**1. Методология информационной безопасности. Наиболее острые проблемы развития теории и практики информационной безопасности.**

Наиболее острые проблемы развития теории и практики информационной безопасности:

* создание теоретических основ и формирование научно-методологического базиса;
* разработка научно-обоснованных нормативно-методических документов;
* стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектах на региональном и государственном уровнях.

**2. Методология информационной безопасности. Основные определения: защита информации, безопасность информации и т.д.**

**Информационная безопасность** – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Под **защитой информации в узком смысле** будем понимать совокупность мероприятий и действий, направленных на обеспечение ее (информации) безопасности – конфиденциальности и целостности - в процессе сбора, передачи, обработки и хранения. Это определение подразумевает тождественность понятий защита информации и обеспечение безопасности информации.

Под **защитой информации**, **в более широком смысле**, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Сущность защиты информации состоит в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию. Эти источники составляют угрозу безопасности информации. Цели и методы защиты информации отражают ее сущность.

**Безопасность информации** – это свойство (состояние) передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность – устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам.

**3. Методология информационной безопасности. Цели защиты информации.**

Защита информации направлена:

* на предупреждение угроз;
* на выявление угроз;
* на обнаружение угроз;
* на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
* на ликвидацию последствий угроз и преступных действий и восстановление статус-кво.

**Предупреждение возможных угроз** и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения информации о преступных деяниях.

**Выявление** имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

**Обнаружение угроз** – это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким: действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

**Пресечение или локализация угроз** – это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам

**Ликвидация последствий** имеет целью восстановление состояния, предшествовавшего наступлению угрозы.

**Основными целями защиты информации являются:**

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

**4. Классификация методов защиты информации.**

Классификация методов защиты информации

•Законодательные (правовые);

•Организационные;

•Технические;

•Комплексные.

**Способы (методы) защиты информации:**

* Препятствие - создание на пути [угрозы](http://aguryanov.blogspot.com/2012/09/blog-post_6947.html) преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.
* Управление - оказание управляющих воздействий на элементы защищаемой системы.
* Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника.
* Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.
* Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)
* Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

**5. Определение политики информационной безопасности.**

**Политика безопасности (ПБ)** - совокупность документированных управленческих решений, направленных на ЗИ и ассоциированных с ней ресурсов.

Определение политики ИБ :

1 Определение документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

• управление доступом;

• антивирусную защиту;

• вопросы резервного копирования;

•проведение ремонтных и восстановительных работ;

• информирование об инцидентах об области ИБ.

2 Определение подходов к управлению рисками.

3 Структуризация контрмер по уровням.

4 Порядок сертификации на соответствие стандартам в области ИБ.

**6. Этапы процесса оценивания рисков.**

**Процесс оценивания рисков** содержит несколько этапов.

1 Идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия).

2 Оценивание угроз.

3 Оценивание уязвимостей.

4 Оценивание существующих и предполагаемых средств обеспечения.

5 Оценивание рисков.

**Идентификация рисков.** Этап заключается в формировании как можно более полного перечня возможных неблагоприятных событий, которые приведут к негативным изменениям и приносящих экономический ущерб объекту исследования. Для идентификации необходимо использовать как объективную имеющуюся информацию, так и субъективную в купе с опытом прошлых лет.

**Оценка вероятности наступления риска.** Суть этапа состоит в оценке предпосылок для возможного наступления рискового события. Оценка проводится на определённый временной интервал и может иметь как краткосрочный, так и долгосрочный характер. К методам оценки вероятностных событий относится статистический, аналитический и экспертный, которые используются одновременно.

**Определение структуры предполагаемого ущерба.** Возможный ущерб может стать не прямым следствием события, а проявиться через негативные изменения, наступившие после и носящие косвенный характер. Исходя из этого, крайне целесообразно структуру каждого возможного ущерба оценивать индивидуально.

**Построение законов распределения ущербов.** Так как точно спрогнозировать вероятность тех или иных событий катастрофы невозможно, оценить возможный ущерб также нельзя. Поэтому этот этап подразумевает построение законов распределения ущерба для каждого вероятного, неблагоприятного события. При оценке рисков используют типовые законы распределения.

**Оценка величины риска.** На данном этапе формируется количественные показатели риска. На их основании будут в дальнейшем базироваться этапы, касающиеся управленческих решений.

**Определение и оценка эффективности возможных методов снижения рисков.** Этап подразумевает создание списка возможных мер воздействия на риск, которые должны подразумевать под собой: методы по избеганию наступления рисковой ситуации, методы направленные на снижение вероятности наступления, методы уменьшающие ущерб, передачи риска иным объектам, компенсацию ущерба.

**Принятие решения об определении перечня действий направленных на управление рисками.** Суть этапа сводится к определению и внедрению оптимального набора методов воздействия на риски.

**Контроль эффективности применённых мер.** Заключительный этап оценки, подразумевающий сбор сведений и их оценку. На данном этапе решается, были ли принятые меры по снижению риска эффективными или нет, если это требуется проводиться корректировка принятых мер.

**7. Особенности реализации программы безопасности, на процедурном и программно-техническом уровнях.**

**Процедурный уровень.**

К нему относятся меры, реализуемые людьми. Опыт, накопленный в отечественных организациях, по реализации процедурных мер пришел из докомпьютерного прошлого и нуждается в существенном пересмотре.

Существуют следующие группы организационных (процедурных) мер:

* управление персоналом,
* поддержание работоспособности,
* планирование восстановительных работ,
* физическая защита,
* реагирование на нарушение безопасного режима.

Для каждой группы должны существовать правила, определяющие действия персонала. Они должны быть учреждены в каждой конкретной организации и отработаны на практике.

**Программно-технический уровень.**

С современной точки зрения информационным системам должны быть доступны следующие механизмы безопасности:

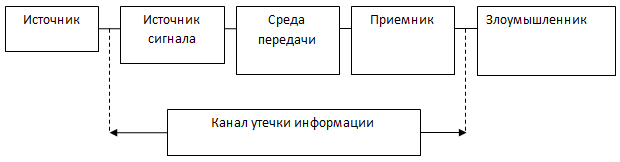
* управление доступом,
* экранирование,
* проверка подлинности пользователей и их идентификация,
* протоколирование и аудит,
* обеспечение высокой доступности,
* криптография.

**8. Технические каналы утечки информации. Основные определения и классификация.**

**Технический канал утечки информации (ТКУИ)** - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Утечка** - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

**Утечка (информации)** по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.



На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала.

Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

**Среда распространения сигнала** - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. . Она характеризуется набором физических параметров, определяющих условия перемещения сигнала.

Среда может быть однородная и неоднородная. Однородная - вода, воздух, металл и т.п. Неоднородная среда образуется за счет перехода сигнала из одной среды в другую, например, акустоэлектрические преобразования.

Приемник выполняет функцию, обратную функции передатчика

Таким образом, описание ТКУИ должно включать в себя:

· источник угрозы (приемник информативного сигнала)

· среда передачи информационного сигнала

· источник (носитель) информации

Классификация по физическим принципам возникновения:

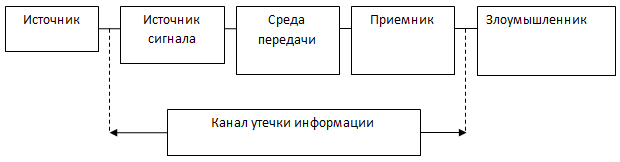
* акустические (распространение звуковых колебаний в любом звукопроводящем материале);
* электромагнитные (опасные напряжения и токи в различных токопроводящих коммуникациях);
* материально-вещественные (бумага, фото, магнитные носители, отходы и.т.п.);
* визуально-оптические (использование видеонаблюдения и фотографии) (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой части спектра).
* радиоканалы (электромагнитные излучения радиодиапазона);

**9. Технические каналы утечки информации. Акустические каналы утечки информации.**

**Технический канал утечки информации** (ТКУИ) - совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.



Акустический канал

**Акустическая информация** - информация, носителем которой является акустический сигнал.

**Акустический сигнал** - возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности.

Различают первичные и вторичные акустические сигналы. К первичным относятся: сигналы, создаваемые музыкальными инструментами, пением, речью; шумовые сигналы, создаваемые для сопровождения различных музыкальных и речевых художественных передач (шум поезда, треск кузнечика и т. п.). Ко вторичным акустическим сигналам относятся сигналы, воспроизводимые электроакустическими устройствами, т. е. первичные сигналы, прошедшие по электроакустическим трактам связи и вещания и соответственно видоизмененные по своим параметрам.

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный - это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих.

Виды технических каналов утечки акустической информации:

· Воздушные

· Электроакустические

· Вибрационные

· Параметрические

· Оптико-электронные(Лазерный)

# **10. Технические каналы утечки информации. Материально-вещественный и визуально-оптический каналы утечки информации.**

**Материально-вещественный канал утечки информации**

Утечка информации по материально‑вещественному каналу обусловлена хищением, копированием и ознакомлением с информацией, представленной на бумажном, электронном или каком-либо другом носителе.

**Визуально-оптический канал утечки информации**

Визуально‑оптический канал образуется вследствие получения информации путем применения различных оптических приборов, позволяющих уменьшить величину порогового контраста и увеличить контраст объекта на окружающем фоне.

Отраженный от объекта свет содержит информацию о внешнем виде объекта, а излучаемый объектом свет – о параметрах излучений.

Запись информации производится в момент отражения падающего света путем изменения его яркости и спектрального состава. Излучаемый свет содержит информацию об уровне и спектральном составе источников видимого света, а в инфракрасном диапазоне по характеристикам излучений можно также судить о температуре элементов излучения.

# **11. Технические каналы утечки информации. Электромагнитные каналы утечки информации.**

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

непреднамеренная передача конфиденциальной информации по некоторой "побочной системе связи"

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

Кроме того, в индукционном канале используется эффект возникновения вокруг кабеля связи ПЭМИ при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Электрический канал утечки информации возникает за счет наводок ПЭМИ технических средств обработки информации (ТСОИ) на соединительные линии ВТСС (вспомогательных технических средств и систем) 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 .

Наводки электромагнитных излучений ТСОИ возникают при излучении элементами ТСОИ информационных сигналов.

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.

Параметрический электромагнитный канал может возникать в процессе облучения ТСОИ побочными электромагнитными излучениями ВТСС, вследствие чего может произойти переизлучение электромагнитной волны, которое будет содержать И, обрабатываемую в ТСОИ.

**12. Пассивные методы защиты информации от утечки по техническим каналам.**

**Пассивные методы ЗИ** предназначены для предотвращения или существенного затруднения перехвата И по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня сигнала.

**Пассивные методы** ЗИ направлены на:

– ослабление побочных электромагнитных излучений на границе контролируемой зоны;

– ослабление наводок информационных сигналов в посторонних проводниках;

– исключение (ослабление) просачивания информационных сигналов технических средств передачи И в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

**Фильтрация**

– высокочастотных трактах передающих и приемных устройств;

– различных сигнальных цепях технических средств;

– цепях электропитания, управления, контроля, коммутации технических средств;

– проводных и кабельных соединительных линиях ;

– цепях пожарной и охранной сигнализации.

**Заземление технических средств**

Основные требования:

– система заземления;

– сопротивления заземляющих проводников, а также земляных шин;

– каждый заземляемый элемент;

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

**Звукоизоляция помещений**

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

**13. Активные методы защиты информации от утечки по техническим каналам.**

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

Основу средств акустической маскировки составляют генераторы помех. На практике наиболее широкое применение нашли генераторы шумовых колебаний. Именно поэтому активную акустическую маскировку часто называют акустическим зашумлением.

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 и музыкальных фрагментов, а также шумовых помех, или формируется из фрагментов скрываемого речевого сигнала при многократном 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.

Ухудшение условий перехвата речевой информации по виброакустическому и оптико-акустическому каналам утечки также может быть достигнуто использованием средств акустической маскировки. В этом случае в качестве конечных устройств генераторов помех используются вибродатчики.

Основные требования, которым должны удовлетворять современные средства виброакустической защиты:

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.

**14. Криптографическая защита информации. Исторические этапы.**

**Криптография** - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.

**Первый период** (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (замена букв другими буквами или символами).

* Скитала, также известная как «шифр древней Спарты», также является одним из древнейших известных криптографических устройств. Скитала представляла собой длинный стержень, на который наматывалась лента из пергамента. На ленту наносился текст вдоль оси скиталы, так, что после разматывания текст становился нечитаемым. Для его восстановления требовалась скитала такого же диаметра.
* Шифр Цезаря. Каждая буква алфавита циклически сдвигается на определённое число позиций. Величину сдвига можно рассматривать как ключ шифрования. Сам Цезарь использовал сдвиг на три позиции. Кроме примитивных шифров в истории использовался и другой подход — полная замена одного алфавита (например, кириллицы) на другой (например, греческий). Не имея ключа, сопоставляющего исходный и используемый алфавиты, прочитать надпись было невозможно.

**Второй период** (хронологические рамки — с IX века на Ближнем Востоке - до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.

• Решётка Кардано

**Третий период** (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.

**Четвёртый период** – с середины до 70-х годов XX века – период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам – линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической», т.е. криптографией с секретным ключом.

**Современный период развития криптографии** (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления – криптография с открытым ключом. Современная криптография образует отдельное научное направление на стыке математики и информатики – работы в этой области публикуются в научных журналах, организуются регулярные конференции. Её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

**15. Криптографическая защита информации. Классификация алгоритмов шифрования.**

Классификация алгоритмов шифрования

1 Симметричные (с секретным, единым ключом, одноключевые, single-key).

1.1. Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

1.2.1. Шифры перестановки (permutation, P-блоки);

1.2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

2 Асимметричные (с открытым ключом, public-

key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

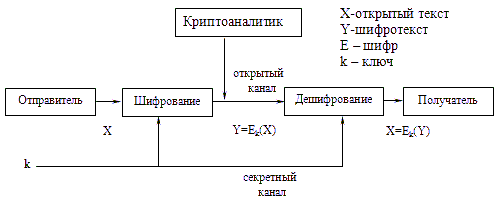
· Эль-Гамаль (ElGamal).



**Тайнопись** предполагает, что отправитель и получатель производят над сообщением преобразования, известные только им двоим.

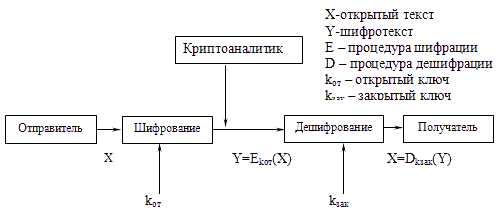
В противовес тайнописи, **криптоалгоритмы с ключом** построены на том принципе, что алгоритм воздействия на передаваемые данные известен всем сторонним лицам, но он зависит от некоторого параметра, который держится в секрете – «ключа», который известен только двум лицам, участвующим в обмене информацией.

Криптосистемы с ключом делятся на симметричные и асимметричные системы шифрования. Модель симметричной системы шифрования



Отличительной чертой **симметричных** алгоритмов шифрования является наличие одного ключа шифрования, который должен быть известен только отправителю и получателю сообщения. Отправитель на ключе k шифрует сообщение, получатель дешифрует полученный шифротекст ключом k. Криптоаналитик может перехватить шифротекст Y, передаваемый по открытым каналам связи, но, так как он не знает ключа, задача вскрытия шифротекста является очень трудоемкой.

Асимметричная система шифрования работает по схеме



Отличительной особенностью **асимметричных** алгоритмов является наличие пары ключей шифрования: открытого kот, который передается второй стороне по незащищенному каналу связи и поэтому может быть известен криптоаналитику, а также закрытого kзак, который известен лишь одному человеку (получателю сообщения) и держится в секрете. Пара ключей обладает тем свойством, что сообщение, зашифрованное на одном из ключей, может быть расшифровано только на другом ключе.

В зависимости от размера блока шифруемой информации криптоалгоритмы делятся на блочные и поточные шифры. Единицей кодирования в *потоковых* шифрах является один бит. Для *блочных* шифров единицей кодирования является блок из нескольких байтов.

Еще одним критерием классификации криптоалгоритмов является тип выполняемых преобразований над блоками открытого текста. По этому критерию криптоалгоритмы разделяют на подстановочные и перестановочные. В перестановочных шифрах блоки информации не изменяются сами по себе, но изменяется их порядок следования. Подстановочные шифры изменяют сами блоки информации по определенным законам.

Деление криптоалгоритмов на моноалфавитные и многоалфавитные характерно для подстановочных шифров. *Моноалфавитные* криптоалгоритмы заменяют блок входного текста (символ входного алфавита) на один и тот же блок шифротекта (символ выходного алфавита). В *многоалфавитных* шифрах одному и тому же блоку входного текста могут соответствовать разные блоки шифротекста, что существенно затрудняет криптоанализ.

**16. Принципы криптографической защиты информации. Симметричные криптосистемы.**

**Симметричные алгоритмы шифрования** (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ.

**Обмен информацией** осуществляется в 3 этапа:

•отправитель передает получателю ключ;

•отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;

•получатель получает сообщение и расшифровывает его.

**Классическим примером** таких алгоритмов являются:

- простая перестановка

- одиночная перестановка по ключу

- двойная перестановка

- перестановка "Магический квадрат"

**Стандарты симметричного шифрования:**

- AES (Advanced Encryption Standard) - американский стандарт шифрования

- ГОСТ 28147-89 - отечественный стандарт шифрования данных

- DES (англ. Data Encryption Standard) - стандарт шифрования данных в США до AES

- 3DES (Triple-DES, тройной DES)

- RC6 (Шифр Ривеста)

- Twofish

- IDEA (International Data Encryption Algorithm)

- SEED - корейский стандарт шифрования данных

- Camellia - шифр сертифицированный для использовании в Японии

- CAST (по инициалам разработчиков Carlisle Adams и Stafford Tavares)

- XTEA - наиболее простой в реализации алгоритм

**17. Принципы криптографической защиты информации. Асимметричные криптосистемы.**

В **асимметричных алгоритмах шифрования** (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

**Схема обмена информацией** такова:

• получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

• отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

• получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

Принципиальное отличие асимметричной криптосистемы от криптосистемы симметричного шифрования состоит в том, что для шифрования информации и ее последую­щего расшифровывания используются различные ключи:

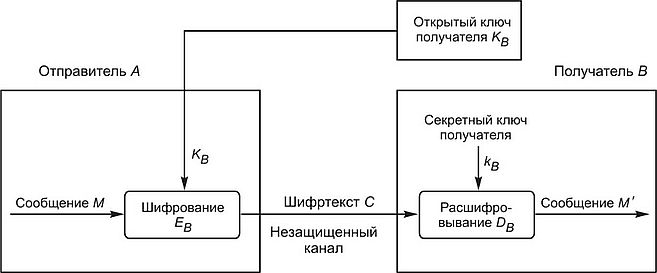
* *открытый ключ* ***К*** используется для шифрования информа­ции, вычисляется из *секретного ключа* **k**;
* *секретный ключ* **k** используется для расшифровывания ин­формации, зашифрованной с помощью парного ему от­крытого ключа **К**.

Асимметричные системы называют также двухключевыми криптографическими системами, или криптосистемами с открытым ключом.

В качестве ключа зашифровывания должен использоваться открытый ключ получателя, а в качестве ключа расшифровыва­ния — его секретный ключ.

**Недостатки асимметричных криптосистем:**

* на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах функций;
* асимметричное шифрование существенно медленнее сим­метричного, реализовать аппаратный шифратор с асимметрич­ным алгоритмом существенно сложнее, чем реализовать аппаратно симметричный алгоритм;
* необходимость защиты открытых ключей от подмены.



**18. Принципы криптографической защиты информации. Основные типы криптоаналитических атак.**

Основные типы криптоаналитических атак:

1 Криптоаналитическая атака при наличии только известного шифротекста. Криптоаналитик имеет только шифротексты C1, С2, ..., Сi, нескольких сообщений, зашифрованных с использованием одного и того же алгоритма шифрования Ек. Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты M1, M2, ..., Мi, по возможности большинства сообщений или, еще лучше, вычислить ключ К.

2 Криптоаналитическая атака при наличии известного открытого текста. Криптоаналитик имеет доступ не только к шифротекстам C1, С2, ..., Ci нескольких сообщений, но также к открытым текстам M1, M2, ..., Mi этих сообщений. Его работа заключается в нахождении ключа К, используемого при шифровании этих сообщений, или алгоритма расшифрованияь Dk любых новых сообщений, зашифрованных тем же самым ключом.

3 Криптоаналитическая атака при возможности выбора открытого текста. Криптоаналитик не только имеет доступ к шифротекстам C1, С2, ..., Сi, и связанным с ними открытым текстам M1, M2, ..., Мi, нескольких сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде.

4 Криптоаналитическая атака с адаптивным выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования. Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

5 Криптоаналитическая атака с использованием выбранного шифротекста. Криптоаналитик может выбирать для расшифрования различные шифротексты C1, С2, ..., Сi, и имеет доступ к расшифрованным открытым текстам M1, M2, ..., Mi. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом.

6 Криптоаналитическая атака методом полного перебора всех возможных ключей. Эта атака предполагает использование криптоаналитиком известного шифротекста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой.

**19. Интеллектуальная собственность. Основные определения: собственность, право собственности, интеллектуальная собственность и т.д.**

В современном праве **собственность** - это «принадлежность средств и продуктов производства определенным лицам - индивидам или коллективам.

**Право собственности** - «совокупность правовых норм, закрепляющих, регулирующих и охраняющих состояние принадлежности (присвоенности) материальных благ конкретным лицам».

Право собственности на вещь обычно сводится к трем правомочиям: праву владения, праву пользования и праву распоряжения имуществом.

* **владение** заключается в дозволенном законом фактическом обладании имуществом,
* **пользование** - в потреблении полезных свойств имущества,
* **распоряжение** - в определении судьбы имущества.

**Интеллектуальная собственность** есть совокупность прав на ниже перечисленные объекты:

- литературные, художественные и научные произведения;

- исполнительская деятельность артистов, звукозаписи, радио- и телевизионные передачи;

- изобретения во всех областях человеческой деятельности;

- научные открытия;

- промышленные образцы;

- товарные знаки, знаки обслуживания, фирменные наименования и коммерческие обозначения;

- защиту против недобросовестной конкуренции, а также все другие права, относящиеся к интеллектуальной деятельности в производственной, научной, литературной и художественной областях.

- совокупность исключительных прав как личного, так и имущественного характера на результаты интеллектуальной и в первую очередь творческой деятельности.

**Объект интеллектуальной собственности** - это материализованный результат нематериального по своей природе мыслительного процесса. На этот материализованный результат у его владельца возникает нематериальное исключительное право.

В большинстве случаев объект интеллектуальной собственности по форме представляет собой вещь, например, книгу или диск с записанной программой, кинофильмом, музыкой и т.п.

**20. Этапы процесса управления объектами интеллектуальной собственности.**

Этапы процесса управления объектами интеллектуальной собственности:

- сбор и анализ информации о предмете интеллектуальной деятельности, формулировка цели деятельности и задач, решение которых необходимо для ее достижения;

- планирование, организация и стимулирование интеллектуальной деятельности для решения поставленных задач, выработка нового знания о предмете интеллектуальной деятельности;

- перевод («превращение») нового знания в информацию путем объективизации идеального результата интеллектуальной деятельности (получение объекта интеллектуальной собственности);

- защита прав на результаты интеллектуальной деятельности, выраженные в объекте интеллектуальной собственности, опираясь на законодательство в области интеллектуальной собственности;

- коммерциализация объекта интеллектуальной собственности, инвестирование вырученных средств в разработку нового объекта интеллектуальной собственности, который начинается со сбора и анализа информации о предмете интеллектуальной деятельности и т.д.

**21. Объекты авторского права и смежных прав.**

Объекты авторского права и смежных прав: литературные, художественные, научные произведения, компьютерные программы, базы данных, музыкальные произведения, исполнительская деятельность артистов, аудио- и видеозаписи, радио- и телевизионные передачи и др.

**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 произведений**

•переводы, обработки, инсценировки, музыкальные аранжировки, обзоры, аннотации, рефераты;

•сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда.

**3 Компьютерные программы**

•Прикладные программы и операционные системы.

• Базы данных или компиляции иных материалов в любой форме.

**22. Классификация авторских прав.**

Авторские права делятся на:

- личные неимущественные (моральные права);

- 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 искажении 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:**

•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;

• передача произведения в эфир;

• иное сообщение произведения для всеобщего сведения;

• перевод произведения на другой язык;

• переделка или иная переработка произведения.

Авторское право распространяется на обнародованные и необнародованные произведения.

**Произведения:**

* литературные;
* научные;
* драматические, сценарные;
* хореографические;
* музыкальные с текстом или без текста;
* аудиовизуальные;
* живописи, графики, скульптуры;
* архитектуры;
* фотографические;
* карты, планы, эскизы и т.д.

**Производные произведения:**

* переводы, обработки, инсценировки, обзоры, аннотации, рефераты;
* сборники произведений: энциклопедии, антологии, атласы.

**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.

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

**23. Патентные исследования: основные определения, территориальные и временные ограничения.**

**Патент** – документ, удостоверяющий приоритет, авторство, исключительное право на использование изобретения (полезной модели, промышленного образца), представляемое государством на определенный период времени, которое позволяет его обладателю запрещать третьим лицам использование (в том числе изготовление, использование, продажу, ввоз) его изобретения. В обмен на предлагаемую охрану заявитель должен полностью раскрыть свое изобретение.

**Территориальное ограничение** – патент действует только на территории страны или региона, выдавшей этот патент. Патент Российской Федерации действует только на территории Российской Федерации, патент Беларуси только на территории Беларуси, Региональный Евразийский патент действует на территориях стран-участниц регионального Соглашения.

**Временное ограничение** – патент имеет определенный срок действия, в Российской Федерации и европейских странах срок действия патента на изобретение равен 20 годам с даты поступления заявки в патентное ведомство. В США и Канаде срок действия патента равен 17 годам, но считая с даты выдачи патента. Такое ограничение по срокам должно дать патентообладателю достаточно времени для извлечения прибыли из своего изобретения, но с другой стороны, не останавливать развитие технического прогресса.

**24. Порядок проведения патентных исследований.**

Патентные исследования проводят при:

1) разработке научно-технических прогнозов;

2) разработке планов развития науки и техники;

3) создании объектов техники;

4) освоении и производстве продукции;

5) определении целесообразности экспорта промышленной продукции и экспонировании ее образцов на международных выставках и ярмарках;

6) продаже и приобретении лицензий;

7) при решении вопроса о патентовании созданных объектов промышленной собственности и в других целях.

**Порядок проведения патентных исследований:**

1. Разработка программы (регламента) исследований;

2. Поиск и отбор патентной и научно-технической информации;

3. Анализ результатов исследований.

**Операции, выполняемые при разработке программы (регламента):**

1 Определение предмета исследования.

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.

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

Осуществляется преимущественно и фондах патентной документации для установления уровня технического решения, границ прав патентообладателя и условий реализации этих прав.

**25. Виды патентно-информационного поиска.**

**Патентно-информационный поиск** при проведении патентных исследований подразделяется на: тематический, именной, нумерационный и др.

**Тематический (предметный) поиск** - поиск патентной информации по названию темы посредством ключевых слов, соответствующих техническим терминам, которые используются в МПК.

Поскольку патентные законодательства большинства стран мира различают такие виды изобретений, как устройство, способ, вещество, биотехнологические продукты, процедура поиска определяется непосредственно объектом поиска, в качестве которого выступает вид изобретения.

Тематический поиск проводится по фонду описаний изобретений, по фондам промышленных образцов либо путем просмотра официальных бюллетеней. В качестве информационно-поискового языка используются классификации изобретений: в Европейских странах и Японии — это МПК, в США — национальная классификация.

Тематический поиск ведут, если нужно определить технический уровень или новизну объекта.

**Именной поиск** - поиск патентных документов по наименованию фирмы-патентообладателя или патентообладателя.

Именной поиск ведут, когда известно имя автора или патентовладельца и надо найти относящийся к ним охранные документы. Он может быть использован, как дополнительный к тематическому поиску

По наименованию фирмы-патентообладателя, заявителя, фамилии автора (авторов) изобретения определяют номера выданных патентов и их принадлежность к определенной рубрике классификации изобретений. Основную задачу именного поиска при установлении патентных прав составляет поиск патентов, принадлежащих тому или иному изобретателю, фирме. Для проведения именного поиска пользуются алфавитно-именными указателями, фирменными указателями и другими торгово-экономическими справочниками.

**Нумерационный поиск** - поиск информации по номеру документа. Осуществляется для установления тематической принадлежности документа и его правового статуса на момент проверки.

Поиск осуществляется по нумерационным указателям. Для патентного фонда, расставленного по рубрикам классификации, необходимо по нумерационному указателю определить индекс классификации, а потом найти нужный документ в фонде.

Патентно-информационный поиск проводится всегда перед подачей заявки на патентование изобретения, полезной модели или промышленного образца. Патентно-информационный поиск не является обязательной процедурой, но без него вероятность отказа в выдачи патента составляет около 95%.

**26. Международная патентная классификация.**

**Международная патентная классификация** — иерархическая система патентной классификации. МПК является средством для классификации патентных документов ([патенты](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D0%B5%D0%BD%D1%82) и [авторские свидетельства](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D1%81%D0%BA%D0%BE%D0%B5_%D1%81%D0%B2%D0%B8%D0%B4%D0%B5%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) на [изобретения](https://ru.wikipedia.org/wiki/%D0%98%D0%B7%D0%BE%D0%B1%D1%80%D0%B5%D1%82%D0%B5%D0%BD%D0%B8%D0%B5), [промышленные образцы](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%B5%D1%86), [полезные модели](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B5%D0%B7%D0%BD%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C), включая опубликованные заявки) единообразной в международном масштабе. Представляет собой инструмент для патентных ведомств и других потребителей, осуществляющих поиск патентных документов.

МПК разделена на восемь разделов. Разделы представляют собой высший уровень иерархии МПК. Каждый раздел обозначен заглавной буквой латинского алфавита от A до Н. Разделы имеют следующие названия:

А: Удовлетворение жизненных потребностей [человека](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA)

В: Различные [технологические процессы](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81); [транспортирование](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82)

С: [Химия](https://ru.wikipedia.org/wiki/%D0%A5%D0%B8%D0%BC%D0%B8%D1%8F); [металлургия](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%B0%D0%BB%D0%BB%D1%83%D1%80%D0%B3%D0%B8%D1%8F)

D: [Текстиль](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BA%D1%81%D1%82%D0%B8%D0%BB%D1%8C); [бумага](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BC%D0%B0%D0%B3%D0%B0)

E: [Строительство](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%BE%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) и [горное дело](https://ru.wikipedia.org/wiki/%D0%93%D0%BE%D1%80%D0%BD%D0%BE%D0%B5_%D0%B4%D0%B5%D0%BB%D0%BE)

F: [Машиностроение](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BE%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%D0%B8%D0%B5); [освещение](https://ru.wikipedia.org/wiki/%D0%9E%D1%81%D0%B2%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5); [отопление](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BE%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5); [двигатели](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%B8%D0%B3%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) и [насосы](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%BE%D1%81); [оружие](https://ru.wikipedia.org/wiki/%D0%9E%D1%80%D1%83%D0%B6%D0%B8%D0%B5) и [боеприпасы](https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D0%B5%D0%BF%D1%80%D0%B8%D0%BF%D0%B0%D1%81); [взрывные](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D1%80%D1%8B%D0%B2) работы

G: [Физика](https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D0%B7%D0%B8%D0%BA%D0%B0)

H: [Электричество](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE)

**27. Введение объектов интеллектуальной собственности в гражданский оборот.**

В соответствии с Гражданским кодексом Республики Беларусь (ст.128) исключительные права на результаты интеллектуальной деятельности (интеллектуальная собственность) относятся к объектам гражданских прав. [Объекты гражданских прав](http://bargu.by/136-obekty-grazhdanskix-pravootnoshenij.html) (ст.129) могут свободно отчуждаться и переходить от одного лица к другому в порядке правопреемства либо иным способом, если они не изъяты из оборота или не ограничены в обороте.

Обязательным элементом процесса управления интеллектуальной собственностью. Необходимым условием введения в гражданский оборот объектов интеллектуальной собственности является их оценка и постановка на бухгалтерский учет. В соответствии с действующими нормативными актами оценка требуется для:

* постановки ОИС на бухгалтерский учет в качестве нематериальных активов;
* передачи полностью или частично имущественных прав на ОИС другому лицу;
* внесения ОИС в уставный фонд юридического лица в виде неденежных вкладов;
* передачи ОИС под залог;
* определения стартовой цены для конкурсов, аукционов и торгов ОИС;
* разрешения имущественных споров;
* возмещения убытков;
* реализации управленческих решений.

Одним из первых нормативных актов, обозначивших ОИС в качестве нематериальных активов, стал Закон РБ «О бухгалтерском учете и отчетности» от 18 октября 1994 г. В статье 3 «Объекты бухгалтерского учета» сказано, что к нематериальным активам относятся «право пользования природными ресурсами, патенты, лицензии, ноу-хау, программные продукты, монопольные права и привилегии (включая лицензии на отдельные виды деятельности), организационные расходы, торговые марки, товарные знаки и знаки обслуживания, брокерские места, иные права и нематериальные активы».

**Нематериальные активы** – это группа активов предприятия, не имеющих материально-вещественного содержания и характеризующихся долговременным использованием в хозяйственном обороте предприятия, способностью приносить доход и, как правило, возможностью отчуждения.

Типовой перечень ОИС учета в составе НМА включает:

* патенты на изобретения, промышленные образцы, товарные знаки;
* свидетельства на товарные знаки, топологии интегральных микросхем;
* компьютерные программы и базы данных;
* лицензионные и авторские договоры;
* технологические процессы;
* конструкторскую документацию;
* отчеты о НИОК(Т)Р;
* и другие.

Нематериальные активы отражаются в бухгалтерском учете и отчетности. Использование объектов интеллектуальной собственности в качестве нематериальных активов предприятий, организаций, постановка их на бухгалтерский учет по сути означает начало процесса коммерциализации инновационной сферы и формирования рынка научно-технической продукции (нововведений). Это создает возможность экономически эффективного использования как имеющихся, так и вновь создаваемых нематериальных активов, изменения структуры уставных фондов, повышения наукоемкости выпускаемой продукции.

Процессы включения интеллектуальной собственности в гражданский оборот развиваются в мире достаточно динамично. Как показывает мировая практика, стоимость отдельных объектов интеллектуальной собственности достигает сотен миллионов долларов, а доля интеллектуальной собственности может составлять более половины всего капитала промышленных предприятий и фирм. Поэтому наличие прав на объекты интеллектуальной собственности является важнейшим показателем экономического состояния и экономической политики фирм – владельцев прав, поскольку включение их в состав нематериальных активов существенным образом влияет на оценку балансовой, страховой, ликвидационной и других форм стоимости, а также на возможности перераспределения стоимости отдельных видов активов. Иначе говоря, позволяет изменить структуру производственного капитала за счет увеличения доли нематериальных активов в стоимости продукции и услуг. По данным Британского института защиты товарных знаков, за период 1980-2000 гг. в Англии и США только 30% рыночной стоимости компаний составляют материальные активы, все остальное – НМА, т.е. патенты, ноу-хау, авторские права и т.д. Так, в компании Coca-Cola соотношение МА и НМА оценивается как 4:96.

В странах СНГ, включая РБ, удельный вес НМА в общей массе активов предприятия пока ничтожно мал по сравнению со странами Запада, где господствует развитая рыночная экономика. Поэтому наш практический опыт по коммерциализации и эффективному использованию НМА в работе хозяйствующих субъектов явно недостаточен. Тем не менее, практическое использование предприятиями НМА требует научного исследования и анализа.

Объекты интеллектуальной собственности как нематериальные активы предприятия или организации могут быть получены путем:

* создания в результате выполнения научно-исследовательских, опытно-конструкторских, технологических работ или иной деятельности;
* приобретения у правообладателей или авторов, в том числе в обмен на другое имущество;
* безвозмездной передачи правообладателями или авторами;
* внесения в уставный фонд вновь создаваемых субъектов хозяйствования, а также при слиянии предприятий.

Учет и отражение в составе имущества на балансе предприятия ОИС в качестве нематериальных активов производятся исходя из оценки их стоимости.

Таким образом, учет ОИС в составе НМА является одной из наиболее актуальных экономических и правовых проблем на данном этапе развития белорусской экономики в целом, сферы НИОКР и наукоемкого производства.

**28. Защита прав авторов и правообладателей.**

**Нарушениями прав авторов***,* влекущими примене­ние гражданско-правовых способов защиты авторских прав, являются*:*

· присвоение права авторства на чужой объект про­мышленной собственности;

· навязанное соавторство;

· исключение из числа соавторов. Защита прав в таких случаях осуществляется предъявлением иска о признании права и восстановлении положения, существовавшего до нарушения права, т.е. о признании авторства, исклю­чении из числа соавторов или, напротив, о включении в число соавторов;

· нарушение права на авторское имя. Оно может со­стоять в искажении имени автора, в неуказании имени автора в заявке на выдачу патента или свидетельства, в различных публикациях об авторстве на объект про­мышленной собственности (в публикации сведений о за­явке, о патенте), в других официальных и неофициаль­ных изданиях и наоборот, указание в публикациях имени автора в случаях, когда он отказался быть упо­мянутым в качестве автора. Автор в таком случае впра­ве требовать внесения соответствующих исправлений в документ или публикацию;

· отказ нанимателя или его правопреемника заклю­чить с работником договор, предусматривающий созда­ние, правовую защиту и использование служебного объекта промышленной собственности. В этом случае автор вправе требовать заключения договора;

· отказ или неправильная выплата вознаграждения автору (соавторам);

· спор между авторами о распределении вознаграж­дения за использование объекта промышленной соб­ственности;

· отказ выплатить автору (соавторам) различные компенсации.

В трех последних случаях автор или соавтор вправе требовать выплаты соответствующих сумм вознагражде­ния или компенсации.

Нарушением исключительного права *правооблада­теля* любого охраняемого объекта промышленной соб­ственности является несанкционированное:

· изготовление,

· применение,

· ввоз, предложение к продаже,

· продажа,

· иное введение в гражданский оборот либо хране­ние с этой целью.

Нарушением исключительного права на охраняемый патентом объект промышленной собственности является также:

· несанкционированное применение способа, охраня­емого патентом на приобретение;

· доведение до посевных кондиций в целях размно­жения охраняемого патентом сорта растения;

· копирование топологии интегральной микросхемы в целом или ее части путем включения данной тополо­гии в интегральную микросхему или иным образом, за исключением копирования только той части, которая не является оригинальной.