излучает СВЧ-сигнал и принимает его вторую гармонику, которая образуется из-за нелинейных эффектов в полупроводниковых приборах. Чтобы исключить ложное срабатывание локатора, создаваемое контактами металл-окисел в строительных конструкциях, более совершенные изделия принимают и анализируют уровни не только второй, но и третьей гармоник.

|  |
| --- |
| Рис 5  Рисунок 3.38. Внешний вид индикатора-частотомера «Raksa-120» |

|  |
| --- |
| Рис 5  Рисунок 3.39. Внешний вид нелинейного локатора SEL SP-61/M «Катран» |

**Анализаторы спектра.** Измерительные приборы, которые широко используются для обнаружения и идентификации сигналов оператором по форме их спектров (рисунок 3.40). Обладая высокой чувствительностью, они могут подключаться к антенне или кабельным линиям и воспроизводить на экране спектральные панорамы или спектры отдельных радиосигналов. Главное преимущество анализаторов спектра высокая скорость сканирования и наглядное отображение результатов. Однако они, как правило, не располагают средствами автоматизации операций обнаружения и довольно дороги.

|  |
| --- |
| Рис 5  Рисунок 3.40. Внешний вид анализатора спектра Agilent Technologies N1996A |

**Сканирующие радиоприемники.** Современные сканеры могут автоматически перестраиваться в диапазоне до нескольких ГГц и обнаруживать сигналы с различными видами модуляции (рисунок 3.41). Эти изделия можно разделить на две группы. Первые обладают уникальными параметрами, однако их размеры, масса и, главное, стоимость весьма высоки.

Изделия второй группы появились в результате эволюции связных, в основном коротковолновых радиоприемников. Сканеры, обладающие высокой чувствительностью, частотной избирательностью и широким диапазоном анализа, обнаруживают сигналы радиомикрофонов с большой достоверностью. Однако эксплуатация их в качестве автономных устройств из-за ограниченных возможностей по вводу, хранению и отображению данных требует весьма высокой квалификации оператора.

**Компьютерные программы управления сканерами.** Большинство современных сканеров можно подключить к компьютеру, который значительно расширяет возможности управления, отображения и хранения информации об исследуемых сигналах. Наряду с функциями управления, а также накопления и обработки данных о радиоспектрах специализированное программное обеспечение способно решать отдельные задачи идентификации сигналов подслушивающих устройств.

|  |
| --- |
| Рис 5  Рисунок 3.41. Внешний вид сканирующего приемника «Скорпион-XL» |

**Микрокомпьютерные комплексы обнаружения радиомикрофонов.** В этих изделиях объединяется аппаратура поиска сигналов: антенны, адаптеры для подключения к кабельным линиям, специализированные сканирующие радиоприемники, а также устройства индикации и регистрации данных. Функции управления и отображения поручаются микрокомпьютеру, который организует также отдельные автоматические процедуры обнаружения и идентификации сигналов.

**Компьютерные комплексы контроля помещений и зданий (радиомониторинга).** Представляют собой аппаратно-программные системы на базе стандартных узлов компьютера и недорогого сканера, которые оснащаются дополнительной аппаратурой и программами (рисунок 3.42). Располагают возможностями для реализации «интеллектуальных» процедур обнаружения любой сложности.

**Тепловизоры.** Техническое средство, обеспечивающее преобразование электромагнитного излучения (теплового), излучаемого различными объектами в видимое изображение (рисунок 3.43). Поиск ЗУ на основе метода теплового неразрушающего контроля базируется на том, что закамуфлированное закладное устройство, сложно обнаруживаемое в видимом диапазоне длин волн, имеет демаскирующие признаки в коротковолновой (3…5 мкм) и длинноволновой (8…14 мкм) областях инфракрасного (ИК) спектра. Работа ЗУ сопровождается поглощением и выделением тепла, изменяя внутреннюю его энергию, которая в состоянии термодинамического равновесия пропорциональна температуре вещества. В результате этого поверхности физических тел (объекта контроля и ЗУ) приобретают специфическое температурное распределение и таким образом могут быть четко разграничены.

|  |
| --- |
| Рис 5  Рисунок 3.42. Внешний вид автоматизированного комплекса радиомониторинга «Крона НМ» |

В случае установки ЗУ в электронную аппаратуру, их обнаружение ведется путем поиска, места контакта электронных компонентов (точечный источник ИК излучения) и модулей, имеющих температуру, в месте контакта значительно превышающую температуру окружающей среды.

|  |
| --- |
| Рис 5  Рисунок 3.43. Внешний вид тепловизора «FLIR b50» |

**РАЗДЕЛ 4 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

**4.1 Техническая укрепленность периметра защищаемого объекта**

Характерной тенденцией развития информационных технологий является процесс интеграции. Этой тенденцией охвачены микроэлектроника и техника связи, сигналы и каналы, системы и сети. В качестве примеров можно сослаться на сверхбольшие интегральные схемы, интегральные сети передачи данных, многофункциональные устройства связи и т.п.

Наряду с интеграцией функциональной, схемотехнической и системной, в последнее время стала активно развиваться интегральная информационная безопасность (ИИБ). Под интегральной безопасностью понимается такое состояние условий функционирования человека, объектов и технических средств, при котором они надежно защищены от всех возможных видов угроз в ходе непрерывного процесса подготовки, хранения, передачи и обработки информации.

Интегральная безопасность информационных систем включает в себя следующие составляющие:

* физическая безопасность (защита зданий, помещений, подвижных средств, людей, а также аппаратных средств — компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
* безопасность связи (защита каналов связи от внешних воздействий любого рода);
* безопасность программного обеспечения (защита от вирусов, логических бомб, несанкционированного изменения конфигурации);
* безопасность данных (обеспечение конфиденциальности, целостности и доступности данных).

Задача обеспечения информационной появилась вместе с проблемой передачи и хранения информации. На современном этапе можно выделить три подхода к ее решению:

* первый (частный) подход основывается на решении частных задач обеспечения информационной безопасности. Этот подход является малоэффективным, но достаточно часто используется, так как не требует больших финансовых и интеллектуальных затрат.
* второй (комплексный) подход основывается на решении комплекса частных задач по единой программе. Этот подход в настоящее время является основным.
* третий (интегральный) подход основан на интеграции различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Третий подход направлен на достижение интегральной информационной безопасности. Понятие интегральной безопасности предполагает обязательную непрерывность процесса обеспечения безопасности, как во времени, так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный доступ, съем информации, терроризм, пожар, стихийные бедствия и т.п.).

Интегральный подход к проблеме информационной безопасности, безусловно, является наиболее перспективным, однако его применение невозможно без развитой инфраструктуры, значительных материальных и интеллектуальных затрат и высокого уровня технических средств. Эти обстоятельства сдерживают развитие интегральной безопасности. В настоящее время на практике встречаются все три подхода к обеспечению информационной безопасности, причем используются они как самостоятельно, так и в различных сочетаниях, что позволило создать, например, охранно-пожарные, тревожные и другие системы малого уровня интеграции.

В какой бы форме ни применялся интегральный подход, он связан с решением ряда сложных разноплановых частных задач в их тесной взаимосвязи. Наиболее очевидными из них являются задачи ограничения доступа к информации, технического и криптографического закрытия информации, ограничения уровней паразитных излучений технических средств, технической укрепленности объектов, охраны и оснащения их тревожной сигнализацией. Однако необходимы решения и других, не менее важных задач. Так, например, выведение из строя руководителей предприятия, членов их семей или ключевых работников может поставить под сомнение само существование данного предприятия. Этому же могут способствовать стихийные бедствия, аварии, терроризм и т.п.

Первым шагом в создании системы физической безопасности (как и информационной безопасности вообще) должен стать анализ угроз (рисков), как реальных (действующих в данный момент), так и потенциальных (способных в будущем).

По результатам анализа рисков с использованием средств оптимизации формируются требования к системе безопасности конкретного предприятия и объекта в конкретной обстановке. Завышение требований приводит к неоправданным расходам, занижение ‑к возрастанию вероятности реализации угроз.

В общем случае система физической безопасности должна включать в себя следующие подсистемы:

* управления доступом (с функцией досмотра);
* обнаружения проникновения, аварийной и пожарной сигнализации (тревожной сигнализации);
* инженерно-технической защиты (пассивной защиты);
* отображения и оценки обстановки;
* управления в аварийных и тревожных ситуациях;
* оповещения и связи в экстремальных ситуациях;
* личной безопасности персонала.

При построении системы физической безопасности, удовлетворяющей сформулированным требованиям, разработчик выбирает и объединяет средства противодействия из числа указанных ниже:

* здания и строительные препятствия, мешающие действиям злоумышленника и задерживающие его;
* аппаратура тревожной сигнализации, обеспечивающая обнаружение попыток проникновения и несанкционированных действий, а также оценку их опасности;
* системы связи, обеспечивающие сбор, объединение и передачу тревожной информации и других данных;
* системы управления, необходимые для отображения и анализа тревожной информации, а также для реализации ответных действий оператора и управления оборонительными силами;
* персонал охраны, выполняющий ежедневные программы безопасности, управление системой и ее использование в нештатных ситуациях;
* процедуры обеспечения безопасности, предписывающие определенные защитные мероприятия, их направленность и управление ими.

На рисунке 4.1 представлены технические средства противодействия и соответствующие подсистемы, имеющиеся в распоряжении разработчика.

|  |
| --- |
| graphics  Рисунок 4.1 - Структура объединенной системы обеспечения безопасности |

Как показывает опыт, успешная разработка системы безопасности возможна только в том случае, когда процесс выбора средств противодействия и объединения их в единую систему разделен на этапы и определены соответствующие каждому этапу задачи. На рисунке 4.2 этот процесс представлен в графической форме.

|  |
| --- |
| graphics  Рисунок 4.2. - Процесс выбора средств противодействия |

Первоначально определяются объекты, которые надо защитить, и их функции. Затем оценивается степень интереса потенциального противника к этим объектам, вероятные виды нападения и вызываемый ими ущерб. Наконец, определяются уязвимые для воздействия области, в которых имеющиеся средства противодействия не обеспечивают достаточной защиты.

Для эффективного применения процесс выбора средств противодействия должен содержать оценку каждого объекта с точки зрения возможных угроз и видов нападения, потенциальной вероятности применения специальных инструментов, оружия и взрывчатых веществ (этапы 3 и 4 на рисунке 4.2). Особо важным допущением в этом процессе является предположение о том, что наиболее ценный для потенциального злоумышленника объект привлечет наибольшее внимание и будет служить вероятной целью, против которой злоумышленник использует основные силы.

Разработка средств противодействия должна соответствовать концепции полной и эшелонированной защиты. Это означает, что средства противодействия следует размещать на концентрических кругах, пересекающих все возможные пути противника к любому объекту. Рисунок 4.3 иллюстрирует данную концепцию. Каждый рубеж обороны организуется таким образом, чтобы задержать нападающего на время, достаточное для принятия персоналом охраны ответных мер.

На заключительном этапе разработчик объединяет выбранные средства противодействия в соответствии с принятой концепцией защиты. Производится также предварительная оценка начальной и ожидаемой общей стоимости жизненного цикла всей системы.

Разработчик должен принимать во внимание такое понятие, как жизненный цикл защищаемых объектов. В частности, он должен учитывать возможные перемещения объектов, а также изменение требований в местах входа.

В том случае, когда внутри одного здания располагаются объекты с существенно разными требованиями к безопасности, применяется разделение здания на отсеки, что позволяет выделить внутренние периметры внутри общего контролируемого пространства и создать внутренние защитные средства от несанкционированного доступа. Периметр обычно выделяется физическими препятствиями, проход через которые контролируется электронным способом или с помощью специальных процедур.

При защите группы зданий, имеющих общую границу или периметр, необходимо учитывать не только отдельный объект или здание, но и место, на котором они расположены. Обычно участки местности с большим количеством зданий имеют общие или частично совпадающие требования по обеспечению безопасности, а некоторые участки имеют ограждение по периметру и единую проходную. Организация общего периметра позволяет уменьшить количество защитных средств в каждом здании и устанавливать их только для наиболее важных объектов или зданий, нападение на которые наиболее вероятно. Аналогичным образом, каждое строение или объект на участке следует оценить с точки зрения их возможностей задержать нападающего.

|  |
| --- |
| graphics  Рисунок 4.3 - Элементы классической системы обеспечения безопасности (охраны) объекта: 1 — охраняемый объект; 2 — задерживающее ограждение; 3 — обнаруживающее ограждение; 4 — контролируемый вход; 5 — зона оценки; 6 — нейтральная зона; 7 — забор; 8 — дальняя защита; 9 — силы внутренней обороны; 10 — силы внешней обороны; 11 — подвижный патруль; 12 — канал связи; 13 — внешний объект; 14 — электроподстанция; 15 — линия электропередачи; 16 — объекты технического обеспечения; 17 — инженерные коммуникации; 18 — радиосигнализация |

С учетом вышеизложенного рассмотрим в качестве примера проблему защиты вычислительных центров.

Надежная система должна обеспечивать защиту помещений и поддерживающей инфраструктуры, аппаратуры, программ, данных и персонала. Требования к таким системам сформулированы, в частности, в федеральном законе ФРГ по охране данных. Закон содержит перечень из девяти требований к защите, которые следует выполнять путем осуществления соответствующих технических и организационных мероприятий. Должны быть исключены:

* неправомочный доступ к аппаратуре обработки информации путем контроля доступа в производственные помещения;
* неправомочный вынос носителей информации персоналом, занимающимся обработкой данных, посредством выходного контроля в соответствующих производственных помещениях;
* несанкционированное введение данных в память, изменение или стирание информации, хранящейся в памяти;
* неправомочное пользование системами обработки информации и незаконное получение в результате этого данных;
* доступ в системы обработки информации посредством самодельных устройств и незаконное получение данных;
* возможность неправомочной передачи данных через ВЦ;
* бесконтрольный ввод данных в систему;
* обработка данных заказчика без соответствующего указания последнего;
* неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Анализ перечисленных требований показывает, что они сводятся к исключению возможности неправомочного доступа к устройствам обработки и передачи информации, похищения носителей информации и проведения актов саботажа. Данные требования могут быть выполнены путем осуществления комплекса мероприятий полицией, администрацией ВЦ и специальными уполномоченными по охране информации.

Разработку концепции защиты рекомендуется проводить в три этапа. На первом этапе должна быть четко определена целевая установка защиты, то есть установлено, какие реальные ценности, производственные процессы, программы, массивы данных необходимо защищать. На этом этапе целесообразно проводить дифференциацию по значимости отдельных объектов, требующих защиты.

На втором этапе должен быть проведен анализ видов преступных действий, которые потенциально могут быть совершены в отношении ВЦ. Важно определить степень реальной опасности таких наиболее широко распространенных категорий преступлений, как экономический шпионаж, терроризм, саботаж, кражи со взломом. Затем необходимо проанализировать наиболее вероятные действия злоумышленников в отношении основных объектов ВЦ, нуждающихся в защите.

Главной задачей третьего этапа является анализ обстановки в ВЦ, в том числе местных специфических условий, производственных процессов, уже установленных в ВЦ технических средств защиты. Собственно концепция защиты должна содержать перечень организационных, технических и других защитных мер, которые обеспечивают максимальную безопасность при заданном остаточном риске и при минимальных затратах на практическое осуществление этих мероприятий.

По уровню физической защиты все зоны и производственные помещения современных ВЦ могут быть подразделены на три группы:

* тщательно контролируемые зоны с защитой высокого уровня;
* защищенные зоны;
* слабо защищенные зоны.

К первой группе относятся, как правило, машинный зал (серверные комнаты), помещения с сетевым и связным оборудованием, архив программ и данных.

Ко второй группе относятся помещения, в которых расположены рабочие места администраторов, контролирующих работу ВЦ, а также периферийное оборудование ограниченного пользования.

В третью группу входят помещения, в которых оборудованы рабочие места пользователей и установлено периферийное оборудование общего пользования.

Современный комплекс защиты территории охраняемых объектов должен включать в себя следующие основные компоненты:

* механическую систему защиты;
* систему оповещения о попытках вторжения;
* оптическую (обычно телевизионную) систему опознавания нарушителей;
* оборонительную систему (звуковую и световую сигнализацию, применение в случае необходимости оружия);
* связную инфраструктуру;
* центральный пост охраны, осуществляющий сбор, анализ, регистрацию и отображение поступающих данных, а также управление периферийными устройствами;
* персонал охраны (патрули, дежурные на центральном посту).

**Механические системы защиты**

Основой любой механической системы зашиты, являются механические или строительные элементы, создающие для лица, пытающегося проникнуть на охраняемую территорию, реальное физическое препятствие. Важнейшей характеристикой механической системы защиты является время сопротивления, то есть время, которое требуется злоумышленнику для ее преодоления. Исходя из требуемой величины названной характеристики должен производиться и выбор типа механической системы защиты.

Как правило, механическими или строительными элементами служат стены и ограды. Если позволяют условия, могут применяться рвы и ограждения из колючей проволоки.

Вышеназванные элементы могут сочетаться в различных комбинациях в одной системе механической защиты. В настоящее время на ценных охраняемых объектах используются системы механической защиты с тройной изгородью, со специальными элементами, затрудняющими попытки перелезания через ограждения, и с применением S-образных мотков колючей проволоки.

При использовании многорядных механических систем защиты датчики оповещения о попытке вторжения целесообразно располагать между внутренним и внешним ограждением. При этом внутреннее ограждение должно обладать повышенным временем сопротивления.

**Системы оповещения**

В современных системах оповещения (системах тревожной сигнализации) о попытках вторжения на охраняемую территорию находят применение датчики нескольких типов. Поскольку основные характеристики подобных систем определяются, главным образом, характеристиками используемых датчиков, рассмотрим принципы действия и особенности применения последних более подробно.

В системах защиты периметра территории без ограды используются микроволновые, инфракрасные, емкостные, электрические и магнитные датчики.

С помощью датчиков первых двух типов формируется протяженная контрольная зона барьерного типа. Действие систем с микроволновыми датчиками основывается на контроле интенсивности высокочастотного направленного излучения передатчика, которое воспринимается приемником. Срабатывание сигнализации происходит при прерывании этого направленного излучения. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, воздействием растительности, атмосферных осадков, передвижением транспортных средств, а также воздействием посторонних передатчиков.

При использовании инфракрасных систем оповещения между передатчиком и приемником появляется монохроматическое световое излучение в невидимой области спектра. Срабатывание сигнализации происходит при прерывании одного или нескольких световых лучей. Ложные срабатывания могут быть обусловлены перемещением в контролируемой зоне животных, сильным туманом или снегопадом.

Принцип действия емкостной системы оповещения основывается на формировании электростатического поля между параллельно расположенными, так называемыми, передающими и воспринимающими проволочными элементами специального ограждения. Срабатывание сигнализации происходит при регистрации определенного изменения электростатического поля, имеющего место при приближении человека к элементам ограждения. Ложные срабатывания могут быть обусловлены перемещением животных, воздействием растительности, обледенением элементов ограждения, атмосферными воздействиями или загрязнением изоляторов.

Электрические системы оповещения базируются на использовании специального ограждения с токопроводящими проволочными элементами. Критерием срабатывания сигнализации является регистрация изменений электрического сопротивления токопроводящих элементов при прикосновении к ним. Ложные срабатывания могут быть вызваны животными, растительностью или загрязнением изоляторов.

Принцип действия систем с магнитными датчиками предполагает контроль параметров магнитного поля. Срабатывание сигнализации происходит при регистрации искажений, которые обусловлены появлением в зоне действия датчиков предметов из ферромагнитного материала. Ложное срабатывание может иметь место из-за изменений характеристик почвы, обусловленных, например, продолжительным дождем.

При наличии механической системы защиты территории (например, ограды, расположенной по периметру) находят применение системы оповещения с вибрационными датчиками, датчиками звука, распространяющегося по твердым телам, акустическими датчиками, электрическими переключателями, а также системы с электрическими проволочными петлями.

Вибрационные датчики закрепляются непосредственно на элементах ограды. Срабатывание сигнализации происходит при появлении на выходе датчиков сигналов, которые обусловлены вибрациями элементов ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем или градом.

Датчики звука также устанавливаются непосредственно на элементы ограды и контролируют распространение по ним звуковых колебаний. Срабатывание сигнализации происходит при регистрации так называемых шумов прикосновения к элементам ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом или срывающимися с элементов ограды сосульками.

В системах оповещения с акустическими датчиками контролируются звуковые колебания, передаваемые через воздушную среду. Срабатывание сигнализации происходит при регистрации акустических сигналов, имеющих место при попытках перерезать проволочные элементы ограды. Ложные срабатывания могут быть обусловлены сильным ветром, дождем, градом, а также различными посторонними шумами.

Действие систем с электрическими переключателями основано на регистрации изменения состояния переключателей, вмонтированных в ограду, которое происходит при соответствующем изменении натяжения проволочных элементов или нагрузки на направляющие трубки ограды. Ложные срабатывания сигнализации могут быть вызваны очень сильным ветром при недостаточном натяжении элементов ограды.

Если в системах оповещения в качестве чувствительных элементов применяются изолированные токопроводящие проволочные элементы, срабатывание сигнализации происходит при перерезании или деформации этих элементов. Ложные срабатывания могут произойти при возникновении неисправности в сети электропитания.

Для контроля участков почвы по периметру охраняемой территории находят применение системы оповещения с датчиками звука, распространяющегося по твердым телам, а также с датчиками давления.

В системах первого типа регистрируются звуковые, сейсмические колебания. Срабатывание сигнализации происходит при регистрации сотрясений почвы, например, ударного шума. Ложные срабатывания могут быть обусловлены перемещением достаточно крупных животных, движением транспорта вблизи охраняемой территории.

В системах второго типа используются пневматические или емкостные датчики давления, позволяющие регистрировать изменения нагрузки на почву. Срабатывание сигнализации происходит при регистрации соответствующего роста давления, например, ударного. Ложные срабатывания возможны из-за перемещений достаточно крупных животных, разгерметизации пневматических датчиков или коррозии.

Для контроля участков охраняемой территории фирмой Multisafe AG разработана система оповещения Multiplain, датчики которой работают на принципе регистрации разности давления. Необходимо отметить, что названный физический принцип до настоящего времени не использовался для обнаружения попыток вторжения на охраняемую территорию. Датчик состоит из двух полых тел с избыточным давлением, которые соединены между собой через специальный преобразователь разности давлений. При возникновении даже незначительной разницы давлений в этих телах в преобразователе срабатывает контакт, через который может коммутироваться цепь включения тревожной сигнализации.

При использовании указанного датчика достаточно просто локализовать участок, на котором сработал чувствительный элемент. Кроме того, преобразователь оснащен устройством автоматического восстановления нулевой точки, что исключает срабатывание контакта при медленных изменениях давления, которые могут быть обусловлены различными возмущающими воздействиями, например, колебаниями температуры. Датчик также нечувствителен к колебаниям и вибрациям, обусловленным движением автомобильного или железнодорожного транспорта.

Чувствительная часть рассматриваемого устройства конструктивно выполнена в виде набора специальных ковриков, которые могут устанавливаться под слоем гравия, дерна, земли или под плитами пешеходных дорожек. Срабатывание контактов в преобразователях происходит при изменении нагрузки не менее чем на 30 кг. Таким образом, система оповещения не реагирует на перемещение мелких животных по контролируемому участку территории. Предварительная нагрузка за счет маскировочного покрытия ковриков может достигать 250 кг/м2 без влияния на их чувствительность.

Приведенное описание позволяет сделать вывод об отсутствии идеальной системы оповещения. Основное техническое требование к подобной системе может быть сформулировано следующим образом: максимально возможная вероятность обнаружения и надежность в сочетании с минимальной частотой ложных срабатываний.

Повышение вероятности обнаружения нарушителя системой оповещения обязательно сопровождается увеличением числа ложных срабатываний. Таким образом, разработка систем оповещения связана, прежде всего, с поиском рационального компромисса относительно соотношения величин названных показателей. Из этого следует, что дальнейшее совершенствование систем оповещения должно обеспечить прежде всего повышение вероятности обнаружения и снижение интенсивности ложных срабатываний путем использования нескольких систем оповещения различного принципа действия в едином комплексе и применения в этих системах микропроцессорных анализаторов.

**Системы опознавания**

Обязательным условием надежного функционирования всего комплекса защиты охраняемой территории является последующий анализ поступающих сообщений о проникновении для точного определения их вида и причин появления. Названное условие может быть выполнено посредством использования систем опознавания.

Наиболее широкое распространение в подобных системах получили телевизионные установки дистанционного наблюдения. Несомненно, что объект со стационарными постами охраны обладает более высокой защищенностью, однако при этом значительно возрастают затраты на его охрану. Так, при необходимости круглосуточного наблюдения требуется трехсменная работа персонала охраны. В этих условиях телевизионная техника становится средством повышения эффективности работы персонала охраны, прежде всего при организации наблюдения в удаленных, опасных или труднодоступных зонах.

Вся контролируемая системой оповещения зона разграничивается на отдельные участки протяженностью не более 100 м, на которых устанавливается, по крайней мере, одна передающая телекамера. При срабатывании датчиков системы оповещения, установленных на определенном участке контролируемой зоны, изображение, передаваемое соответствующей телекамерой, автоматически выводится на экран монитора на центральном посту охраны. Кроме того, при необходимости должно быть обеспечено дополнительное освещение данного участка. Немаловажно, чтобы внимание дежурного охранника было быстрее привлечено к выведенному на экран монитора изображению.

Фактические причины срабатывания сигнализации во многих случаях могут быть идентифицированы только при условии достаточно высокой оперативности дежурного охранника. Важно, что данное положение, прежде всего, имеет место при действительных попытках вторжения на охраняемую территорию и при преднамеренных обманных действиях злоумышленников. Одним из перспективных путей выполнения выше сформулированного условия является применение устройства видеопамяти, которое обеспечивает автоматическую запись изображения сразу же после срабатывания сигнализации. При этом дежурному охраннику предоставляется возможность вывести из устройства памяти на экран монитора первые кадры изображения и идентифицировать причину срабатывания датчиков системы оповещения.

В ряде телесистем наблюдения применены передающие камеры, ориентация которых может дистанционно меняться дежурным охранником. При включении сигнализации тревоги служащий охраны должен ориентировать телекамеру на участок, где сработали датчики системы оповещения. Практический опыт показывает, однако что такие телеустановки менее эффективны по сравнению с жестко ориентированными передающими телекамерами.

Отличительной особенностью некоторых объектов является их большая протяженность. Большое количество площадок таких объектов может быть расположено на значительном удалении друг от друга, что серьезно удорожает монтаж и эксплуатацию оборудования. В этих случаях можно применить систему малокадрового телевидения типа Slowscan. Она функционирует на больших дальностях, имеет невысокую стоимость и совместима с любой существующей замкнутой телевизионной системой, которая уже установлена на объекте. Для передачи видеокадров и команд в этой системе используется телефонная сеть общего пользования.

Особые преимущества в системах охраны имеют камеры на приборах с зарядовой связью (ПЗС). По сравнению с обычными трубочными камерами они обладают меньшими габаритами, более высокой надежностью, практически не нуждаются в техническом обслуживании, отлично работают в условиях низкой освещенности, обладают чувствительностью в инфракрасной области спектра. Однако, наиболее важным является то, что видеоинформация на чувствительном элементе указанной камеры сразу представлена в цифровой форме и без дополнительных преобразований пригодна для дальнейшей обработки. Это дает возможность легко идентифицировать различия или изменения элементов изображения, реализовать в камере встроенный датчик перемещений. Подобная камера со встроенным детектором и маломощным ИК-осветителем может вести наблюдение охраняемой территории и при появлении нарушителя в поле зрения распознавать изменения элементов изображения и подавать сигнал тревоги.

**Оборонительные системы**

Для предотвращения развития вторжения на охраняемую территорию используется оборонительная система, в которой находят применение осветительные или звуковые установки. В обоих случаях субъект, пытающийся проникнуть на охраняемую территорию, информируется о том, что он обнаружен охраной. Таким образом, на него оказывается целенаправленное психологическое воздействие. Кроме того, использование осветительных установок обеспечивает благоприятные условия для действий охраны.

Для задержания преступника охрана предпринимает соответствующие оперативные меры или вызывает милицию (полицию). Если злоумышленнику удалось скрыться, то для успеха последующего расследования важное значение приобретает информация, которая может быть получена с помощью рассмотренной выше системы опознавания.

В особых случаях функции оборонительной системы выполняет специальное ограждение, через которое пропущен ток высокого напряжения.

**Связная инфраструктура**

Современный рынок технических средств предоставляет разработчикам широкие возможности выбора аппаратуры и каналов связи. Однако, с учетом интегрального подхода, в качестве связной инфраструктуры целесообразно использовать структурированные кабельные системы.

**Центральный пост и персонал охраны**

Сложные комплексы защиты охраняемых территорий, состоящие, как правило, из нескольких систем, могут эффективно функционировать только при условии, что работа всех технических установок постоянно контролируется и управляется с центрального поста охраны. Учитывая повышенную психологическую нагрузку на дежурных охранников центрального поста, необходимость оперативной выработки и реализации оптимальных решений в случае тревоги, к центральным устройствам комплексов защиты предъявляются особые требования. Так, они должны обеспечивать автоматическую регистрацию и отображение всех поступающих в центральный пост сообщений и сигналов тревоги, выполнение всех необходимых процедур. Важную роль играет и уровень эргономики аппаратуры, которой оснащаются рабочие места дежурных охранников.

**Интегральный комплекс физической защиты**

На рисунке 4.4 (см. след. страницу) представлена блок-схема интегрального комплекса физической защиты объекта, обеспечивающего функционирование всех рассмотренных выше систем. Отличительной особенностью подобных комплексов является интеграция различных подсистем связи, подсистем обеспечения безопасности в единую систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.

Необходимо отметить, что в рассматриваемой блок-схеме технические средства скомпонованы по системам достаточно условно для того, чтобы схема приобрела более логичную форму и была бы более понятна. На самом деле одни и те же средства выполняют различные функции для разных систем обеспечения безопасности.

**4.2 Системы охранно-пожарной сигнализации**

**Система охранно-пожарной (тревожной) сигнализации** - совокупность совместно действующих технических средств охраны, предназначенных для обнаружения и (или) сигнализации о наличии опасности (рисунок 4.5).

|  |
| --- |
| Безымянный  Рисунок 4.5. – Структурная схема системы охранно-пожарной сигнализации |

**Извещатели** — устройства, как для ручной подачи сигнала «тревога», так и автоматически реагирующие на появление тревожных факторов;

**Приемно-контрольный прибор (ПКП)** – прием сигнала тревоги от извещателей и трансляция его в соответствующую службу безопасности (пожарная охрана, Департамент охраны МВД), индикация номера объекта от которого принят сигнал и управление исполнительными устройствами;

**Исполнительные устройства** – оповещение о тревоге и ее ликвидация.

**Система электропитания** – бесперебойное электропитание устройств входящих в систему сигнализации.

**Средства обнаружения (извещатели)**

- радиоволновые и радиолучевые средства обнаружения - позволяют оборудовать скрытые или маскируемые рубежи охраняемого периметра объекта;

- оптические средства обнаружения - используются для блокирования объемов помещений, проходов, коридоров, периметров;

- сейсмические средства обнаружения - регистрируют и обрабатывают сигналы, возникающие в результате колебаний подстилающей поверхности (грунт) при пересечении человеком охраняемой зоны. Предназначены для блокирования участков протяженных рубежей периметров объектов;

- магнитометрические средства обнаружения - предназначены для регистрации факта проноса в их зоне обнаружения предметов, выполненных из металлов или их сплавов, а так же других материалов.

|  |
| --- |
| graphics  Рисунок 4.4 - Блок-схема интегрального комплекса физической защиты объекта |

**Пожарные извещатели**

- пороговые (безадресные), которые настроены изготовителем на определенное значение контролируемого параметра, при достижении которого извещатель передает в приемно-контрольный прибор (ПКП) сигнал «ПОЖАР» путем замыкания контактов своего реле;

- пороговые (адресные). Имеют один или несколько встроенных порогов срабатывания и индивидуальный адрес в системе;

- адресно-аналоговые. Регистрируют и передают в ПКП текущее значение контролируемого параметра и свой индивидуальный адрес.

Для обнаружения возгорания используются следующие принципы активации пожарных извещателей:

- концентрация в воздухе частиц дыма;

- температура окружающей среды;

- излучение открытого пламени.

Для обнаружения возгорания могут использоваться следующие основные пожарные извещатели:

***Ручные извещатели*** необходимы для принудительного перевода человеком системы в режим сигнализации о пожаре (рисунок 4.6). Они могут быть реализованы в виде рычагов или кнопок, покрытых прозрачными материалами (легко разбиваемыми при пожаре). Чаще всего они устанавливаются в легкодоступных местах общего пользования.

***Тепловые извещатели*** реагируют на изменение температуры окружающей среды (рисунок 4.7). Тепловые пороговые пожарные извещатели выдают сигнал «пожар» при достижении пороговой температуры, ***дифференциальные*** – фиксируют пожароопасную ситуацию по скорости нарастания температуры.

|  |
| --- |
| pogar-znak  Рисунок 4.6 - Внешний вид ручного извещателя ИПР-Р |

|  |  |
| --- | --- |
| 330  а) | mak-dm-isp-01__orig  б) |
| Рисунок 4.7 - Внешний вид теплового извещателя ИП103-4/1 (а) и дифференциального теплового извещателя МАК-ДМ (б) | |

Тепловые извещатели устанавливаются в следующих случаях:

- в контролируемом объеме применяемые материалы таковы, что при горении они, дают больше жара, чем дыма (например, облицовка стен деревянными панелями);

- когда распространение дыма затруднено вследствие либо малого объема помещения (например, за подвесными потолками), либо внешних условий (низкая температура, большая влажность воздуха);

- когда в воздухе присутствует высокая концентрация каких-либо аэрозольных частиц, не имеющих отношение к процессам горения (пыль, копоть, мука и т.д.).

Контактный пороговый тепловой извещатель выдает тревожный сигнал при превышении заранее заданной предельно допустимой температуры. При нагревании расплавляется контактная пластина, электрическая цепь разрывается и вырабатывается тревожный сигнал. Обычно пороговая температура составляет 75 °C (рисунок 4.7 а).

В качестве чувствительного элемента может применяться и полупроводниковый прибор. При росте температуры сопротивление цепи падает, и сила тока в ней увеличивается. При превышении пороговой величины электрического тока вырабатывается тревожный сигнал. Полупроводниковые чувствительные элементы имеют более высокую скорость реагирования, величина пороговой температуры может быть задана произвольно, а при срабатывании датчика не происходит разрушения прибора.

Дифференциальные тепловые извещатели обычно состоят из двух термоэлементов, один из которых располагается внутри корпуса извещателя, а второй помещен снаружи (рисунок 4.7 б). Токи, протекающие через эти две цепи, подаются на входы дифференциального усилителя. При увеличении температуры ток, протекающий по наружной цепи, резко изменяется. Во внутренней цепи он почти не меняется, что приводит к дисбалансу токов и формированию тревожного сигнала. Использование термопары позволяет исключить влияние плавных температурных изменений, вызванных естественными причинами. Эти датчики являются наиболее быстрыми по скорости реагирования и устойчивыми в работе.

***Линейные тепловые извещатели.*** Конструкция представляет собой четыре медных проводника с оболочками из специального материала с отрицательным температурным коэффициентом. Проводники упакованы в общий кожух так, что плотно соприкасаются своими оболочками. Провода соединяются в конце линии попарно между собой, образуя две петли, соприкасающиеся оболочками. Принцип действия: при увеличении температуры оболочки изменяют свое сопротивление, изменяя также общее сопротивление между петлями, которое и измеряется специальным блоком обработки результатов. По величине этого сопротивления и принимается решение о наличии возгорания. Чем больше длина кабеля (до 1,5 км), тем выше чувствительность прибора.

***Дымовые извещатели*** предназначены для обнаружения наличия заданной концентрации частиц дыма в воздухе (рисунок 4.8).

Дым – совокупность аэрозольных частиц, выделяющихся в процессе горения различных материалов.

Состав частиц дыма может быть различным и зависит от химической природы горящего вещества, а концентрация и скорость движения – от распределения воздушных потоков в контролируемой зоне. Дымовые пожарные извещатели определяют лишь один параметр: концентрацию частиц дыма до определенной скорости их движения (обычно до 10 м/с). Однако, поскольку состав частиц может быть разным, используются оптоэлектронные и ионизационные пожарные извещатели.

|  |
| --- |
| store_apendix_large709_638  Рисунок 4.8 - Внешний вид дымового извещателя ИП-212-88Х (автономный) |

***Ионизационный дымовой извещатель.*** Чувствительная часть извещателя состоит из двух камер – измерительной внешней камеры и полугерметичной контрольной камеры внутри (рисунок 4.9). В контрольной камере находится радиоактивная фольга из америция-241 характеризующейся интенсивностью излучения ниже уровня фона (0,9 мкКюри), благодаря которой, между измерительной и контрольной камерами протекает ток при включении напряжения питания извещателя.

Поток радиоактивных частиц направляется в две отдельные камеры: изолированную от окружающей воздушной среды контрольную и открытую для внешнего воздуха измерительную. При попадании частиц дыма в измерительную камеру происходит уменьшение силы тока, протекающего через нее, поскольку при этом происходит уменьшение длины пробега альфа-частиц и увеличение рекомбинации ионов. Для принятия решения о наличии дыма, формируется разностный сигнал из сигналов, поступающих с измерительной и контрольной камеры.

Такие пожарные извещатели имеют срок службы не менее 5 лет и требуют специальной их утилизации.

|  |  |
| --- | --- |
| neploxov_pic3  а) | Безымянный  б) |
| Рисунок 4.9 - Конструкция ионизационногодымового извещателя 1151EIS (а) и принцип его работы (б) | |

Ионизационные дымовые извещатели хорошо функционируют в качестве извещателей общего назначения, они с минимальной задержкой регистрируют быстро распространяющиеся (с открытым пламенем) пожары и очень часто используются для защиты имущества.

***Оптический дымовой извещатель.*** Их принцип функционирования основан эффекте оптического рассеивания инфракрасного излучения (ИК) ближнего ИК-диапазона на частицах дыма. Измерительная камера такого устройства содержит ИК-светодиод и фотоприемник (оптоэлектронную пару), ориентированные друг относительно друга так, чтобы излучение светодиода в нормальных условиях не попадало на фотоприемник (рисунок 4.10). Оптоэлектронная пара размещается в оптической камере.

При попадании частиц дыма в оптическую камеру на них происходит рассеивание излучения ИК-светодиода, вследствие чего часть ИК-излучения попадает на фотоприемник, что обеспечивает формирование на его выходе электрического сигнала. Чем больше концентрация рассеивающих частиц дыма в воздухе, тем выше уровень сигнала. При превышении определенного порода задымления извещатель сигнализирует о наличии возгорания.

|  |  |
| --- | --- |
| 1316333899_pozharka-k-aps  а) | Безымянный  б) |
| Рисунок 4.10 - Внешний вид оптического дымового извещателя ИП-212-63 (а) и принцип его работы (б) | |

Извещение “ПОЖАР” формируется по ослаблению ИК-излучения светодиода дымом. Такого типа извещатели используются когда необходимо минимальным количеством извещателей перекрыть большие по площади пространства помещений или при высоких потолках контролируемого помещения (выше 3,5 м), когда время достижения дымом других извещателей велико.

Пожарные извещатели применяются в составе систем пожарной сигнализации и используются совместно с приемно-контрольными приборами.

**Приёмные устройства пожарной сигнализации** (приемно-контрольные приборы) (рисунок 4.11) служат для:

- получения от извещателей сигналов о пожаре или значений контролируемых ими параметров;

- индикации номера объекта, от которого принят сигнал;

- управления звуковой и световой сигнализацией о пожаре;

- подачи управляющего сигнала на устройства пожарной автоматики;

- трансляции сигнала тревоги в пожарную охрану.

**Типы систем тревожной сигнализации**

***Пороговая (безадресная) сигнализация.*** Это наиболее распространенный тип сигнализации в виду невысокой стоимости оборудования. Тем не менее, затраты на ее монтаж и техническое обслуживание высоки за счет большого расхода кабельной продукции, а также невысокой надежности извещателей. Защита от их ложных срабатываний обеспечивается за счет увеличения количества извещателей (два вместо одного на точку), что приводит к некоторому вынужденному удорожанию системы в целом. Принятие решения о наличии тревоги в большей степени зависит от извещателя, а не от ПКП. Целесообразно применение на небольших и средних объектах.

|  |
| --- |
| Безымянный  Рисунок 4.11 - Внешний приемно-контрольного прибора Сигнал-20П SMD |

***Адресная сигнализация.*** Появление данного типа сигнализации было вызвано необходимостью точного определения места возникновения тревоги. Каждый извещатель имеет свой адрес или адресную метку и настройку на один или несколько порогов. Позволяет точно определять место возникновения тревоги. Но избыточночть по количеству извещателей и высокие затраты на обслуживание остаются такими же, как в обычных системах за счет того, что используются пороговые извещатели.

***Адресно-аналоговая сигнализация.*** Самый современный тип сигнализации. Обеспечивает помимо точного определения места возникновения тревоги возможность регистрации ее на самой ранней стадии за счет отслеживания не фиксированных порогов, а текущих значений контролируемых параметров. Решение о наличии тревоги принимает ПКП на основании анализа динамики изменения величины периодически регистрируемых и передаваемых извещателями значений. Позволяют в зависимости от условий эксплуатации (типов помещений, запыленности извещателей, времени суток и т.д.) программно изменять чувствительность извещателей, устанавливать произвольно пороги срабатывания отдельно для каждого извещателя. Система, гибко настраиваемая под условия эксплуатации и особенности каждого помещения

**4.3 Системы видеонаблюдения**

**Телевизионная система видеонаблюдения** – совокупность совместно действующих объединенных линиями связи технических средств, предназначенных для видеонаблюдения за состоянием охраняемого объекта (его части), а также видеозаписи или подачи сигнала тревоги при изменении ситуации на нем (рисунок 4.12).

|  |
| --- |
| Безымянный  Рисунок 4.12 – Структурная схема системы видеонаблюдения |

**Видеокамера** – техническое средство, обеспечивающее преобразование светового потока в полный телевизионный сигнал.

**Устройство сравнения** – техническое средство, выполняющее сравнение яркостей текущего изображения с тестовым изображением, извлекаемым из **устройства памяти**, что позволяет решить задачу обнаружения объекта наблюдения (человек или автотранспортное средство).

**Оповещение** – сообщение, несущее информацию об изменении контролируемых параметров состояния охраняемых объектов или технических средств и систем охраны, формируемое для восприятия человеком в виде речевых, звуковых и (или) световых сигналов.

**Исполнительное устройство** – техническое средство, позволяющее при обнаружении объекта наблюдения включить **устройство видеорегистрации** для записи телевизионного сигнала и **устройство связи** для оповещения группы быстрого реагирования.

**Группа быстрого реагирования** – под ней подразумеваются сотрудники, обеспечивающие физическую охрану объекта, обязанные локализовать проникновение на его территорию.

**4.4 Системы контроля и управления доступом**

**Система контроля и управления доступом (СКУД)** – совокупность совместно действующих средств (механических, электромеханических, электрических, электронных), обеспечивающих контроль и управление доступом и обладающих технической, информационной, программной и эксплуатационной совместимостью, предназначенных для ограничения и санкционирования перемещения людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории охраняемых объектов.

|  |
| --- |
| Безымянный  Рисунок 4.13. – Структурная схема системы видеонаблюдения |

**Идентификатор** – уникальный признак субъекта доступа.

**Устройство ввода идентификационных признаков (УВИП)** – электронные устройства для ввода идентификатора.

**Устройство управления** – устанавливают режим доступа и обеспечивают прием и обработку информации с УВИП, управление УПУ, отображение и регистрацию информации.

**Управляемые преграждающие устройства (УПУ)** – обеспечивающие физическое препятствие доступу людей, транспорта и других объектов.

**Виды идентификаторов**

**Пароль** - последовательность символов, известная только одному человеку, вводимая вручную;

**Устройство** - малогабаритное техническое средство, содержащее последовательность символов, вводимых контактным или бесконтактным способом;

**Биометрия** - физиологические или поведенческие характеристики человека вводимые контактным или бесконтактным способом.

**Способы ввода идентификатора**

* Ручной – ввод идентификатора субъектом путем набора пароля на клавиатуре;
* Контактный – использование устройства аутентификации (touch memory, карта с магнитной полосой и т.д.);
* Бесконтактный (RFID, proximity устройства и т.д.).

По способу управления преграждающими устройствами (дверьми, турникетами, шлюзами и т.д.) все системы можно классифицировать следующим образом:

* автономные (локальные) — для управления одним или несколькими преграждающими устройствами, без передачи информации на центральный пульт и без контроля со стороны оператора;
* централизованные (сетевые) — для управления преграждающими устройствами с обменом информацией с центральным пультом, контролем и управлением системой со стороны оператора;
* универсальные, включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под руководством центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании или центральном устройстве.

По количеству точек доступа и пользователей СКУД можно подразделять на:

* малые — единица точек доступа (офисы);
* средние — десятки точек доступа и тысячи пользователей (банки, предприятия, учреждения, гостиницы);
* большие — сотни точек доступа и десятки тысяч пользователей (крупные промышленные предприятия, аэропорты).

Автономные системы предназначены для обеспечения контроля и управления доступом в отдельное помещение (рисунок 4.13).

|  |
| --- |
| skd1  Рисунок 4.13 - Структурная схема автономной СКУД |

Такая система состоит из автономного контроллера, хранящего в себе базу данных идентификаторов и управляющего работой остальных элементов системы. В качестве исполнительного устройства используется электромагнитный замок, либо защелка. Для идентификации пользователя используются различные типы карт с соответствующими считывателями (магнитные, Proximity, штриховые). Контроллер работает, как правило, с одним считывателем на вход (считыватель на выход используется лишь в особо важных помещениях); для открытия замка изнутри помещения обычно используется либо кнопка, либо датчик-коммутатор движения. Для обеспечения правильности работы всей системы используется датчик положения двери.

Для обеспечения нормального режима работы системы контроля доступа, дверь оснащается доводчиком, а контроллер — резервным источником питания.

Типичным примером автономного контроллера является контроллер обеспечивающий работу с одним считывателем Proximity карточки или Touch Memory считывателем, позволяющий обеспечить автономный контроль за доступом в отдельное помещение.

Автономные системы с накоплением информации, выполняют те же задачи, что и системы описанные выше. Единственным отличием является возможность системы накапливать информацию обо всех проходах через точку прохода (дверь, турникет) — время, дата, идентификационный номер. Данная информация хранится в памяти контролера и может быть по необходимости востребована. Для получения информации и представления её в наглядном виде используется специальное программное обеспечение (ПО). ПО позволяет оператору системы решать задачи: отслеживания перемещения сотрудников по территории, учета рабочего времени сотрудников, визуально контролировать личность владельца Proximity карточки или брелка Touch Memory.

Характерным примером данной системы служит контролер с программным обеспечением. Контролеры являются переходным звеном к сетевым системам, так как, могут они объединятся в единую сеть, для получения накопленных данных от многих точек прохода.

|  |
| --- |
| skd2  Рисунок 4.14 - Автономная СКУД с накоплением информации |

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

Выделяют четыре характерных типа точек доступа, где может быть применен контроль:

* проходные;
* офисные помещения;
* помещения с повышенным уровнем безопасности;
* объекты на улице (ворота, шлагбаумы для автостоянок и т.д.).

|  |
| --- |
| skd3  Рисунок 4.15. Сетевая СКУД |

Управляемые преграждающие устройства (турникеты) могут быть полуростового типа, реже используются турникеты с перекрытием проема в полный рост. Турникеты в большинстве своем не обеспечивают физического препятствия для проникновения, а служат только для упорядочивания потока людей и помогают службе охраны контролировать вход на объект. Таким образом, основная их задача — ограничить возможность прохода нескольких человек по одному допуску (идентификатору). Турникеты могут быть оборудованы средствами сигнализации, срабатывающими при попытках обхода. Шлюзы или кабины относятся к преграждающим устройствам блокирующего типа. Они могут при необходимости сдержать человека в точке доступа. Шлюзы применяются на объектах с повышенным уровнем безопасности. При этом они часто оснащаются дополнительными средствами контроля (металлодетекторами, детекторами взрывчатых и радиоактивных веществ и т.п.). На проходных может возникнуть потребность в телевизионном контроле. При этом ввод кода, или считывание идентификатора пользователя, сопровождается вводом изображений из базы данных и с телекамеры на монитор охранника, (режим видеоидентификации), который производит их равнение.

Основной особенностью построения СКУД на больших объектах, является организация нескольких автоматизированных рабочих мест (АРМ) на базе персональных компьютеров, объединенных в локальную компьютерную сеть. Весь персонал, обслуживающий СКУД, имеет доступ к единой базе данных, находящейся на сервере системы. Такие системы обычно содержат АРМы: «проходная» (с возможностью видеоидентификации), бюро пропусков, администратор, дежурный службы безопасности. В системе используется несколько сетей контроллеров, каждая из которых подключается к территориально ближайшему компьютеру, но управление всей системой может осуществляться с любого рабочего места при наличии соответствующих прав у оператора.

Построенная по такой схеме СКУД может обеспечить централизованное управление на объекте, содержащем несколько зданий, значительно удаленных друг от друга.

|  |
| --- |
| skd4  Рисунок 4.16. Сетевая СКУД большого объекта |

**РАЗДЕЛ 5 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

**5.1 Вредоносные программы и антивредоносное программное обеспечение**

Классификация по вредоносной нагрузке:

1. Создание помех в работе оборудования;

2. Установка других вредоносных программ;

3. Использование для получения персональных данных и мошенничества.

По методу размножения:

1. Эксплойт - представляет собой набор данных, вызывающий ошибку при обращении к нему.

2. Логическая бомба - вредоносное действие совершается при выполнении некоторого условия;

3. Троянская программа - не имеет собственного механизма размножения.

4. Компьютерный вирус - размножается в пределах компьютера и через сменные носители.

5. Сетевой червь - способен самостоятельно размножаться по сети.

По среде обитания:

1. Файловые - внедрение в исполняемые файлы путем их дублирования (компаньон-вирусы) или использования особенностей организации файловой системы (link-вирусы).

2. Загрузочные - запись в загрузочный сектор диска (boot-сектор) или в сектор системного загрузчика жесткого диска (master boot record).

3. Макровирусы - использование возможности программ обработки информации для переноса тела вируса (Word, Excel и т.д.).

4. Сетевые - используют возможности протоколов компьютерных сетей.

Жизненный цикл вирусов.

1. Стадия хранения:

хранение на носителе внедренным в объект;

наиболее уязвим на данной стадии.

Способы защиты от обнаружения:

шифрование части тела вируса;

модификация кода загрузчика.

Модификация кода загрузчика. Цель — обеспечить текстуальные различия с оригиналом при неизменных результатах работы:

изменение порядка независимых инструкций;

замена части инструкций на эквивалентные по результату работы;

введение зашумляющих инструкций.

Полиморфные вирусы — не имеют ни одного постоянного участка кода.

Стелс вирусы — обеспечивают собственное скрытие в системе за счет перехвата и контроля прерываний.

Резидентные вирусы — в оперативной памяти ПК оставляют свою резидентную часть, которая перехватывает прерывания ОС к объектам и заражает их.

2. Стадия исполнения:

выполнение деструктивных действий;

загрузка вируса;

поиск жертвы;

заражение жертвы;

выполнение деструктивных функций;

передача управления программе-носителю.

Способы распространения:

1. Электронная почта - маскирование “зараженных” исполняемых файлов под текстовые документы. Использование HTML ссылок на активные компоненты ActiveX, Java и т.д.

2. “Троянские” web-сайты - используются уязвимостей браузера для запуска на целевом ПК активных компонентов.

3. Локальная сеть - посредством внедрения тела вируса, в файлы, размещенные на сервере (login.com и т.д.).

Типовые признаки деятельности вируса:

появление сообщений об ошибках;

искажение наборов данных;

истощение ресурсов ПК;

невозможность загрузки ОС.

Общие способы защиты

1. Ограничение физического доступа.

2. Работа с правами пользователя.

3. Обновление ПО.

4. Отключение функции автозапуска в ОС.

5. Контроль за сменными носителями.

Методы обнаружения вирусов

1. Сравнение с эталоном - поиск вируса по его “маске”. Обнаружение известных вирусов.

2. Эвристический анализ - обнаружение вируса за счет отслеживания его последовательности действий. Обнаружение не известных вирусов.

3. Антивирусный мониторинг - обнаружение вирусов на “лету” за счет загрузки резидента антивирусной программы в оперативную память ПК.

4. Обнаружение изменений - обнаружение вирусов на основе предварительно полученных характеристик областей диска.

Виды антивирусных программ

1. Программы-фаги (сканеры).

Достоинства:

обнаружение и удаление тела вируса;

возможность резидентного функционирования;

универсальность по типу обнаруживаемых вирусов.

Недостатки:

относительно низкая скорость поиска;

большой размер антивирусных баз;

необходимость постоянной их актуализации.

2. Ревизоры дисков (CRC-сканеры).

Достоинства:

Используют антистелс алгоритмы;

обнаруживают вирус любого типа.

Недостатки:

Не обнаруживают вирусы во вновь получаемых файлах (электронная почта, сменные носители и т.д.).

3. Программы-блокировщики.

Достоинства:

обнаружение вируса на стадии загрузки;

обнаруживают вирус любого типа.

Недостатки:

не обеспечивают уничтожение вируса;

психологическое воздействие на пользователя (назойливость).

4. Программы-иммунизаторы.

Достоинства:

сообщают о “заражении” или блокируют его.

Недостатки:

иммунизация от определенного типа вируса;

сложность иммунизировать файлы от всех известных вирусов.

**5.2 Управление логическим доступом**

Дискреционное управление доступом (Discretionary Access Control; DAC), которое подразумевает следующее:

‑ 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).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной (рисунок 5.1).

|  |
| --- |
| image002  Рисунок 5.1 – Схематичное изображение матрицы доступа |

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы (О1…Оn) соответствует строка, а субъекту (С1…Сn) ‑ столбец. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как «доступ на чтение» (Read Only), «доступ на запись» (Write Only), «доступ на чтение-запись» (Read-Write) и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей дискреционного управления доступом. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата зависимое условие), часы (време-зависимое условие) в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия доступа к объектам обычно используются в системах управления базами данных. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение о доступе субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа (МД) ‑ наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД. Каждый из этих способов представления МД имеет свои достоинства и недостатки, обуславливающие область их применения. Поэтому в каждом конкретном случае надо знать, во-первых, какое именно представление использует средство защиты и, во-вторых, какие особенности и свойства имеет это представление.

Избирательное управление доступом является основой требований к классам C2 и C1 стандарта США «Критерий оценки безопасности компьютерных систем» (Trusted Computer Systems Evaluation Criteria, известна как «Оранжевая книга»).

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности (accountability), а также имеет приемлемую стоимость и небольшие накладные расходы.

Мандатное управление доступом (Mandatory Access Control; MAC), 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.

В случае, если совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру, и, таким образом, в системе можно реализовать иерархически не исходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула (Bell-LaPadulla model), включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: простым условием защиты (simple security condition) и \*-свойством (\*-property). В упрощенном виде они определяют, что информация может передаваться только «наверх», то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, ‑ если не выше (\*-свойство).

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Полномочное управление доступом составляет основу требований к классу B1 («Оранжевая книга»), где оно используется совместно с избирательным управлением.

Основное назначение полномочной политики безопасности ‑ регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая требованиям последней иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах МО США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами:

‑ отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

‑ высокой стоимостью реализации и большими накладными расходами.

**5.3 Основы построения криптосистем**

Для защиты информации в каналах связи используются два вида шифрования: линейное (канальное) и абонентское.

Линейное шифрование производится на выходе узла связи, расшифрование - на входе узла связи. При этом используются поточные шифры и между узлами поддерживается сплошной поток битов шифрованного текста. Шифруется и заголовок, и информационная часть пакетов. Все это затрудняет анализ потоков сообщений, так как адреса источника и получателя зашифрованы, непрерывность трафика обеспечивается передачей пустых (незначащих) сообщений. При линейном шифровании трафик уязвим только в узлах связи, так как там информация обрабатывается в открытом виде, поэтому узлы связи должны быть хорошо защищены.

При абонентском шифровании каждое сообщение шифруется в его источнике и расшифровывается только получателем, при этом используется ключ, известный только этой паре абонентов. Сообщение, зашифрованное абонентом, может еще подвергаться и линейному шифрованию. Таким образом, абонентское шифрование обеспечивает конфиденциальность передаваемого сообщения, линейное - конфиденциальность, защиту трафика от анализа.

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

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, имеет вид (рисунок 5.2).

|  |
| --- |
| Рисунок 5.2 – Обобщенная схема симметричной криптографической системы |

Отправитель генерирует открытый текст исходного сообщения , которое должно передаваться по открытому каналу. Отправитель шифрует текст с помощью обратимого преобразования  и ключа :  и получает шифротекст , который отправляет получателю. Получатель, приняв шифротекст , расшифровывает его с помощью обратного преобразования  и получает исходное сообщение в виде открытого текста :.

Преобразование  выбирается из семейства криптографических преобразований, называемых **криптоалгоритмами**. Параметр, с помощью которого выбирается конкретное преобразование, называется **криптографическим ключом** . Система, в которой осуществляется шифрование и расшифрование сообщений, называется **криптосистемой***.*

Формально криптосистема – это однопараметрическое семейство  обратимых преобразований  из пространства  сообщений открытого текста в пространство  шифрованных текстов. Параметр  (ключ) выбирается из конечного множества , называемого пространством ключей. Криптосистема может иметь разные варианты реализации: набор инструкций; аппаратные или программные средства; аппаратно-программные средства.

Вообще говоря, преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Поэтому различают два класса криптосистем: симметричные криптосистемы и асимметричные криптосистемы. Иногда их называют: одноключевые (с секретным ключом) и двухключевые (с открытым ключом). Схема симметричной криптосистемы с одним секретным ключом  была показана на рисунок 5.2. Обобщенная схема асимметричной криптосистемы с двумя разными ключами  и  показана на рисунок 5.3.

В этой криптосистеме один из ключей является открытым , а другой  – секретным. Для этой криптосистемы , а .

|  |
| --- |
| Рисунок 5.3. – Обобщенная схема асимметричной криптографической системы |

В симметричной криптосистеме секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей, например, спецсвязью. В асимметричной криптосистеме передают по незащищенному каналу только открытый ключ, а секретный ключ сохраняют в месте его генерации.

Злоумышленник при атаке на криптосистему может не только считывать шифротексты, передаваемые по каналу связи, но и пытаться их изменить по своему усмотрению.

Любая попытка со стороны злоумышленника расшифровать шифротекст  для получения открытого текста  или зашифровать свой собственный текст  для получения правдоподобного шифротекста , не имея подлинного ключа, называется криптоатакой.

Свойство криптосистемы, противостоять криптоатаке называется криптостойкостью. Оно измеряется в затратах злоумышленника, которые он несет, вскрывая криптосистему. Например, криптостойкость может выражаться в количестве машинного времени, затраченного на вскрытие криптосистемы.

Фундаментальное правило криптоанализа заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации.

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В таких системах для шифрования данных используется один ключ, а для расшифрования другой (отсюда и название - асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно. Для расшифровывания данных получатель шифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифровывания не может быть определен из ключа шифрования.

Обобщенная схема асимметричной криптосистемы с открытым ключом показана на рисунок 5.4.

В этой криптосистеме применяют два различных ключа: - открытый ключ отправителя А; - секретный ключ получателя В. Генератор ключа целесообразно располагать на стороне получателя В (чтобы не пересылать секретный ключ  по незащищенному каналу). Значения ключей ,  – зависят от начального состояния генератора ключей.

Раскрытие секретного ключа  по известному ключу  должно быть вычислительно неразрешимой задачей.

|  |
| --- |
| Рисунок 5.4 – Обобщенная схема асимметричной криптосистемы с открытым ключом |

Характерные особенности асимметричных криптосистем:

1. Открытый ключ  и криптограмма С могут быть отправлены по незащищенному каналу, т.е. могут быть известны противнику.
2. Алгоритмы шифрования  и расшифрования  являются открытыми.
3. Защита информации в асимметричной криптосистеме основана на секретности ключа .

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

1. Вычисление пары ключей  получателем В на основе начального условия должно быть простым.
2. Отправитель А, зная открытый ключ  и сообщение М, может легко вычислить криптограмму .
3. Получатель В, используя секретный ключ  и криптограмму С, может легко восстановить исходное сообщение .
4. Противник, зная открытый ключ , при попытке вычислить секретный ключ  наталкивается на непреодолимую вычислительную проблему.
5. Противник, зная пару , при попытке вычислить исходное сообщение М, наталкивается на непреодолимую вычислительную проблему.

**Последовательность действий абонентов криптосистемы RSA**

**Действия получателя криптограммы В:**

1. В генерирует два произвольных больших простых числа  и . Эти числа должны быть примерно одинаковыми, размерностью 100‑150 десятичных разрядов. Они должны быть секретными.
2. В вычисляет значение модуля  и функции Эйлера  и выбирает значение открытого ключа  с соблюдением условий: , , т.е.  и  должны быть взаимно простыми.
3. В вычисляет значение секретного ключа , используя расширенный алгоритм Евклида: .
4. В посылает А пару чисел  по открытому каналу.

**Действия отправителя криптограммы А:**

1. Разбивает исходный текст  на блоки , , т.е. . Величина .
2. Шифрует каждое число  по формуле  и отправляет криптограмму .

Получатель В, получив криптограмму, расшифровывает каждый блок секретным ключом , , и восстанавливает весь текст .

**Реализуемость и безопасность RSA**

Покажем, что при расшифровании восстанавливается исходный текст. Согласно обобщению Эйлером малой теоремы Ферма: если , то , или . Открытый  и закрытый  ключи в алгоритме связаны соотношением , или  для некоторого целого . Таким образом, процесс шифрования, а затем расшифрования некоторого сообщения  выглядит следующим образом:

.

В процессе применения RSA злоумышленник может иметь: , ,  – и организовать дешифрование двумя способами:

1. По , ,  получить . Для этого он решает задачу вычисления  из уравнения . Эта задача вычислительно трудна.
2. По  вычислить , , затем найти  и вычислить  и дешифровать сообщение .

Однако задача разложения большого числа на простые множители вычислительно сложна.

Пользователи А и В должны быстро осуществлять все вычисления: вычислять , шифровать и расшифровывать.

Вычисление  с использованием алгоритма Евклида ‑ довольно быстрый процесс и не представляет трудности. Шифрование и расшифрование ‑ возведение большого числа в большую степень ‑ требует определенных затрат времени, но, с учетом наличия быстрых алгоритмов и быстродействия современных компьютеров, это приемлемая процедура.

При обмене сообщениями через сети телекоммуникаций 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.

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к кото­рым относятся:

* активный перехват - нарушитель, подключившийся к сети, пе­рехватывает документы (файлы) и изменяет их;
* маскарад - абонент С посылает документ абоненту В от имени абонента А;
* ренегатство - абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал;
* подмена - абонент В изменяет или формирует новый доку­мент и заявляет, что получил его от абонента А;
* повтор - абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.

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  подписываемого документа . Вычисленное значение хэш-функции  представляет собой один короткий блок информации , характеризующий весь документ  в целом. Затем число  «шифруется» секретным ключом отправителя. По­лучаемая при этом пара чисел представляет собой ЭЦП для дан­ного документа . 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».

При проверке ЭЦП получатель сообщения снова вычис­ляет хэш-функцию  принятого по каналу документа , по­сле чего при помощи открытого ключа отправителя проверяет, со­ответствует ли полученная подпись вычисленному значению  хэш-функции.

Принципиальным моментом в системе ЭЦП является не­возможность подделки ЭЦП пользователя без знания его секрет­ного ключа подписывания.

В качестве подписываемого документа может быть ис­пользован любой файл. Подписанный файл создается из непод­писанного путем добавления в него одной или более электронных подписей. Каждая подпись содержит следующую информацию:

* дату подписи;
* срок окончания действия ключа данной подписи;
* информацию о лице, подписавшем файл (Ф.И.0., должность, краткое наименование фирмы);
* идентификатор подписавшего (имя открытого ключа);
* собственно цифровую подпись.

**5.4 Обеспечение безопасности в системах электронной коммерции**

Электронная коммерция предполагает взаимодействие между партнерами посредством информационных технологий, что существенно повышает гибкость, эффективность и масштабность бизнес-процессов.

**Информационная технология** – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

В системах электронной коммерции проведение транзакций обеспечивается посредством автоматизированных банковских систем реализующих механизм контроля доступа клиентов банка к их счетам, причем такой доступ выполняется владельцем удаленно, т.е. без физического присутствия в офисе банка, что требует соответствующих процедур обеспечения безопасности.

Таким образом, для реализации удаленного доступа необходимо выполнить последовательно следующие процедуры:

1. **Идентификация** - процесс присвоения уникального признака субъекту, по которому он в последствии будет опознан автоматизированной системой;

2. **Аутентификация** - проверка подлинности идентификатора субъекта;

3. **Авторизация** - предоставление субъекту прав доступа к объекту.

Указанные процедуры поддерживаются в автоматизированных системах **ядром безопасности** - элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Таким образом, **идентификатор** – это определенный вид информации, предоставляемый субъектом системе при его аутентификации. Такой информацией являются:

1. Пароль - отличительная характеристика субъекта представляющая собой секретную информацию, которая неизвестна непосвященным людям.

2. Устройство аутентификации - некоторый уникальный предмет, находящийся у субъекта и являющийся его отличительной характеристикой (например, смарт-карты, OTP-токены и т.д.).

3. Биометрия - измеримая физиологическая или поведенческая черта живого человека.

В настоящее время широко распространены в системах электронной коммерции парольная аутентификация (информация вводима с клавиатуры) и устройства аутентификации (банковские платежные карты).

Для аутентификации участников систем электронной коммерции может использоваться протокол Kerberos, который предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты – пользователи, а также клиентские и серверные программные средства. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило – клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую часть данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент – именно тот, за кого себя выдает. При этом секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) – они только использовались для шифрования (рисунок 5.5).

|  |
| --- |
| 10-1  Рисунок 5.5 – Схема проверки сервером S подлинности клиента C |

Взаимодействие участников системы электронной коммерции включает в себя не только операции, связанные с куплей-продажей товаров и услуг, но и операции, направленные на поддержку извлечения прибыли, - создание спроса на товары и услуги, поддержку клиентов после продажи и т.п. (рисунок 5.6.).

|  |
| --- |
| Рис 2  Рисунок 5.6 – Схема взаимодействия участников системы электронной коммерции |

Платежные средства способствуют обмену товаров и услуг и отвечают специфическим требованиям. Каждое средство имеет свою социальную и технологическую историю, определяющую их использование в специфических областях. На сегодняшний день банки предлагают большое количество платежных средств, связанных с автоматической обработкой транзакций и постепенной дематериализацией денег, отличающихся по способу применения в разных странах.

Можно выделить следующие виды платежных средств:

‑ наличные (в форме металлических монет или бумажных банкнот);

‑ кредитные переводы;

‑ прямое дебетование;

‑ межбанковские переводы;

‑ платежные карты (кредитные или дебетовые).

Развивающиеся виды платежных средств основаны на дематериализованных деньгах, хранящихся в смарт-картах, электронных или виртуальных кошельках.

Для обеспечения безопасности транзакций в сети Интернет используются различные протоколы, наиболее известными из которых являются SSL и SET.

Самый известный протокол Интернета ‑ SSL (Secure Socket Layer). Этот протокол был разработан компанией Netscape и является составной частью всех известных Интернет-браузеров и Web-серверов (сегодня используется версия 3.0 протокола SSL). Протокол реализуется между транспортным и сеансовым уровнями эталонной модели взаимодействия открытых систем (OSI). Это, с одной стороны, означает возможность использования протокола для организации защищенной сессии между программами, работающими по различным протоколам прикладного уровня OSI (FTP, SMTP, Telnet, HTTP и т.п.), а с другой ‑ закрытие любых данных, передаваемых в SSL-сессии, что приводит к снижению производительности протокола.

Последняя версия протокола SSL поддерживает режимы аутентификации:

‑ взаимную аутентификацию сторон;

‑ одностороннюю аутентификацию сервера (без аутентификации клиента).

Как следует из описания протокола SSL, асимметричные алгоритмы шифрования используются только на этапе установления защищенной сессии. Для защиты информационного обмена от несанкционированного доступа используются только симметричные алгоритмы. Это делается в первую очередь для того, чтобы повысить производительность протокола SSL.

Достоинства протокола:

1. Широкое распространение протокола SSL, которое объясняется в первую очередь тем, что он является составной частью всех известных Интернет-браузеров и Web-серверов. Это означает, что фактически любой владелец карты, пользуясь стандартными средствами доступа к Интернету, получает возможность провести транзакцию с использованием SSL;

2. Простота протокола для понимания всех участников ЭК;

3. Хорошие операционные показатели (скорость реализации транзакции). Последнее достоинство связано с тем, что протокол в процессе передачи данных использует только симметричные протоколы шифрования.

Недостатками протокола SSL в приложении к ЭК являются:

1. Отсутствие аутентификации клиента Интернет-магазином, поскольку сертификаты клиента в протоколе почти не используются. Использование «классических» сертификатов клиентами в схемах SSL является делом практически бесполезным. Такой «классический» сертификат, полученный клиентом в одном из известных центров сертификации, содержит только имя клиента и, что крайне редко, его сетевой адрес.

2. Протокол SSL не позволяет аутентифицировать клиента обслуживающим банком.

3. При использовании протокола SSL торговое предприятие (ТП) аутентифицируется только по своему адресу в Интернете (URL). Это значит, что клиент, совершающий транзакцию ЭК, не аутентифицирует ТП в полном смысле. Аутентификация ТП только по URL облегчает мошенническим ТП доступ к различным системам ЭК. В частности, торговые предприятия, занимающиеся сбором информации о картах клиентов, могут получить сертификат в каком-либо известном центре сертификации общего пользования на основании только своих учредительных документов.

4. Протокол SSL не поддерживает цифровой подписи, что затрудняет процесс разрешения конфликтных ситуаций, возникающих в работе платежной системы (цифровая подпись используется в начале установления SSL-сессии при аутентификации участников сессии). Для доказательства проведения транзакции требуется либо хранить в электронном виде весь диалог клиента и ТП (включая процесс установления сессии), что дорого с точки зрения затрат ресурсов памяти и на практике не используется, либо хранить бумажные копии, подтверждающие получение клиентом товара.

5. При использовании SSL не обеспечивается конфиденциальность данных о реквизитах карты для ТП.

Для операций с кредитными карточками используется протокол SET (Secure Electronic Transactions), разработанный совместно компаниями Visa, MasterCard, Netscape и Microsoft.

В отличие от SSL протокол SET узко специализирован. Целью SET является обеспечение необходимого уровня безопасности для платежного механизма, в котором участвует три или более субъектов. При этом предполагается, что транзакция реализуется через Интернет.

На базовом уровне SET осуществляет следующие функции:

**Аутентификация.** Все участники кредитных операций идентифицируются с помощью электронных подписей. Это касается клиента-покупателя, продавца, банка, выдавшего кредитную карточку, и банка-продавца.

**Конфиденциальность.**Все операции производятся в зашифрованном  
виде.

***Целостность сообщений.*** Информация не может быть подвергнута модификации по дороге, в противном случае это будет сразу известно.

**Совместимость.**Должна быть предусмотрена совместимость с любыми программными продуктами и с любыми сервис-провайдерами.

**Независимость от транспортного протокола.** Безопасность операций не должна зависеть от уровня безопасности транспортного протокола. Такие гарантии особенно важны, так как протокол SET ориентирован для работы в Интернет.

**5.5 Противодействие атакам**

Атака на автоматизированную систему (АС) - действие или последовательность действий нарушителя, которые приводят к реализации угроз, путем использования уязвимостей этой АС.

Уязвимости АС:

‑ недостатки аппаратно-программных средств по вине разработчика

‑ добавленные администратором при настройке АС

‑ уязвимости внесенные пользователем

Цель атаки – нарушение одной из функций системы:

‑ конфиденциальности;

‑ целостности;

‑ доступности.

Атака может быть активной (результат - изменение данных) или пассивной (результат — раскрытие данных). При этом факт атаки необязательно означает, что она достигла цели. Степень успешности атаки зависит от уязвимости системы и эффективности контрмер.

Этапы атаки:

1. Сбор информации.

Изучение окружения. Провайдер целевой системы, адреса доверенных узлов, трафик, режим работы организации, телефонные номера и т.д.

Идентификация топологии сети. Количество компьютеров, способ их соединения, организация выхода в глобальную сеть.

Идентификация узлов сети. Разведка IP-адреса узла, его доступности.

Идентификация сервисов и портов. Определяется наличие установленных сервисов (Telnet, FTP, Web- сервера и т.д.) наличие доступа к ним, открытость портов.

Идентификация операционной системы. Тип операционной системы.

Определение уязвимостей узла. На основе ранее собранной информации.

2. Реализация атаки.

‑ проникновение в систему;

‑ контроль над системой.

3. Завершение атаки.

Устранение следов атаки с целью невозможности идентификации атакующего.

‑ маскирование внедренной программы;

‑ изменение контрольных сумм файлов;

‑ очистка журнала регистрации событий.

Общая классификация атак:

‑ регулярные (проводятся на любую систему вне зависимости от состава ее аппаратно-программных средств);

‑ использующие ошибки политики безопасности или администрирования;

‑ использующие ошибки программно-технических средств системы (“баги”).

Противодействие атакам — комплекс организационно-технических мероприятий, направленных на обнаружение, анализ и реагирование на инциденты безопасности, атаки или несанкционированный доступ.

Организационно-правовая составляющая:

- документированная политика безопасности;

- положения о распознавании и противодействии атакам;

- наличие компетентных специалистов.

Реализация положений политики безопасности, в части распознавания и противодействия атакам

Содержание политики безопасности:

- зона ответственности;

- правила использования информационных ресурсов;

- план мероприятий проводимых в случае распознавания атаки;

- ответственность персонала.

Техническая составляющая

Штатные средства - сетевые журналы сетевых устройств, операционных систем и приложений;

Специализированные средства - средства распознавания и противодействия атакам.

Системы обнаружения вторжений (IDS)

Функции:

Обнаружение - идентификация атаки или подозрительной активности в отношении ресурсов сети или хостов и уведомление наблюдающей станции;

Реагирование - блокирование или смягчение происходящего события и профилактика системы от последующих атак;

Предотвращение - остановка обнаруженной атаки частично или в некоторых случаях полностью.

IDS уровня узла (HIDS) - контролирующие отдельный узел (рисунок 5.7);

Сетевые IDS (NIDS) - контролирующие сегмент ЛВС (рисунок 5.7);

IDS уровня рабочей станции - контролирующие отдельную рабочую станцию;

“Системы-ловушки” (honeypots) - эмулирующие отдельный узел или целый сегмент сети, выглядящие заведомо уязвимыми и привлекательными для потенциальной атаки;

Сканеры уязвимостей (vulnerability scanner) - сетевые или уровня узла.

Для противодействия несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рисунок 5.8). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно экран входит в состав защищаемой сети.

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то брандмауэр должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP.

|  |
| --- |
| Рисунок 5.7 – Схема размещения датчиков IDS |

|  |
| --- |
| image002  Рисунок 5.8 – Схема размещения межсетевого экрана |

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко.

**Виртуальная частная сеть** (VPN - Virtual Private Network) - объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных (рисунок 5.9).

Мероприятия по обеспечению информационной безопасности:

1. Аутентификация взаимодействующих сторон.

2. Криптографическая защита передаваемых данных.

3. Проверка подлинности и целостности передаваемой информации.

|  |
| --- |
| image001  Рисунок 5.9 – Схема реализации виртуальной частной сети |

Устройства VPN:

1. VPN – клиент - программный или программно-аппаратный комплекс на базе ПК;

2. VPN – сервер - программный или программно-аппаратный комплекс на базе серверного оборудования.

3. Шлюз безопасности - сетевое устройство, подключаемое к двум сетям.

Особенности передачи данных в VPN:

1. Криптозащита всего пакета.

2. Инкапсулирование.

3. Туннелирование.

**РАЗДЕЛ 6 ОСНОВЫ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ**

**6.1 Авторское право и смежные права**

Известно несколько определений интеллектуальной собственности. В ст. 2 (VIII) Конвенции, учреждающей Всемирную организацию интеллектуальной собственности, принятой в 1967 году, это понятие определяется следующим образом: «... "Интеллектуальная собственность" включает права, относящиеся к:

* литературным, художественным и научным произведениям;
* исполнительской деятельности артистов, звукозаписи, радио- и телевизионным передачам;
* изобретениям во всех областях человеческой деятельности;
* научным открытиям;
* промышленным образцам;
* товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям;
* защите против недобросовестной конкуренции, а также все другие права, относящиеся к интеллектуальной деятельности в производственной, научной, литературной и художественной областях».

Общие положения относятся равным образом и к авторским, и к смежным правам. Они регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), постановок, исполнений, фонограмм, передач организаций эфирного и кабельного вещания (смежные права).

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

Источниками регулирования авторского права являются как законы РБ, так и международные договоры. Если последними установлены иные правила, чем те, которые содержатся в Законе, то применяются правила международного договора.

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме.

1. Произведения

* литературные (включая компьютерные программы и базы данных);
* научные (статьи, монографии, отчеты);
* драматические и музыкально-драматические, сценарные;
* хореографические и пантомимы;
* музыкальные с текстом или без текста;
* аудиовизуальные;
* живописи, графики, скульптуры и другие изобразительного искусства;
* декоративно-прикладного искусства;
* архитектуры, градостроительства и садово-паркового искусства;
* фотографические;
* карты, планы, эскизы и иные, относящиеся к архитектуре, географии,
* топографии, другим наукам и технике;
* другие произведения.

2. Производные произведения

* переводы, обработки, инсценировки, музыкальные аранжировки, обзоры,
* аннотации, рефераты;
* сборники произведений: энциклопедии, антологии, атласы
* и другие составные произведения как результат творческого труда.

3. Компьютерные программы (все виды программ)

* прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код.
* базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества.

Авторские права распространяются на:

* произведения, обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) на территории РБ, независимо от гражданства авторов и их правопреемников;
* произведения авторов-граждан РБ (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ;
* произведения авторов-граждан других государств (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ - в соответствии с международными договорами РБ.

Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

Передача права собственности на материальный объект или право владения материальным объектом само по себе не влечет передачи каких-либо авторских прав на произведение, выраженное в этом объекте.

Авторские права делятся на личные неимущественные (моральные права - droit moral) и имущественные (экономические) права.

Личные неимущественные права:

* признаваться автором произведения (право авторства);
* использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);
* обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
* право на защиту произведения, включая его название, от всякого рода искажений или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

Принадлежат автору независимо от его имущественных прав и сохраняются за ним даже после уступки исключительных прав на использование произведения.

Имущественные права: исключительное 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 компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;
* 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.

Автор принятого архитектурного проекта вправе требовать от заказчика предоставления права на участие в реализации своего проекта при разработке документации для строительства и при строительстве здания или сооружения.

Автор имеет право на авторское вознаграждение за каждый вид использования произведения.

Три категории произведений, не охраняемых авторским правом:

* официальные документы (законы, судебные решения, иные тексты законодательного, административного и судебного характера), а также их официальные переводы;
* государственные символы и знаки (флаги, гербы, ордена, денежные знаки и иные государственные символы и знаки);
* произведения народного творчества; сообщения о событиях и фактах, имеющие информационный характер.

Авторское право на произведение науки, литературы и искусства возникает в силу факта его создания и не требует регистрации произведения, иного специального оформления произведения или соблюдения каких-либо формальностей.

Презумпция авторства заключается в том, что при отсутствии доказательства иного, автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения.

Соавторство:

* созданное в соавторстве произведение, принадлежит соавторам совместно независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение. Каждый из соавторов вправе использовать созданную им часть произведения, имеющую самостоятельное значение, по своему усмотрению, если иное не предусмотрено соглашением между ними. Однако, если произведение образует одно неразрывное целое, то ни один из соавторов не вправе без достаточных к тому оснований запретить использование произведения.
* положения об авторском праве на составные, аудиовизуальные и служебные произведения.

Авторское право на составные произведения.

Автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и расположение материалов как результат творческого труда (составительство).

Составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное.

Авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором.

Авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений.

2. Лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания.

Авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

Авторское право на производные произведения.

1. Переводчикам и авторам других производных произведений принадлежит авторское право на осуществленные ими перевод, инсценировку, аранжировку или другую переработку при условии соблюдения ими прав автора произведения.

2. Авторское право переводчика и авторов других производных произведений не препятствует иным лицам осуществлять свои переводы и переработки тех же произведений.

Авторское право на аудиовизуальные произведения

1. Авторами аудиовизуального произведения являются режиссер-постановщик, автор сценария, автор специально созданного для аудиовизуального произведения музыкального произведения с текстом или без текста.

2. Заключение договора на создание аудиовизуального произведения влечет за собой передачу авторами этого произведения производителю исключительных прав на воспроизведение, распространение, публичное исполнение, сообщение для всеобщего сведения, а также субтитрирование и дублирование текста, если иное не предусмотрено договором. Указанные права действуют в течение срока действия авторского права на аудиовизуальное произведение.

Производитель аудиовизуального произведения вправе при любом использовании этого произведения указывать свое имя или наименование либо требовать такого указания.

3. Автор музыкального произведения с текстом или без текста сохраняет право на вознаграждение за публичное исполнение его музыкального произведения при использовании аудиовизуального произведения, включающего данное музыкальное произведение.

4. Авторы ранее существовавших произведений, включенных в аудиовизуальное произведение или переработанных для него, сохраняют авторское право на свои произведения и могут использовать их отдельно от аудиовизуального произведения.

Ограничения имущественных прав.

1. Воспроизведение произведения в личных целях

- исключительно физическим лицом в единичных экземплярах

2. Не распространяется на воспроизведение:

- произведений архитектуры в форме зданий или других сооружений; баз данных или существенных частей из них;

- компьютерных программ, нотных текстов и книг (полностью) посредством репродуцирования.

3. Использование произведения без согласия автора и без выплаты авторского вознаграждения с обязательным указанием автора произведения и источника заимствования:

- цитирование в научных, исследовательских, учебных, полемических, критических и информационных целях отрывков, использование их в качестве иллюстраций в изданиях, радио- и телепередачах, звуко- и видеозаписях учебного характера, воспроизведение в газетах и т.п.

4. Репродуцирование произведений библиотеками, архивами и образовательными учреждениями с обязательным указанием автора произведения и источника заимствования в единичном экземпляре без извлечения прибыли .

5. Воспроизведение компьютерных программ только для архивных целей или для замены правомерно приобретенного экземпляра, для обеспечения совместной работы с другими программами без использования для создания других компьютерных программ, аналогичных адаптируемой.

Срок действия авторского права

1. Срок охраны авторского права.

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

2. Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние и могут свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения..

3. Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора без ограничения срока.

Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом РБ при отсутствии наследников.

Служебные объекты авторского права.

В отношении служебных произведений российское законодательство отказалось от традиционного для советского авторского права подхода, который заключался в установлении предельного срока на использование служебного произведения работодателем в три года. Эта норма зачастую трактовалась как социальная гарантия прав авторов, но на самом деле она совершенно не учитывала существующее многообразие служебных произведений и прежде всего произведений, создание которых требует объединения значительного числа авторов и серьезных капитальных затрат (программы для ЭВМ, аудиовизуальные произведения, периодические издания и многие другие).

Авторское право на служебные произведения.

Личные неимущественные права на произведение, созданное в порядке выполнения служебного задания или служебных обязанностей (служебное произведение), принадлежат автору.

Исключительные права на использование служебного произведения принадлежат лицу, с которым автор состоит в трудовых отношениях (работодателю), если в договоре между ними не предусмотрено иное.

Автор служебного произведения не вправе препятствовать его обнародованию нанимателем.

Сформулировано положение, призванное согласовать интересы авторов и работодателей. Прежде всего, подтвержден принцип принадлежности автору авторского права на произведение, созданное в порядке выполнения служебных обязанностей или служебного задания работодателя. Вместе с тем введена презумпция принадлежности работодателю исключительных прав на использование служебного произведения, если в договоре между ним и автором не предусмотрено иное. Одновременно сняты все ограничения на выплату вознаграждения автору за использование служебного произведения и подчеркнуто, что размер авторского вознаграждения за каждый вид использования служебного произведения и порядок его выплаты устанавливаются договором между автором и работодателем, а также в договорах, заключаемых организациями, управляющими правами авторов на коллективной основе, с пользователями.

Субъекты авторского права и смежных прав.

Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской самодеятельности и т.д. защищаются авторским правом.

Но недееспособные, став субъектами авторского права, не имеют права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

За авторами - гражданами РБ и их правопреемниками авторское право признается на все произведения независимо от места их обнародования или нахождения в какой-либо объективной форме.

Если произведение обнародовано либо не обнародовано, но существует на территории РБ в какой-либо объективной форме, то авторское право распространяется на такое произведение независимо от гражданства автора.

За гражданами других государств, обнародовавшими свои произведения за пределами РБ, авторское право признается в соответствии с международными договорами РБ.

Лицо, обозначенное в качестве автора на оригинале или экземпляре произведения, считается его автором, если отсутствует доказательство иного.

При обнародовании произведения анонимно или под псевдонимом (за исключением случаев, когда псевдоним автора не вызывает сомнения в его личности), издатель имя или наименование которого обозначено на произведении, при отсутствии доказательств иного, считается представителем автора и имеет право защищать права автора и обеспечивать их осуществление.. Это положение действует до тех пор, пока автор не раскроет свою личность и не заявит о своем авторстве.

Авторское право может принадлежать нескольким лицам - соавторам. Авторское право на произведение, созданное совместным творческим трудом двух или более лиц, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение.

Соавторство всегда является результатом соглашения о совместной работе. По крайней мере, между соавторами должно быть хотя бы устное или подразумеваемое соглашение о создании коллективного произведения.

Недействительным является соавторство, навязанное автору лицам, от которого так или иначе зависит использование произведения.

Оказание автору технической помощи соавтора не порождает. При соавторстве должно быть творческое участие лиц в создании произведения.

В юридической литературе выделяют два вида соавторства: нераздельное и раздельное.

Нераздельное соавторство возникает в отношении произведения, составляющего одно неразрывное целое. При нераздельном соавторстве выделить долю каждого автора в произведении невозможно, поэтому все соавторы пользуются неделимым авторским правом на всё произведение в целом и на каждую его часть.

Раздельное соавторство возникает на одно произведение, каждая часть которого выполнена самостоятельным автором, и долю каждого из них можно легко установить (соавторство композитора и либреттиста, соавторство на учебник группы авторов и т.д.). В этом случае наряду с совместным и неделимым правом всех соавторов на произведение в целом каждый из авторов сохраняет свое право на созданную им часть произведения, имеющую самостоятельное значение. Например, можно требовать указания своего авторства в отношении этой части и самостоятельно распоряжаться ее использованием, поскольку такое осуществление возможно отдельно от других частей, если иное не предусмотрено соглашением между соавторами.

Отношения между соавторами могут быть определены их соглашением. При отсутствии такого соглашения авторское право на коллективное произведение осуществляется всеми соавторами совместно. Споры между соавторами разрешаются судом.

Субъектами авторского права после смерти автора становятся наследники. Наследование авторских прав может происходить как по закону, так и по завещанию. Особенности наследования авторских прав следующие.

Прежде всего, по наследству к наследникам переходят не все авторские права, а только их часть. В законе указывается, что по наследству не переходят право авторства, право на авторское имя и право на защиту репутации автора.

Однако и в отношении этих прав к наследникам переходят права на защиту названных прав от нарушений со стороны третьих лиц, если только автор не назначил для этих целей специальное лицо.

В отличие от прав на произведения самих авторов, которые носят пожизненный характер, авторские права наследников ограничены установленным законом сроком. Авторские права наследников действуют в течение 50 лет после смерти автора, считая с 1 января года, следующего за годом смерти.

Из этого общего правила есть ряд исключений: а) если произведение создано в соавторстве, то 50-летний срок исчисляется после смерти последнего из соавторов; б) если произведение впервые выпущено в свет после смерти автора, то авторское право действует в течение 50 лет после выпуска его в свет; в) если автор был репрессирован и реабилитирован посмертно, то произведение охраняется 50 лет после реабилитации; г) если автор воевал или работал во время Великой Отечественной войны, то срок охраны увеличивается на четыре года и т.д.

Важной особенностью наследования авторских прав является то, что авторские права переходят к наследнику в бездолевом порядке, как единое целое, не подлежащее ни выделу, ни разделу. Это означает, что распоряжаться перешедшими по наследству авторскими правами наследники должны совместно и по взаимному согласию, а в случае спора - по решению суда.

Помимо наследников авторские права могут переходить к иным правопреемникам. В их роли выступают издательства, театры киностудии и другие организации, занимающиеся использованием произведений. Они приобретают авторские права на основании заключенных с авторами и наследниками авторских договоров.

Становясь обладателями авторских прав, эти организации используют произведения и распоряжаются ими такими способами, которые предусмотрены конкретными авторскими договорами, и в установленных ими пределах.

1. Субъекты смежных прав:

- исполнители, производители фонограмм, организации эфирного или кабельного вещания

2. Сфера действия смежных прав:

- исполнители – граждане и не граждане РБ, исполнения которых:

имеют место на территории РБ, или включены в фонограммы,, или не записаны на стенограмму, но содержатся в передачах организаций эфирного или кабельного вещания, охраняемые в соответствии с Законом.

3. Права исполнителя: на имя; на защиту репутации; на использование исполнения в любой форме, включая право на получение вознаграждения за каждый вид использования исполнения.

Исключительное право на использование:

- передавать в эфир или сообщать для всеобщего сведения по кабелю исполнение; записывать ранее не записанное исполнение; воспроизводить запись исполнения; передавать в эфир или по кабелю запись исполнения; распространять оригинал или экземпляры исполнения, записанного на фонограмму; сдавать в прокат оригинал или экземпляры записанного на фонограмму исполнения; сообщать для всеобщего сведения исполнение, записанное на фонограмму, по проводам или средствами беспроволочной связи.

4. Права производителя фонограммы: на использование ее в любой форме, включая право на получение вознаграждения за каждый вид использования фонограммы: воспроизводство; переработку; распространение; импортирование; сдача в прокат; доведение до всеобщего сведения.

5. Использование фонограммы, опубликованной в коммерческих целях:

* публичное исполнение фонограммы;
* передача фонограммы в эфир;
* иное сообщение фонограммы для всеобщего сведения.

6. Права организаций эфирного вещания.

7. Права организаций кабельного вещания.

8. Ограничения прав исполнителей, производителей фонограмм, организаций эфирного или кабельного вещания.

Допускается воспроизведение фонограмм: для включения в обзор о текущих событиях отрывков из исполнения, фонограммы, передачи организации эфирного или кабельного вещания; исключительно в целях обучения или научного исследования; для цитирования в форме отрывков из исполнения.

9. Защита авторского права и смежных прав в установленном порядке в судебных и других органах в соответствии с их компетенцией.

10. Способы обеспечения исков по делам о нарушении авторского права и смежных прав через суд: определение о запрещении, о наложении ареста и изъятии.

11. Коллективное управление имущественными правами обладателей авторского права и смежных прав в случаях, когда их трудно практически осуществить в индивидуальном порядке, могут осуществлять организации, порядок создания и деятельности которых определяется законодательством РБ.

Передача имущественных прав. Авторский договор.

Имущественные права автора могут быть уступлены полностью или в части и могут быть переданы по письменному договору, подписанному автором и лицом (правообладателем), которому уступаются имущественные права для использования по авторскому договору.

В первом случае авторский договор разрешает использование произведения определенным способом и в установленных договором пределах только лицу, которому эти права передаются, и дает такому лицу право запрещать подобное использование произведения другим лицам.

Во втором случае пользователю разрешается использование произведения наравне с обладателем исключительных прав, передавшим такие права, и с другими лицами, получившими разрешение на использование этого произведения таким же способом. Права, передаваемые по авторскому договору, считаются неисключительными, если в договоре прямо не предусмотрено иное.

Наиболее распространенные виды авторского договора:

- изобретательский,

- постановочный,

- сценарный,

- художественного заказа,

- об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства.

Принципы и условия возникновения, реализации и защиты авторских и смежных прав

В качестве основных задач авторского права чаще всего в юридической литературе называются две следующие задачи. С одной стороны, авторское право должно стимулировать деятельность по созданию произведений науки, литературы и искусства. В этих целях авторское право способствует созданию условий для занятия творческим трудом; обеспечивает правовое признание и охрану достигнутых творческих результатов, закрепление за авторами прав на использование создание ими произведений и получение доходов и т.д. С другой стороны, задачей авторского права считается создание условий для широкого использования произведений в интересах общества. Иными словами, повышение уровня охраны прав авторов ни в коем случае не должно препятствовать использованию их произведений в целях образования и просвещения или служить помехой в стремлении самой широкой аудитории читателей, зрителей, слушателей знакомиться с ними.

Указанные задачи авторского права тесным образом связаны с его принципами. Принципы авторского права - это его основные начала, отправные идеи, которые обладают универсальностью, высшей императивностью и общезначимостью. Они пронизывают содержание всей системы авторского права, предопределяют всю юрисдикционную деятельность и воплощаются в субъективных правах и обязанностях участников авторских правоотношений. Не будучи закрепленными в конкретных статьях закона, принципы авторского права выводятся из анализа всей совокупности авторско-правовых норм. Знание принципов позволяет ориентироваться в обширном авторском законодательстве, правильно толковать и применять на практике отдельные его нормы, а также решать вопросы, на которые нет прямого ответа в действующем законодательстве.

К числу основных принципов авторского права, отраженных в содержании его норм на современном этапе развития, относятся следующие.

Во-первых, принципом авторского права может и должен считаться принцип свободы творчества. Данный принцип, лишь недавно наполненный реальным содержанием, пронизывает собой все авторское законодательство и конкретизируется в целом ряде его норм.

Обеспечивая свободу творчества, авторское право охраняет все произведения науки, литературы и искусства независимо от их назначения, достоинств и способа выражения. В этих же целях закон не ограничивает круг охраняемых произведений каким-либо перечнем и охраняет любые результаты творческой деятельности, существующие в объективной форме. Творцы произведений свободны в выборе темы, сюжета, жанра и формы воплощения создаваемых ими художественных образов, а также самостоятельно решают вопросы о выпуске своего произведения в свет, приданию произведению окончательной формы и т.п.

Во-вторых, принципом авторского права является сочетание личных интересов автора с интересами общества. Хотя данный принцип, безусловно, проявляется и в других институтах права интеллектуальной собственности и гражданского права в целом, в авторском праве он имеет особое значение. В основе авторского права лежит признанное за автором монопольное право на использование созданного им произведения. Определение разумных границ этой монополии на протяжении веков являлось одной из главных проблем авторского права. В настоящее время уже никто не утверждает, что авторы должны иметь неограниченный контроль за использованием своих произведений. Ничем не ограниченная монополия необходима и возможна лишь в отношении необнародованных произведений. Если же произведение с согласия автора стало доступно для всеобщего сведения, его права на произведение не могут быть столь обширными, чтобы полностью игнорировать интересы других граждан и общества в целом. Законы демократического общества не только гарантируют охрану интеллектуальной собственности, но и закрепляют право членов общества на участи в культурной жизни и пользование достижениями культуры.

В-третьих, в качестве одного из принципов российского авторского права может быть выдвинуто положение о неотчуждаемости личных неимущественных прав автора. В этом состоит одно из существенных отличий российского авторского права от авторского права ряда зарубежных стран. По российскому авторскому законодательству, личные неимущественные права автора (право на авторство, право на имя и пр.) не могут перейти к другим лицам, хотя бы сам автор и выразил на это свое согласие. Подобное соглашение не будет иметь юридической силы и является недействительным. Поэтому даже в тех случаях, когда произведение создано в порядке выполнения служебного задания, личные неимущественные права сохраняются за автором и должны быть во всех случаях обеспечены. Этими же соображениями продиктованы нормы законодательства, устанавливающие, что право авторства, право на авторское имя, право на защиту репутации автора не переходят по наследству, что в случаях так называемого «свободного» использования произведений обязательно указание имени автора и т.д. Что же касается имущественных прав авторов, то они могут передаваться другим лицам по авторскому договору, в порядке наследования, а также в силу закона (служебные произведения).

В-четвертых, для современного авторского права характерен принцип свободы авторского договора. Данный принцип заменил собой присущий ранее действующему авторскому праву принцип нормативной регламентации основных прав и обязанностей сторон по авторским договорам. Наиболее ярким выражением последнего было существование так называемых типовых авторских договоров (издательских, сценарных, постановочных и др.), которые имели нормативное значение и подробно регламентировали отношения авторов и пользователей произведений. Конечно, было бы неверно сводить роль типовых договоров лишь к ограничению свободы сторон в распоряжении принадлежащими им правами. Одной из главных функций типовых договоров было ограждение авторов от произвола пользователей произведений, стремление гарантировать авторам определенный минимальный уровень прав. Условия конкретных авторских договоров, ухудшающие положение авторов по сравнению с типовым договором, признавались недействительными и заменялись условиями, закрепленными в типовом договоре.

Вместе с тем присутствие в законодательстве правил, детально регулирующих сферу отношений, которая в принципе должна определяться прежде всего свободным волеизъявлением самих сторон, трудно признать нормальным явлением. В этой связи новое российское и белорусское авторские законодательства отказались от жесткой регламентации отношений сторон авторского договора. В нем закрепляются лишь возможные типы авторских договоров, а также указываются условия, которые должны быть в обязательном порядке согласованы сторонами. Что касается законных интересов авторов, то они обеспечиваются, с одной стороны, запретом включать в авторские договоры явно кабальные для авторов условия, например, условие о передаче прав на произведения, которые автор может создать в будущем, и, с другой стороны, правилами, предоставляющими авторам определенные права, например, на расторжение авторского договора по истечении пяти лет с даты его заключения, если конкретный срок договора сроками не определен, или налагающими на пользователей произведений определенные обязанности, например, по выплате автору аванса по договору заказа. Кроме этих и других указанных в законе ограничений, стороны свободны в определении содержания авторского договора.

Возникновение авторского права.

1. На произведения науки, литературы и искусства в силу факта их создания без соблюдения каких-либо формальностей.

2. Исключительные имущественные права подтверждаются знаком охраны авторского права, которым помещается каждый экземпляр произведения и обязательно состоит из трех элементов:

* латинской буквы "С" в окружности;
* имени (наименования) обладателя исключительных имущественных прав;
* года первого опубликования произведения.

3. При отсутствии доказательств иного автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения (презумпция обладателя авторского права).

4. При опубликовании произведения анонимно или под псевдонимом (за исключением случая, когда псевдоним автора не оставляет сомнения в его личности) издатель, имя или наименование которого обозначено на произведении, при отсутствии доказательств иного считается представителем автора и в этом качестве имеет право защищать права автора и обеспечивать их осуществление.

Настоящее положение будет действовать до тех пор, пока автор такого произведения не раскроет свою личность и не заявит о свое

**6.2 Промышленная собственность**

Объекты промышленной собственности (изобретения, полезные модели, промышленные образцы, селекционные достижения, топологии интегральных микросхем, нераскрытая информация, товарные знаки и знаки обслуживания, географические указания, наименования мест происхождения товаров и др.)

Служебные объекты промышленной собственности.

Служебный объект промышленной собственности (ОПС) относится к области деятельности нанимателя при наличии какого-либо из следующих условий:

- деятельность, которая привела к созданию ОПС, относится к служебным обязанностям работника;

- ОПС создан в связи с выполнением работником конкретного задания, полученного от нанимателя;

- при создании ОПС работником были использованы опыт или средства нанимателя.

Право на подачу заявки и получение патента на служебный ОПС принадлежит нанимателю.

Работник, создавший предполагаемый служебный ОПС, обязан письменно уведомить об этом нанимателя. Уведомление должно быть подписано работником и содержать характеристику созданного объекта, раскрывающую его с полнотой, достаточной для определения пригодности этого объекта в деятельности нанимателя, а также материалы, необходимые для оформления заявки на служебный ОПС. Если указанный ОПС создан совместным творческим трудом нескольких работников, в уведомлении указывается вклад каждого работника в создание этого ОПС.

Уведомление о создании предполагаемого служебного ОПС должно быть зарегистрировано в установленном нанимателем порядке в день его подачи, о чем работник, создавший ОПС, извещается в письменной форме.

Наниматель обязан в трехмесячный срок со дня получения уведомления о создании служебного ОПС подать заявку в НЦИС либо уступить право на подачу заявки и получение патента автору созданного служебного ОПС с сохранением за собой права использования служебного ОПС на условиях лицензионного договора, письменно сообщив автору о принятом решении.

Наниматель обязан предоставить работнику копии заявочных материалов, информировать его о ходе экспертизы, а также предоставлять для рассмотрения связанную с этим корреспонденцию и переписку с патентным органом.

В случае, если наниматель отказался от притязания на ОПС или в течение трех месяцев со дня получения уведомления о его создании не подал заявку в патентный орган, автор имеет право подать заявку на получение патента на свое имя и использовать ОПС без каких-либо ограничений.

Автор служебного ОПС, права на который принадлежат нанимателю, имеет право на вознаграждение. Если в создание служебного ОПС внесли творческий вклад два или более работников, то размер вознаграждения для каждого из них определяется в соответствии с их вкладом, указанным в уведомлении о создании служебного ОПС.

Минимальные ставки вознаграждения за создание и использование ОПС установлены Положением о порядке и условиях государственного стимулирования создания и использования объектов промышленной собственности (утв. постановлением М РБ от 6 марта 1998 г. № 368):

- за создание - 10 базовых величин;

- за использование - 10 % от прибыли или 15 базовых величин.

В случае неполучения патента на служебный ОПС по причинам, зависящим от нанимателя, при установлении вида и размера вознаграждения за него учитывается также не полученный работником, создавшим ОПС, доход, который он мог бы получить oт использования служебного ОПС, защищенного патентом.

Обнаружив факт неполучения патента на служебный ОПС по причинам, зависящим от нанимателя, работник, создавший ОПС, должен незамедлительно сообщить ему об этом в письменном заявлении. В срок не позднее трех месяцев с момента подачи заявления наниматель обязан установить размер вознаграждения.

Условия соглашения между нанимателем и работником, создавшим служебный ОПС, о выплате вознаграждения за него могут изменяться по взаимному согласию сторон . Однако выплаченное работнику вознаграждение не может быть истребовано нанимателем.

Наниматель в случае принятия им решения о подаче заявки на получение патента на служебный ОПС имеет право на подачу заявки и получение патента за границей, о чем должен проинформировать в письменной форме работника, создавшего служебный ОПС, указав страны, где он собирается истребовать защиту. В государствах, где наниматель не получает охрану, подать заявку и получить патент на свое имя имеет право работник, создавший ОПС, письменно уведомив об этом нанимателя.

Наниматель или его правопреемник в случае утраты интереса в получении патента на служебный ОПС после подачи заявки на его выдачу или в поддержании патента в силе обязан своевременно предложить автору служебного ОПС безвозмездную уступку права та получение патента или самого патента. Наниматель имеет право отказаться от защиты ОПС, если работник не запросит передачу права на него в течение трех месяцев с момента получения письменного предложения нанимателя.

При уступке нанимателем или его правопреемником патента на служебный ОПС третьим лицам, а также в случае ликвидации юридического лица автор имеет преимущественное право на приобретение патента на объявленных условиях. При этом соответственно применяются нормы гражданского законодательства РБ о праве преимущественной покупки.

Работник, создавший служебный ОПС, и наниматель, а также третьи лица, обладающие сведениями о служебном ОПС, обязаны воздерживаться от несогласованного между собой разглашения сведений о служебном ОПС до даты официальной публикации сведений о заявке либо других сведений о служебном ОПС.

Прекращение трудового договора, заключенного между работником, создавшим служебный ОПС, и нанимателем, не влияет на их права и обязанности, вытекающие из Положения и возникшие в период действия договора.

Выдача патента

Выдача патента патентообладателю производится патентным органом после публикации сведений о патенте на изобретение, полезную модель, промышленный образец.

При наличии нескольких лиц, имеющих право на получение патента, им выдается один патент с указанием всех патентообладателей.

Регистрация товарного знака и выдача свидетельства на товарный знак

На основании решения о регистрации товарного знака патентный орган в течение месяца с даты получения документа об уплате установленной пошлины производит регистрацию товарного знака в Государственном реестре товарных знаков и знаков обслуживания РБ.

Субъекты права промышленной собственности.

Субъектом права промышленной собственности является работодатель. Для различных объектов промышленной собственности субъекты права и срок действия прав представлены в таблице 5.1.

Таблица 5.1. Субъекты права промышленной собственности



Система выдачи охранных документов

Правовая охрана объектов промышленной собственности осуществляется в рамках государственной, а также международных (надгосударственных) патентных систем. Уполномоченные организации выдают от имени государства или группы государств соответствующий охранный документ.

Одной из наиболее распространенных коммерчески значимых форм правовой охраны является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование объекта промышленной собственности и запрещает всем третьим лицам их использование в коммерческих целях без разрешения патентообладателя. Являясь одновременно правовым, техническим и информационным документом, патент выступает не только в качестве формы правовой охраны от несанкционированного использования, но и своеобразным экономическим стимулом для инвестиций в научные исследования и промышленность.

Права на объекты ИС ограничены территорией государства, выдавшего охранный документ или регламентировавшего другие формы охраны, и носят срочный характер.

Условия патентоспособности объектов промышленной собственности.

Изобретение.

Объект изобретения:

- устройство (например, машина, прибор, инструмент, деталь и др.)

- вещество (сплав, смесь, раствор, химическое соединение и др,)

- биотехнологический продукт (штамм микроорганизма и др.)

- применение устройства, способа, вещества, биотехнологического продукта по определенному (новому) назначению.

Объекты (технические решения) признаются изобретениями, если удовлетворяют следующим 3-м критериям:

- новизны,

- изобретательского уровня

- промышленной применимости.

Изобретение признается новым, если оно не является частью уровня техники.

Изобретение имеет изобретательский уровень, если оно для специалиста явным образом не следует из уровня техники.

Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения (мировая новизна).

Изобретение является промышленно применимым, если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении и других сферах деятельности.

Право на изобретение удостоверяется патентом. Заявка проходит формальную и патентную экспертизы. Патент действует в течение 20 лет с возможностью продления не более чем на 5 лет (если для применения средства, в котором использовано изобретение, требуется получение разрешение уполномоченного органа).

Штамм (strain, line, variety) - культура генетически однородных микроорганизмов, вирусов, опухолевых клеток и т.д. с одинаковыми морфологическими и биологическими свойствами.

Полезная модель.

- техническое решение, относящееся к устройствам и удовлетворяющее критериям новизны и промышленной применимости. Критерии аналогичны критериям изобретения. Требование изобретательского уровня к полезной модели не применяется.

- право на полезную модель удостоверяется патентом. Заявка проходит формальную экспертизу. Патент действует в течение 5 лет с возможным продлением этого срока не более чем на 3 года.

Промышленный образец.

Художественное или художественно-конструкторское решение изделия, определяющее его внешний вид. При этом под изделием понимается предмет как промышленного, так и кустарного производства.

Критерии:

- новизна;

- оригинальность.

Промышленный образец признается новым, если совокупность его существенных признаков не известна из сведений, ставших общедоступными в мире до даты приоритета.

Промышленный образец признается оригинальным, если его существенные признаки обусловливают творческий характер особенностей изделия. К существенным признакам относятся признаки, определяющие эстетические и (или) эргономические особенности внешнего вида изделия, его формы, конфигурации, орнамента и сочетания цветов.

Право на промышленный образец охраняется государством и удостоверяется патентом. Срок действия патента - 10 лет с возможностью продления на срок до 5 лет.

Селекционные достижения.

В соответствии с ГК права на новые сорта растений и новые породы животных (селекционные достижения) охраняются при условии выдачи патента. В свою очередь патент в соответствии с законодательством Беларуси может быть получен только на сорт растения.

Закон «О патентах на сорта растений» определяет сорт как группу растений, которая независимо от патентоспособности определяется признаками, характеризующими данный генотип или комбинацию генотипов, и отличается от других групп растений того же ботанического таксона хотя бы одним признаком. Сорт может быть представлен несколькими растениями, одним растением либо одной или несколькими частями растения при условии, что такая часть или части могут быть использованы для воспроизводства целых растений сорта.

Сорту предоставляется правовая охрана, если он обладает новизной, отличимостью, однородностью и стабильностью.

Сорт считается новым, если на дату подачи заявки на выдачу патента на сорт посадочный или плодовый материал этого сорта не продавался либо не передавался иным образом селекционером или его правопреемником или с их разрешения другими лицами для использования на территории РБ ранее, чем за один год до даты подачи заявки, а на территории любого иного государства - ранее, чем за четыре года до даты подачи заявки. Указанная льгота по новизне для иностранных граждал и юридических лиц в отношении древесных культур и винограда устанавливается на срок в шесть лет до даты подачи заявки.

Сорт считается отличимым, если он явно отличается от любого другого сорта, существование которого к моменту подачи заявки является общеизвестным.

Сорт считается однородным, если с учетом особенностей его размножения растения этого сорта достаточно однородны по своим признакам.

Сорт считается стабильным, если его основные признаки остаются неизменными после неоднократного размножения или в конце каждого цикла размножения (в случае особого цикла размножения). Право на сорт удостоверяется патентом.

Патент действует в течение 25 лет с даты регистрации сорта в Реестре охраняемых сортов.

Топология интегральной микросхемы

- зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними.

Правовая охрана распространяется только на оригинальную топологию, т.е. топологию, которая создана в результате творческой деятельности автора.

Право на топологию удостоверяется свидетельством.

Исключительное право на использование топологии действует в течение десяти лет.

Свидетельство на топологию удостоверяет авторство, приоритет топологии и исключительное право на ее использование.

Объем правовой охраны, предоставляемой топологии, определяется совокупностью ее элементов и связей, представленных в депонируемых материалах.

Нераскрытая информация. Коммерческая тайна. Ноу-хау.

Относительно универсальная форма и очевидная альтернатива патентованию. Способ охраны различных технических решений и возможность выбора подходящей для определенного интеллектуального продукта формы правовой охраны.

Более употребительным для обозначения нераскрытой информации являются термины «ноу-хау» (хотя в узком смысле ноу-хау это только секреты производства) или «коммерческая тайна». Специфичность данного объекта проявляется, например, в том, что в качестве нераскрытой информации могут охраняться объекты, обладающие признаками патентуемых (устройства, способы и т.п.). Поэтому можно определить ноу-хау как отдельный режим охраны (режим засекречивания), существующий наряду с авторско-правовым и патентно-правовым режимами.

В соответствии со статьей 1010 Гражданского кодекса РБ под нераскрытой информацией понимается техническая, организационная или коммерческая информация, в том числе секреты производства (ноу-хау), не известная третьим лицам.

Возникновение права на защиту нераскрытой информации не обусловлено какими-либо формальными процедурами, оно лишь обусловлено определенными требованиями, которые установлены пунктом 1 статьи 140 названного кодекса, которая корреспондирует нераскрытую информацию с определением служебной и коммерческой тайны. Отметим также, что вопросы охраны коммерческой тайны урегулированы в соответствующем Положении, утвержденном постановлением СМ РБ от 6 ноября 1992 г. № 670.

Товарные знаки и знаки обслуживания

- обозначения, способствующие отличию товаров и услуг одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц.

В качестве товарных знаков регистрируются обозначения, которые могут быть представлены в графической форме:

- словесные,

- буквенные,

- цифровые,

- изобразительные,

- трехмерные, включая форму товара или его упаковку, другие обозначения и их комбинации.

Товарный знак может быть зарегистрирован в любом цвете или цветовом сочетании. На товарный знак выдается свидетельство, срок действия которого составляет 10 лет и может быть продлен каждый раз не более, чем на 10 лет.

Географическое указание

включает в себя понятия

1) наименование места происхождения товара — действительное или историческое название географического объекта (страны, населенного пункта, местности и др.), используемое для обозначения товара, особые свойства которого исключительно или главным образом определяются характерными для этого географического объекта природными условиями или иными факторами либо сочетанием природных условий и этих факторов (например, минеральная вода «Минск», имеющая особые свойства, обусловленные природными условиями места ее добычи);

2) указание происхождения товара — обозначение (изображения или название географического объекта), прямо пли косвенно указывающее на место действительного происхождения или изготовления товара (например указание «Сделано в Беларуси», размещаемое на любых товарах отечественного производства).

Право пользования наименованием места происхождения товара предоставляется на основании его регистрации в НЦИС и удостоверяется свидетельством. Срок действия свидетельства - 10 лет с возможностью периодического продления на 10 лет, как и у товарного знака. Владелец свидетельства на наименование места происхождения товара обладает только правом пользования зарегистрированным наименованием места происхождения товара и оно предоставляется любому лицу, находящемуся в том же географическом объекте и производящему товар с теми же свойствами.

Правовая охрана осуществляется на основании его использования (указание не требует регистрации) и состоит в недопущении использования фальшивых географических указаний и введении потребителя в заблуждение относительно действительного места происхождения товара.

Географическое указание

Не допускает возможности их уступки или передачи права пользования ими по лицензионному договору.

Фирменное наименование - это специальное наименование, являющееся частью полного или сокращенного наименования юридического лица, используемое для отличия его от других коммерческих организаций, осуществляющих свою деятельность в тождественной или сходной области предпринимательства или в других областях деятельности.

Состоит из двух частей: обязательной и произвольной, выдуманной.

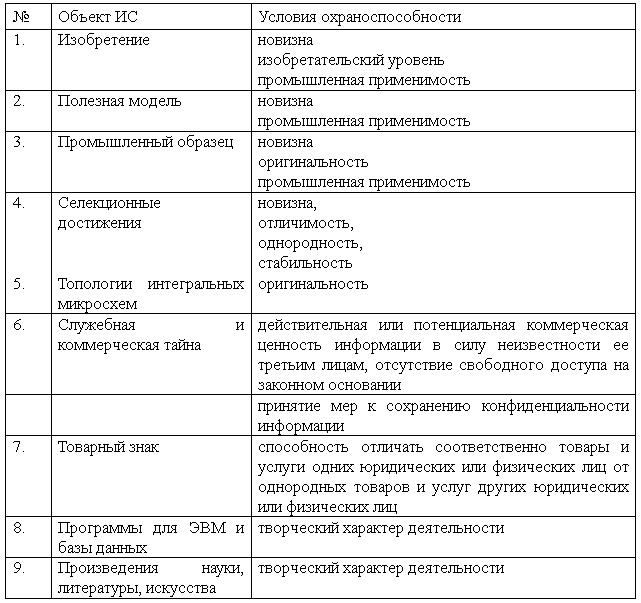
Обязательная часть включает указание на организационно-правовую форму юридического лица (например, унитарное предприятие), а также в необходимых случаях указание на собственника (например, республиканское) и основное направление деятельности (например, предприятие общественного питания).

Произвольная (закавыченная) часть представляет собой собственно название юридического лица (например, «Атлант»).

Фирменное наименование является особым объектом исключительного права. Оно не регистрируется самостоятельно, как, например, товарный знак. Оно определяется при утверждении устава и регистрируется в рамках процедуры регистрации юридического лица. Сведения о юридическом лице, включая присвоенное ему наименование, включаются в Единый государственный регистр юридических лиц и индивидуальных предпринимателей. Органом, который осуществляет предварительное согласование фирменных наименований и ведет названный регистр, является Министерство юстиции РБ.

В общем виде условия патентоспособности объектов промышленной собственности представлены в таблице 5.1.

Таблица 5.1. Требования, предъявляемые к патентоспособным объектам ИС



**6.3 Патентная информация**

Патентные исследования (патентный поиск) - это исследования технического уровня и тенденций развития объектов техники, их патентоспособности, патентной чистоты и конкурентоспособности на основе патентной и другой информации.

Патентные исследования проводятся при:

- разработке научно-технических прогнозов для перспективного планирования;

- разработке планов развития науки и техники;

- составлении заявок на разработку и освоение продукции;

- создании объектов техники (научные исследования и разработка);

- освоении и производстве продукции.

Целью патентных исследований является:

поиск и отбор объективных данных для обеспечения высокого технического уровня и конкурентоспособности объекта техники, использования современных научно-технических достижений и исключения неоправданного дублирования исследований разработок.

Объект (патентных) исследований — объект хозяйственной деятельности и сама хозяйственная деятельность субъекта.

Объект хозяйственной деятельности — объекты техники, в том числе создаваемые по Государственному оборонному заказу, объекты промышленной (интеллектуальной) собственности, ноу-хау, услуги, предоставляемые хозяйствующим субъектом.

Хозяйствующий субъект — любой участник народнохозяйственной деятельности.

Конкурентоспособность — способность объекта хозяйственной деятельности в определенный период обеспечить коммерческий или иной успех на конкретном рынке в условиях конкуренции или противодействия.

Инжиниринг — выполнение различных инженерных работ, оказание консультационных услуг на коммерческой основе.

К участникам хозяйственной деятельности относят предприятие, организацию, концерн, ассоциацию, акционерное общество и другие объединения (далее — предприятие) независимо от форм собственности и подчинения, государственного заказчика, а также лица, занимающиеся индивидуальной трудовой деятельностью.

Согласно документу СТБ 1180-99. «Патентные исследования. Содержание и порядок проведения» по своему характеру и содержанию патентные исследования относятся к прикладным научно-исследовательским работам и являются неотъемлемой составной частью обоснования принимаемых решений народнохозяйственных задач, связанных с созданием, производством, реализацией, совершенствованием, использованием, ремонтом и снятием с производства объектов хозяйственной деятельности.

(К объектам техники также условно отнесены и научно-техническая продукция, штаммы микроорганизмов, технологические процессы, включая химические процессы, биотехнологические, медицинские препараты, способы диагностики, профилактики и лечения).

Патентные исследования могут проводиться как в виде самостоятельной научно-исследовательской работы, так и в составе других работ.

Патентные исследования проводятся на основе анализа источников патентной информации с привлечением других видов научно-технической информации, содержащих сведения о последних научно-технических достижениях, с целью исследования уровня и тенденций развития соответствующей отрасли науки и отсутствия дублирования разработок.

На основе результатов анализа изученной патентной документации и соответствующей отрасли науки научно-технической литературы определяется эффективность научных разработок и возможность их защиты патентами на изобретения, полезные модели и промышленные образцы.

При проведении патентных исследований используются все доступные источники патентной и другой научно-технической информации.

Патентные исследования проводят хозяйствующие субъекты:

— исполнители (разработчики) программ (межгосударственных, государственных, региональных, отраслевых и других) создания, развития производства и использования объектов техники;

— исполнители фундаментальных исследований с практическим выходом продукции и исследований прикладного характера — исполнители НИР и ОКР;

— заказчики (основные потребители объектов хозяйственной деятельности);

— изготовители (поставщики) объектов хозяйственной деятельности.

В зависимости от практической потребности патентные исследования проводят:

— заказчик (основной потребитель) — при прогнозировании, перспективном и текущем планировании, определении направлений, темпов развития средств технического обеспечения своей деятельности, исследовательском проектировании, формировании заказов исполнителям, поставщикам, при использовании (эксплуатации) продукции;

— исполнитель научно-исследовательских работ — при прогнозировании, перспективном и текущем планировании научных исследований, выборе направлений исследований для создания новых и модернизации существующих объектов техники и их технико-экономическом обосновании; при определении инжиниринговых услуг; при изыскании, исследовании применения объектов техники по новому назначению; при выполнении научно-исследовательских работ и их этапов; при осуществлении научно-технического сотрудничества;

— исполнитель (разработчик, проектант, проектировщик) — при прогнозировании, перспективном и текущем планировании своей деятельности; при обосновании необходимости выполнения конкретных работ; в процессе выполнения опытно-конструкторских, проектно-конструкторских, проектных, технологических, изыскательских и других работ (в том числе аванпроектов) и их этапов; при обосновании выбора форм реализации и обеспечения условий реализации продукции; при решении вопросов использования опыта и знаний сторонних организаций и фирм; при определении инжиниринговых услуг; при осуществлении научно-технического сотрудничества;

— изготовитель (поставщик) — при перспективном и текущем планировании развития производства или его модернизации, постановке продукции на производство, при решении вопросов повышения качества продукции, совершенствования технологии, материального, технологического обеспечения производства, приобретения зарубежного оборудования и лицензий; при совершенствовании продукции; при решении вопросов реализации продукции и обеспечения оптимальных ее условий, включая сервисные услуги поставленной продукции; при решении вопросов кооперирования производства, создании совместных предприятий;

— все хозяйствующие субъекты — при решении вопросов правовой охраны объектов промышленной (интеллектуальной) собственности.

Проведение патентных исследований и представление их результатов предусматривают в договорной и (или) планово-технической документации\* на выполнение работ.

Планы (в том числе календарные), программы (например, программы научно-исследовательских работ), ведомости исполнения опытно-конструкторских работ, графики (генеральные, сетевые, линейные) выполнения работы, тактико-технические, технические задания и другие принятые хозяйствующим субъектом документы, определяющие содержание, сроки, порядок выполнения и требования к результатам работы, выполняемой по договору.

Поставщики и разработчики комплектующих изделий, оборудования, материалов, технологии, созданных (создаваемых) не по единому исходному техническому документу, а в ином порядке, представляют результаты патентных исследований на эти объекты головному исполнителю (исполнителю) работ, заказчику, изготовителю конечной продукции по их запросам по отдельному договору.

В этой документации предусматривают необходимость применения требований настоящего стандарта при организации, проведении, оформлении и использовании результатов патентных исследований.

В договорной документации на проведение работ определяют права и обязанности сторон, в том числе в отношении результатов патентных исследований, условия конфиденциальности, а также ответственность сторон за последствия, вызванные отказом от проведения патентных исследований, выполнением их в ограниченном объеме, отказом от использования их результатов и т.д.

Необходимость привлечения сторонних организаций к проведению патентных исследований определяет исполнитель работы. Участие сторонних организаций в проведении патентных исследований или их выполнение сторонними организациями оформляют договором (контрактом).

Необходимость проведения патентных исследований при выполнении составных частей работ или при разработке комплектующих изделий, материалов, технологии, осуществляемых по единому исходному техническому документу (техническому, тактико-техническому заданию), определяет головной исполнитель работы, оформляя проведение патентных исследований.

Стандартизация в патентной документации.

Основа патентных исследований - информационный поиск. Современными средствами доступа к мировым информационным ресурсам являются компьютерные сети, в частности Интернет. Патентные документы в настоящее время, кроме традиционного вида - на бумажных носителях, представлены в виде электронных баз данных ЕПВ, ВОИС, USA, De, Fr и др. Кроме этого, Национальный центр интеллектуальной собственности и РНТБ имеют базу данных на CD-ROM дисках и DVD-ROM дисках, специализированный поисковый интерфейс МIМОЗА. При этом в Национальном центре интеллектуальной собственности на основе поисковой базы данных GLOBAL PAT и PAJ в формате «первая страница» сформированы поисковые системы для оценки релевантности документов в ускоренном режиме (до 10 документов в секунду). Кроме этого, предусмотрена возможность соединения с сервером ESP@CENET для доступа к полнотекстовым документам.

Основные составляющие патентных исследований.

I. Исследование технического уровня и тенденций развития объектов техники.

II. Оценка патентоспособности новых технических решений.

III. Проверка патентной чистоты объектов техники.

IV. Анализ конкурентоспособности объектов техники.

Исследование технического уровня и тенденций развития объектов техники, их патентоспособности, патентной чистоты, конкурентоспособности на основе патентной и другой информации.

I. Исследование технического уровня и тенденций развития объектов техники.

Технический уровень объекта техники - степень реализации в изучаемом (исследуемом, разрабатываемом) объекте техники прогрессивных технических решений в сравнении с аналогами.

Перспективные направления разработки, освоения и постановки на производство конкурентоспособной продукции

1. Поиск, отбор и использование технических решений, на которые прекратили действие патенты (свыше 30 млн. штук).

2. Поиск и отбор охраняемых технических решений, закупка лицензий (заключение лицензионных договоров).

3. Выявление перспективного направления (аналога), его усовершенствование, позволяющее уйти из-под действия охранного документа.

4. Создание абсолютно нового технического решения (пионерское изобретение).

II. Оценка патентоспособности новых технических решений.

Патентоспособность - возможность получения какого-либо охранного документа на данный объект (техническое решение) в одной или нескольких странах.

Изобретению в любой области техники предоставляется правовая охрана, если оно относится к продукту или способу, является новым, имеет изобретательский уровень и промышленно применимо.

Изобретение является новым, если оно не является частью уровня техники.

Изобретение имеет изобретательский уровень, если оно для специалиста явным образом не следует из уровня техники.

Изобретение является промышленно применимым, если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении и других сферах деятельности.

Полезная модель является новой, если совокупность ее существенных 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.

Промышленным образцом, которому предоставляется правовая охрана, признается художественное или художественно-конструкторское решение изделия, определяющее его внешний вид и являющееся новым и оригинальным. При этом под изделием понимается предмет промышленного или кустарного производства.

Промышленный образец признается новым, если совокупность его существенных признаков неизвестна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца.

Промышленный образец признается оригинальным, если его существенные признаки обусловливают творческий характер особенностей изделия.

III. Проверка патентной чистоты объектов техники.

Патентная чистота - юридическое свойство объекта техники, заключающееся в том, что он может быть свободно использован в данной стране без опасности нарушения действующих на ее территории патентов на объекты промышленной собственности, принадлежащих третьим лицам.

Критерии патентной чистоты объекта техники

•  в отношении изобретений (полезных моделей): не использование хотя бы одного из существенных признаков каждого изобретения, входящего в объект техники;

•  в отношении промышленных образцов: отсутствие общего сходства, дающего впечатление об идентичности при разновременном восприятии.

Объект техники не обладает патентной чистотой:

•  если все признаки изобретения, защищенного патентом, использованы в проверяемом объекте;

•  если в проверяемом объекте использованы все признаки изобретения, защищенного патентом, и имеются другие дополнительные признаки;

•  если в проверяемом объекте не использован один из существенных признаков, но он заменен другим эквивалентным признаком.

Если в проверяемом объекте не использован хотя бы один из существенных признаков изобретения, защищенного патентом, и этот признак не заменен техническим эквивалентом, то объект обладает патентной чистотой.

IV. Анализ конкурентоспособности объектов техники.

Проведенный комплекс исследований по определению технического уровня и тенденций развития объектов техники, их патентоспособности и патентной чистоты является одним из критериев, по которому определяется конкурентоспособность объекта техники.

Особенности проведения патентных исследований (статистических, содержательных, конъюнктурных) на стадиях и этапах жизненного цикла продукции.

Порядок проведения патентных исследований.

1. Разработка программы (регламента) исследований;

2. Поиск и отбор патентной и научно-технической информации;

3. Анализ результатов исследований.

Операции (работы), выполняемые при разработке программы (регламента):

1. Определение предмета исследований (объект в целом, его составные части, или элементы).

2. Определение стран (фирм) поиска.

3. Определение видов информационных источников;

4. Определение глубины поиска.

5. Определение примерного классификационного индекса МПК с помощью алфавитно-предметного указателя (АПУ) к МПК (МКИ), включающего перечень ключевых понятия соответствующих индексов системы классификации МПК;

6. Уточнение классификационного индекса с помощью соответствующего индекса раздела МПК.

Патентно-информационный поиск при проведении патентных исследований (тематический, именной, нумерационный и др.)

Особенности проведения патентных исследований на стадиях и этапах жизненного цикла продукции.

Патентные исследования включают статистические, содержательные, конъюнктурные.

Наука России в цифрах: 2005. Cтат. сб. - М.: ЦИСН, 2005.

Предлагаемый сборник продолжает серию статистических публикаций Центра исследований и статистики науки (ЦИСН) и адресован широкому кругу читателей. В нем приведены основные показатели состояния и уровня развития научного потенциала России за 1998-2004 гг. и ряд прогнозных показателей на 2005 г., результаты инновационной деятельности в промышленности и сфере услуг и сведения об использовании информационно-коммуникационных технологий в экономике России за 2002-2004 гг. В сборник включены данные по международным сопоставлениям. Представленная информация базируется на современных методологических подходах к статистике науки и полностью отвечает требованиям международных статистических стандартов. При подготовке сборника использованы материалы Росстата, Минобрнауки России, Роснауки, Роспатента, ВАК России, Статкомитета СНГ, ОЭСР и собственные методические разработки ЦИСН. Приведенные данные в ряде случаев уточняют ранее опубликованные.

Термином жизненный цикл (ЖЦ) принято отражать совокупность процессов и этапов развития организмов живой природы, технических систем, продуктов производства от моментов зарождения или появления потребности их создания и использования до прекращения функционирования или применения. Это соответствует всеобщему закону развития любых изделий, событий или процессов между их началом и концом, которые определяют цикл их создания, существования и применения.

Все виды продукции, технологии и услуг имеют определенный жизненный цикл. Различают жизненный цикл продукции, отдельной компании и даже в целом целой отрасли, который, по сути, является суммарной величиной жизненных циклов соответствующей группы продукции-аналогов по физическим характеристикам или потребительскому назначению.

Жизненный цикл продукции (ЖЦП) — все этапы «жизни» продукции:

* дизайнерская задумка,
* конструкторская и технологическая подготовка производства,
* изготовление,
* обслуживание,
* утилизация и т.п.

Типовая модель процессов жизненного цикла сложной системы начинается с концепции идеи системы или потребности в ней, охватывает проектирование, разработку, применение и сопровождение системы, и заканчивается снятием системы с эксплуатации. В основном, применяется по отношению к сложной наукоемкой продукции высокотехнологичных предприятий.

Модель жизненного цикла системы обычно разделяют на последовательные периоды реализации — стадии или этапы. Каждый подобный период включает основные реализуемые в нем процессы, работы и задачи, при завершении которых может потребоваться переход к следующему периоду реализации.

Общую модель жизненного цикла сложной системы обычно разделяют на следующие основные этапы с последующей адаптацией каждого из них в модели жизненного цикла конкретной системы:

- потребностей;

- исследование и описание основных концепций;

-·и разработка;

-·системы;

-·и производство;

-·и продажа;

-·эксплуатация;

-·сопровождение и мониторинг;

-·снятие с эксплуатации (утилизация).

**6.4** **Коммерческое использование объектов интеллектуальной собственности**

Основные трудности в области коммерциализации ИС, которые тормозят процессы формирования и реализации научно-технического продукта состоят в следующем:

- нормативно-законодательная проблема;

- проблема оценки ИС;

- кадровая проблема.

Перечисленные проблемы не умаляют значимость и других, связанных, например, с финансированием, созданием необходимой инфраструктуры, рыночной востребованностью научно-технических новшеств и др.

Главное отличие инвестиционного процесса от инновационного состоит в том, что в первом случае товаром может быть только внедренный в производство результат, а во втором - и ноу-хау, и патент, и свидетельство, и объекты авторского права. Причем интеллектуальный результат на каждом этапе инновационного проекта может выступать как готовый научно-технический продукт. В рамках инвестиционного проекта такой продукт возникает только на заключительном этапе. К сожалению, до сих пор очень малое количество разработчиков, и еще меньшее инвесторов понимает значение этих отличий, а, следовательно, и выгод, которые можно получить при грамотном вовлечении ИС в хозяйственный оборот предприятия.

Основные формы передачи прав на объекты интеллектуальной собственности.

Допустим, что в результате проведенной НИОКР на вашем предприятии внедрена технологическая линия по производству определенной продукции. Что мешает конкурентам воспроизвести эту линию, выпускать аналогичную продукцию и при более умелом менеджменте попытаться вытеснить вас с рынка. Если же вы фиксируете свою интеллектуальную собственность, предпринимаете охраноспособные действия и вводите эту собственность в состав имущества, то конкуренты вынуждены будут либо уйти с рынка, либо пользоваться вашими трудами, но уже на законном основании в виде покупки права пользования по лицензионному соглашению.

В таком случае предприятие получает дополнительный доход, возможность формировать и регулировать рынок, что также является преимуществом коммерциализации ИС. Кроме того, введение результата интеллектуальной деятельности в хозяйственный оборот увеличивает стоимость всего предприятия, что очень важно при его оценке на предмет получения инвестиций или при сделках по продаже предприятия, поглощении, слиянии и т. д. Еще один плюс - минимизация налогообложения за счет отнесения амортизационных отчислений на затраты предприятия.

Коммерциализация ИС в нормативно-законодательном смысле предполагает пересечение трех главных нормативных отраслей: права, налогового обеспечения, бухгалтерского учета. Многие нормы данных отраслей противоречат друг другу. Это - коллизии норм: гражданского права и бухгалтерского учета; налогового и бухгалтерского учета.

Один из вариантов комплекса мер, который необходимо провести, если речь идет о коммерциализации ИС.

1) Выявление и идентификация ИС, т.е. проведение инвентаризации результатов научно-технической деятельности, НИОКР и отделение одних объектов от других. Идентификация - самый неопределенный момент. Это касается, прежде всего, товарных знаков. Когда товарный знак может стать активом, а не просто расходами в рекламных целях? Или, если у организации в результате проведенных НИОКР появилось несколько патентов, то как разделить (идентифицировать) обособленную стоимость каждого из них? На эти вопросы отечественное законодательство не дает ответа. Поэтому на данном этапе необходимо четкое оформление первичных документов, которые впоследствии могут послужить основанием для самого факта существования объекта и его оценки. Все зависит от того, как предприятие получило ИС у другого предприятия или физического лица.

2) Оформление прав на ИС. На этом этапе надо определить, кому принадлежат права собственности на созданный объект. Здесь очень важную роль играет финансовый источник создания. И если вы пользовались бюджетными средствами, затраченными на гражданские исследования и разработки, то право собственности закреплено за государством. В этом случае можно рассчитывать только на лицензионное соглашение.

Таким образом, ИС также будет вовлечена в хозяйственный оборот страны, но не обязательно в оборот вашего предприятия. Гражданский кодекс РБ устанавливает другую норму, указывая, что данный вопрос может решаться по согласованию сторон, но обязательно в письменном виде. Если права собственности принадлежат вам, то необходимо решить, стоит ли легализовать данный объект. Это зависит от вида полученной ИС, но уже не в юридическом смысле, а в бухгалтерском.

В бухгалтерской практике различают следующие три вида ИС:

- способные стать нематериальными активами (далее - НМА);

- подлежащие правовой охране, но не оформленные;

- не подлежащие правовой охране.

3) Оценка объекта ИС. Нормативная база по этому вопросу развита очень слабо. Наиболее благополучно обстоит дело с оценкой актива, созданного собственными силами. В отношении безвозмездно полученных активов или вкладов в уставный капитал нет установленных норм определения рыночной цены. Критерии оценки рыночной стоимости научно-технической продукции до сих пор четко не выработаны. И обоснованная оценка ИС почти всегда зависит от квалификации и профессионализма специалиста, занимающегося оценкой. Нельзя опустить вопрос и об авторских вознаграждениях, поскольку разработчики зачастую переоценивают свою ИС. Выполнение их требований может повлечь за собой завышение ее цены и, как следствие, упадок интереса к разработке со стороны рынка. Согласно Налоговому кодексу РБ и бухгалтерскому учету коммерциализации подлежат объекты промышленной собственности. Такие результаты, как отчеты, методики, ТУ, не могут быть коммерциализованы в полном смысле, поскольку механизм авторского права не защищает права собственников. А незащищенные права не могут стать имуществом предприятия.

Поэтому сегодня возникают трудности с коммерциализацией огромного количества научно-технических результатов, принадлежащих отечественным разработчикам, за границей.

Если вы решили ввести в состав имущества ИС в виде нематериального актива (НМА), то необходимо, чтобы этот объект ИС отвечал семи очень жестким единовременным условиям:

а) отсутствие материально-вещественной (физической) структуры;

б) возможность идентификации (выделения, отделения) организацией от другого имущества;

в) использование в производстве продукции, при выполнении работ или оказании услуг либо для управленческих нужд организации;

г) использование в течение длительного времени, т. е. срока полезного использования продолжительностью свыше 12 месяцев или обычного операционного цикла, если он превышает 12 месяцев;

д) организация не предполагает последующую перепродажу данного имущества;

е) способность приносить организации экономические выгоды (доход в будущем);

ж) наличие надлежаще оформленных документов, подтверждающих существование самого актива и исключительного права у организации на результаты научно-технической деятельности (РНТД) (патенты, свидетельства, другие охранные документы, договор уступки (приобретения) патента, ТЗ и т. п.).

Законодательством установлен специальный порядок передачи имущественных прав на объекты промышленной собственности, так как они являются особенным объектом гражданского права.

В пункте 2 статьи 983 ГК РБ указано, что обладатель исключительного права на объект ИС вправе передать это право другому лицу полностью или частично, разрешить другому лицу использовать объект ИС и вправе распорядиться им иным образом.

И далее, в ч. 1 п. 1 статьи 984 ГК РБ: «Имущественные права, принадлежащие обладателю исключительных прав на объект ИС, могут быть переданы правообладателем полностью или частично другому лицу по договору, а также переходят по наследству и в порядке правопреемства при реорганизации юридического лица — правообладателя».

Обладатель имущественных прав на объект промышленной собственности может внести их в уставный фонд двумя способами:

I - уступить все или часть прав коммерческой организации, в уставный фонд которой вносятся эти права (в этом случае все имущественные права на объект промышленной собственности окончательно переходят коммерческой организации) (оформляется договором уступки) ;

II - предоставить коммерческой организации, в уставный фонд которой вносятся эти права, право использовать объект промышленной собственности определенное время по исключительной или неисключительной лицензии (в этом случае коммерческая организация получает только часть имущественных прав и только на определенное время, а основные права остаются у обладателя) (оформляется лицензионными договорами).

Классификация договоров, их структура и содержание

Договоры, заключаемые в сфере интеллектуальной собственности, оформляются в соответствии с нормами, представленными в:

- Гражданском кодексе Республики Беларусь (раздел III, гл. 23, раздел IV, гл. 53, раздел V, гл. 60, 66, 67);

- Постановлении СМ РБ от 22.05.2003 г. № 681 «О регистрации лицензионных договоров, договоров уступки и договоров залога прав на объекты интеллектуальной собственности» (в ред. от 08.06.2004 г.);

- Правилами рассмотрения и регистрации договоров уступки товарного знака и лицензионных договоров о предоставлении права на использование товарного знака, утвержденные приказом Государственного патентного комитета РБ от 30.12.1998 г. № 52 (в ред. от 25.06.2004 г.);

- Правилами рассмотрения и регистрации договоров уступки патента и лицензионных договоров о передаче права на использование изобретения, полезной модели, промышленного образца, утвержденные приказом Государственного патентного комитета РБ от 07.12.1999 г. № 50 (в ред. от 16.06.2003 г.).

Для полной или частичной передачи прав на объекты ИС (товарные знаки, изобретения, полезные модели, промышленные образцы, программы для ЭВМ и БД) по закону об ИС требуется подписание специальных договоров: лицензионных договоров и договор уступки.

Лицензионный договор (его еще называют лицензионным соглашением) составляется с целью разрешения какому-либо лицу использования объекта ИС на определенных условиях и на определенный срок.

Договор об уступке объекта ИС передает исключительной право на использование объекта другому лицу.

Лицензионный договор и договор уступки подлежат обязательной регистрации в НЦИС, иначе такой договор считается недействительным.

В связи с этим при составлении таких договоров необходимо учитывать не только пожелания сторон, но и те требования, которые предъявляются к данным договорам нормативно-правовыми актами и проверяются НЦИС.

Классификация лицензионных договоров

Некоторые виды выработаны международной правовой практикой, например, полная лицензия, которая представляет собой куплю-продажу объекта ИС. Следовательно, лицензионный договор является именно продажей разрешения на использование объекта ИС.

Лицензионные договора классифицируют в зависимости от:

1) Предмета лицензионного договора.

В зависимости от предмета лицензионного договора, т.е. в зависимости от вида объекта ИС, они делятся на договора:

- о передаче права на использование изобретения;

- о передаче права на использование полезной модели;

- о передаче права на использование промышленного образца;

- о передаче права на использование знака для товаров и услуг;

- о передаче права на использование "ноу-хау" и пр.

2) По объему исключительного права лицензиата относительно лицензиара и третьих лиц различают договоры:

- неисключительной (простой) лицензии;

- исключительной лицензии;

- полной (неограниченной) лицензии;

- ограниченной лицензии;

- возвратные лицензии;

- безотзывные;

- открытой лицензии;

- сублицензии.

3) В зависимости от способа охраны предмета лицензионные договоры делятся на:

- патентные;

- беспатентные;

- комплексные;

- перекресная лицензия ("кросс-лицензия").

Лицензионный договор

Лицензия - это широко используемое в ряде сфер деятельности понятие, которое в переводе с латинского означает право, разрешение.

Термин "лицензия" может быть широко определен как право или права какого-либо лица выполнять то, что без подобной лицензии было бы незаконным.

Это значение термина "лицензия" часто используется в связи с правами или привилегиями, обычно предоставляемыми правительством неправительственным субъектам для различных целей.

Другое обычное использование термина "лицензия" вытекает из прямого или косвенного наделения правительством полномочиями других субъектов на выполнение определенных действий.

Еще одно использование термина "лицензия" связано с недвижимостью.

ДОГОВОР ЛИЦЕНЗИОННЫЙ - соглашение о предоставлении прав на коммерческое и производственное использование изобретений, технических знаний, товарных знаков. Сторонами, заключающими договор, выступают лицензиар и лицензиат.

Договор патентной лицензии - это соглашение о предоставлении лицензии.

По лицензионному договору обладатель исключительного права (лицензиар) передает право на использование охраняемого объекта другому лицу (лицензиату), а последний принимает на себя обязанность вносить лицензиару обусловленные договором платежи и осуществлять другие действия, предусмотренные договором.

ОСНОВНЫЕ ПОНЯТИЯ

ЛИЦЕНЗИАР - собственник, владелец изобретения, патента, технического или технологического новшества, выдающий, продающий другому лицу (лицензиату) лицензию, предоставляющую право использования этих нововведений в установленных договором пределах.

ЛИЦЕНЗИАТ - лицо, приобретающее у собственника патентов, технических или технологических новшеств, изобретений за соответствующую плату право пользоваться этими нововведениями в пределах, зафиксированных в лицензионном договоре.

ЛИЦЕНЗИОННАЯ ТОРГОВЛЯ - форма международной торговли технологическими и техническими новшествами (ноу-хау), патентами, лицензиями на изобретения.

ЛИЦЕНЗИОННОЕ ВОЗНАГРАЖДЕНИЕ - плата за предоставление права на использование лицензий, ноу-хау, других объектов, предметов лицензионного соглашения.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ - договор о передаче прав на использование лицензий, ноу-хау, товарных знаков, технических знаний, инжиниринговых услуг.

ЛИЦЕНЗИОННЫЙ ПЛАТЕЖ - плата владельцу интеллектуальной собственности за право Использования этой собственности в коммерческих целях.

В рамках лицензионных договоров происходит частичная передача исключительных патентных прав на изобретения, полезные модели и промышленные образцы. Отдельные типы данных договоров делятся на виды и разновидности по содержанию объектов передаваемых прав. К примеру, в лицензиях на изобретения можно выделить лицензионные договоры на устройства, способы, вещества, штаммы и т. д.

Важным критерием разделения договоров патентной лицензии на виды является объем передаваемых прав. По этому критерию различают лицензии исключительные и неисключительные. Существуют и другие основания классификации патентно-лицензионных договоров.

Лицензионный договор составляется в письменной форме. Договоры об уступке и лицензионные договоры о предоставлении прав на объекты промышленной собственности подлежат регистрации в Патентном ведомстве. Авторские договоры составляются в письменной форме. При продаже и предоставлении массовым пользователям доступа к программам для ЭВМ и базам данных допускается применение особого порядка заключения договоров, например, путем изложения типовых условий договора на передаваемых экземплярах программ для ЭВМ и баз данных.

Виды лицензионных договоров

Лицензионные договоры заключаются партнерами на передачу различных объектов, с различным объемом передаваемых правомочий, для различных целей.

Объектами лицензионных договоров выступают как объекты, которые имеют правовую охрану ПС, так и объекты, которые не имеют правовой охраны (на которые поданы заявки на выдачу охранных документов).

Форма договора

Лицензионные договоры о передаче прав на:

- изобретения;

- полезные модели;

- промышленные образцы;

- сорта растений;

- топологии интегральных микросхем;

- товарные знаки (знаки обслуживания);

- секреты производства (ноу-хау).

Передача прав по авторским договорам

По лицензионным договорам, как правило, передаются права на объекты промышленной собственности.

Если автор передает другому лицу свои имущественные права на использование объекта авторского права, то заключается авторский договор.

На практике часто возникает необходимость оформления лицензионных договоров, которые по своему смыслу, форме и другим показателям отличаются от основных видов. Возникновение таких лицензионных договоров обусловливается, прежде всего, желанием сторон урегулировать свои отношения как можно быстрее, доступнее, согласно своей цели, применяя при этом приобретенный мировой опыт в определенной ситуации, с помощью современных технологий и не вступая при этом в непосредственный контакт друг с другом.

В зависимости от способа передачи и условий использования лицензии могут быть таких видов:

- чистые;

- сопутствующие;

- поворотные;

- открытые;

- принудительные;

- обязательные;

- зависимые;

- единоличные лицензии;

- клик-лицензии;

- клик-рэп лицензии.

Основными факторами, которые способствуют успешному лицензионному соглашению, являются значимость научно-технического достижения, его эффективность, надежная правовая защита, освоенность в производстве

Виды лицензий

Существует два основных вида лицензий: исключительная и неисключительная.

При исключительной лицензии лицензиату передается право на использование изобретения, полезной модели или промышленного образца в пределах, оговоренных договором, с сохранением за лицензиаром права на его использование в части, не передаваемой лицензиату.

При неисключительной лицензии лицензиар, предоставляя лицензиату право на использование изобретения, полезной модели или промышленного образца, сохраняет за собой все права, подтверждаемые патентом, в том числе и на предоставление лицензий третьим лицам.

Простая лицензия предусматривает передачу права лицензиату использовать объект в установленных границах, сохраняя лицензиару право применять объект на той же территории или в тех же пределах.

Разрешение исключительного лицензиата третьим лицам использовать изобретение оформляется в виде сублицензионного договора.

За рубежом широко применяется так называемая "параллельная" лицензия, основанная на передаче права использования хорошо известного товарного знака для товаров, не имеющих отношения к товарам, вместе с которыми знак приобрел широкую известность у потребителей. Многие владельцы популярных товарных знаков, желая получить дополнительные финансовые и рекламные выгоды, передают по соглашению заинтересованным фирмам, право использовать их на разнообразных товарах. Например, товарные знаки "Кока-Кола" и "Будвайзер", приобретшие известность в качестве товарных знаков тонизирующего напитка и пива, приобретаются фирмами с целью их применения на рубашках, шляпах, сумках, зеркалах и т.д.

Территория, на которую распространяется действие лицензионного соглашения, не может быть шире, чем территория правовой охраны ОИС.

В лицензионной практике сложились две основные формы оплаты по лицензионному договору:

- паушально - производится в установленном размере единовременно или с рассрочкой платежа;

- роялти – производится поэтапно периодически в зависимости от экономического результата, получаемого пользователем (лицензиаром) от использования ОИС по лицензии, в определенном договором периоде в процентном отношении к выбранной базе роялти.

Передача прав по авторским договорам

Виды договоров в области авторского и смежных прав:

- авторские (лицензионные) договоры;

- авторский договор заказа;

- договор об использовании программ для ЭВМ и баз данных;

- договор об использовании исполнения и постановок;

- договор об использовании фонограмм;

- договор об использовании эфирных и кабельных передач.

- договор об издании и переиздании произведений в оригинале (издательский договор);

- договор о публичном выполнении неопубликованных произведений (постановочный договор);

- договор об использовании неопубликованного произведения в кинофильме, на радио или в телевизионной передаче;

- договор о создании произведения изобразительного искусства с целью публичного показа;

- договор об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства;

- другие договоры о передаче произведений литературы, науки и искусства для использования любым другим способом.

Составление договора о передаче прав и лицензионного договора на изобретение (полезную модель).

Заявителем предоставляются:

* заполненное заявление на составление договора;
* копия патента на изобретение (полезную модель);
* дополнительные материалы (при необходимости);
* оплата услуг за составление договора.

Заявитель получает:

* составленный договор о передаче прав или лицензионный договор на изобретение (полезную модель).

Регистрация договора о передаче прав и лицензионного договора.

Цель: Государственная регистрация договора о передаче прав или лицензионного договора на торговую марку.

Срок выполнения: 2 календарных месяца.

Заявителем предоставляются:

* 3 экземпляра (оригинала) договора;
* оформленная доверенность на ведение делопроизводства;
* оплата услуг и госсбора за публикацию сведений о передаче права или выдаче лицензии.

Заявитель получает:

* 2 экземпляра договора с отметкой НЦИС;
* решение НЦИС о внесении в реестр ведомостей о передаче прав или выдаче лицензии.

Составление договора о передаче прав и лицензионного договора на торговую марку

Цель: Полная передача (продажа) или выдача разрешения (лицензии) на использование исключительных прав на торговую марку.

Заявителем предоставляются:

* заполненное заявление на составление договора;
* копия свидетельства о регистрации торговой марки;
* дополнительные материалы (при необходимости);
* оплата услуг за составление договора.

Заявитель получает:

* составленный договор о передаче прав или лицензионный договор на торговую марку.

РЕГИСТРАЦИЯ ЛИЦЕНЗИОННОГО ДОГОВОРА

Лицензионные договора считаются действительными, если они составлены в письменном виде и подписаны сторонами. Права, переданные по договору, для третьих лиц (судебных органов, налоговой инспекции, нарушителей прав и пр.) будут действительными и будут охраняться законом только после регистрации лицензионного договора в НЦИС.

Организация работ по продаже лицензий

Общая схема работ по разработке и коммерциализации ИС выглядит следующим образом:

1. Выяснение сути разработки и определение существенности предлагаемых улучшений с точки зрения требований рынка.

2. Выявление аналогов. Анализ преимуществ и недостатков разработки.

3. Выявление требований рынка.

4. Выяснение вопросов защиты ИС.

5. Определение состава ИС.

6. Выявление состава авторов и владельца разработки.

7. Определение степени защиты ИС

8. Выявление уровня завершенности разработки.

9. Оценка целесообразности коммерциализации разработки.

10. Всестороннее сравнение разработки с лучшими мировыми аналогами.

11. Определение перспективности разработки.

12. Первичная оценка рынка.

13. Заключение необходимых юридических договоров с владельцем разработки.

14. Поиск потенциальных покупателей и внешних инвесторов (если необходимо).

15. Презентация разработки.

16. Доработка технологии, проведение опытно-конструкторских работ, адаптация под нужды покупателя.

17. Продажа технологии.

18. Техническое сопровождение проданной разработки.

Договор уступки

Уступка прав - универсальный институт обязательственного права, обычно означает передачу прав в том же объеме, в котором они существовали у кредитора. Уступка требований на срок действующим законодательством не предусмотрена.

По договору уступки патентообладатель обязуется передать все права на использование охраняемого объекта изобретения, полезной модели, промышленного образца, другому лицу, на условиях предусмотренных договором.

Заявление о регистрации договора подписывается всеми лицами, которым принадлежит патент, если их согласие не зафиксировано ни в каком другом представляемом документе.

Договора уступки подлежат обязательной государственной регистрации в НЦИС, без чего они считаются недействительными.

Государственная регистрация договоров

Для государственной регистрации лицензионных договоров в НЦИС представляются:

1) заявление;

2) оригинал и копия лицензионного договора;

3) для юридического лица - копия свидетельства о государственной регистрации, заверенная в установленном законодательством порядке;

4) для физического лица - копии удостоверения личности заявителя и свидетельства о государственной регистрации индивидуального предпринимателя, заверенные в установленном законодательством порядке;

5) перечень наименований объектов авторских и смежных прав, используемых лицензиатом и иные документы, подтверждающие сведения, содержащиеся в лицензионном договоре.

6. Регистрация не производится в случае непредставления заявителем полного пакета документов, необходимых для регистрации лицензионных договоров. Решение об отказе в регистрации сообщается заявителю в письменной форме.

7. Регистрация производится путем внесения в государственный реестр лицензионных договоров соответствующей записи и выдачи заявителю ГРУ установленного образца.

ГРУ является документом, подтверждающим произведенную регистрацию лицензионного договора и дающим право его обладателю использовать произведения и объекты смежных прав. ГРУ оформляется на бланке установленного образца за подписью руководителя либо лицом, его замещающим, и заверяется гербовой печатью. Срок действия ГРУ не может превышать срока действия лицензионного договора.

8. При продлении срока действия лицензионного договора продлевается и срок действия ГРУ на основании представленного заявления и копии лицензионного договора.

Продление срока действия ГРУ осуществляется один раз и в тот же срок, что и регистрация лицензионных договоров.

**6.5** **Защита прав авторов и правообладателей**

"Человеческий гений является источником всех произведений искусства и изобретений. Эти произведения являются гарантией жизни, достойной человека. Долг государства - обеспечить надежную охрану всех видов искусства и изобретений", - гласит надпись на куполе здания штаб-квартиры Всемирной организации ИС в Женеве. Исторически ИС была и остается одним из основных и необходимых элементов прогресса и развития всего человечества.

Права на результаты интеллектуальной деятельности стимулируют авторов создавать новые произведения и изобретения, а также регулируют отношения между ними и пользователями, обеспечивая тем самым универсальную охрану интересов всех.

В пункте 2 ст. 27 Всеобщей декларации прав человека, принятой Организацией Объединенных Наций в 1948 году, установлено, что каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является.

Любое демократическое государство старается обеспечить надежную защиту прав на результаты интеллектуальной деятельности.

Защита ИС становится одним из наиболее важных факторов, которые определяют положение страны в целом. Надежный уровень защиты стимулирует научные эксперименты, развитие культуры, искусства и литературы, практическое применение достижений науки и техники, и международный обмен ими.

Особенно негативно нарушение прав ИС отражается на наиболее передовых и наукоемких отраслях, которые требуют огромных затрат на проведение научных изысканий и опытов. Контрафактная продукция, которая имеет более низкую цену, вытесняет с рынка товары разработчиков технологий, ослабляя при этом моральные и материальные стимулы для дальнейшего исследования.

Законодательство РФ и РБ предоставляет авторам и иным правообладателям достаточно широкий спектр способов защиты их прав.

Под способами защиты обычно понимают предусмотренные законодательством средства, с помощью которых могут быть достигнуты пресечение, предотвращение, устранение нарушений права, его восстановление и (или) возмещение потерь, вызванных нарушением права.

Способы защиты авторских прав в зависимости от того, к области каких правовых отношений они относятся, могут быть разделены на гражданско-правовые, административно-правовые и уголовно-правовые. Конечно, наибольшую значимость и эффективность наряду с уголовно-правовыми имеют гражданско-правовые способы защиты авторских прав.

В гражданском законодательстве можно выделить два уровня регулирования способов защиты гражданских прав.

Первый уровень заключается в определении таких способов защиты, которые носят универсальный характер и могут быть применены для защиты любого субъективного гражданского права. Данные способы перечислены в ст.12 ГК РФ. К ним относятся: признание права, самозащита права, возмещение убытков, взыскание неустойки, компенсация морального вреда.

Второй уровень представляет собой установление законом способов, применяемых для защиты только определенных видов гражданских прав или для защиты от определенных нарушений. Применительно к нарушениям авторских прав такие способы предусмотрены ст.49 Закона РФ «Об авторском праве и смежных правах» в редакции от 20.07.2004 г. Между тем, сравнительный анализ указанных норм гражданского законодательства, судебной практики свидетельствует о том, что из обычно используемых способов защиты авторских прав лишь три прямо не закреплены в ст. 12 ГК РФ (взыскание дохода, выплата компенсации, публикация судебного решения в целях защиты репутации).

Анализируя способы защиты, можно отметить, что исходными для применения являются нормы пунктов 1, 2 ст. 48 и абз. 1 п. 1 ст. 49 Закона, согласно которым за нарушение предусмотренных данным Законом авторских прав наступает гражданская, административная и уголовная ответственность. Физическое или юридическое лицо, которое не выполняет требований Закона, является нарушителем авторских прав и в отношении него могут быть применены гражданско-правовые и иные меры защиты.

Гражданско-правовые способы - правовые меры принудительного характера, восстанавливающие (признающие) нарушенные (оспариваемые) права, или пресечение такого нарушения, посредством имущественного воздействия на нарушителя прав автора или патентообладателя:

• признание права, в том числе права преждепользования;

• восстановления положения, существовавшего до нарушения права;

• прекращение действий, нарушающих право или создающих угрозу его нарушения;

• возмещение убытков, включая упущенную выгоду;

• принятие иных законных мер, связанных с защитой права.

Нарушение исключительного права - несанкционированное (патентообладателем) изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью продукта, содержащего ОИС (запатентованное изобретение, полезную модель, промыщленный образец, а также применение способа, охраняемого патентом на изобретение, или введение в хозяйственный оборот либо хранение с этой целью продукта, изготовленного непосредственно способом, охраняемым патентом на изобретение).

Уголовная ответственность за нарушение прав авторов и патентообладателей устанавливается:

в случае незаконного использования ОПС, разглашения сущности изобретения до официальной публикации, присвоение авторства, принуждения к соавторству.

Общеизвестно, что споры в области ИС относятся к делам особой сложности. Поэтому с целью обеспечения правильного и своевременного рассмотрения и разрешения споров, касающихся охраны прав в области ПС, в марте 2000 года была создана судебная коллегия по патентным делам Верховного Суда РБ.

Требование о прекращении действий, нарушающих право или создающих угрозу его нарушения, является одним из наиболее распространенных способов защиты авторских прав. Чаще всего этот способ защиты применяется в сочетании с возмещением убытков или выплатой компенсации. При этом прекращение действий, нарушающих право или создающих угрозу его нарушения, ведет к пресечению нарушения авторских прав, а возмещение убытков или выплаты компенсации направлены на предоставление правообладателям денежной компенсации за потери, которые уже были ими понесены.

Помимо требования о прекращении незаконного распространения программ или баз данных правообладатель может заявить и требования о прекращении иных действий, нарушающих его права или создающих угрозу такого нарушения (реклама контрафактных экземпляров произведений, допечатка их тиража и т.п.).

Следующим способом защиты является возмещение убытков. Под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). Обычно при нарушении авторских прав реальный ущерб отсутствует, и убытки состоят только из упущенной выгоды.

Убытки возмещаются по общему правилу в денежной форме, но по просьбе истца в счет возмещения убытков ему могут быть переданы контрафактные экземпляры произведения.

Альтернативой возмещению убытков является взыскание дохода, полученного нарушителем вследствие нарушения авторских прав. Данная мера в случае отсутствия реального ущерба практически совпадает с предыдущей, а при наличии реального ущерба становится по сравнению с ней более невыгодной. Здесь также существует проблема доказывания размера дохода нарушителя.

Наиболее действенными и востребованными практикой являются три способа защиты авторских прав: возмещение убытков, взыскание незаконно полученного дохода и выплата компенсации.

В сфере защиты авторских прав потерпевшие гораздо чаще требуют взыскать не реальный ущерб, а упущенную выгоду, которая могла бы быть получена правообладетелем в условиях нормальной реализации принадлежащих ему исключительных прав. Поскольку доказать наличие убытков и документально обосновать их размер, особенно в части упущенной выгоды, бывает не всегда просто, законодательство предоставляет возможность требовать взыскания с нарушителя либо всего дохода, полученного им вследствие нарушения авторских прав, либо требовать выплаты компенсации по своему усмотрению.

Разрешение споров в области интеллектуальной собственности

Все гражданско-правовые споры относительно ИС по процедуре урегулирования распределяются на четыре категории:

а) обязательное рассмотрение спора во внесудебном порядке, например, досрочное прекращение регистрации товарного знака, признание патента или регистрации товарного знака недействительной;

б) обязательное рассмотрение спора в судебном порядке, например, о включении в состав авторов (исключении из состава авторов) изобретения, признание патентообладателем;

в) альтернативное рассмотрение во внесудебном или судебном порядке, например дела о недобросовестной конкуренции;

г) споры, урегулирование которых возможно как в судебном или административном порядке, так и в порядке договоренности сторон (мирное урегулирование в досудебном порядке или на стадии рассмотрения в суде/административном органе).

Важнейшим элементом системы авторских правоотношений является защита авторских прав, под которой понимается юридически обеспеченная возможность применения к нарушителю материально-правовых мер принудительного характера, направленных на признание и восстановление нарушенного или оспариваемого права. Действующее отечественное законодательство предусматривает три вида ответственности за нарушение авторских прав: административную, уголовную и гражданско-правовую.

Административная ответственность за нарушение авторских прав предусмотрена ст. 167-9 «Нарушение авторских, смежных и патентных прав» Кодекса об административных правонарушениях РБ.

Уголовное законодательство Республики Беларусь предусматривает два состава преступления в области авторского права. В частности, уголовно наказуемым в соответствии со ст.201 «Нарушение авторских, смежных, изобретательских и патентных прав» Уголовного кодекса Республики Беларусь является:

\* присвоение авторства либо принуждение к соавторству (наказывается общественными работами, или штрафом, или исправительными работами на срок до двух лет);

\* незаконное распространение или иное незаконное использование объектов авторского права.., совершенное в течение года после наложения административного взыскания за такое же нарушение или сопряженное с получением дохода в крупном размере (наказывается общественными работами, или штрафом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет).

Вместе с тем закон об авторском праве и смежных правах включает достаточно большой перечень мер, направленных на защиту авторских прав. В соответствии с п.2 ст. 40 ЗоАП правообладатели в судебном порядке вправе требовать от нарушителей авторских прав совершения следующих действий.

1. Признание авторских прав. Для пресечения несанкционированного использования результата творческого труда необходимо доказать наличие исключительных прав на него. Этим доказательством может быть авторский договор между автором и правообладателем, которому передано то или иное исключительное право. На практике часты случаи присвоения авторства. В такой ситуации при доказывании приоритета нельзя игнорировать расположение на произведении знака охраны авторского права. Возможны и другие способы фиксации приоритета: высылка авторских материалов самому себе по почте и сохранение закрытого конверта до возникновения спорной ситуации, регистрация произведения у нотариуса, хранение подлинника в депозитном хранилище и др.

2. Восстановление положения, существовавшего до нарушения авторского права. Данную форму защиты в полной мере можно использовать только для защиты произведения от искажения. Например, автор, обнаружив, что без его ведома внесены изменения, вправе потребовать восстановления формы своего произведения. Этот вид защиты эффективен лишь до обнародования результата творческого труда. В противном случае восстановить положение, существовавшее до нарушения авторского права, практически невозможно.

3. Пресечение действий, нарушающих авторские права или создающих угрозу их нарушения. Данная мера, как правило, применяется в сочетании с другими способами защиты. При этом правообладатели требуют запретить бездоговорному пользователю дальнейшее использование тех или иных результатов творческого труда.

Пресекаются действия, нарушающие авторские права или создающие угрозу их нарушения, путем обеспечения иска.

4. Возмещение убытков, включая упущенную выгоду. В основе этой формы защиты лежит общий гражданско-правовой принцип полного возмещения причиненных убытков. В соответствии со ст.14 ГК РБ под убытками понимаются:

\* расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение имущества (реальный ущерб);

\* неполученные доходы, которое это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

5. Выплата компенсации. По общему правилу на лице, чьи права нарушены, лежит бремя доказательства как самого факта нарушения авторских прав, так и размера понесенных в этом случае убытков. Иногда определить величину убытков крайне сложно. Это связано с тем, что «пираты» при изготовлении контрафактной продукции не ведут бухгалтерию и не платят налоги. Нельзя получить учетную документацию ни от нарушителя, ни от налоговых и статистических органов. Поэтому для обеспечения эффективной защиты авторских прав законодатель ввел возможность выплаты денежной компенсации. Размер ее может составлять от 10 до 50 тыс. минимальных заработных плат. Компенсация, как правило, рассчитывается на основании величины предполагаемых убытков.

Досудебное урегулирование споров по вопросам охраноспособности объектов промышленной собственности в патентном органе

Дела, рассматриваемые во внесудебном или судебном порядке, подразделяются на две основные группы:

* защита нарушенного права,
* защита от притязаний, в т.ч. необоснованных притязаний третьих лиц.

Обе эти группы дел, в равной мере сложны и процедурно оформляются одинаково, опыт ведения дел одной группы может эффективно использоваться при ведении дел другой группы.

Досудебное урегулирование споров по вопросам охраноспособности ОПС в РБ осуществляет Апелляционный совет как специализированное подразделение НЦИС.

В своей деятельности Апелляционный совет руководствуется Конституцией РБ, иными актами законодательства РБ, международными договорами и соглашениями РБ в области охраны ОПС, а также Положением об Апелляционном совете при патентном органе.

Основными задачами Апелляционного совета являются:

1. Досудебное урегулирование споров по вопросам охраноспособности ОПС РБ, вынесение решений по рассмотренным жалобам, возражениям и заявлениям;

2. Обеспечение охраняемых законом прав заявителей, патентообладателей, владельцев товарных знаков и знаков обслуживания, обладателей прав на топологии интегральных микросхем, интересов иных физических и юридических лиц при рассмотрении жалоб, возражений и заявлений;

3. Разработка предложений по совершенствованию законодательства в области ОПС на основе практики рассмотрения жалоб, возражений и заявлений;

4. Совершенствование порядка рассмотрения споров на основе анализа практики их рассмотрения в Апелляционном совете и международной практики.

В соответствии с возложенными на него задачами Апелляционный совет:

1. Рассматривает жалобы физических и юридических лиц:

a. На решение предварительной экспертизы об отказе в выдаче патента на изобретение;

b. На решение предварительной экспертизы по заявке на регистрацию товарного знака об отказе в принятии к рассмотрению заявки или о принятии к рассмотрению заявки с измененным перечнем товаров и (или) услуг, для которых испрашивалась регистрация;

c. На решение патентной экспертизы об отказе в выдаче патента на изобретение, промышленный образец, сорт растения;

d. На решение экспертизы об отказе в регистрации товарного знака в отношении заявленных товаров и (или) услуг, принятое по результатам повторной экспертизы;

e. На решение экспертизы о регистрации товарного знака в отношении части товаров и (или) услуг, принятое по результатам повторной экспертизы;

f. На решение предварительной экспертизы об отказе в принятии к рассмотрению заявки на регистрацию и предоставление права пользования наименованием места происхождения товара;

g. На решение об отказе в регистрации наименования места происхождения товара и предоставлении права пользования им;

h. На решение об отказе в предоставлении права пользования уже зарегистрированным наименованием места происхождения товара;

i. На решение экспертизы об отказе в регистрации топологии интегральной микросхемы;

2. Рассматривает возражения физических и юридических лиц:

a. На решение предварительной экспертизы об отказе в принятии к рассмотрению заявки на сорт растения;

b. Против выдачи патента на изобретение, патента на полезную модель, патента на промышленный образец, патента на сорт растения;

c. Против регистрации товарного знака;

d. Против регистрации наименования места происхождения товара;

e. Против выдачи свидетельства на право пользования наименованием места происхождения товара;

3. Рассматривает заявления физических и юридических лиц:

a. О признании товарного знака общеизвестным в РБ;

b. О прекращении действия регистрации наименования места происхождения товара и свидетельства на право пользования им;

4. Рассматривает иные жалобы, возражения и заявления, если их рассмотрение отнесено к компетенции Апелляционного совета законодательством РБ;

5. По результатам рассмотрения жалоб, возражений и заявлений выносит решения в соответствии с законодательством РБ.

- Решение Апелляционного совета может быть обжаловано в порядке, установленном законодательством РБ;

6. Разрабатывает в пределах своей компетенции информационные письма и иные необходимые документы по ведению дел Апелляционным советом;

7. Вносит в установленном порядке предложения по совершенствованию правового регулирования экспертизы заявок на выдачу патентов на изобретение, полезную модель, промышленный образец, сорт растения, на регистрацию товарного знака, знака обслуживания и на предоставление правовой охраны иным объектам ПС, а также порядка рассмотрения жалоб, возражений и заявлений Апелляционным советом;

8. Готовит ежегодные публикации о результатах своей деятельности в официальных изданиях НЦИС;

9. Готовит и реализует предложения по совершенствованию своей структуры, улучшению организации и технологии своей работы;

10. Для решения стоящих перед ним задач и осуществления своей деятельности взаимодействует со структурными подразделениями НЦИС и организациями по вопросам, отнесенным к его компетенции.

Нарушения прав интеллектуальной собственности

Результаты интеллектуальной деятельности могут быть использованы третьими лицами только с согласия правообладателя. В противном случае речь пойдет о нарушении исключительных прав.

Правовая охрана промышленной собственности — крупный и специфический пласт юридической деятельности. Обратимся к части, касающейся гражданской ответственности за нарушение прав на результаты интеллектуальной деятельности, говоря о которых, мы будем иметь в виду не только продукты непосредственно умственного и творческого труда, такие, как изобретения, полезные модели и промышленные образцы, но и средства индивидуализации продукции, работ, услуг, то есть товарные знаки (знаки обслуживания).

Действующим законодательством установлено, что материальные права на эти объекты принадлежат физическим и юридическим лицам, владеющим соответствующим охранным документом, патентом (на изобретение, полезную модель и промышленный образец) или свидетельством на товарный знак (знак обслуживания).

1. Нарушением прав ИС признается любое действие, которое приводит или может привести к нарушению исключительных имущественных или личных неимущественных прав на ОИС.

2. Контрафактными экземплярами признаются материальные носители результатов интеллектуальной деятельности или средств индивидуализации, изготовление, распространение или иное использование, а также импорт или хранение которых приводят или могут привести к нарушению прав ИС.

3. Контрафактные экземпляры подлежат конфискации по решению суда (статья 243).

Законом могут быть предусмотрены случаи конфискации материалов и оборудования, используемых для изготовления контрафактных экземпляров.

За несоблюдение интересов обладателей прав на промышленную собственность как Патентный закон РБ, так и Закон РБ «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» предусматривают такие виды ответственности, как гражданская, административная и уголовная. Однако если первый говорит лишь о возможности применения этих наказаний, по сути, отсылая к другим законодательным нормам, в частности, Гражданского, Административного и Уголовного кодексов, то Закон о товарных знаках помимо простого указания видов ответственности содержит подробный перечень мер гражданско-правового воздействия на нарушителей, который шире приведенного в ГК РБ.

Итак, если вы являетесь обладателем охранного документа на изобретение, полезную модель, промышленный образец или товарный знак, это означает, что вам принадлежат исключительные права на эти объекты промышленной собственности. В случае нарушений вы сможете их защитить, обратившись к патентным поверенным, а также в суд или другие правоохранительные органы.

Гражданско-правовые способы защиты прав авторов и правообладателей

Нормальный гражданский оборот предполагает не только признание за субъектами определенных гражданских прав, но и обеспечение их надежной правовой охраной. В соответствии со сложившейся в науке традицией понятием «охрана гражданских прав» охватывается вся совокупность мер, обеспечивающих нормальный ход реализации прав. В него включаются меры не только правового, но и экономического, политического, организационного и иного характера, направленные на создание необходимых условий для осуществления субъективных прав. Что касается собственно правовых мер охраны, то к ним относятся все меры, с помощью которых обеспечивается как развитие гражданских правоотношений в их нормальном, ненарушенном состоянии, например закрепление гражданской право-, дееспособности субъектов, установление обязанностей ит.п., так и восстановление нарушенных или оспоренных прав и интересов.

Наряду с таким широким пониманием охраны в науке и законодательстве используется и понятие охраны в узком смысле слова. В этом случае в него включаются лишь те, предусмотренные законом меры, которые направлены на восстановление или признание гражданских прав и защиту интересов при их нарушении или оспаривании. В целях избегания терминологической путаницы охрану в узком значении этого слова принято именовать защитой гражданских прав.

В общем виде право на защиту можно определить как предоставленную правомочному лицу возможность применения мер правоохранительного характера для восстановления его нарушенного или оспариваемого права. Согласно традиционной концепции право на защиту является составной частью самого субъективного права наряду с правом на собственные действия, а также правом требовать определенного поведения от обязанных лиц.

Предметом защиты являются не только субъективные гражданские права, но и охраняемые законом интересы. Субъективное гражданское право и охраняемый законом интерес являются очень близкими и зачастую совпадающими правовыми категориями, в связи с чем они не всегда разграничиваются в литературе. В основе всякого субъективного права лежит тот или иной интерес, для удовлетворения которого субъективное право и предоставляется правомочному лицу. Одновременно охраняемые интересы в большинстве случаев опосредуются конкретными субъективными правами, в связи с чем защита субъективного права представляет собой и защиту охраняемого законом интереса.

Формы и способы защиты гражданских прав

Защита субъективных гражданских прав и охраняемых законом интересов осуществляется в предусмотренном законом порядке, т.е. посредством применения надлежащей формы, средств и способов защиты. Под формой защиты понимается комплекс внутренне согласованных организованных мероприятий по защите субъективных прав и охраняемых законом интересов. Различаются две основные формы защиты - юрисдикционная и неюрисдикционная.

Юрисдикционная форма защиты есть деятельность уполномоченных государством органов по защите нарушенных или оспариваемых субъективных прав. Суть её выражается в том, что лицо, права и законные интересы которого нарушены неправомерными действиями, обращается за защитой к государственным или иным компетентным органам (в суд, арбитражный, третейский суд, вышестоящую инстанцию и т.д.), которые уполномочены принять необходимые меры для восстановления нарушенного права и пресечения правонарушения.

В рамках юрисдикционной формы защиты, в свою очередь, выделяются общий и специальный порядок защиты нарушенных прав. По общему правилу, защита гражданских прав и охраняемых законом интересов осуществляются в судебном порядке. Основная масса гражданско-правовых споров рассматривается районными, городскими, областными и иными судами общей компетенции. Наряду с ними судебную власть осуществляют арбитражные суды, которые разрешают споры, возникающие в процессе предпринимательской деятельности.

В качестве средства защиты гражданских прав и охраняемых законом интересов выступает, по общему правилу, иск, т.е. обращенное к суду требование об отправление правосудия, с одной стороны, и обращенное к ответчику материально-правовое требование о выполнение лежащей на нем обязанности или о признании наличия или отсутствия правоотношения, с другой стороны.

Специальным порядком защиты гражданских прав и охраняемых законом интересов следует признать административный порядок их защиты. Он применяется в виде исключения из общего правила, т.е. только в прямо указанных в законе случаях. Средством защиты гражданских прав, осуществляемой в административном порядке, является жалоба, подаваемая в соответствующий управленческий орган лицом, права и законные интересы которого пострадали в результате правонарушения.

В некоторых случаях в соответствие с законом применяется смешанный, т.е. административно-судебный порядок защиты нарушенных гражданских прав. В этом случае потерпевший, прежде чем предъявить иск в суд, должен обратиться с жалобой в государственный орган управления. В таком порядке разрешаются, например, отдельные споры патентного характера, некоторые дела, возникающие из правоотношений в сфере управления, и др.

Неюрисдикционая форма защиты охватывает собой действия граждан и организаций по защите гражданских прав и охраняемых законом интересов, которые совершаются ими самостоятельно, без обращения за помощью к государству или иным компетентным органам. В гражданском кодексе указанные действия объединены в понятие самозащита гражданских прав и рассматриваются в качестве одного из способов защиты гражданских прав.

Защита гражданских прав и охраняемых законом интересов обеспечивается применением предусмотренных законом способов защиты.

Под способами защиты субъективных гражданских прав понимаются закрепленные законом материально-правовые меры принудительного характера, посредством которых производится восстановление (признание) нарушенных (оспариваемых) прав и воздействие на правонарушителя. Общий перечень этих мер даётся в ГК РБ, где говориться «защита гражданских прав осуществляется путём:

·- признания права;

·- восстановления положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения;

·- признание оспоримой сделки недействительной и применения последствий её недействительности, применения последствий недействительности ничтожной сделки;

·- признание недействительным акта государственного органа или органа местного самоуправления;

·- самозащиты права;

·- присуждение к исполнению обязанностей в натуре;

·- возмещение убытков;

·- взыскание неустойки;

·- компенсации морального вреда;

·- прекращение или изменение правоотношения;

·- неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону;

·- иными способами, предусмотренными законом».

Как правило, обладатель нарушенного права может воспользоваться не любым, а вполне конкретным способом защиты своего права. Зачастую способ защиты нарушенного права прямо определен специальным законом, регламентирующим конкретное гражданское правоотношение. Наибольшую практическую значимость при этом имеет то обстоятельство, что, по общему правилу, меры ответственности, в отличие от мер защиты, применяются лишь к виновному нарушителю субъективного права и выражаются в дополнительных обременениях в виде лишения правонарушителя определенных прав и возложение на него дополнительных обязанностей. Среди способов защиты гражданских прав мерами ответственности могут быть признаны лишь возмещение убытков, взыскание неустойки и компенсация морального вреда; все остальные являются мерами защиты.

Восстановление положения, существовавшего до нарушения права, как самостоятельный способ защиты применяется в тех случаях, когда нарушенное регулятивное субъективное право в результате правонарушения не прекращает своего существования и может быть реально восстановлено путем устранения последствий правонарушения. Восстановление положения, существовавшего до нарушения права, может происходить посредством применения как юрисдикционного, так и неюрисдикционного порядка защиты.

Распространенным способом защиты субъективных прав является пресечение действий, нарушающих право или создающих угрозу его нарушения. Как и признание права, данный способ защиты может применяться в сочетании с другими способами защиты, например взысканием убытков или неустойки, или иметь самостоятельное значение.

Признание оспоримой сделки недействительной и применение последствий ее недействительности, применение последствий недействительности ничтожной сделки представляют собой частые случаи реализации такого способа защиты, как восстановление положения, существовавшего до нарушения права, так как совпадают с ним по правовой сущности. Наиболее очевидным это является при приведение сторон, совершивших недействительную сделку, в первоначальное положение.

Защита прав и охраняемых законом интересов граждан и юридических лиц может осуществляться путем признания недействительным акта государственного органа или органа местного самоуправления. Это означает, что гражданин или юридическое лицо, гражданские права или охраняемые законом интересы которого нарушены изданием не соответствующего закону или иным правовым актам административного акта, а в случаях предусмотренных законом, - и нормативного акта, имеют право на их обжалование в суд.

К рассмотренному способу защиты близко примыкает и такой способ защиты гражданских прав, как неприменение судом акта государственного органа или органа местного самоуправления, противоречащего закону.

Присуждение к исполнению обязанности в натуре, нередко именуется в литературе еще реальным исполнением, как самостоятельный способ защиты гражданских прав характеризуется тем, что нарушитель по требованию потерпевшего должен реально выполнить те действия, которые он обязан совершить в силу обязательства, связывающего стороны.

Возмещение убытков и взыскание неустойки представляют собой наиболее распространенные способы защиты гражданских прав и охраняемых законом интересов, которые применяются в сфере как договорных, так и внедоговорных отношений. В данном случае имущественный интерес потерпевшего удовлетворяется за счет денежной компенсации понесенных им имущественных потерь. При этом такая компенсация может быть либо прямо указана с размером причиненного вреда (возмещение убытков), либо связана с ними лишь косвенным образом или вообще независима от него (взыскание неустойки). Основной формой компенсации причиненного потерпевшему ущерба является возмещение убытков; взыскание неустойки (штрафа) производиться в случаях прямо предусмотренных законом или договором. Под убытками понимаются расходы, которые лицо, чьё право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение имущества (реальный ущерб), а также неполученные доходы, которые лицо получило бы при обычных условия гражданского оборота, если бы его право не было нарушено (упущенная выгода).

Такой способ защиты гражданских прав, как компенсация морального вреда, состоит в возложении на нарушителя обязанности по выплате потерпевшему денежной компенсации за физические или нравственные страдания, которые тот испытывает в связи с нарушением его прав. Применение данного способа защиты ограничивается двумя основными обстоятельствами. Во-первых, требование о компенсации морального вреда могут быть заявлены только конкретными гражданами, т.к. юридические лица физических и нравственных страданий испытывать не могут. Вопрос о возмещение вреда, причиненного деловой репутации юридического лица, лежит в несколько иной плоскости. Во-вторых, нарушенные права должны носить, по общему правилу, личный неимущественный характер.

Административная и уголовная ответственность за нарушение авторских, смежных и патентных прав

Специальным порядком защиты авторских и смежных прав и охраняемых законом интересов, следует признать административный порядок их защиты. Он применяется в виде исключения из общего правила, т.е. только в прямо указанных в законе случаях. Средством защиты авторских и смежных прав, осуществляемой в административном порядке, является жалоба, подаваемая в соответствующий управленческий орган лицом, права и законные интересы которого пострадали в результате правонарушения со стороны иного физического или юридического лица.

В некоторых случаях в соответствии с законом применяется смешанный, т.е. административно-судебный порядок защиты нарушенных авторских и смежных прав. В этом случае потерпевший прежде, чем подать иск в суд, должен обратиться с жалобой в государственный орган управления.

Административные способы защиты ИС

Гражданским законодательством допускается защита гражданских прав в административной форме, но лишь в случаях, предусмотренных законом.

В настоящее время авторское законодательство прямо не предусматривает таких случаев. Однако в данной форме могут защищены не все права, а лишь те, реализация которых возложена на то или иное звено исполнительной власти.

Возможность защиты должна быть предусмотрена компетенцией органов управления. Принципиальное значение имеет то обстоятельство, что любое решение, вынесенное при разрешении спора в административном порядке, может быть оспорено в суде. Средством защиты при использовании административной формы является жалоба или заявление.

В НЦИС могут быть поданы в соответствии с Патентным законом РБ, Законом РБ "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров" и международными договорами РБ следующие возражения и заявления.

1.1. Возражение на решение об отказе в выдаче патента на ОИС.

1.2. Возражение на решение о признании заявки на ОИС отозванной.

1.3. Возражение против выдачи патента на ОИС.

1.4. Возражение против действия на территории РФ, РБ ранее выданного авторского свидетельства или патента СССР на изобретение, свидетельства или патента СССР на промышленный образец, евразийского патента на изобретение, выданного в соответствии с Евразийской патентной конвенцией от 9 сентября 1994 года.

1.5. Возражение на решение, принятое по результатам формальной экспертизы заявки на регистрацию товарного знака и знака обслуживания, регистрацию и предоставление права пользования наименованием места происхождения товаров или на предоставление права пользования уже зарегистрированным наименованием места происхождения товара, об отказе в принятии ее к рассмотрению.

1.6. Возражение на решение экспертизы заявленного обозначения по заявке на регистрацию товарного знака, регистрацию и предоставление права пользования наименованием места происхождения товаров или на предоставление права пользования уже зарегистрированным наименованием места происхождения товара, а также на решение о предоставлении или об отказе в предоставлении охраны, осуществленной в соответствии с Мадридским соглашением о международной регистрации знаков от 14 апреля 1891 г., пересмотренное в Брюсселе 14 декабря 1900 г., в Вашингтоне 2 июня 1911 г., в Гааге 6 ноября 1925 г., в Лондоне 2 июня 1934 г., в Ницце 15 июля 1957 г. и в Стокгольме 14 июля 1967 г. и измененное 28 сентября 1979 г. или Протоколом к Мадридскому соглашению о международной регистрации знаков, принятым в Мадриде 27 июня 1989 г.

1.7. Возражение на решение о признании отозванной заявки на регистрацию товарного знака, регистрацию и предоставление права пользования наименованием места происхождения товаров или на предоставление права пользования уже зарегистрированным наименованием места происхождения товара.

1.8. Возражение против предоставления правовой охраны товарному знаку, наименованию места происхождения товара, выдачи свидетельства на право пользования наименованием места происхождения товара, против действия на территории РФ произведенной в СССР регистрации товарного знака, знака обслуживания, а также против предоставления охраны международной регистрации знака на территории РФ.

1.9. Возражение против предоставления правовой охраны товарному знаку на имя агента или представителя лица, которое является обладателем исключительного права на этот товарный знак в одном из государств - участников Парижской конвенции по охране ПС от 20 марта 1883 года.

1.10. Заявление о признании товарного знака общеизвестным в Российской Федерации.

1.11. Заявление о досрочном прекращении правовой охраны товарного знака в случае превращения зарегистрированного товарного знака в обозначение, вошедшее во всеобщее употребление как обозначение товаров определенного вида.

1.12. Заявление о досрочном прекращении правовой охраны товарного знака, а также о досрочном прекращении правовой охраны международной регистрации знака на территории РФ в связи с неиспользованием товарного знака непрерывно в течение любых трех лет после его регистрации или предоставления правовой охраны международной регистрации знака на территории РФ.

1.13. Заявление о прекращении правовой охраны наименования места происхождения товара и действия свидетельства на право пользования им или о прекращении действия свидетельства на право пользования наименованием места происхождения товара.

1.14. Возражение против предоставления правовой охраны общеизвестному в РФ товарному знаку.

По результатам рассмотрения возражения НЦИС может принять решение о его удовлетворении, об отказе в удовлетворении, о прекращении делопроизводства. При этом решение может предусматривать отмену, изменение или оставление в силе оспариваемого решения.

Решения Палаты могут быть обжалованы в суде (п.9 ст.21, п.2 ст.29 Патентного закона).

Судебный порядок рассмотрения споров в области интеллектуальной собственности

Признание права осуществляется через обращение в суд, который должен подтвердить наличие или отсутствие у истца данного права. Например, это способ защиты применяется в случае, если оспаривается само наличие у субъекта авторских прав или принадлежность авторских прав не определена (например, при анонимном опубликовании произведения) или, иск о признании права авторства на созданное изобретение.

Снятие такой неопределенности, создание условий для реализации всех прав субъекта и предупреждение со стороны третьих лиц действий, препятствующих осуществлению таких прав, является целями применения обращения в суд.

Требование о признании права, может относиться, к личным неимущественным правам автора, к имущественным правам или ко всей совокупности авторских прав. В случае если оспаривание права сопровождалось его нарушением, суд может обязать нарушителя сделать за свой счет объявление о существовании определенного права и его принадлежности.

Судебная практика показывает, что требование о выплате компенсации является одним из самых распространенных способов защиты нарушенных авторских прав. Популярность этого способа защиты объясняется именно тем обстоятельством, что дает возможность предъявления требований о выплате компенсации и освобождает истца от обязанности доказывания точных размеров своих убытков или доходов ответчика. Для присуждения компенсации достаточно доказать факт наличия убытков, а их размеры могут быть оценены приблизительно, при этом не требуется документального подтверждения размеров убытков. При отсутствии убытков компенсация не выплачивается.

Истец по своему усмотрению может требовать от нарушителя либо возмещения убытков, включая упущенную выгоду, либо взыскания доходов, полученных ответчиком в результате нарушений, либо выплаты компенсации.

Защиту нарушенных или оспоренных гражданских прав осуществляет в соответствии с подведомственностью дел, установленной процессуальным законодательством, суд, арбитражный суд или третейский суд в области разрешения споров по сделкам международного характера (международный коммерческий арбитраж).

В соответствии с Федеральным конституционным законом РФ от 31 декабря 1996 г. "О судебной системе РФ " правосудие в РФ осуществляется только судами.

Согласно п.4 Федерального конституционного закона к федеральным судам отнесены: Конституционный Суд РФ; Верховный Суд РФ и составляющие его систему федеральные суды общей юрисдикции; Высший Арбитражный Суд РФ и составляющие его систему федеральные арбитражные суды. Суды осуществляют судебную власть в РФ.

Третейские суды не входят в судебную систему, они осуществляют защиту в соответствии с Федеральным законом РФ "О третейских судах в РФ" от 4 июля 2002 года N 102-ФЗ. Спор на разрешение третейского суда может быть передан лишь при наличии соглашения об этом сторон спорного правоотношения. Выбор между государственными судами и третейским судом предоставлен спорящим сторонам.

Подведомственность дел каждому из судов определяется: Федеральным конституционным законом "О Конституционном Суде РФ", Гражданским процессуальным кодексом (ГПК), Арбитражным процессуальным кодексом (АПК).

Для разграничения компетенции судов общей юрисдикции и арбитражных судов в процессуальном законодательстве использованы два критерия: субъективный состав спорящих сторон и (или) характер правоотношений, из которых возникает спор. Прежде всего, подведомственность спора предопределена субъектами спорных правоотношений. Суды общей юрисдикции в соответствии со ст. 22 ГПК РФ рассматривают и разрешают исковые дела с участием граждан, организаций, органов государственной власти, органов местного самоуправления о защите нарушенных или оспариваемых прав, свобод и законных интересов, по спорам, возникающим из гражданских, семейных, трудовых, жилищных, земельных, экологических и иных правоотношений. Споры в сфере предпринимательской и иной экономической деятельности осуществляются арбитражными судами.

Патентно-правовые споры могут рассматриваться в суде общей юрисдикции и в арбитражных судах в соответствии с правилами о подведомственности и подсудности, в т.ч. и на рассмотрение третейского суда.

Традиционно споры об авторских правах в арбитражной практике считаются наиболее трудными.

В соответствии со ст. 31 Патентного закона РФ в судебном порядке рассматриваются следующие споры:

- об авторстве изобретения, полезной модели, промышленного образца;

- об установлении патентообладателя;

- о нарушении исключительного права на изобретение, полезную модель, промышленный образец;

- о заключении и об исполнении договоров о передаче исключительного права (уступке патента) и лицензионных договоров на использование изобретения, полезной модели, промышленного образца;

- о праве преждепользования;

- о праве послепользования;

- о размере, сроке и порядке выплаты вознаграждения автору изобретения, полезной модели, промышленного образца в соответствии с настоящим Законом;

- о размере, сроке и порядке выплаты компенсаций, предусмотренных настоящим Законом;

- другие споры, связанные с охраной прав, удостоверяемых патентом.

Защита патентных прав может осуществляться любыми предусмотренными законом способами. Вместе с тем Патентный закон (ст.14) устанавливает три способа, которые используются наиболее часто:

1. Прекращение нарушения патента;

2. Возмещение лицом, виновным в нарушении патента, причиненных убытков;

3. Публикация решения суда в целях защиты деловой репутации.

Патент на изобретение, полезную модель или промышленный образец признается недействительным полностью или частично на основании принятого по возражению решения патентного органа или вступившего в законную силу решения суда, в том числе решения суда, принятого по результатам рассмотрения спора об авторстве.

Полномочия Конституционного Суда РФ установлены ст.3 Федерального конституционного закона от 21 июля 1994 г. "О Конституционном Суде РФ". К ним отнесена проверка конституционности закона, примененного или подлежащего применению в конкретном деле. Проверка осуществляется по жалобам граждан на нарушение конституционных прав и свобод и по запросам судов.

Как программисты могут защищать свои авторские права?

В отличие от музыки и стихов, которые сегодня пишут все, кому не лень, причем считая себя в этом большими специалистами, программирование имеет свою специфику. Людей, способных написать работающую программу (неважно - хорошую или плохую, удобную или никому не нужную) гораздо меньше, чем людей, которые могут связать несколько слов в предложение или с помощью специальных программ и инструментов сочинить нечто похожее на музыку.

Речь идет о профессиональных и состоявшихся программистах, могущих сотворить нечто такое, чего не могут программисты средней руки. Новичкам, как и везде, сложнее "выбить" для себя идеальные условия, поскольку им сложнее доказать, что найти им адекватную замену работодатель (или пользователь) не сможет. В этом случае основной целью такого новичка является не получить наиболее выгодные условия использования первой его программы, а доказать, что он классный специалист, который, несмотря на свой еще небольшой опыт, заткнет за пояс очень многих.

Как и в случае любого другого договора, прежде всего Вам надо решить, что Вы хотите получить: признание, возможность карьерного роста, разовую выплату или проценты с коммерческой реализации Ваших программ. Исходя из этого - займите позицию в переговорах.

Какое все это имеет отношение к авторскому праву. Авторское право как таковое имеет одну цель: защитить авторов тогда, когда контроль за созданным ими произведениями утрачен, когда ничто, кроме соответствующего законодательства, не может помешать любому использовать то или иное произведение. Контроль над произведением утрачивается сразу, как только с произведением знакомится кто-то помимо самого автора. Потом, если нет соответствующего законодательного запрета, с произведением можно сделать все, что угодно.

Именно поэтому наиболее эффективно защитить свои права можно тогда, когда контроль над произведением еще не утрачен, т.е. до создания (или передачи прав на) произведения заключив с работодателем (пользователем) договор, в котором будут четко оговорены все устраивающие Вас условия. В этом случае крайне важно, чтобы подписываемый Вами договор был грамотно составлен.

Если Вы идете наниматься на постоянную работу программистом, постарайтесь предвидеть, что бы Вы хотели получать, в случае если созданный Вами в будущем продукт получит широкое распространение. Если чувствуете в себе силы - настаивайте на заключении с Вами дополнительного соглашения о правилах использования созданных Вами программ. Вероятность того, что работодатель согласится на Ваши условия, конечно, невелика, но все может быть!

Какой минимум защиты предоставляет программистам Российское (Белорусское) законодательство? Вы всегда вправе настаивать на заключении договора на более выгодных условиях.

Компьютерные программы приравниваются законодательством большинства государств к литературным произведениям, вне зависимости от того, на каком программном языке и в какой форме (исходный текст или объектный код) написана программа. Отношения в связи с созданием и использованием программ регулируются Законом РФ "О правовой охране программ для электронных вычислительных машин и баз данных" 1992 г.

Огромное значение имеет то обстоятельство, пишете ли Вы программу для себя или это входит в круг Ваших обычных служебных обязанностей. При прочих равных (т.е. при отсутствии договора об ином) - если Вы пишете программу самостоятельно, то первичные имущественные права принадлежат Вам, но если Ваша деятельность по написанию программы входит в круг Ваших служебных обязанностей, то первичными исключительными имущественными правами на использование Вашей программы будет обладать Ваш работодатель. Нельзя полагать, что если между Вами и работодателем не заключено вообще никакого соглашения, то Ваша позиция окажется более прочной. Если работодатель докажет трудовой характер существующих между вами отношений, то будет считаться, что Вы написали программу в рамках служебных обязанностей, и, следовательно, все права автоматически будут признаваться за работодателем.

Эти имущественные права включают в себя право на выпуск в свет программы, ее воспроизведение в любой форме, ее распространение, а также модификацию программы или любое иное использование программы. Если все исключительные права на использование программы будут принадлежать Вашему работодателю, то именно он будет принимать решение о том, выпускать ли Вашу программу, на каких условиях и т.п. Если у Вас нет дополнительного соглашения с работодателем, то ничего, кроме заработной платы, установленной Вам по трудовому договору, за использование программы Вам причитаться не будет. Более того, работодатель будет иметь полное право похоронить Вашу программу и вообще никогда ее не выпустить и не разрешить ее выпуск Вам.

Независимо от того, кому принадлежат права на использование произведения, создателю программы (т.е. физическому лицу, творческим трудом которого создана программа или ее часть) принадлежат следующие личные неимущественные права: право признаваться автором программы, право определять форму указания имени автора программы (в форме подлинного имени, в форме псевдонима или анонимно), а также право на неприкосновенность (целостность) программы.

Вне зависимости от того, кому принадлежат исключительные права на использование программы, и от того, что записано в Вашем договоре, никто не вправе Вам запретить разрабатывать другую программу на ту же тему. Главное, чтобы в ней не было такого количества текстовых сходств с оригиналом программы, которое бы давало правообладателю основания заявить, что при создании новой программы Вы использовали принадлежащий правообладателю объект авторского права. Если Вы пишете программу для себя, то наилучшим способом доказать, что она создана именно Вами, является запись программы на CD-R (который, естественно, надо полностью закрыть) и последующая отправка этого CD-R себе самому по почте заказным письмом. Конверт вскрывать не надо. Главное, что на нем будет отметка почты о дате отправления, а внутри будет находиться объективное доказательство тому, что такая программа есть.

Отдельно хочется сказать о регистрации программ в Агентстве, о чем говорится в ст. 13 Закона. Действительно, правообладатель всех имущественных прав на программу для ЭВМ или базу данных непосредственно или через своего представителя в течение срока действия авторского права может по своему желанию зарегистрировать программу для ЭВМ или базу данных путем подачи заявки в Российское агентство по правовой охране программ для ЭВМ, баз данных и топологии интегральных микросхем.

Вместе с этим, ст. 4 того же Закона содержит четкое указание на то, что "авторское право на программу для ЭВМ или базу данных возникает в силу их создания. Для признания и осуществления авторского права на программу для ЭВМ или базу данных не требуется депонирования, регистрации или соблюдения иных формальностей".

Таким образом, регистрация программы в Агентстве является лишь дополнительным средством для защиты прав в отношении программы. Преимуществом такой регистрации является возможность правообладателя ссылаться на такую регистрацию для доказывания своих прав на ту или иную программу. Однако, необходимо подчеркнуть, что, несмотря на то, что регистрация, безусловно, имеет свои преимущества, отсутствие регистрации не может служить основанием для отказа в иске.

За защитой своего права правообладатели могут обратиться в суд, арбитражный или третейский суд.

Гражданские дела по спорам, вытекающим из применения законодательства об авторском праве рассматривает Судебная коллегия по делам интеллектуальной собственности Верховного Суда РБ.

Органы и организации, имеющие право проверять соблюдение авторских прав

* милиция (криминальная (УБЭП, УСТМ), милиция общественной безопасности),
* антимонопольные органы,
* таможенные органы,
* государственные инспекции и надзоры (например, торгинспекция, госсвязьнадзор),
* общества потребителей,
* сами правообладатели (в порядке обеспечения доказательств).

Кто несет ответственность?

* уголовная ответственность - непосредственный нарушитель, должностное лицо (руководитель),
* административная ответственность - непосредственный нарушитель, должностное лицо, юридическое лицо,
* налоговая ответственность - должностное лицо, юридическое лицо,
* гражданско-правовая ответственность - непосредственный нарушитель (суд общей юрисдикции), юридическое лицо (арбитражный суд).

В соответствии со статьей 40 «Защита авторского права и смежных прав» Закона РБ «Об авторском праве и смежных правах» правообладатели вправе требовать: пресечения действий, нарушающих авторские или смежные права или создающих угрозу их нарушения, возмещения убытков, взыскания дохода, полученного нарушителем вследствие нарушения авторского права и смежных прав, выплаты компенсации, принятия иных предусмотренных законодательными актами мер, связанных с защитой авторского или смежных прав.

В соответствии со статьей 201 «Нарушение авторских, смежных, изобретательских и патентных прав» Уголовного кодекса Республики Беларусь присвоение авторства либо принуждение к соавторству, а равно разглашение без согласия автора или заявителя сущности изобретения, полезной модели, промышленного образца или иного объекта права ПС до официальной публикации сведений о них - наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет. Незаконное распространение или иное незаконное использование объектов авторского права, смежных прав или объектов права ПС, совершенные в течение года после наложения административного взыскания за такое же нарушение или сопряженные с получением дохода в крупном размере, - наказываются общественными работами, или штрафом, или ограничением свободы на срок до трех лет, или лишением свободы на срок до двух лет.

В соответствии со статьей 167/9 «Нарушение авторских, смежных и патентных прав» Кодекса РБ об административных правонарушениях незаконное распространение или иное незаконное использование объектов авторского права, смежных прав или объектов промышленной собственности, а также сорта растения или топологии интегральной микросхемы - влечет наложение штрафа в размере до пятидесяти минимальных заработных плат с конфискацией контрафактных экземпляров объектов авторского права, смежных и патентных прав, а также материалов и оборудования, используемых для их изготовления, или без конфискации.