

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал ордена Трудового Красного Знамени
федерального государственного бюджетного образовательного учреждения
высшего образования
«Московский технический университет связи и информатики»

А.Г. ЖУКОВСКИЙ

Методические указания
По выполнению практического занятия №1
по дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Тема: Правовая защита от компьютерных преступлений и защита
интеллектуальной собственности**

Направление подготовки 09.03.01 Информатика и вычислительная техника

Ростов-на-Дону
2022

Методические указания
по выполнению практического занятия №1
по дисциплине
«Основы информационной безопасности»

Составитель: А.Г. Жуковский, проф. каф. «ИТСС»

Рассмотрено и одобрено
на заседании кафедры «ИТСС»
Протокол от «19» декабря 2022 г., №5.

Практическое занятие №1

Тема: ПРАВОВАЯ ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

1. ПРАВОВАЯ ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

1.1. Классификация компьютерных преступлений

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений.

По кодификатору Интерпола (в 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен в более чем 100 странах) все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q.

Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

QA - Несанкционированный доступ и перехват

QD - Изменение компьютерных данных

QF - Компьютерное мошенничество

QR - Незаконное копирование

QS - Компьютерный саботаж

QZ - Прочие компьютерные преступления

Например, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:

QAH - "Компьютерный абордаж" (хакинг - hacking): неправомерный доступ в компьютер или сеть. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

QAI - перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея,

коммуникационных каналов, принтера и т. д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

QAT - кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая терминология:

- "Жучок" (bugging) - характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;

- "Откачивание данных" (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

- "Уборка мусора" (scavenging) - характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т. д. Электронный вариант требует исследования данных, оставленных в памяти машины;

- метод следования "За дураком" (piggybacking), характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

- метод "За хвост" (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;

- метод "Неспешного выбора" (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

- метод "Поиск бреши" (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

- метод "Люк" (trapdoor), являющийся развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу;

- метод "Маскарад" (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

-метод "Мистификация" (spoofing), который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

Анализ компьютерных преступлений

С целью совершенствования методов расследования, правоохранительные органы проводят анализ КП. Разрабатываются системы адаптации «традиционных» методов расследования преступлений с использованием компьютерных средств.

Диапазон компьютерных преступлений в настоящее время расширился и включает кроме традиционного мошенничества также киберслежку, мошенничество с инвестициями, сексуальные домогательства, кражу информации, внутригосударственный и международный терроризм, нарушение авторских прав, фальсификацию систем, насильственные преступления, жестокое обращение с пожилыми.

По мере развития электронной коммерции число компьютерных преступлений будет соответствующим образом расти. Для анализа преступлений теперь требуются не только региональные, но и международных средств анализа. Эти системы могут объединять преступления по местоположению, времени и методу действий, что может помочь прогнозировать потенциальные будущие угрозы.

В университете Карнеги-Меллона создана группа «скорой компьютерной помощи» Computer Emergency Response Team (CERT), которая ставит своей целью анализ и разработку мер противодействия компьютерным преступлениям.

Проделанная этой группой работа показывает, насколько важно понять мотивы преступника. Понимание целей, которые ставит перед собой злоумышленник, позволяет определять его будущие поступки.

Для выявления нарушений системной защиты используются методы активной добычи данных. Такой подход предполагает анализ поступков, которые приводят к нарушениям, и сравнивает их с поведением при нормальной работе. Добывается информация о часто встречающейся последовательности действий. Эти сведения используются для создания автоматического классификатора, который способен различать агрессивное и нормальное поведение.

1.2. Криминалистические особенности расследования компьютерных преступлений

Главная проблема при расследовании преступлений в банковских компьютерных системах заключается в установлении самого факта совершения преступления.

Особенность состоит в том, что для того, чтобы утверждать, что было совершено преступление с использованием компьютера, необходимо доказать:

-факт, что компьютерная информация, к которой произведен несанкционированный доступ, охраняется законами Российской Федерации;

-факт, что злоумышленником были осуществлены определенные неправомерные действия;

-факт, что самими несанкционированными действиями нарушены права собственника информации;

-факт несанкционированного доступа к средствам компьютерной техники либо попытка получения такого доступа;

-факт использования злоумышленником полученных в результате неправомерных действий денежных средств в своих целях. Например, необходимо доказать, что доступ был не санкционированным с целью совершения преступления. Тогда установлению и доказыванию подлежит:

-факт, что действительно были совершены несанкционированные манипуляции, например, с программным обеспечением; что, эти манипуляции были недозволенными; лицо, совершавшее их, знало об этом и осуществляло их с целью преступного умысла.

Комплекс следственных действий обязательных для первоначального этапа расследования должен включать:

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей машинной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному отношению программного обеспечения или носящих иные следы подготовки к хищению денежных средств.

2. Исследование: журналов сбойных ситуаций, рабочего времени ЭВМ, по передачи смен операторами; средств защиты и контроля банковских компьютерных систем, регистрирующих пользователей, моменты включения (активации) системы либо подключение к ним абонентов с определенным индексом или без такового; протоколов вечернего решения, представляющих собой копию действий операторов, отображенную на бумажном носителе в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня; контрольных чисел файлов; всего программного обеспечения ЭВМ; "прошитых" микросхем постоянно запоминающих устройств, микропроцессоров и их схемного исследования.

3. Получение и анализ технических указаний по обработке ежедневной бухгалтерской информации с перечнем выходящих форм.

4. Допрос лиц из числа инженеров - программистов, занимавшихся разработкой программного обеспечения и его сопровождением, специалистов отвечающих за защиту информации и специалистов электронщиков, занимающихся эксплуатацией и ремонтом вычислительной техники.

5. Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах.

В ходе судебно-бухгалтерской экспертизы устанавливаются нарушения требований положений о документообороте, их причины (с целью совершения преступления, злоупотребления или ошибки) и ответственные лица за эти нарушения.

Результаты программно-технической экспертизы, как заключение экспертов, играют роль доказательств в процессе суда. С помощью таких экспертиз могут решаться следующие задачи:

1. Воспроизведение информации, содержащейся на физических носителях.

2. Восстановление информации, ранее содержавшейся на физических носителях и в последствии стертый или измененной по различным причинам.

3. Установление времени ввода, изменение, уничтожение либо копирование той или иной информации.

4. Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.

5. Установление авторства, места, средства, подготовки и способа изготовления документов (файлов, программ).

6. Выяснения возможных каналов утечки информации из компьютерной сети и помещений.

7. Выяснение технического состояния, исправности программно-аппаратных комплексов, возможности их адаптации под конкретного пользователя.

8. Установления уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

1.3. Международные стандарты и соглашения в области безопасности информационных технологий

Ключевым аспектом решения проблемы безопасности информационных технологий (ИТ) является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ. Необходимо было разработать эту систему в виде международного стандарта.

В 1990 г. Международной организацией по стандартизации (ISO) была начата разработка международного стандарта критериев оценки для общего

использования. Версия 1.0 ОК была завершена ССЕВ в январе 1996 г. и одобрена ISO в апреле 1996 г. Бета-версия 2.0 ОК появилась в октябре 1997 г.

В результате этих работ появился Международный стандарт ISO/IEC 15408-99 "Критерии оценки безопасности информационных технологий" или так называемые "Общие критерии".

В России аналогичный стандарт подготовлен в 2001г. Это ГОСТ Р ИСО/МЭК 15408-1-2001 «Критерии оценки безопасности информационных технологий».

Данный стандарт содержит общие критерии (ОК) оценки безопасности информационных технологий и предназначен в качестве руководства при разработке и при приобретении коммерческих продуктов или систем с функциями безопасности ИТ.

ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК

ОК безопасности продуктов и систем ИТ предназначены в основном для потребителей, разработчиков и оценщиков.

ОК предоставляют потребителям, независимую от реализации структуру, называемую профилем защиты (ПЗ), для выражения их специфических требований к мерам безопасности ИТ в объекте оценки.

Кроме указанного выше используется также ГОСТ Р50922-96 «Защита информации. Основные термины и определения».

В настоящее время разработан и действует еще один международный стандарт ISO/IEC 17799 "Безопасность информационных систем".

Представители 26 европейских стран, а также Канады, США, ЮАР и Японии подписали 23 ноября 2001 г. в Будапеште конвенцию по борьбе с киберпреступностью. Конвенция разрабатывалась специальным комитетом Совета Европы при участии юристов США и других стран в течение четырех лет. Семнадцатью государствами, включая Россию, документ не подписан, считая, что она нарушает права человека.

Контрольные вопросы

1. Назовите особенности расследования компьютерных преступлений.
2. Какие задачи решаются судебно-бухгалтерской и программно-технической экспертизами при проведении следственных действий?
3. Существующая классификация компьютерных преступлений. Методы НСД.
4. Методы и приемы предупреждения компьютерных преступлений. Анализ компьютерных преступлений.

5. В каких документах представлены нормы правового обеспечения защиты информации в АС?
6. Что представляет собой документ «Политика безопасности»?
7. Какие документы необходимо представить для присвоения класса защищенности АС?
8. Выполнение каких правил безопасности обеспечивается путем реализации «Политики безопасности»?
9. Где указаны требования к безопасности компьютерных сетей в РФ?
10. Международные соглашения в информационной сфере.

2. ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

2.1. Объекты интеллектуальной собственности

Результатом интеллектуальной деятельности является информационный продукт, который представляется на рынке в виде информационных товаров и услуг.

Впервые же понятие “интеллектуальная собственность” прозвучало у нас в 1990 году в тексте Закона “О собственности в РСФСР”.

Законодательными актами РФ регламентируется право собственности на информацию, полученную юридическими и физическими лицами в результате интеллектуальной деятельности. Это исключительное право представляет собой интеллектуальную собственность.

Определение “интеллектуальная собственность” дано в Конвенции, учреждающей Всемирную организацию интеллектуальной собственности (ВОИС), принятой на Стокгольмской конференции в 1967 году и ратифицированной в 1968 году СССР. В российском законодательстве вопросы защиты ИС рассмотрены в 1-й и 2-й частях ГК РФ.

Интеллектуальная собственность (ГК часть 1, ст. 138) - исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполненных работ или услуг (фирменное наименование, товарный знак и т. п.). Использование результатов интеллектуальной деятельности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

Уточнения даны в 4-й части ГК РФ, принятой 18.12.2006г. № 230.

Результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и

предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

- 1) произведения науки, литературы и искусства;
- 2) программы для электронных вычислительных машин (программы для ЭВМ);
- 3) базы данных;
- 4) исполнения;
- 5) фонограммы;
- 6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- 7) изобретения;
- 8) полезные модели;
- 9) промышленные образцы;
- 10) селекционные достижения;
- 11) топологии интегральных микросхем;
- 12) секреты производства (ноу-хау);
- 13) фирменные наименования;
- 14) товарные знаки и знаки обслуживания;
- 15) наименования мест происхождения товаров;
- 16) коммерческие обозначения.

На результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации) признаются интеллектуальные права, которые включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права и иные права (право следования, право доступа и другие).

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности: авторское право, патентное право, и секреты производства.

Авторское право - форма правовой защиты в отношении литературных, художественных и научных произведений.

Патентное право - форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

Секреты производства (ноу-хау) - форма правовой защиты любых полезных сведения (производственных, технических, экономических, организационных и других).

Историческая справка.

Первый закон об авторском праве был принят в Англии в 1710 году. Охрана личных прав давалась на 14 лет с продлением еще на 14 лет.

Первым патентным законом была Декларация Венецианской республики в 1474г. Изобретатель получал привилегию (патент) на 10 лет.

В России выдача привилегий началась с 1748г. Общий закон «О привилегиях...» появился в 1812г.

В РФ до недавнего времени действовали следующие законодательные акты, защищающие права граждан и юридических лиц на результаты своей интеллектуальной деятельности.

1. Закон РФ “Об авторском праве и смежных правах”, от 9.07.93г. №5351-1 (редакция от 20.07.04г. №72).

2. Закон РФ “Патентный закон РФ”, от 23.09.92г. № 3517-1.

3. Закон РФ “О правовой охране программ для ЭВМ и баз данных”, от 23.09.92г. №3523-1.

4. Закон РФ “О правовой охране топологий интегральных микросхем”, от 23.09.92г. №3526-1.

5. Закон РФ “О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров”, от 23.09.92г. № 3520-1.

6. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, от 22.03.91г. №948-1. (Ред. от 9 октября 2002 г №122-ФЗ).

7. Закон РФ "О защите конкуренции", от 26.07.2006г. Ш35-ФЗ.

После вступления в силу с 1 января 2008г 4-й части Гражданского кодекса РФ, которая посвящена нормированию прав на результаты интеллектуальной собственности, потеряло силу большинство указанных выше законов РФ, касающихся защиты ИС.

Заключены следующие международные конвенции и соглашения, связанные с охраной интеллектуальной собственности:

1. Конвенция по охране промышленной собственности от 20 марта 1883г. (редакция от 2 октября 1979г.), заключенная в Париже.

2. Конвенция по охране литературных и художественных произведений от 9 сентября 1886г., заключенная в Берне (последняя редакция 1971г.).

3. Конвенция о международной регистрации фабричных и товарных знаков от 14 апреля 1891г. (редакция от 2 октября 1979г.), заключенная в Мадриде.

4. Всемирная (Женевская) конвенция об авторском праве от 6 октября 1952г., заключенная в Женеве.

5. Конвенция по охране интересов производителей фонограмм от незаконного воспроизведения фонограмм от 29 октября 1971г., заключенная в Женеве.

6. Конвенция, учреждающая всемирную организацию интеллектуальной собственности от 14 июля 1967г. (редакция 2 октября 1979г.), заключенная в Стокгольме.

7. Брюссельская конвенция о распространение несущих сигналов, передаваемых через спутники от 21.мая 1974г.

8. Евразийская патентная конвенция 1994 г.

9. Гаагское соглашение по международному депонированию промышленных образцов от 28 ноября 1960г. (редакция от 2 октября 1979г.).

10. Международная конвенция об охране интересов исполнителей, производителей фонограмм и вещательных организаций, заключенной в Риме 26 октября 1961г. ("Римская конвенция").

Рассмотрим основные правовые нормы защиты ИС.

2.2. Правовые нормы защиты интеллектуальной собственности

ПРАВОВАЯ ОХРАНА АВТОРСКИХ И СМЕЖНЫХ ПРАВ

Закон регулирует отношения, возникающие при создании и использовании произведений науки, литературы и искусства (авторское право), фонограмм исполнителей, постановок, передач организаций эфирно или кабельного вещания (смежные права).

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

-устной (выступление, исполнение и т.д.);

-звуко- или видеозаписи;

-изображения (рисунок, чертеж, теле-, фотокадр и т.д.);

-объемно-пространственной (скульптура, макет и т.д.);

-в других формах.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

Автор - физическое лицо, творческим трудом которого создано произведение. Авторское право не распространяется на идеи, методы, процессы, системы, концепции, принципы, открытия, факты.

Не являются объектами авторского права: официальные документы (законы, судебные решения и т. п.); государственные символы и знаки (флаги, гербы, ордена и т.п.); произведения народного творчества;

сообщения о событиях и фактах, имеющие информационный характер.

Авторское право на произведение возникает в силу факта его создания. Для возникновения и осуществления авторского права не требуется регистрации произведения или соблюдения каких - либо формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя в соответствии с правилами статьи 1262 настоящего Кодекса.

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов: латинской буквы "С" в окружности:

имени (наименования) обладателя исключительных прав; года первого опубликования произведения.

При опубликовании произведения анонимно или под псевдонимом представителем автора в соответствии с данным Законом является издатель,

который имеет право защищать права автора пока автор не раскроет свою личность.

При соавторстве (произведение создано двумя и более лицами) авторское право принадлежит соавторам совместно, независимо от характера и структуры произведения (неразрывное целое или имеет отдельные самостоятельные части).

Если произведение создано в порядке выполнения служебных обязанностей, (служебное произведение) то авторское право на него принадлежит автору служебного произведения, а исключительные права на его использования - работодателю.

Авторское вознаграждение при этом определяется договором между автором и работодателем.

Автору в отношении его произведений принадлежат личные неимущественные

права (право признаваться автором, право обнародовать или разрешать обнародовать произведения, право на защиту произведения от искажения и др. посягательств) и исключительные имущественные права (право на использование - воспроизводить, показывать, исполнять, распространять и т.д.).

Авторское право действует в течении всей жизни автора и 70 лет после его смерти.

В сфере авторского права до 70-х годов прошлого века в России срок действия исключительных прав составлял 15 лет после смерти автора, с 1973 г. был увеличен до 25 лет.

В 1991 г. в «Основах гражданского законодательства Союза ССР» срок действия авторских прав составил 50 лет.

В 2004 г. были приняты поправки к Закону РФ «Об авторском праве и смежных правах» где действие авторского права установлено с учетом действующих международных норм в течении всей жизни автора и 70 лет после его смерти

Поправки, вступившие в силу с 1 сентября 2006 г., означают, что размещенные в сети, например, тексты книг или музыкальные файлы в формате mp3 охраняются авторским правом так же, как обычные книги или компакт- диски. Они подпадают под действие ст. 146 Уголовного кодекса РФ ("Нарушение авторских и смежных прав"), предусматривающей наказание для пиратов в виде лишения свободы на срок до пяти лет.

Теперь владельцы mp3-сайтов, например, должны подписать лицензионные соглашения со всеми поставщиками музыки.

Истечение срока действия авторского права на произведения означает их переход в общественное достояние.

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.

Знак охраны смежных прав - буква "Р" в окружности, имя обладателя прав и год первого опубликования фонограммы.

Исключительное право на исполнение действует в течение всей жизни исполнителя, но не менее пятидесяти лет, считая с 1 января года, следующего за годом, в котором осуществлены исполнение, либо запись исполнения, либо сообщение исполнения в эфир или по кабелю. По истечении срока действия исключительного права на исполнение это право переходит в общественное достояние.

Исключительное право на фонограмму действует в течение пятидесяти лет, считая с 1 января года, следующего за годом, в котором была осуществлена запись.

В соответствии с законом запрещается импортировать экземпляры фонограмм в целях распространения, переделывать, продавать и воспроизводить без разрешения их правообладателей.

ПРАВОВАЯ ОХРАНА ПРОГРАММ ДЛЯ ЭВМ И БАЗ ДАННЫХ

Программы для ЭВМ и базы данных относятся Законом к объектам авторского права. Программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных - как сборникам.

Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Правообладатель в течение срока действия исключительного права на программу для ЭВМ или на базу данных может по своему желанию зарегистрировать такую программу или такую базу данных в федеральном органе исполнительной власти по интеллектуальной собственности.

1. Исключительное право изготовителя базы данных возникает в момент завершения ее создания и действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее создания. Исключительное право изготовителя базы данных, обнародованной в указанный период, действует в течение пятнадцати лет, считая с 1 января года, следующего за годом ее обнародования.

2. Сроки, предусмотренные пунктом 1 настоящей статьи, возобновляются при каждом обновлении базы данных.

Импорт, тиражирование, продажа, а также иное введение в гражданский оборот экземпляров программ без разрешения их правообладателей является нарушением авторского права.

Суд может наложить арест на все экземпляры произведения, в отношении которых предполагается, что они являются контрафактными, а также на материалы и оборудование, используемые или предназначенные для их изготовления или воспроизведения

Контрафактными признаются экземпляры программы, изготовление или использование которых влечет за собой нарушения авторского права.

Свободное воспроизведение произведения в личных целях (статья 1273).

Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях, за исключением:

- 1) воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;
- 2) воспроизведения баз данных или их существенных частей;
- 3) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса (например, для архивных целей);
- 4) репродуцирования книг (полностью) и нотных текстов;
- 5) видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;
- б) воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ АВТОРСКИХ ПРАВ

1. Техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

2. В отношении произведений не допускается:

- 1) осуществление без разрешения автора или иного правообладателя действий, направленных на то, чтобы устранить ограничения использования произведения, установленные путем применения технических средств защиты авторских прав;
- 2) изготовление, распространение, сдача в прокат, предоставление во временное безвозмездное пользование, импорт, реклама любой технологии, любого технического устройства или их компонентов, использование таких технических средств в целях получения прибыли либо оказание соответствующих услуг, если в результате таких действий становится невозможным использование технических средств защиты авторских прав либо эти технические средства не смогут обеспечить надлежащую защиту указанных прав.

В случаях нарушения исключительного права на произведение или на объект смежных прав правообладатель вправе требовать по своему выбору от нарушителя возмещения убытков либо выплаты компенсации:

в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда;

в двукратном размере стоимости экземпляров произведения или в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения.

Предусмотрена также уголовная ответственность за нарушение авторских и смежных прав (Уголовный кодекс РФ статья 146).

1. Незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, - наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, - наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

ОХРАНА ТОПОЛОГИИ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Топология - это зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними.

Автору топологии интегральной микросхемы, принадлежат следующие интеллектуальные права:

- 1) исключительное право;
- 2) право авторства.

Предоставляемая правовая охрана распространяется только на оригинальную топологию. Оригинальной является топология, созданная в результате творческой деятельности автора.

Автором топологии признается физическое лицо, в результате творческой деятельности которого эта топология была создана.

Право автора на топологию является неотъемлемым личным правом и охраняется законом бессрочно.

Правообладатель в течение срока действия исключительного права на топологию интегральной микросхемы может по своему желанию зарегистрировать топологию в федеральном органе исполнительной власти по интеллектуальной собственности.

Топология, содержащая сведения, составляющие государственную тайну, государственной регистрации не подлежит.

Автору принадлежит исключительное право использовать эту топологию по своему усмотрению, в частности путем изготовления и распространения ИМС с такой топологией, включая право запрещать

использование этой топологии другим лицам без соответствующего разрешения.

Нарушением исключительного права на использование топологии признается совершение следующих действий без разрешения автора или иного правообладателя:

воспроизведение топологии в целом или частично, за исключением копирования только той ее части, которая не является оригинальной;

ввоз на территорию Российской Федерации, продажа и иное введение в гражданский оборот топологии, или интегральной микросхемы, в которую включена эта топология, или изделия, включающего в себя такую интегральную микросхему.

Имущественные права на топологию, созданную в порядке выполнения служебных обязанностей или по заданию работодателя, принадлежат работодателю, если договором не предусмотрено иное.

Правообладатель для оповещения о своем исключительном праве на топологию вправе использовать знак охраны, который помещается на топологии, а также на изделиях, содержащих такую топологию, и состоит из выделенной прописной буквы "Т" ("Т", [Т], Т*, буквы "Т" в окружности, или буквы "Т" в квадрате), даты начала срока действия исключительного права на топологию и информации, позволяющей идентифицировать правообладателя.

Исключительное право на использование топологии действует в течении десяти лет.

Автор топологии и иной правообладатель вправе требовать:

признания прав;

возмещения причиненных убытков.

За защитой своего права автор может обратиться в суд (арбитражный или третейский).

Автор может требовать правовую охрану топологии в зарубежных странах.

Если международным договором РФ установлены иные правила, чем те, которые содержатся в настоящем Законе, то применяются правила международного договора.

ОХРАНА ОБЪЕКТОВ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

Кодекс регулирует имущественные, а также личные неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием изобретений, полезных моделей (конструкторское выполнение) и промышленных образцов (внешний вид).

Исключительное право на изобретение, полезную модель или промышленный образец признается и охраняется при условии их государственной регистрации, на основании которой федеральный орган исполнительной власти по интеллектуальной собственности выдает патент на изобретение, полезную модель или промышленный образец.

Срок действия исключительного права на изобретение, полезную модель, промышленный образец и удостоверяющего это право патента исчисляется со дня подачи заявки на выдачу патента и составляет:

двадцать лет - для изобретений;

десять лет - для полезных моделей;

пятнадцать лет - для промышленных образцов.

Условия патентоспособности изобретения.

Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

Изобретение является новым, если оно не известно из уровня техники.

Изобретение имеет изобретательский уровень, если оно для специалиста явным образом не следует из уровня техники.

Не являются изобретениями:

- 1) открытия;
- 2) научные теории и математические методы;
- 3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;
- 4) правила и методы игр, интеллектуальной или хозяйственной деятельности;
- 5) программы для ЭВМ;
- 6) решения, заключающиеся только в представлении информации.

В соответствии с настоящим пунктом исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

Не предоставляется правовая охрана в качестве изобретения:

- 1) сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами;
- 2) топологиям интегральных микросхем.

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Право на получение патента, созданного работником в связи с выполнением им своих служебных обязанностей или полученным от работодателя заданием, принадлежит работодателю, если договором между ними не предусмотрено иное.

При этом автор имеет право на вознаграждение, соразмерное выгоде, которая получена работодателем или могла бы быть им получена. Вознаграждение выплачивается в размере и на условиях, определяемых на основе соглашения между ними.

Патентообладателю принадлежит исключительное право на использование охраняемых патентом изобретения, полезной модели или промышленного образца по своему усмотрению, если такое использование не нарушает прав других патентообладателей.

Нарушением исключительного права патентообладателя признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот, содержащего запатентованное изобретение.

Правительство Российской Федерации имеет право в интересах обороны и безопасности разрешить использование изобретения, полезной модели или промышленного образца без согласия патентообладателя с уведомлением его об этом в кратчайший срок и с выплатой ему соразмерной компенсации.

На изобретения, содержащие сведения, составляющие государственную тайну распространяются положения раздела «Особенности правовой охраны и использования секретных изобретений» настоящего Кодекса.

Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана не предоставляется.

Ответственность за нарушение прав авторов.

Присвоение авторства, принуждение к соавторству, незаконное разглашение сведений об объекте промышленной собственности влекут за собой уголовную ответственность в соответствии с законодательством Российской Федерации.

Уголовный кодекс статья 147. Нарушение изобретательских и патентных прав

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, - наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, - наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

ПРАВО НА СЕКРЕТ ПРОИЗВОДСТВА (НОУ-ХАУ)

Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной

деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание. С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

ПРАВА НА СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ ЮРИДИЧЕСКИХ ЛИЦ, ТОВАРОВ, РАБОТ, УСЛУГ И ПРЕДПРИЯТИЙ

Защита фирменного наименования, товарных знаков, знаков обслуживания и наименования мест происхождения товаров.

Закон регулирует отношения, возникающие в связи с регистрацией, правовой охраной и использованием товарных знаков, знаков обслуживания и наименований мест происхождения товаров.

На территории Российской Федерации действует исключительное право на фирменное наименование, включенное в единый государственный реестр юридических лиц.

Исключительное право на фирменное наименование возникает со дня государственной регистрации юридического лица и прекращается в момент исключения фирменного наименования из единого государственного реестра юридических лиц в связи с прекращением юридического лица либо изменением его фирменного наименования.

Юридическое лицо, нарушившее правила настоящей статьи, обязано по требованию правообладателя прекратить использование фирменного наименования, тождественного фирменному наименованию правообладателя или сходного с ним до степени смешения, в отношении видов деятельности, аналогичных видам деятельности, осуществляемым правообладателем, и возместить правообладателю причиненные убытки.

Товарный знак и знак обслуживания - это обозначения, способные отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц.

На товарный знак, то есть на обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей, признается исключительное право, удостоверяемое свидетельством на товарный знак.

Правовая охрана ТЗ предоставляется на основе его государственной регистрации и действует в течении 10 лет. Срок действия ТЗ может быть продлен каждый раз на 10 лет.

Государственная регистрация товарного знака осуществляется федеральным органом исполнительной власти по интеллектуальной собственности в Государственном реестре товарных знаков и знаков обслуживания Российской Федерации

Правообладатель для оповещения о своем исключительном праве на товарный знак вправе использовать знак охраны, который помещается рядом с товарным знаком, состоит из латинской буквы "R" или латинской буквы "R" в окружности - ®, либо словесного обозначения "товарный знак" или "зарегистрированный товарный знак" и указывает на то, что применяемое обозначение является товарным знаком, охраняемым на территории Российской Федерации.

ТЗ может быть выполнен в любом цвете или цветном изображении.

Не допускается регистрация ТЗ:

- состоящих только из обозначений;
- не обладающих различительной способностью;
- представляющих собой государственные гербы и эмблемы; официальные названия государств и т. п. Такие обозначения могут быть включены в ТЗ как неохраняемые элементы, если на это имеется согласие соответствующего компетентного органа или их владельца.

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

Правообладатель вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

1) в размере от десяти тысяч до пяти миллионов рублей, определяемом по усмотрению суда исходя из характера нарушения;

2) в двукратном размере стоимости товаров, на которых незаконно размещен товарный знак, или в двукратном размере стоимости права использования товарного знака, определяемой исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование товарного знака.

Наименование мест происхождения товара - это официальное или неофициальное наименование страны, населенного пункта, местности или другого географического объекта.

Исключительное право использования наименования места происхождения товара, предоставляется на основе его регистрации федеральным органом исполнительной власти по интеллектуальной собственности.

Обладатель свидетельства об исключительном праве на наименование места происхождения товара для оповещения о своем исключительном праве может помещать рядом с наименованием места происхождения товара знак охраны в виде словесного обозначения "зарегистрированное наименование места происхождения товара" или "зарегистрированное НМПТ",

указывающий на то, что применяемое обозначение является наименованием места происхождения товара, зарегистрированным в Российской Федерации.

Товары, этикетки, упаковки товаров, на которых незаконно использованы наименования мест происхождения товаров или сходные с ними до степени смешения обозначения, являются контрафактными.

Свидетельства на право пользования наименованием места происхождения товара действует в течении 10 лет и продлевается каждый раз на 10 лет.

Ответственность за незаконное использование наименования места происхождения товара.

Правообладатель вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

- 1) в размере от десяти тысяч до пяти миллионов рублей, определяемом по усмотрению суда исходя из характера нарушения;
- 2) в двукратном размере стоимости товаров, на которых незаконно размещено наименование места происхождения товара.

Контрольные вопросы

1. Назовите правовые формы охраны интеллектуальной собственности.
2. Что понимается под исключительными правами на объекты интеллектуальной собственности?
3. Правовая охрана авторских смежных прав.
4. Правовая охрана программ для ЭВМ и баз данных.
5. Правовая охрана объектов промышленной собственности.
6. Охрана исключительного права на секрет производства.
7. Правовая защита фирменного наименования, товарных знаков, знаков обслуживания и наименования мест происхождения товаров.