УВАЖАЕМЫЕ СТУДЕНТЫ! Изучите и законспектируйте новый теоретический материал тезисно по плану лекции.

Ответьте на контрольные вопросы

Результаты работы, фотоотчет, предоставить преподавателю на e-mail: xvsviv@rambler.ru в трехдневный срок с момента получения задания.

При возникновении вопросов по приведенному материалу обращаться по следующим номерам телефонов:072-138-93-11.

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Лекция

Закон о защите информации. Авторское право, патент, лицензия, производственные секреты

План лекции

1. Авторское право

2. Патентование

3. Товарные знаки

4. Споры из-за интеллектуальной собственности

1. Авторское право

Авторское право - в объективном смысле - совокупность норм гражданского права (институт), регулирующих отношения по признанию авторства и охране имущественных и неимущественных прав авторов и правообладателей; в субъективном смысле - совокупность имущественных и неимущественных прав авторов и иных правообладателей.

В соответствии со ст.1261 IVч. Гражданского кодекса, авторские права на все виды **программ для ЭВМ** (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы.

Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения результата, включая подготовительные материалы, полученные в ходе разработки **программы для ЭВМ**, и порождаемые ею аудиовизуальные отображения.

Авторское право действует с момента создания программы для ЭВМ или базы данных в течение всей жизни автора и 50 лет после его смерти. Использование программ для ЭВМ или баз данных третьими лицами осуществляется на основании договора с правообладателем.

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, использовать знак охраны авторского права ©. Правовая охрана распространяется на все виды компьютерных программ, в том числе на операционные системы и программные комплексы, которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код.

Законодательством предусмотрена государственная регистрация программ для ЭВМ и баз данных по желанию правообладателя. Правовая основа охраны программных продуктов как объектов интеллектуального права заложена в ст. 1261,1262 и 1280 четвертой части ГК РФ.

ГК РФ Статья 1261. Программы для ЭВМ

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

(студенты просматривают в Интернете ст. 1262, 1280, конспектируют, затем рассказывают)

В этих нормах законодательства содержатся следующие положения, имеющие принципиальное значение для борьбы с "компьютерным пиратством":

- программы для ЭВМ и базы данных относятся к объектам авторского права;

- автору или иному правообладателю принадлежит исключительное право осуществлять и/или разрешать выпуск в свет, воспроизведение, распространение и иное использование программы для ЭВМ или базы данных;
- имущественные права на программные продукты могут быть переданы кому-либо только по договору;
- незаконное использование программ для ЭВМ либо иное нарушение авторских прав на программы для ЭВМ влечет за собой гражданско-правовую, административную, уголовную ответственность.

Таким образом, использование программы для ЭВМ кем бы то ни было в соответствии с законом должно осуществляться на основании договора с правообладателем. Применительно к массовым пользователям допускается особый порядок заключения договора путем изложения его типовых условий на передаваемых экземплярах программ для ЭВМ. Вскрытие покупателем упаковки экземпляра программы для ЭВМ является действием, с помощью которого он выражает своё согласие с условиями так называемой "оберточной" лицензии. Другим примером такого действия, когда покупатель выражает своё согласие с условиями лицензионного соглашения, в которых описаны его основные права по использованию продукта, является выбор опции "Согласен" в момент установки продукта на компьютер пользователя. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе осуществлять её запись в память одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем. Использование программных продуктов без разрешения правообладателя нарушает его имущественные права и, следовательно, является правонарушением.

Проблема защиты авторских прав приобрела особую актуальность с развитием цифровых технологий и Интернета. Несмотря на постоянное совершенствование законодательства, в том числе международного, в сфере авторского права, а также непрерывное совершенствование и усложнение технических и программных средств, направленных на предотвращение нарушений в этой области, пиратское использование интеллектуальной собственности стало массовым явлением, ущерб от которого в глобальном масштабе превышает многие миллиарды долларов. Крайне актуальной задача защиты авторских прав является для тех, чья работа связана со

СМИ, как печатными, так и электронными, а также рекламной деятельностью. Как только текст, фотография или видеозапись представлены публично, автор или правообладатель практически теряет контроль над возможным несанкционированным использованием материала. Для всех очевидна острота этой проблемы, когда речь идет о размещении тех или иных работ в Интернете, однако на практике очень часто грубые нарушения авторского права имеют место и тогда, когда представленный в виде цифрового файла материал предоставляется, например, в издательство или напрямую в типографию.

Проведем анализ возможностей существующих технических и программных методов и средств, предназначенных для защиты от нарушений прав авторов.

Технические и программные методы защиты авторских прав можно разделить на 3 группы:

1) методы, предусматривающие наличие явной подписи, указывающей на автора или владельца прав на материал;

2) методы, предусматривающие наличие скрытой авторской «подписи», внедряемой в цифровой файл, как правило, с использованием стеганографических технологий;

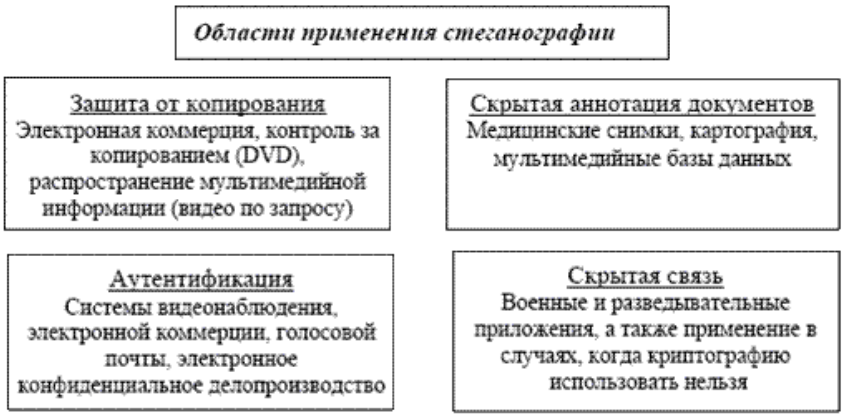
3) методы защиты от несанкционированного копирования, распространения и использования авторского материала, например, путем защиты от копирования CD или DVD, содержащих защищаемые цифровые файлы.

Рассмотрим первую группу методов – методов «**подписывания**» авторских материалов. Явное наличие подписи под текстом, фотографией, рисунком или иным изображением, а также указание авторства в титрах видеозаписи никоим образом не защищает материал от незаконного использования. Некоторым исключением можно считать ситуацию, когда прямо по фотографии наносится надпись (водяные знаки), указывающая на автора работы, причем такая надпись, что ее незаметное удаление практически невозможно. Очевидно, что в этом случае мы имеем дело с приемом, который портит фотографию настолько, что ее пиратское воспроизведение становится бессмысленным. Такой метод часто применяется при размещении фотоизображений в Интернете, наряду с другим методом, предполагающим размещение изображения столь малого размера и плохого качества, что его

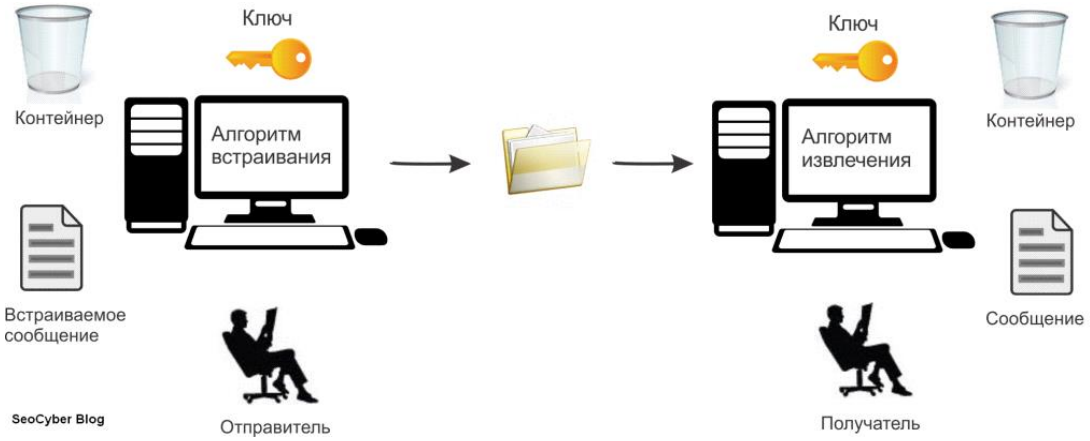
использование невозможно. Понятно, что методы «подписывания» авторских материалов не способны обеспечить защиту прав авторов.

Вторая группа методов предусматривает скрытное внедрение в графический аудио- или видеофайл **специальной информации**, включая информацию о правообладателе, его почтовом и электронном адресе, телефоне и других данных (скрытное внедрение данных в текстовые файлы также возможно, но с целью защиты авторских прав не используется, так как присутствие «явной» подписи не портит текст). Наличие информации об авторе материала дает возможность лицам, заинтересованным в его использовании связаться с автором с целью заключения с ним соглашения о законном использовании его работы. С другой стороны, наличие стеганографически внедренных данных, в принципе, позволяет «отследить» размещение материала в Интернете, а значит, выявить факты возможного его несанкционированного использования. Рассмотрим эту группу методов более подробно.

Стеганография (в переводе с греческого – тайнопись) – техника скрытой передачи или скрытого хранения информации. Известна история о Демерате, который хотел предупредить союзников в Спарте об угрозе нападения со стороны Ксерксов. В Древней Греции сообщения писались палочками на дощечках, покрытых слоем воска. Так вот, для того, чтобы послать скрытое сообщение, Демерат соскоблил с дощечки воск, написал сообщение непосредственно на самом дереве и покрыл дощечку воском заново, в результате чего, дощечка спокойно прошла досмотр стражников-центурионов и не вызвала никаких подозрений. В V веке тиран Гистий находился под наблюдением царя Дария в Сузах. Гистий хотел послать скрытое сообщение своему родственнику в город Милет. Для этого он побрил голову своего раба, сделал на его черепе татуировку, и когда волосы раба снова отрасли, отправил его в путь.



Основной принцип компьютерной стеганографии предполагает использование двух типов файлов – **файл-сообщение**, которое должно быть скрыто, и **файл-контейнер**, в котором должно быть скрыто сообщение. Контейнер – любой файл или поток данных, в который может быть скрыто встроена информация. Если контейнер не содержит встроенное сообщение, то он называется пустым. Контейнер, содержащий встроенную информацию, называется заполненным или стегоконтейнером. В нашем случае в роли файла-контейнера выступает цифровой файл, в который необходимо внедрить информацию о владельце авторских прав. Важнейшим требованием к стегоконтейнеру является внешняя неотличимость пустого и заполненного контейнеров, чтобы наличие скрытой информации для стороннего наблюдателя никак внешне не проявлялось.



Весь процесс стеганографии можно условно разделить на пять этапов:

Первый этап – выбор файла, который необходимо скрыть.

Второй этап – выбор контейнера, в котором будет скрываться передаваемый файл. Для сокрытия файла (стегосообщения) объем контейнера, в котором он будет скрываться, должен не менее чем в 8 раз превышать объем самого сообщения. Чтобы скрыть файл весом 500КБ, понадобится контейнер весом 4000КБ.

Третий этап – выбор, непосредственно, стенографической программы. Одной из самых распространенных программ для Windows является S-Tools. Эта программа позволяет прятать информацию в графических файлах типа bmp и gif, а так же в звуковых файлах типа wav. Ознакомиться с программой и скачать ее можно тут. Другой, не менее распространенной, является программа Steganos for Win95, которая также проста в обращении, как и S-Tools, однако она использует иной криптографический алгоритм. Она позволяет скрывать данные внутри файлов типа dib, bmp, html, voc, ASCII, wav.

Четвертый этап – непосредственно сама кодировка файла. То есть, после того, как вы поймете, какое сообщение вы хотите зашифровать, выберете для него контейнер и программу для шифрования, вы можете приступать к кодировке информации.

Пятый этап – отправка сообщения и декодирование.

https://habrahabr.ru/post/166583/ - о стеганографии и php

Одним из основных и наиболее перспективных направлений использования стеганографии является встраивание цифровых водяных знаков (ЦВЗ) (watermarking), способствующих защите авторских прав на графические и аудио- или видеофайлы от пиратства и обеспечивающих возможность контроля за распространением защищенной информации.

Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в графический, аудио-, видео- или иной файл с целью контроля его использования. Для внедрения и распознавания цифровых водяных знаков разработано специальное программное обеспечение. Программы распознавания ЦВЗ позволяют извлекать информацию о владельце авторских прав и о том, как вступить с ним в контакт. Программы обнаружения ЦВЗ позволяют контролировать распространение защищенной информации. Таким образом, основной областью применения ЦВЗ является защита интеллектуальной собственности от копирования и несанкционированного использования.

Основным недостатком методов, предусматривающих внедрение в цифровых водяных знаков, является их неспособность предотвратить незаконное использование авторских материалов.

Третья группа методов защиты авторских прав направлена на блокирование несанкционированного копирования и использования авторского материала. Следует отметить, что такая задача является типичной задачей защиты информации, решение которой часто является обязательной для обеспечения информационной безопасности. Очевидно, что если тем или иным методом обеспечить защиту от несанкционированного копирования графических, аудио- или видеофайлов, то их пиратское использование становится невозможным и задача защиты автор- ских прав решается наиболее успешно. Таким образом, можно считать, что наилучшим способом защиты прав авторов на материалы, представленные в цифровом виде, является обеспечение информационной безопасности носителей этих данных или защита соответствующих файлов от копирования.

На сегодняшний день самыми распространенными являются методы, обеспечивающие защиту от копирования информации, записанной на CD или DVD. Несмотря на то, что такие методы широко используются, почти все они обладают существенным недостатком – недоступностью для «простого» пользователя, не являющегося профессионалом-компьютерщиком и не обладающего определенными аппаратными средствами. Кроме того, не все существующие методы достаточно надежны и зачастую легко обходятся с помощью специальных «хакерских» программ.

2. Патентование

Патент следует рассматривать не столько как документ, сколько как способ оформления уникальных идей. С его помощью разработчик изобретения закрепляет за собой права создателя несмотря на характер изделия — будь то устройство, вещество, способ, научный или технический метод. Срок действия патента зависит от страны патентования, объекта патентования и составляет от 5 до 25 лет

Служба интеллектуальной собственности – ведомство, которое выдает патент на изобретение. Патентование изобретений происходит путем подачи соответствующей заявки, которая представляет собой следующий комплекс сведений и бумаг:

- подробное описание изобретения;
- формулы и чертежи изобретения;

- заявление автора изобретения о необходимости получения патента.

Патентное право в России регулируется Главой 72 Гражданского кодекса РФ и иными нормативно-правовыми актами Российской Федерации (напр. федеральным законом N 316-ФЗ «О патентных поверенных» от 30.12.2008; приказом Минобрнауки РФ N 322 «Об утверждении Административного регламента исполнения Федеральной службой по интеллектуальной собственности, патентам и товарным знакам государственной функции по осуществлению …» от 29.10.2008, и других).

В соответствии с п.1 ст. 1363 ГК РФ, срок действия исключительного права на изобретение, полезную модель, промышленный образец и удостоверяющего это право патента исчисляется со дня подачи первоначальной заявки и при условии соблюдения требований, установленных ГК РФ, составляет:

- для изобретений — 20 лет;
- для полезных моделей — 10 лет;
- для промышленных образцов — 5 лет.

В Российской Федерации **на программное обеспечение** патент не выдается, однако в соответствии с положениями Бернской конвенции об охране литературных и художественных произведений, в состав которой РФ вступила 13 марта 1995г., и Гл. 70 Гражданского кодекса РФ – компьютерные программы охраняются как литературные произведения, т.е. компьютерные программы входят в перечень объектов авторского права.

Однако, поскольку защита авторским правом распространяется только на текст кода, функции программного обеспечения остаются не защищенными. Вследствие этого, для защиты разработок в области программного обеспечения применяют патентование **функций или алгоритмов**, описывая их с помощью аппаратных средств либо элементов устройств, в которых применяются данные функции или алгоритмы. Таким образом, объектом патентования становится устройство или способ.

Такой подход при патентовании программ ЭВМ применяется и в Российской Федерации, и во многих других странах. Преимущество такого патентования заключается в том, что защита распространяется именно на алгоритм и функции программы, т.е. любая программа, которая обладает такими функциями, будет

нарушать этот патент, вне зависимости от того, на каком языке программирования она написана.

Международно-правовая охрана компьютерных программ возможна по двум различными правовыми режимами - режимом, применяемым к литературным произведениям и режимом, который применяется к патентам. В первом случае программа идентифицируется по тексту кода (см. Бернская конвенция), в другом, по признакам применяемых для изобретений, предлагаемых для патентования (нужно доказать «инновационность», «новизну», и «коммерческую пригодность» (в США также "неочевидность" и "полноту описания").

3. Товарные знаки

Товарный знак (также **Товарная марка**; ™) — обозначение (словесное, изобразительное, комбинированное или иное), «служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей».

Согласно Закону РФ «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров», **товарный знак** — обозначение, служащее для индивидуализации товаров, выполняемых работ или оказываемых услуг юридических или физических лиц.

Право на товарный знак охраняется законом. Товары, этикетки, упаковки товаров, на которых незаконно нанесен товарный знак или сходное с ним до степени смешения обозначение, являются контрафактными.

На зарегистрированный товарный знак выдается специальное свидетельство. В соответствии со ст. 5 указанного Закона в качестве товарных знаков могут быть зарегистрированы словесные, изобразительные, объемные и другие обозначения или их комбинации в любом цвете или цветовом сочетании.

4. Споры из-за интеллектуальной собственности

1. Шоколад "Алёнка"

Московская кондитерская фабрика "Красный Октябрь", выпускающая шоколад под брендом "Аленка", требовала взыскать компенсацию в размере более 310 миллионов рублей с кондитерской фабрики "Славянка" (Белгородская область) за нарушение исключительных прав на товарный знак.

"Славянка" выпускала шоколад под названием "Алина" в упаковке, выполненной в аналогичной цветовой гамме и с изображением девочки, как установили суды, "в похожем цветастом головном платке, из-под которого выбивается челка".

Спор дошел до Высшего арбитражного суда РФ и был отправлен на новое рассмотрение в первую инстанцию. Там длившееся два с половиной года разбирательство завершилось подписанием мирового соглашения: "Славянка" обязалась прекратить выпуск шоколада в спорном оформлении и выплатить истцу 15 миллионов рублей. В свою очередь, "Красный Октябрь" отказался от взыскания остальных 37 миллионов рублей компенсации, рассчитанной судом.

Контрольные вопросы

1. Что является основным источником права в области обеспечения информационной безопасности в России?

2. Что включают в себя нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации?

3. Кто в России осуществляет межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную и служебную тайну?

4. Кто регулирует деятельность в области защиты информации?

5. Что такое сертификация?