МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт Права
(наименование института полностью)

Кафедра «Гражданское право и процесс»
(наименование кафедры)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

«Гражданское право; семейное право; международное частное право»
(направленность (профиль)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Гражданско-правовое регулирование отношений в сфере информационной безопасности (доменные имена)

Студент С.С. Краснов _____
(И.О. Фамилия) (личная подпись)

Научный руководитель А.В. Маркин _____
(И.О. Фамилия) (личная подпись)

Руководитель программы д.ю.н., доцент, В.Г. Медведев _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Допустить к защите

Заведующий кафедрой к.ю.н., доцент, А.Н. Федорова _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Тольятти 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Эволюционная интеграция информационных технологий, направленных на хранение и обработку огромных массивов разнородной и слабоструктурированной информации и информационно-телекоммуникационных технологий, направленных на создание телекоммуникационных сетей, в соответствии с теорией больших систем привела, за счет так называемого системного эффекта эмерджентности к формированию новой структуры, обладающей новыми свойствами, которыми не обладает ни один элемент в отдельности , а именно информационного виртуального пространства , в котором информация существует в особой, в частности для традиционного права, электронной форме. Эффект эмерджментности и большое количество пользователей в силу синергического эффекта привело к формированию глобального межгосударственного цифрового пространства, позволившего обеспечить доступ к огромным информационным ресурсам большинству жителей Земли. В свою очередь стремительное развитие мирового цифровое пространство явилось аттрактором перехода к следующей стадии в развитии человеческого общества- информационному обществу.

Большинство ученых XX- XXI в.в., как в области гуманитарных, в том числе юриспруденции, наук так и естественно- технических наук связывали развитие цивилизации на основе перехода к информационному обществу в основе которого лежат информация и знания, а соответственно в которой решающую роль будут играть отрасли, связанные с их получением, распространением и обработкой.

Сущность информационного общества составляют следующие взаимосвязанные процессы:

— опережающий рост рынка информации и знания как фактора производства, по сравнению с рынками природных ресурсов, труда и капитала;

— высокий уровень информационных потребностей всех членов общества;

—информационная инфраструктура превращается в условие, определяющее не только национальную конкурентоспособность, но и национальную безопасность;

— информация и знания становятся движущей силой, определяющей политику, экономику, социальную жизнь.

В Конституции РФ сформулирована основополагающая норма информационного права на доступ к информации: "Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом…"[1].

Однако переход к информационному обществу характеризуется рядом противоречий. Одним из центральных является то, что темпы развития информационного общества таковы, что право отстает от темпов развития информационных технологий и потому многие правовые отношения, например, в Интернете остаются де юре неурегулированными.

Кроме этого, анализ законотворческих процессов показывает, что в своей реализации они все больше приближаются к виду специальных информационных технологий, например то же административное право, уже просто немыслимо без информационных технологий хранения и обработки значительных документальных массивов.

Указанные выше потребности информационного общества в правовом регулировании возникающих в нем информационных отношений предопределяет интерес ученых- юристов и специалистов-практиков к роли информации в обществе и связанных с ней информационно-правовым отношениям, что позволяет говорить о формировании новой отрасли права-информационного права .

[1]«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // СПС КонсультантПлюс. Ст.29

Таким образом, формирование информационного права является следствием формирования информационного общества.

Существующая структура отрасли информационного права включает следующие подотрасли: компьютерное право, право информационной безопасности, право массовой информации, интернет-право, регулирующие определенные виды информационных отношений, являющихся особым родом общественных отношений.

Информационная безопасность является многогранным понятием, об этом свидетельствует существующее множество его определений. Поэтому целесообразно рассмотреть основные подходы к формированию этого понятия.

В рамках одного подхода под информационной безопасностью понимают- состояние общества, при котором обеспечена защита личности, общества и государства в информационном пространстве от воздействия на них организованных или стихийно возникающих информационных потоков.

В рамках другого подхода содержание информационной безопасности сводиться к трем ключевым составляющим:

1) состояние безопасности информационного пространства;

2) состояние безопасности информационной инфраструктуры;

3) состояние безопасности самой информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность, доступность.

Третий подход исходит из того, что информационное пространство представляет собой симбиоз информационно-технической (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологической составляющих. Следовательно, информационную безопасность общества можно также представить как интеграцию информационно-технической и информационно-психологической безопасностей.

Анализ, рассмотренных выше подходов показывает, что информационная безопасность - довольно емкая и многосторонняя проблема, затрагивающая не только определение защиты информации, но и объектов и методов этой защиты.

Особое место отводится информационной безопасности в современных условиях в области гражданского права.

В соответствии с теорией гражданского права, объектами гражданских прав, для которых вопросы информационной безопасности наиболее значимы являются:

- информация как объект гражданских прав;
- интеллектуальная собственность как объект гражданских прав;
- личные неимущественные права.

Информация является объектом гражданских прав только в том случае, если ее обладатель может извлечь какую-либо имущественную выгоду. Обычно эта информация определяется как служебная или коммерческая тайны.

Например, работники, разгласившие тайну вопреки трудовому договору, обязаны возместить причиненные убытки.

Гражданско-правовое регулирование вопросов интеллектуальной собственности особенно актуально, в силу простоты технической реализации и быстродействия операций копирования и распространения, при использования программного обеспечения.

Гражданско-правовое регулирование вопросов электронной подписи особенно актуально, в силу простоты технической реализации, быстродействия операции и частоты использования. Статья 10 Федерального закона от 11 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (принят ГД РФ 25.03.2011) определяет обязанности участников электронного взаимодействия «1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом…»[2]

Особую группу объектов гражданских прав, для которых гражданско-правовое регулирование сегодня социально значимо, образуют личные неимущественные права, под которыми понимаются: жизнь, здоровье, достоинство личности, личная неприкосновенность, честь, деловая репутация, неприкосновенность частной жизни, личная и семейная, медицинская, банковская тайна и т.д.

Это связано с тем, что при правовом регулировании взаимоотношений в Интернете необходимо учитывать:

1. Такие предметы отношений, как сайт, веб-страница, домен, IP-адрес, электронно-цифровая подпись, электронная почта, аккаунты в социальных сетях и т.п.
2. Анонимность пользователей.
3. Низкая стоимость доступа к сети Интернет.
4. Высокая скорость распространения информации.
5. Простота охвата большой аудитории.

[2]Федеральный закон от 11 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (принят ГД РФ 25.03.2011) // СПС КонсультантПлюс ст.10

С учетом данных обстоятельств проблема обеспечения информационной безопасности в контексте развития норм гражданского права представляется весьма актуальной как в научном, так и в прикладном плане.

Объектом исследования является комплекс общественных отношений, связанных с использованием доменных имен.

Предметом исследования является гражданско-правовое регулирование отношений в области доменных имен.

Цель исследования - комплексное регулирование гражданско-правовых отношений в сфере информационной безопасности (доменные имена)

Задачи исследования:

1.Изучить исторические аспекты возникновения и развития информационной безопасности.

2.Изучитьзарубежный опыт правового регулирования информационной безопасности.

3.Проанализировать основные принципы информационной безопасности на примере триады CIA (КЦД).

4. Выявить основные проблемы гражданско-правового регулирования информационной безопасности в РФ

5. Исследовать правовую природу доменных имен в аспекте информационной безопасности.

6. Исследовать нормативное правовое регулирование доменного имени в современных условиях на основе анализа и классификации нормативно-правовых актов.

7. Исследовать основные противоречия в сфере гражданско-правового регулирования доменных имен и порождаемые ими гражданско-правовые нарушения.

8. Разработать процедуры выбора и регистрации доменного имени

9. Разработать процедуры разрешения гражданско- правовых споров по доменным именам

10. Разработать процедуры обеспечительных мер при доменных спорах

Методология проведения исследования.

Методологической основой исследования являлись общенаучные и специальные юридические методы исследования: логический, исторический, системный и сравнительно-правовой анализ. Метод системного анализа применялся для определения правовой природы доменного имени. Метод сравнительно-правового анализа применялся для выработки предложений по совершенствованию гражданско- правового регулирования доменных имен.

Теоретическая база исследования

Теоретическую базу исследования составили труды российских ученых: Звягина В.А, ГерцевойЕ. Н., ГринкевичА. П., Иванова В.В. Микаевой А. С., Попцова А. В., Савельева А.И., Серго А. Г., и зарубежных Дж. М. Андерсона (J. M. Anderson), Дж. Андресса (J. Andress) , Белинда Айзека(BelindaIsaac), Дункан Карли (DuncanCurley), Себастьяна Баума (SebastianBaum), Эмерсона Х. Тиллера (Emerson H. Tiller).

Нормативная база исследования

Нормативную базу исследования составляют"Конвенция по охране промышленной собственности" (Заключена в Париже 20.03.1883) (ред. от 02.10.1979), Конституция РФ, Гражданский кодекс Российской Федерации, федеральные законы Российской Федерации, нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

Эмпирическую основу исследования составляет российская судебно-арбитражная практика разрешения споров по доменным именам.

Научная новизна

Научная новизна диссертационной работы заключается в том, что на основе комплексного исследования правовых вопросов, в области доменных именв гражданском обороте:

1. определена правовая природу доменного имени и его место в системе объектов гражданских прав как самостоятельного средства

интеллектуальной собственности наряду с традиционными средствами (товарными знаками, коммерческими обозначениями и т.п.);

2. определены ключевые причины возникновения судебных споров по доменным именам и систематизированы основные правонарушения в сфере доменных имен.

Положения, выносимые на защиту

1.Одним из центральных вопросов гражданско-правового регулирования в области информационной безопасности является регулирование прав на доменное имя, поскольку затрагивает все три базовых принципа информационной безопасности: конфиденциальность, целостность, доступность.

2.Необходимо включение доменных имен в перечень объектов гражданского оборота, с учетом того, что доменное имя все больше будет приобретать свойства товарного знака, а значит свойства интеллектуальной собственности.

3. Основные противоречия в сфере гражданско-правового регулирования доменных имен и порождаемые ими гражданско-правовые нарушения

4. Процедуры разрешения гражданско- правовых споров в области доменных имен (выборе регистрации, трансфер, наследование, обеспечительные меры).

Апробация результатов исследования

Сформулированные в диссертации предложения были представлены на Всероссийской научно-практической конференции по безопасности Тольятти: Волжский университет имени В.Н. Татищева, 2018 и XVI Международной научно-практической конференции «Татищевские чтения: Актуальные проблемы науки и практики» - Тольятти: Волжский университет имени В.Н. Татищева, 2019.

Личный вклад автора в исследование- исследование было выполнено автором полностью самостоятельно.

Структура и объем магистерской диссертации– диссертация состоит из введения, трех глав, заключения и списка используемой литературы и источников в количестве 31; общий объем составляет 84страницы.

Глава 1 ОБЩИЕ ПОЛОЖЕНИЯ И ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Исторические аспекты возникновения и развития информационной безопасности.

Информационная безопасность возникла в следствии:

-появления коммуникаций между людьми;

- осознанием возможности нанести действенный ущерб путем неправомерного использования результатов этих коммуникаций

1 этап — до 1895 года — характеризуется использованием в основном устных и письменных коммуникаций, соответственно в этот период необходимо было защитить информацию личного или государственного значения, как правило закрепленную в виде письменных документов.

Методами защиты информации в этот период были:

-помещение документов в особые хранилища: сейфы,

тайники и т.п.;

-шифрование информации.

Главным достижением этого периода, с точки зрения информационной безопасности, стала разработка основ криптографии в следствии разработки широкого использования шифров.

2 этап до 1950 гг. — характеризуется созданием и бурным развитием телефонной и радиосвязи, радиолокации и гидроакустики

Методами защиты информации в этот период были:

- технологии кодирования информации;

- технологии помехоустойчивости

-противодействие активным и пассивными электромагнитном помехами.

Достижениями этого периода, с точки зрения информационной безопасности были:

-разработка теории криптографии;

-разработка теории помехозащищенности;

-разработка теории передачи сообщений;

-разработка теории радиолокации;

-разработка теории гидроакустики;

- разработка электронных коммутаторов, многоканальной связи.

3 этап до 1960 года — центральное место в этот период занимает появление и лавинообразное распространение ЭВМ.

Методами защиты информации в этот период были:

- новые технологии криптографии;

-технологии администрирования;

- организация доступа к ЭВМ.

Достижениями этого периода, с точки зрения информационной безопасности были:

-разработка алгоритмических языков программирования;

-разработка теории и технологий разработки и сопровождения банков и баз данных;

- разработка общей теории информации.

4 этап до 1970 года — центральное место в этот период занимает появление и лавинообразное распространение локальных компьютерных сетей.

Методами защиты информации в этот период были:

- новые технологии криптографии;

-технологии администрирования;

- сетевые технологии ограничения доступа;

- организация доступа к локальным сетям ЭВМ.

Достижениями этого периода, с точки зрения информационной безопасности были:

-разработка технологии компьютерных сетей;

-разработка теории и технологий разработки и сопровождения распределенных банков и баз данных;

- разработка общей теории компьютерной безопасности.

5 этап по 2000 года — центральное место в этот период занимают появление и лавинообразное распространение:

- сети Интернет;

-мобильных коммуникационных устройств.

Следствием этих двух факторов стало появление организованных групп-хакеров, похищающих информацию с многочисленных компьютеров не только частных лиц, но и организаций и даже государственных структур для получения экономических выгод.

Методами защиты информации в этот период были:

- новые технологии криптографии;

- новые технологии администрирования;

-новые технологии беспроводной связи;

- новые сетевые технологии ограничения доступа;

- организация доступа к глобальной компьютерной сети Интернет.

- правовые методы.

Достижениями этого периода, с точки зрения информационной безопасности были:

-разработка технологии глобальных информационно-коммуникационных сетей;

-разработка теории и технологий разработки и сопровождения распределенных банков и баз данных;

- разработка общей теории компьютерной безопасности;

- разработка новых критериев безопасности (триада CIA и ее модификации);

-разработка законодательной базы: стратегии, доктрины, законы, положения и т. д.;

- разработка технологии криптографии с открытым ключом.

6 этап по настоящее время - определяющим фактором сегодня является развитие мирового цифрового пространства.

Для обеспечения информационной безопасности на этом этапе необходимо:

- создание новых критериев информационной безопасности человечества;

- разработка новых технологий криптографии, а не только с открытым ключом;

-формирование новой отрасли права- информационного права, включающая составной частью информационную безопасность.

1.2 Зарубежный опыт правового регулирования информационной безопасности.

Центральным законами, регулирующим информационную безопасность в США являются:

- закон об информационной безопасности;

- закон о совершенствовании информационной безопасности.

В соответствии с ними:

- ответственным за выпуск стандартов и руководств по информационной безопасности является конкретный исполнитель – Национальный институт стандартов и технологий;

-все федеральные информационные системы обязаны быть обеспечены системой их информационной защиты;

- негосударственный сектор имеет право на разработку Национальным институтом стандартов и технологий руководств, средств и методов для своих нужд;

- упрощены операций с криптосредствами.

В связи с тем, что право в США носит прецедентный характер, существует документ, формализующий большинство прецедентов и известный как «Оранжевая книга»

«Степень доверия оценивается по трем критериям:

1. Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Чем выше степень доверия системы, тем строже и многообразнее должна быть политика безопасности.

2. Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС. Он показывает, насколько корректны механизмы, отвечающие за политику безопасности.

3. Механизм подотчетности (протоколирования) – доверенная система должна фиксировать все события, касающиеся безопасности.

В Оранжевой книге предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности.

Требование1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности.

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.

Требование 3. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы.

Требование 4. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать: независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты.

Требование 6. Непрерывность защиты. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита

должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом.

Приведенные выше базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности

Группа D. Минимальная защита.

Группа C. Дискреционная защита.

Группа B. Мандатная защита.

Группа A. Верифицированная защита»з

Классы безопасности

Определяется 4 уровня доверия:

Эти уровни обозначены буквами – D, C, B, A.

Уровень D–неудовлетворительный в плане информационной безопасности.

При переходе в направлении уровня А требования к системе ожесточаются…»[4].

Центральными законами, регулирующим информационную безопасность в Англии являются:

-закон о перехвате коммуникационных сообщений;

- закон о защите информации;

- закон о реабилитации правонарушителей;

- закон о телекоммуникациях;

- закон о полиции;

- закон о вещании;

- закон о защите от преследований.

В соответствии с ним:

---

[4]Department of Defense Tristed Computer System Evaliatin Criteria- Dod 520028-STD,Desember 26, 1985

-создан независимый комиссариат по защите информации;

-юридические лица, использующие персональные данные и ведущие учетные записи, обязаны регистрироваться в комиссариате по защите информации;

- соблюдение требований Директивы о защите информации, принятой Европейским Союзом;

В связи с прецедентный характером английского права МВД издало рекомендации по установке подслушивающих устройств.

Его особенность в отсутствии контроля за перехватами информации со стороны судебных и государственных органов.

Англия подписала ряд международных договоров:

-конвенцию о защите частных лиц в отношении персональных данных

-директиву ОЭСР о защите неприкосновенности частной жизни и международных обменов персональными данными.

Центральными законами, регулирующим информационную безопасность в Германии являются:

- ФЗ о защите персональных данных;

- поправка к Конституции, разрешающая полиции устанавливать подслушивающие устройства;

- закон "Об информационных и коммуникационных (мультимедиа) услугах"

- закон, разрешающий Федеральной криминальной службе содержать национальный банк генетических данных;

- закон земли Бранбенберг, открывающий гражданам доступ к государственным базам данных.

В соответствии с ними:

- все 16 земель Германии имеют собственные законы о защите персональных данных;

-устанавливаются определенные механизмы защиты информации, в информационно- телекоммуникационных сетях;

-устанавливаются определенные требования к цифровой подписи;

-за исполнение закона отвечают:

- на государственном уровне -Федеральная комиссия по защите персональных данных;

- на уровне каждой из земель- комиссия по защите персональных данных;

- на уровне негосударственного сектора- комиссар по защите персональных данных, в каждой из земель;

-необходимо получить разрешения на осуществление деятельности по обработке данных.

Германия подписала ряд международных договоров:

-Конвенция о защите частных лиц в отношении автоматической обработки персональных данных.

-Европейская конвенция о защите прав и основных свобод человека.

-Директива ОЭСР о защите неприкосновенности частной жизни и международных обменов персональными данными.

Центральными законами, регулирующим информационную безопасность в Чехии являются:

- закон о информационной безопасности;

- стратегия кибербезопасности на 2015 – 2020 гг.

В соответствии с ними:

-созданы: Национальный центр компьютерной безопасности;

-поддержка развития возможностей полиции расследовать и преследовать в судебном порядке преступления в информационной сфере;

- правительственная «Компьютерная группа реагирования на чрезвычайные ситуации»;

-компьютерные команды экстренной готовности.

Чехия подписала ряд международных договоров:

- меморандум о взаимопонимании между НАТО и Чешской Республикой;

- договор о информационной безопасности с ЕС.

1.3 Триада CIA (КЦД)

Прежде всего необходимо проанализировать существующие многочисленные точки зрения на понятие информационной безопасности. В работе Дж. М. Андерсона (J. M. Anderson), указывается, что «эта проблема частично связана с нечетким фундаментальным определением информационной безопасности…»[5]Несмотря на их отличия, краеугольным камнем для всех является триада КЦД- CIA.

В 1974 году Джерри Зальцер и Майкл Шрёдер изложили принципы триады в статье "Защита информации в компьютерных системах", написанной Зальцером и Шредером опубликованной в "Communications of the ACM".

Эти принципы:

— «конфиденциальность» — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;

— «целостность» — свойство сохранения правильности и полноты активов;

— «доступность» — свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

Для краткости эти принципы именуются триадой CIA.

После появления Интернета, облачных вычислений и др. потребовалось расширить количество принципов.

Вскоре ОЭСР предложила свою собственную модель информационной безопасности, интегрирующую девять принципов: осведомлённость, ответственность, противодействие, этика, демократия, оценка риска, разработка и внедрение безопасности, управление безопасностью.

В 2002-м году Дон Паркер предложил свой "Паркеровский гексагон".В работе Дж. Андресса (J. Andress)отмечается «Там, где триадасостоит из

[5] Anderson, J. M. Why we need a new definition of information security // Computers & Security. — 2003. — Vol. 22, no. 4. — P. 308

конфиденциальности, целостности и доступности, Паркерианская гексада состоит из этих трех принципов, а также владения или контроля, подлинности и полезности…»[6]

NIST увеличила количество принципов до 33, обеспечив методическую поддержку каждого из них путем разработки соответствующих руководств.

Министерство обороны США определило следующие принципы:

- подверженность системы риску;

-доступность уязвимости;

-способность эксплуатировать уязвимость.

В 2011 году международный консорциум The Open Group опубликовал стандарт управления информационной безопасностью O-ISM3.

Стандарт определяет цели безопасности:

-приоритетные цели безопасности (конфиденциальность);

- долгосрочные цели безопасности (целостность);

- цели качества информации (целостность);

- цели контроля доступа (доступность);

- технические цели безопасности.

Несмотря на различные существующие модели информационной безопасности в основе всех их находится классическая триада CIA.

Следует отметить, что триада CIA подразумевается, когда в контексте информационной безопасности говорят о:

- триаде КЦД- российские авторы;

- принципах;

- аттрибутах безопасности;

- свойствах;

- фундаментальных аспектах;

- информационных критериях;

- важнейших характеристиках;

[6] Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. P. 6

-базовых структурных элементах.

Информационная безопасность- развивающееся понятие о чем свидетельствуют, в частности, попытки отдельных организаций трансформировать понятие "информационной безопасности" в другие, например управление рисками, security governance и т.д.

Остановимся на содержании элементов этой триады более подробно.

Конфиденциальность

Конфиденциальность информации достигается предоставлением к ней доступа тому, кому она необходима для выполнения порученной ему в организации.

Причиной возникновения проблем этой группы является нарушение движения информационных потоков или ошибки в системе доступа.

1). Ошибки администрирования:

-неправильное формирование групп пользователей и определение прав их доступа;

-отсутствие политики формирования паролей пользователей.

2). Ошибки алгоритмов доступа к данным.

Примером нарушениями конфиденциальности является кража личности.

Средствами обеспечения конфиденциальности, в частности являются:

-классификация информации: на конфиденциальную, для внутреннего пользования и публичную;

-шифрование информации.

Целостность

Роль достоверности данных, хранящихся в файлах, базах данных или передаваемых по телекоммуникационным сетям трудно переоценить. Информация должна быть защищена от целенаправленного или случайного изменения, а также от каких-либо модификаций в при хранении, обработке или передаче.

Причины нарушения целостности информации:

- непосредственные действия на носитель информации;

- информационное воздействие;

- человеческий фактор;

- выход из строя оборудования, программного обеспечения;

Для сохранения целостности информации необходимо применение ряда контрольных мер:

-ограничение круга лиц, имеющих право изменять информацию лишь в силу выполнения служебных обязанностей;

- принцип разграничения полномочий- двойной контроль;

-внесение любых изменений должны быть осуществлены только корректно сформированными транзакциями.

-действия, влекущие изменения, должны быть обязательно протоколироваться.

Доступность

Принцип доступности- информация должна быть только доступна лицам, имеющим на это право.

Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо не возможен за время, требуемое за время необходимое для выполнения определенных операций.

Основными причинами, приводящими к нарушению этогопринципа, являются:

-саботаж;

-человеческие ошибки по невнимательности или слабой подготовки;

-отказ в обслуживании сетей связи;

- неудачно проведённая модернизация оборудования;

- некорректная переустановка программ.

Следует уделять особое внимание критичности времени простоя, которое приводит к недопустимым рискам.

Примером нарушения доступности является выход из строя сервера, на котором расположена требуемая для принятия решения информация.

1.4 Основные проблемы гражданско-правового регулирования информационной безопасности в РФ

В указе Президента РФ информационная безопасность Российской Федерации определяется как«состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз…»[7].

Основными проблемами информационной безопасности в гражданском праве являются:

1). Коммерческая или служебная тайна

2). Правовое регулирование использования электронной цифровой подписи в электронных документах

3). Правовые проблемы создания и эксплуатации информационных систем

4).Регулирование использования информационно-телекоммуникационных сетей Интернет.

Наиболее сложными являются последние, поэтому рассмотрим их более подробно.

Основными проблемами «в сети Интернет, нуждающимися в скорейшем нормативно-правовом урегулировании, являются:

1. Распространение экстремистских материалов в сети Интернет.

2. Проблемы, связанные с защитой прав интеллектуальной собственности в сети Интернет.

3. Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

4. Защита персональных данных.

5. Правовое регулирование электронной торговли в сети Интернет.

[7]Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"// СПС Консультант Плюс

6. Пропаганда, незаконная реклама наркотических средств и психотропных веществ.

7. Незаконное распространение порнографических материалов в сети Интернет.

8. Клевета в сети Интернет.

9. Мошенничество в сети Интернет.

Регулированию нормами гражданского права подлежат:

1. Проблемы, связанные с защитой прав интеллектуальной собственности в сети Интернет.

2. Проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя).

3. Защита персональных данных.

4. Правовое регулирование электронной торговли в сети Интернет.

5. Клевета в сети Интернет.

6. Мошенничество в сети Интернет»[8]

Фундаментальным направлением является создание российского государственного сегмента сети "Интернет", в соответствии с Указом Президента РФ «Федеральной службе охраны Российской Федерации обеспечивать поддержание, эксплуатацию и развитие российского государственного сегмента сети "Интернет"…»[9].

Проведенный анализ показывает, что одним из центральных вопросов является гражданско- правовое регулирование прав на доменное имя,в силу того, что:

-наибольшее количество судебных дел, связанных с гражданско-правовым регулированием информационной безопасности, относится к спорам по доменным именам;

---

[8] А. С. Микаева Проблемы правового регулирования в сети Интернет и их причины// Актуальные проблемы российского права. 2016. № 9 (70) С.68

[9] Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет")// СПС КонсультантПлюс

- правовое урегулирование этого вопроса позволит во многом успешно разрешать и большинство других проблем.

Вопросы, связанные с правовым регулированием прав на сетевой адрес, приобретают международный характер. На данный момент судебные споры, касающиеся доменных имен, являются наиболее частыми в судебной практике.

В соответствии с вышеизложенным, субъектами права являются государственные и муниципальные организации, юридические и физические лица.

Как показано в работе А.С. Серго «К основным характеристикам субъекта права на доменное имя следует отнести возможность принадлежности права на доменное имя только одному лицу и возможность принадлежности доменного имени любому субъекту права (физическому или юридическому лицу, органу государственной власти или местного самоуправления)…»[10].

Таким образом в данной главе рассмотрены исторические аспекты возникновения и развития информационной безопасности, проанализированы
зарубежный опыт правового регулирования и принципы информационной безопасности на основе триады CIA (КЦД), сформулированы основные проблемы гражданско-правового регулирования информационной безопасности в РФ.

[10]Серго А.Г. Правовой режим доменных имен и его развитие в гражданском праве: Автореф. дис.на соиск. уч. степ. д-ра юрид. наук. М., 2011. С.16

ГЛАВА 2 ОБЩАЯ ХАРАКТЕРИСТИКА И АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГРАЖДАНСКО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ДОМЕННЫХ ИМЕН

2.1 Доменные имена и информационная безопасность

Каждый компьютер в глобальной сети имеет персональный IP-адрес, который представляет собой конкретную последовательность цифр (например, 356.279.6.16). «Для удобства запоминания и восприятия была создана доменная система имен (Domain Name System – DNS)…»[11], поскольку, цифровые адреса запоминаются трудно проще использовать знаковое сочетание символов.

Доменное имя – это уникальное сочетание символов латинского алфавита, которое определяет конкретный информационный ресурс среди огромного количества других, т.е.представляет собой адрес, длиной от 2 до 63-х символов. Таким образом, чтобы получить доступ к конкретному информационному ресурсу нужно зайти на сайт в сети Интернет, на котором он расположен, а для этого необходимо знать доменное имя.

Создание доменного имени подразумевает размещение веб-страницы на сервере с определенным IP-адресом.

Каждый раз, вводится название домена в браузер, служба DNS определяет, какому электронному серверу соответствует заданное имя, и какой конкретно сайт вам необходимо предоставить.

DNS-сервер – это программное обеспечение, осуществляющее преобразование цифрового адреса в доменное имя и наоборот.

Каждое имя домена состоит из нескольких частей, разделенных точками. Число этих уровней чаще всего ограничивается от 2 до 3.

В последовательном порядке справа налево следует верхний и последующие (по убыванию) уровни. Доменом верхнего уровня или доменной зоной называют окончание:

---

[11]. Серго А. Г. Доменные имена в свете нового законодательства М.: ГОУ ВПО РГИИС, 2010. С.13

-имеющее отношение к географической принадлежности (например, домен «.RU» – России а «.BY» — Беларуси);

-имеющее отношение к определенному виду деятельности («.info» – информационный, «.travel» – туристический и «.org» – некоммерческий).

Домены второго уровня – это уникальные в своей группе (в родительской иерархии) имена, регистрируемые у организаций-регистраторов. Например, abdullinru.ru – это домен второго уровня.

Третьего уровня – это безграничные имена, регистрируемые у посредников (организаций владеющих доменами 2-го уровня). Выглядят они следующим образом: name.abdullinru.ru, где name – это поддомен основного сайта.

Рассмотрим нарушения триады CIA, связанные с нарушением прав на доменные имена.

Конфиденциальность - доступна информация, к которой нет имеются права доступа.

Целостность- нарушение непреднамеренные и преднамеренные – модификация информации.

Доступность - недоступна информация, к которой имеются права доступа.

Правоотношения:

-на первичном рынке доменных имён, правоотношения возникают между регистратором доменного имени и физическим или юридическим лицом, покупающим доменное имя.

-на вторичном рынке доменных имён, правоотношения возникают между физическим или юридическим лицом, продающим и покупающим доменное имя.

При этом под регистрацией или покупкой подразумевается покупка права администрирования доменного имени на определенный срок, как правило на год.

Передача прав на домен представляет собой сделку, т.е. «действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей»[12], следовательно, к ней нужно применять все статьи Гражданского кодекса Российской Федерации, касающиеся сделок (Статьи 153-165).

2.2 Нормативное правовое регулирование доменного имени в современных условиях. Анализ и классификация нормативно-правовых актов

Международные законы

Важнейшее значение в нормативном регулировании доменных имен имеет Парижская конвенции по охране промышленной собственности 1883 года.

Особенно Статья 10-bis и Статья 10.ter

«Статья 10.bis

[Недобросовестная конкуренция]

(1) Страны Союза обязаны обеспечить гражданам стран, участвующих в Союзе, эффективную защиту от недобросовестной конкуренции.

(2) Актом недобросовестной конкуренции считается всякий акт конкуренции, противоречащий честным обычаям в промышленных и торговых делах.

(3) В частности, подлежат запрету:

1) все действия, способные каким бы то ни было способом вызвать смешение в отношении предприятия, продуктов или промышленной или торговой деятельности конкурента;

2) ложные утверждения при осуществлении коммерческой деятельности, способные дискредитировать предприятие, продукты или промышленную или торговую деятельность конкурента;

3) указания или утверждения, использование которых при осуществлении коммерческой деятельности может ввести общественность в

[12] ГерцеваЕ. Н., ГринкевичА. П. Доменные споры. Судебная практика в России: Эксмо, Москва, 2011 С.201

заблуждение относительно характера, способа изготовления, свойств, пригодности к применению или количества товаров».[13]

В соответствии со статьей 10-bis Парижской конвенции по охране промышленной собственности ее действие распространяется только на промышленные и торговые делах при осуществлении коммерческой деятельности.

«Статья 10.ter

[Товарные знаки, фирменные наименования, ложные
указания, недобросовестная конкуренция: средства
защиты, право обращаться в суд]

(1) Страны Союза обязуются обеспечить гражданам других стран Союза законные средства для эффективного пресечения всех действий, указанных в статьях 9, 10 и 10.bis.

(2) Кроме того, они обязуются предусмотреть меры, позволяющие союзам и объединениям, существование которых не противоречит законам их стран и которые представляют заинтересованных промышленников, изготовителей или торговцев, действовать через суд или административные органы с целью пресечения действий, предусмотренных в статьях 9, 10 и 10.bis, в той мере, в какой это допускает закон страны, где испрашивается охрана, для союзов и объединений данной страны»[14].

Среди Российских законов наибольшее значение при регулировании доменных имен имеют следующие:

1). Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция)

«Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию,

[13]Парижская конвенции по охране промышленной собственности 1883 годаСт. 10-bis
[14]Там же. Ст.10.ter

распространение которой в Российской Федерации запрещено» (введена Федеральным законом от 28.07.2012 N 139-ФЗ).

1. В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (далее - реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра

оператора реестра - организацию, зарегистрированную на территории Российской Федерации »[15].

2). "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018)

«ГК РФ Статья 1484. Исключительное право на товарный знак

1. Лицу, на имя которого зарегистрирован товарный знак (правообладателю), принадлежит исключительное право использования товарного знака в соответствии со статьей 1229 настоящего Кодекса любым не противоречащим закону способом (исключительное право на товарный знак), в том числе способами, указанными в пункте 2 настоящей статьи. Правообладатель может распоряжаться исключительным правом на товарный знак.

2. Исключительное право на товарный знак может быть осуществлено для индивидуализации товаров, работ или услуг, в отношении которых товарный знак зарегистрирован, в частности путем размещения товарного знака:

1) на товарах, в том числе на этикетках, упаковках товаров, которые производятся, предлагаются к продаже, продаются, демонстрируются на

территории Российской Федерации, либо хранятся или перевозятся с этой целью, либо ввозятся на территорию Российской Федерации;

2) при выполнении работ, оказании услуг;

3) на документации, связанной с введением товаров в гражданский оборот;

4) в предложениях о продаже товаров, о выполнении работ, об оказании услуг, а также в объявлениях, на вывесках и в рекламе;

5) в сети "Интернет", в том числе в доменном имени и при других способах адресации.

---

[15] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД РФ 14.07.2006) // СПС КонсультантПлюс Ст.15

3. Никто не вправе использовать без разрешения правообладателя сходные с его товарным знаком обозначения в отношении товаров, для индивидуализации которых товарный знак зарегистрирован, или однородных товаров, если в результате такого использования возникнет вероятность смешения…»[16] .

3). Постановление Президиума Суда по интеллектуальным правам от 15 октября 2013 г. № СП-23/3 “Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору”

Административные регламенты

В настоящее время для разрешения возникающих вопросов в отношении регистрации прав доменных имен Интернет-корпорацией по назначению имен и нумерации сети Интернет (Internet Corporation for Assigned Names and Numbers, ICANN) приняты в 1999 году основные документы:

-Единая Политика Рассмотрения Споров о Доменных Именах (Uniform Domain Name Dispute Resolution Policy или UDRP);

- Правила для Единой Политики Рассмотрения Споров о Доменных Именах.

В настоящее время создано несколько центров, назначение которых – рассмотрение доменных конфликтов в зонах общего пользования (COM, NET, ORG), в отдельных национальных доменах первого уровня (например, .nu, .tv, .ws).

Данные центры не стоит путать с судами – созданная структура призвана разрешать вопросы, связанные с передачей доменов во внесудебном порядке.

[16] Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018) Ст. 1484

В работе Эмерсон Х. Тиллера (Emerson H. Tiller) представлены « обзор и критика разрешения споров по доменным именам ICANN»[17]

5). «Правила регистрации доменных имен в домене. РФ» и «Положения о приоритетной регистрации доменных имен в домене. РФ»Координационный центр доменов RU/РФ.

Координационный центр национального домена сети Интернет (сокращенно - Координационный центр доменов RU/РФ), созданный в 2001 году как некоммерческая организация, - это администратор российских доменов верхнего уровня .RU и.РФ.

В его функции входит:

- выработка правил регистрации доменных имен в доменах .RU и .РФ;
- аккредитация регистраторов второго уровня;
- развитие российских доменов верхнего уровня.

2.3Основные противоречия в сфере гражданско-правового регулирования доменных имен и порождаемые ими гражданско-правовые нарушения

Центральным противоречием является отсутствие правового статуса у доменного имени. Что создает предпосылки для большинства правонарушений в этой области, в том числе и не умышленных.

Например, право на доменное имя позволяет администратору:

-указывать это имя в качестве интернет-адреса;

- размещать по этому адресу сайт;

-выделять последующие уровни, для регистрируемых администраторов последующего уровня;

- определять коммерческую политику и т. п.

Эти полномочия администратора на сегодня слабо ограничены законодательно, в силу того, что юридически не закреплен правовой статус доменных имен.

[17] Emerson H. Tiller. ICANN's Uniform Domain Name Dispute Resolution Policy: An Overview and Critique // Internet Law & Business. Vol. 1, No. 8. June 2000. p. 589

Поэтому на сегодня гражданско-правовые отношения в области доменных имен, осуществляется на основе:

- наиболее общих норм существующего законодательства Российской Федерации;

- положений и правил административных регламентов, которые разрабатывают сами регистрирующие негосударственные организации, такие как Интернет-корпорация по назначению имен и нумерации сети Интернет (ICANN) и Координационный центр доменов RU/РФ.

Это центральное противоречие порождает основные гражданско-правовые правонарушения в области доменных имен, к которым относятся:

- прекращение поддержки доменного имени регистратором;

- блокирование управлением домена организации со стороны физических лиц;

- плохая «репутация» доменного имени;

- неправомерное использование брендов известных организаций или фирм, за счет совпадающих или сходных до степени смешения доменных имен и товарных знаков;

- фишинг доменов;

- «угон» доменов;

-размещение неправомерной информации;

- неправомерное наследование доменов, в случае если они являются ценным активом;

- неправомерным доменным трансфером;

- невозможность обеспечить выполнение решений суда при доменных спорах;

-неправомерный выбор подведомственности данной категории споров и ответчиков.

Существующие подходы к определению понятия доменного имени.

Рассматривая правовую сущность, необходимо исходить из того, чтосущность в общем смысле- это суть, содержание, основные качества,

свойства чего-нибудь, а правовая – относящаяся к праву. Поэтому, исследовать правовую сущность это исследовать основные свойства чего-нибудь, с точки зрения права.

В исследованиях в специалистов содержатся различные подходы к сущности понятия «доменное имя».

В работе Попцова А.В.выделяются следующие «две важные функции - функцию адресации в сети Интернет и индивидуализации информационного ресурса (веб-сайта). При этом, доменные имена обладают коммерческой ценностью, например, могут приносить прибыль, выступая в качестве объектов продажи и инвестирования или индивидуализируя информационный ресурс в сети Интернет»[18].

В работе Звягина В. А. выделяются следующие «функции доменных имен: адресная, идентификационная, индивидуализирующая, информационная (рекламная) и функция географической привязки»[19]. Автором также отмечаются некоторые свойства, относящиеся к объектам интеллектуальной собственности.

В работе Серго А. Г.«определена роль доменного имени как средства индивидуализации в сети Интернет для развития конкурентных отношений и даны предложения по совершенствованию законодательства в сфере доменных имен и средств индивидуализации на основе отечественного и международного опыта.

Доменные имена «стали ценным активом, имеющим высокую коммерческую ценность, и предметом повседневной необходимости для любого предпринимателя.

Стоимость доменного имени вполне сопоставима со стоимостью товарного знака и имеет схожий механизм ценообразования»[20].

---

[18]Попцов А.В. Правовое регулирование доменного имени в Российской Федерации: Автореф. дис. на соиск. уч. степ., канд. юрид. наук. М., 2009. С.12

[19]Звягин В.А. Проблемы правового регулирования использования исключительных прав на фирменные наименования и прав на доменные имена: Автореф. дис. на соиск. уч. степ., канд. юрид. наук. М., 2011. С. 9

[20]Серго А.Г. Правовой режим доменных имен и его развитие в гражданском праве: Автореф. дис. на соиск. уч. степ., д- ра юрид. наук. М., 2011. С. 16

Основными свойствами являются:

- адресная;

- идентификационная;

-индивидуализирующая, информационная (рекламная);

- функция географической привязки».

При несомненно важнейших функциях адресной и идентификационной, сегодня все большее значение приобретет коммерческая стоимость доменного имени (стоимость отдельных доменов доходит до 14 миллионов долларов) и с течением времени, в силу экспоненциального характера увеличения объемов информации в мире, будет только возрастать.

В работе Себастьян Баум (Sebastian Baum)также «Вопросы о том, следует ли выделять общие термины частным лицам в качестве доменных имен (mitwohnzentrale.de) и должны ли суды передавать доменные имена в случае конфликта между двумя правообладателями на одно доменное имя (shell.de и vossius.de) анализируются на основе экономических критериев…»[21].

Поэтому доменное имя все больше будет приобретать свойства товарного знака, а значит свойства интеллектуальной собственности, что необходимо учитывать при разработке законодательных актов.

Для рассмотрения противоречий при регистрации доменных имен необходимо дать основные определения.

Администратор доменного имени (пользователь) — лицо, на имя которого зарегистрировано доменное имя.

Под администрированием доменного имени понимается управление:

- порядком использования доменного имени;

- технической составляющей его функционирования.

[21] Sebastian Baum. Domain Name Conflicts in Germany — An Economic Analysis of the Federal High Court's Recent Decisions// European Business Organization Law Review, Vol 4, Issue 1, March 2003 p. 137

Домен — область пространства доменных имен сети Интернет, имеющая идентификационное имя.

Регистрация доменного имени — запись регистратора в реестр доменного имени и его администратора.

Реестр — центральная база данных домена. РФ, содержащая информацию о зарегистрированных доменных именах, администраторах доменов.

Техническая поддержка реестра домена .РФ обеспечивается АНО "Российский Научно- Исследовательский институт развития общественных сетей" (Рос НИИРОС).

Процедура регистрации доменного имени:

- выбрать доменное имя;

- убедиться, что выбранное доменное имя свободно (информационный сервис WHOIS);

-выбрать регистратора;

- для регистрации домена заполнить анкету на сайте регистратора;

- оплатить счет любым из способов способом предложенным регистратором.

Процедура регистрации свидетельствует о том, что договора на регистрацию доменов, заключаются в форме оферты, под которой, согласно статье 435 ГК РФ «признается адресованное одному или нескольким конкретным лицам предложение, которое достаточно определенно и выражает намерение лица, сделавшего предложение, считать себя заключившим договор с адресатом, которым будет принято предложение».

Однако, при желании, возможно и подписание бумажной версии договора. Регистрация доменного имени считается завершенной после внесения в реестр информации о нем. Срок управления администратором зарегистрированного доменного имени, как правило составляет один год, после чего необходимо продлить договор.

Сегодня существует достаточно большое количество регистраторов, с разной стоимостной политикой.

Из сказанного выше следует, что регистрация доменного имени регистратором для физических или юридических лиц является правом последних управлять определенным доменным именем в течении определенного времени, как правило один год и таким образом представляет собой услугу и должно регулироваться договором оказания услуг.

Основное противоречие здесь заключается в том, что юридически основные требования к подобным договорам, в отличие , например от договоров по оказанию транспортных услуг, никак не закреплены в силу неопределенности правовой природы самого доменного имени и устанавливаются самими негосударственными организациями, которые не только могут изменять их по собственному усмотрению, но и вообще прекратить свою деятельность.

Например, компании-регистратора могут возникнуть серьезные проблемы, связанные с:

- лишением аккредитации;

- внутренними производственными конфликтами.

Так, как с точки зрения реестра доменов администратор конкретного имени зависит от администратора более высокого уровня (регистратора), то потеря управления регистратором домена верхнего уровня автоматически приведет к потере управления всех доменов нижнего уровня и соответственно к большим репутационным и экономическим потерям фирм, например при интернет- торговле.

Таким образом, это противоречие порождает такое гражданско-правовое правонарушение как одностороннее прекращение поддержки доменного имени регистратором при выполнении своих обязанностей владельцем доменного имени.

Необходимо предусмотреть в законодательстве меры по тому, кто принимает на себя ответственность за дальнейшее поддержание домена и в какие сроки.

Следующее противоречие связано с регистрацией доменного имени, которое раньше уже существовало.

Основное противоречие здесь заключается в том, что с одной стороны регистратор регистрирует любые доменные имена, за исключением действующих на данный момент, а с другой стороны владелец доменного имени узнает о плохой «репутации» домена только по прошествии нескольких недель. Ситуация, в основном, относиться к форс-мажорным.- «угон» доменов;

Например, фирма регистрирует дорогой домен с известным и легко запоминающимся именем, добавляет на него эксклюзивный контент, а трафик его на протяжении длительного времени остается очень маленьким или вообще отсутствует. Чаще всего, в этом случае имя домена совпадает или похоже до степени смешения с именем домена, имеющего, в прошлом, плохую репутацию.

Эти домены необязательно принадлежали злоумышленникам на них могли располагаться сайты интернет-магазинов, корпоративные порталы компаний, которые в результате взлома стали распространять вредоносный код.

Репутацию доменов отслеживают поисковики, браузеры и антивирусы.

Основная проблема сайта, который попал в блэклист – это ограничение доступа к нему, и, как следствие, резкое падение трафика.

Кроме потери трафика, попадание в вирусные базы грозит репутации компании-владельца. Предупреждение о том, что сайт мошеннический и угрожает безопасности, скорее всего оставит негативное впечатление о владельце сайта, а информация о блокировке может быстро распространиться по соцсетям.

Следующее противоречие связано с регистрацией доменного имени на сотрудника компании.

Оно заключается в принадлежности права на доменное имя только одному лицу (физическому или юридическому), которое может его и не использовать, т.е. фактически блокировать. Таким образом, это противоречие порождает такое гражданско-правовое правонарушение как «угон» домена.

Например, если сотрудник, при создании сайта организации зарегистрировал домен на себя, то при его увольнении фирма практически теряет контроль над доменом, на котором базируются элементы современного бизнеса-сайт, электронная почта, визитки и др..

В результате владельцы компании, для которой доменное имя может являться важным, а иногда единственным ценным активом, его лишаются.

Наиболее простой метод- договориться с бывшим сотрудником компании, являвшимся администратором домена, о передаче (продаже) домена.

При трансфере доменного имени может возникнуть противоречие, заключающееся в том, что продавец и покупатель имеют аккаунты у разных регистраторов. Это противоречие порождает гражданско-правовое правонарушение трансфера доменного имени.

Например, если вы передаете права на домен другому человеку или компании, то здесь возможны два сценария развития событий:

1. Передача в рамках одного регистратора

Покупатель домена имеет аккаунт у того же регистратора, у которого зарегистрирован домен продавца. В таком случае передача не составит особого труда.

2. Передача от одного регистратора к другому

Покупатель домена имеет аккаунт у другого регистратора, и хочет перенести домен к нему. Такой вариант является очень сложным и требует гораздо больше усилий:

-для начала нужно уведомить текущего регистратора о том, что вы хотите перенести домен к другому. Чаще всего, это делается путем отправки письменного заявления, и/или сканов ваших документов, которые подтверждают личность. А также не забыть создать аккаунт у нового регистратора, и указать его;

- текущий регистратор свяжется с новым администратором и согласует процедуру передачи;

- в течении трех дней новый регистратор сделает необходимые действия, и принимает управление доменов на себя.

Если судебное разбирательство неизбежно, то необходимо доказать, что домен принадлежит организации.

К таким доказательствам относятся:

-имя домена совпадает с фирменным наименованием компании или с зарегистрированной торговой маркой (товарным знаком);

- содержание сайта полностью соответствует деятельности организации.

В некоторых случаях просто не удавалось изыскать правовых способов решения проблемы и организации приходится регистрировать новое доменное имя со всеми вытекающими отсюда репутационными и коммерческими издержками.

Основное содержание «доменных споров» обычно составляют конфликты между владельцами доменов и владельцами товарных знаков или фирменных наименований. Как правило, вторые пытаются отсудить домены у первых. Наиболее простым вариантом является мировое соглашение, когда ответчик «обязуется передать все права, относящиеся к доменному имени, включая право его администрирования, истцу»[22].

Регистрация и покупка доменных имен может осуществляться как с целью размещения на них сайтов, так и с целью инвестирования (перепродажи).

[22]Постановление ФАС Московского округа от 13.07.2010 N КГ-А40/7026-10 по делу N А40-100094/09-110-663

Инвесторы на вторичном рынке доменов подразделяются на:

-домейнеров- покупка «красивых» имен с перепродажей их по завышенной цене.

-киберсквоттеры, которые как показывает Дункан Карли (Duncan Curle)«приобретают имена сходных с известными брендами, угрожая перепродажей их конкурентам или размещение неудобной информации…»[23].

Основное противоречие заключается в том, что обладание зарегистрированным товарным знаком не позволяет его владельцу предотвращать регистрацию сходных до степени смешения доменных имен иными юридическими или физическими лицами.

Это противоречие порождает следующие гражданско-правовые правонарушения:

- блокирование управлением домена организации со стороны физических лиц;

- плохая «репутация» доменного имени;

- неправомерное использование брендов известных организаций или фирм, за счет совпадающих или сходных до степени смешения доменных имен и товарных знаков;

-размещение неправомерной информации.

Необходимо, учитывать физическое или юридическое лицо покупает или регистрирует доменное имя одинаковое или сходное до степени смешения с официально зарегистрированным товарным знаком другой фирмы или раскрученным брендом.

При решении данного спора необходимо опираться на:

-Статьи 10-bis и 10.terПарижской конвенции по охране промышленной собственности 1883 года;

- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция);

[23]DuncanCurley. Cybersquatters Evicted Protecting Names Under the UDRP // Entertainment Law Review. Vol. 12, No. 3. 2001. p. 91

- Федеральный закон от 11 декабря 2002 г. N 166-ФЗ "О внесении изменений и дополнений в Закон Российской Федерации "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров"

- ГК РФ Статья 1484. Исключительное право на товарный знак.

В случае, если физическое лицо покупает или регистрирует доменное имя одинаковое или сходное до степени смешения с официально зарегистрированным товарным знаком другой фирмы или раскрученным брендом, анализ судебной практики показывает, что наиболее значимыми юридическими фактами в данном случае являются:

- сроки регистрации доменного имени и товарного знака;

- используется домен или не используется;

-содержание сайта, который расположен на домене наносит репутационный урон фирме с зарестрированным товарным знаком;

- содержание сайта, который расположен на домене соотносится ли группой товаров или услуг, идентифицирующихся с зарегистрированным товарным знаком;

- состоит доменное имя и товарный знак из общеупотребительных слов.

В случае если регистрация доменного имени произошла раньше регистрации товарного знака, то отсудить доменное имя практически невозможно.

В противном случае необходимо доказать, что доменное имя используется для предпринимательской деятельности.

Физические лица не имеет права вести предпринимательскую деятельность с группой товаров или услуг, идентифицирующихся с зарегистрированным товарным знаком.

Выходом для физических лиц в данной ситуации является регистрация доменного имени через фирму-посредника.

В случае если в нотариально заверенных копиях с соответствующих сайтов содержание не относится к области деятельности фирмы, то отсудить доменное имя практически невозможно.

Сходная ситуация складывается в том случае, если доменное имя не используется, поскольку физическое лица практически блокирует использование доменного имени владельцем товарного знака, вынуждая последнего выкупить доменное имя.

С другой стороны, доменные имена могут содержать элементы, общеупотребительных слов, что также порождает противоречие: доменные имена могут содержать общепринятые символы и слова, а зарегистрировать эти символы и слова в качестве товарного знака нельзя (ст. 6 Закона о товарных знаках).

Если юридическое лицо покупает или регистрирует доменное имя, совпадающее точно или до степени смешения с зарегистрированным товарным знаком другой фирмы или раскрученным брендом, то анализ судебной практики показывает, что наиболее значимыми юридическими фактами в данном случае являются:

- сроки регистрации доменного имени и товарного знака;

- используется домен или не используется;

-содержание сайта, который расположен на домене наносит репутационный урон фирме с зарегистрированным товарным знаком;

- содержание сайта, который расположен на домене соотносится ли группой товаров или услуг, идентифицирующихся с зарегистрированным товарным знаком;

-правообладатели зарегистрировали одинаковые товарные знаки, для товаров различных классов МКТУ;

- состоит доменное имя и товарный знак из общеупотребительных слов;

- является ли доменное имя не просто совпадающим, а сходным до степени смешения с товарным знаком;

- количество доменных имен, сходны до степени смешения с товарным знаком зарегистрированных на одного владельца.

Основные подходы к решению большинства споров такие же, как рассмотренные в предыдущем параграфе, однако основную роль здесь играет, при прочих равных условиях, экономическая составляющая.

Действительно, фирма, имеющая доменное имя идентичное или совпадающее до степени смешения с товарным знаком другой фирмы, получает дополнительные конкурентные преимущества:

- при одинаковых товарных классах МКТУ, фактически перехватывать заказы у фирмы, имеющей раскрученный бренд, используя его «для рекламы другого юридического лица»[24];

- при различных товарных классах МКТУ, фактически рекламировать свою продукцию клиентам фирмы, имеющей раскрученный бренд;

- увеличивая трафик, повышать рейтинг своего сайта по посещаемости, фактически увеличивая его коммерческую стоимость.

Одним из ключевых доказательств, которые анализируются судом является распечатка интернет-страниц сайтов истца и ответчика.

Правообладателю товарного знака в иске будет отказано, если он не доказал:

- правомерность использования доменного имени на территории Российской Федерации в отношении своих товаров и услуг;

- отсутствие у администратора домена законных прав и интересов в отношении доменного имени;

- недобросовестность его использования.

Существующая сегодня ситуация , позволяющая зарегистрировать доменное имя, одинаковое или сходное до степени смешения с чужим товарным знаком, и не использовать его, является благоприятной для большого числа злоупотреблений, заключающейся в возможности

[24]Постановление Президиума ВАС РФ от 08.12.2009 N 9833/09 по делу N А40-53937/08-51-526

блокировки доменного имени и принуждении владельца товарного знака или раскрученного бренда к выкупу доменного имени.

С течением времени стоимость доменов возрастает в силу:

- раскрученности бренда;

- увеличения трафика и т. п.

В следствии чего доменное имя становиться ценным активом и превращается в важный элемент бизнеса, вплоть до того, что оно является единственным ценным ресурсом фирмы, последнее порождает острые судебные споры, иногда длящиеся годами.

Основное противоречие здесь заключается в том, что с точки зрения российского законодательства регистрация доменного имени — это услуга, оказываемая юридическим лицом физическому или юридическому лицу. То есть администратор не покупает домен — он лишь получает право администрирования домена, а соответственно, поскольку услугу наследовать нельзя, то и право на управление доменом нельзя наследовать. Это противоречие порождает возможности для правонарушений со стороны третьих лиц.

Проблемы при наследовании доменов можно условно разделить на две группы:

-администратор домена умер;

- компания ликвидируется, доменное имя является ценным активом и учредителям нужно разделить этот актив.

Если администратор домена умер, то коммерческая компания-регистратор вовсе не обязана передать право управления наследникам администратора.

В настоящий момент наиболее удобным способом передачи доменов по наследству является оформление их на юридическое лицо, владельцем которого является тот, кто заинтересован в корректном переводе доменов на наследников. В таком случае наследники унаследуют домены вместе с

юридическим лицом: наследование долей в компаниях более четко регулируется законодательством.

При разделе имущества обанкротившейся компании с доменными именами также возникают серьезные трудности. Если владельцев бизнеса несколько, раздел доменного имени между ними может оказаться весьма проблематичной задачей. Право управления доменом не набор мебели, включающий двенадцать стульев. «Разрезать» данное право на несколько частей не просто, а очень сложно. Особенно если претендующие на домен учредители компании находятся в конфликте.

Одним из подходов здесь может служить продажа домена и включение его в общую стоимость разделяемого имущества.

Практика обеспечительных мер по доменным спорам, еще не сформировалась.

Исполнения судебного решения о запрете ответчику использовать в доменном имени, идентичное или совпадающее до степени смешения с товарным знаком фирмы- истца обозначение, правами на которое обладает истец может столкнуться с трудностями.

В большинстве практических случаев продажа администратором спорного доменного имени происходит практически сразу после того, как он узнает, что к нему предъявлен судебный иск. Продажадоменного имени, как правило, осуществляется другому лицу, которое обычно не знает о существовании судебного иска.

Основное противоречие здесь заключается в том, что в соответствии с правилами регистрации доменных имен администратору доменного имени требуется всего несколько дней, чтобы передать права администрирования домена другому администратору, обычно не больше трех дней.

С другой стороны, в соответствии с п. 9.1 Правил регистрации доменных имен, хотя ограничение на передачу прав действует, пока администратор не представит регистратору доказательств завершения судебного разбирательства, однако оно не может сохраняться непрерывно

более сорока пяти календарных дней, по истечении которых администратор имеет право передать администрирование другому лицу или отказаться от его использования.

Противоречие здесь заключается в том, что судебное разбирательство по доменным спорам длится дольше значительно чем сорок пять календарных дней.

Учитывая вышеизложенное, можно с уверенностью утверждать, что только принятие судом обеспечительных мер может являться гарантией того, что права по администрированию спорного домена перейдут к администратору, определенному, как имеющего на него право по решению суда.

Вопросы обеспечительных мерах по доменным спорам сегодня во многом регулируются на основании Постановления Президиума Суда по интеллектуальным правам«Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору» от15 октября 2013 года[25] .

В котором разъясняются вопросы о том, как должны применяться судами нормы процессуального права об обеспечительных мерах при разрешении доменных споров.

В частности, абзац 4 п. 2 указанной справки предусматривает запрет администратору:

- совершать какие-либо действия с доменом, включая отчуждение, отказ, смену регистратора;

- аннулировать доменное имя;

- передавать права на администрирование доменного имени другому лицу.

Большое практическое значение имеет вопрос о подсудности споров по доменным именам.

---

[25]Постановления Президиума Суда по интеллектуальным правам «Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору» от15 октября 2013 года пункт 2.

Основное противоречие здесь заключается в том, что истцы:

- подают свои заявления в суды общей юрисдикции;

- качестве ответчиков указывают не владельцев доменного имени, а регистраторов этого доменного имени.

В результате истцы после судебного разбирательства, иногда довольно длительного получают отказ в своих исках, ответчики получают время для проведения блокирующих действий.

При разрешении данного противоречия необходимо опираться на:

- Постановление Президиума Высшего Арбитражного Суда РФ

N 9833/09 от 8 декабря 2009 года;

-Постановление Президиума Суда по интеллектуальным правам «Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору» от 15 октября 2013 года.

Таким образом в данной главе выявлены взаимосвязи доменных имен и информационной безопасности, на основетриады CIA. Проанализировано нормативное правовое регулирование доменного имени в современных условиях. Выявлены основные противоречия в сфере гражданско-правового регулирования доменных имен и порождаемые ими гражданско-правовые нарушения.

ГЛАВА 3 СОВЕРШЕНСТВОВАНИЕ ПРОЦЕДУРЫ ВЫБОРА, РЕГИСТРАЦИИ ДОМЕННЫХ ИМЕН, А ТАКЖЕ РАЗРЕШЕНИЯ ГРАЖДАНСКО-ПРАВОВЫХ СПОРОВ ПО ДОМЕННЫМ ИМЕНАМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1 Совершенствование процедуры выбора и регистрации доменного имени

При наличии больших пробелов не только в российском, но и в международном законодательстве, по поводу как определения самого доменного имени, так и формализации правоотношений, возникающих при его правоприменении , основными документами в этой области для нашей страны являются Правила регистрации доменных имен в доменах .RU и .РФ, разработанные АНО «Координационный центр национального домена сети Интернет» и являющиеся обязательными для всех администраторов доменных имен.

Домен в зоне .RU может состоять из букв латинского алфавита, цифр и знака дефиса «-» и «должен быть не менее 2 и не более 63 символов…»[26]

Доменное имя должно:

1). быть достаточно просто запоминаемым;

2). отражать по возможности, содержательную составляющую информационных ресурсов, которые предполагается размещать по этому адресу;

3). не должно противоречить общественным интересам, принципам гуманности и морали, особенно как показано в работе Белинда Айзек (Belinda Isaac) не совпадать с «именамиизвестных авторов и знаменитостей…»;[27]

4). не должно совпадать с специализированными обозначениями.

К специализированным обозначениям, обычно, относят несколько «групп:

---

[26]"Правила регистрации доменных имен в доменах .RU и .РФ" (утв. решением Координационного центра национального домена сети Интернет от 05.10.2011 N 2011-18/81) (ред. от 28.02.2019) С.4

[27]BelindaIsaac. Personal Names and the UDRP: A Warning to Authors and Celebrities // Entertainment Law Review. Vol. 12, No. 2. 2001. p. 44.

-международные не патентуемые названия (INN) фармакологических препаратов;

- названия международных организаций;

-личные имена;

- фирменные наименования;

- географические названия и указания на происхождение…»[28]

5). быть «свободным».

Убедиться, что выбранное доменное имя свободно можно с помощью информационного сервиса WHOIS, по адресу https://whois.ru/ , на котором находятся данные о всех действующих доменах. Если выбранного доменного имени в данной базе нет, то его можно регистрировать.

На этом же сервисе можно оставить заявку на регистрацию уже освобождаемых доменов, если вам подойдут их имена.

Вместе с ростом числа организаций и фирм растет количество администраторов доменных имен, а следовательно, и количество компаний-регистраторов. В зависимости от подходов к ведению бизнеса эти компании могут различаться и формой собственности, и внутренней организацией, и тарифами, и практикой ведения дел. Таким образом выбор компании регистратора важный этап, при котором нельзя руководствоваться единственным критерием – стоимостью регистрации.

Остановимся на этом вопросе подробнее.

Если под зарегистрированным доменным именем размещаются какие-то ресурсы, то домен нужно привязать к определенным серверам DNS, которые связаны с конкретным доменом через общую, глобальную иерархию систем адресации.

То есть сам сервер, на котором размещен сайт, может работать бесперебойно, но, если откажут серверы DNS, то попасть на этот сервер по привычному адресу не получится. Таким образом, сайт просто исчезнет из

[28]Дашян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет– М.:"Волтерс Клувер", 2007.С.119

пространства Интернета. Так что надежность серверов DNS играет важную роль в обеспечении доступности веб-сайтов и других онлайн-ресурсов, в том числе систем электронной почты. Часто услуга размещения DNS предоставляется хостинг-провайдерами.

Серверы DNS часто служат объектом атак со стороны хакеров, типа «отказ в обслуживании». Отказавшие DNS-серверы не смогут обслуживать запросы, и размещенные под соответствующим доменом ресурсы будут недоступны.

DNS-серверы могут быть взломаны хакером. В таком случае получивший доступ к серверу хакер сможет управлять и доменом или несколькими доменами, обслуживаемым этим DNS-сервером. Это означает, что хакер может перенаправить трафик с ресурсов администратора на какие-нибудь свои ресурсы. С точки зрения пользователя Сети, новые хакерские онлайн-ресурсы будут доступны под теми же самыми доменами, которые ранее соответствовали легальным сайтам или адресам электронной почты. Другими словами, происходит «угон» домена в интересах хакера.

Необходимо также учитывать, что устойчивая работа Интернета, возможна лишь при надежной работе телекоммуникационной инфраструктуры, функции «по управлению государственным имуществом и оказанию государственных услуг в сфере электросвязи…»[29], в соответствии с Постановлением Правительства Российской Федерации возложены на Федеральное агентство связи (Россвязь), которое через своего оператора связи должно обеспечить «пользователю возможность пользования услугами связи по передаче данных 24 часа в сутки…»[30].

Степенью уверенности в том, что у компании-регистратора не возникнет серьезных проблем возрастает при учете следующих рекомендаций:

---

[29]Постановление Правительства Российской Федерации от 30 июня 2004 г. № 320 «Об утверждении Положения о Федеральном агентстве связи» п.1

[30]Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных» п.7

-использовать услуги по аренде DNS, предоставляемые крупными регистраторами или хостинг-провайдерами;

- одновременно использовать нескольких DNS-серверов, находящихся у разных провайдеров;

- страна, где зарегистрирована компания- Россия;

- как давно оказывает подобные услуги;

- количество клиентов;

- какой % рынка занимает;

-где территориально расположены сервера – наиболее предпочтительный вариант- Россия;

- существует и какой тестовый период;

- стоимостная политика;

-существует ли техническая поддержка;

- наличие положительных отзывов.

Данная информация доступна в интернете на сайтах фирм, публикующих рейтинг компаний- регистраторов и провайдеров.

3.2 Совершенствование процедуры разрешения гражданско- правовых споров по доменным именам

При регистрации доменного имени ранее существовавшего, но затем прекратившего существование и имеющего плохую репутациюметоды гражданского права в данном случае должны носить предупредительный характер

Необходимо сделать проверку домена и брать домены только с нулевой или хорошей историей.

В случае если на сайте долгое время находился неуникальный контент, вирусы, запрещающие материалы (для взрослых, экстремизм, пропаганда наркотиков и другое), покупались или продавались некачественные ссылки, публиковались переоптимизированные статьи, спам и т. д., то скорее всего доменное имя такого сайта находится под фильтрами и заблокировано.

Узнать про все фильтры и блокировки нереально, можно лишь догадываться, анализируя данные, сохранившиеся в истории на некоторых специальных сервисах.

Наиболее же авторитетными для проверки доменов являются: сервисы безопасного поиска Яндекса и Google

Яндекс и Google ведут свои базы подозрительных и опасных доменов: Yandex Safe Browsing и Google Safe Browsing. Эти базы формируются в результате сканирования проиндексированных сайтов антивирусным ботом.

Бот проверяет сайт на фишинг, скрытые перенаправления, загрузку вирусного кода или опасных файлов. Если обнаруживает угрозу, то домен попадает в чёрный список поисковой системы. После этого он может оказаться в чёрном списке одного или нескольких антивирусных сервисов.

Через безопасный поиск Яндекса репутацию сайта проверяют Opera и Firefox (русские редакции), а также Яндекс.Браузер. Через безопасный поиск от Google — Chrome, Firefox и Safari. Браузеры ограничивают серфинг по сайтам, которые "забанил" поисковик.

О попадании в чёрный список поисковых систем можно узнать, например, из панели Вебмастера Яндекса или консоли Google, если заранее добавить в них сайт.

Агрегатор VirusTotal

VirusTotal — это агрегатор информации о вирусах и опасных сайтах. В него стекаются данные от 67 сервисов, среди которых Kaspersky, Dr.Web, ESET, Trustwave, CleanMX, PhishLab и др. Эти сервисы сами выгружают свои базы по угрозам и заражениям в общую базу VirusTotal. Поэтому, если домен или IP-адрес окажется в чёрном списке хотя бы одного из этих 67 антивирусных сервисов, об этом узнают все, кто использует базу VirusTotal.

Через VirusTotal удобно проверять статус домена в различных антивирусах. С его помощью можно быстро обнаружить блокировку сайта конкретным антивирусом, чтобы спасти репутацию домена.

База Роскомнадзора

Реестр запрещённых сайтов Роскомнадзора содержит информацию обо всех сайтах, которые нарушают законы РФ. Интернет-провайдеры обязаны блокировать все сайты из этого реестра.

Роскомнадзор добавляет в базу не только домены, но и IP-адреса. Поэтому заблокированным может оказаться самый безобидный сайт — если ему достался «забаненный» IP. Так бывает, когда сайт размещён на виртуальном хостинге с нарушающим закон ресурсом, или когда его серверу присвоен IP-адрес, который попал под блокировку раньше. Часто от блокировок Роскомнадзора страдают ни в чём не повинные пользователи бесплатных тарифов Cloudflare.

Если домен или IP-адрес подпал под санкции, процесс удаления из чёрных списков может занимать от суток до нескольких недель.

Быстрее всего происходит исключение сайта из блэклистов Google: обычно сутки, если к сайту не были применены ручные санкции.

Чуть дольше процесс у Яндекса. Исключение сайта из санкционного списка может занимать от двух дней до двух недель. Помимо автоматического запроса в случае Яндекса имеет смысл отправить ещё и запрос на разблокировку через форму обратной связи.

Дольше всего выводить сайты из чёрных списков антивирусных сервисов. В некоторые из них (особенно это касается малоизвестных и новых) сайт может попасть по ошибке, например, в результате так называемого ложного срабатывания. Если у сервиса не предусмотрен автоматический вывод домена из "бана", то придётся отправлять заявку, а её рассмотрение может затянуться на несколько недель.

Избежать блокировок домена, спасти его репутацию или хотя бы снизить вероятность попадания сайта в чёрный список поможет мониторинг безопасности. Его задача — обнаружить проблему раньше бота поисковой системы или антивирусного сервиса. Если проблема обнаружена, специалист сможет быстро её устранить и, таким образом, уберечь сайт от попадания в "бан".

Первый способ, которым вы можете воспользоваться, — это специальный инструмент проверки истории у официального регистратора.

Второй способ, связан с использованием специальных сервисов.

Whoishistory.ru

Whoishistory.ru — стандартный сервис для просмотра общедоступной информации о домене. Работает только с доменными зонами .ru, .su, .рф.

Показываются отдельно данные за каждый год:

- Сервера хостинга, где расположен.

-Статус доступности.

-Кем зарегистрирован. Если на физическое лицо, то конкретно на когоне показывается.

-У какого регистратора он приобретён.

-Дата регистрации (возраст).

-Даты, когда он продлевался.

По этим данным самое главное, что можно увидеть, — был он ранее кем-то занят или нет и как давно занят.

Если увидите, что он уже использовался, анализируем следующим сервисом.

Linkpad.ru

Linkpad.ru — инструмент для анализа входящих, исходящих и внутренних ссылок на сайте. Если ранее на домене находился сайт, и он нормально индексировался, то данный сервис покажет, какие ссылки на этом сайте стояли и какие на него ссылались.

Однако наиболее надежным способом является предварительная регистрация.

Предварительная регистрация (Add Grace Period). Он продолжается несколько дней, в течение которых регистратор ожидает поступления оплаты за регистрацию от администратора домена. То есть сначала домен регистрируется бесплатно и позже при непоступлении оплаты освобождается. Важно понимать, что подобная услуга доступна отнюдь не

всем и далеко не во всех случаях, по она весьма распространена среди крупных игроков на рынке доменов и оказывается вполне официальный в соответствии с действующей политикой ICANN.

В браузерах, использующих Safe Browsing API (Google Chrome, Яндекс. Браузер, Opera, Firefox и Safari), при переходе на «забаненный» поисковиком сайт выдаётся красный экран блокировки и предупреждение о вирусах или мошенничестве.

Если сайт «забанен» антивирусом, то при попытке пользователей с тем же антивирусом открыть его, проактивная защита будет предупреждать об угрозе безопасности или вовсе блокировать доступ.

Предварительная заявка на регистрацию домена в зоне РФ – это когда Вы до начала открытой регистрации, делаете заявку на регистрацию интересующего вас домена в зоне. РФ на сайте одного из регистраторов. В период открытия свободной регистрации, регистратор попробует зарегистрировать Ваше доменное имя. Однако это не гарантирует, что домен будет зарегистрирован на вас, поскольку регистраторы будут выполнять заявки на регистрацию в том же порядке, в каком они поступили к ним. То есть, если сейчас у biz.ru, допустим, уже 300 заявок, и Вы подаёте 301-ю заявку, то и обработана ваша заявка будет 301-й.

Достоинство предварительной регистрации, в том, что она позволяет бесплатно тестировать домен в течение некоторого промежутка времени. С помощью подобного тестирования проверяется репутация домена, но и его привлекательность для пользователей Интернета: если после регистрации на домене появляется достаточно большой трафик посещаемости, значит, домен стоит вложения средств в регистрацию.

Как было показано выше,одна из самых больших проблем, создающих серьезные риски, — неверное делегированиеполномочий но управлению доменом внутри компаний и официальных организаций. Права управления, полученные администратором домена, требуют надежного фиксирования и не менее надежных механизмов авторизации, иначе у администратора

возникнут трудности с проведением прав в жизнь. Права по управлению доменом фиксируются в специальных базах данных, которые имеются у администраторов доменов первого уровня и у компаний-регистраторов.

Во избежание такой ситуации юридическим лицам следует:

- выбирать доменное имя, совпадающее с фирменным наименованием компании, а еще лучше с его торговой маркой (товарным знаком);

-убедиться в отсутствии зарегистрированного ранее товарного знака, в котором используется обозначение тождественное или сходное до степени смешения с доменом, а также поданных в Роспатент ранее заявок на регистрацию такого товарного знака. Это можно проверить по базе Роспатента;

- провести предварительную регистрацию домена;

- проверить доменное имя, как указано в выше на его «репутацию»;

- регистрировать домены на организацию, а не на отдельных сотрудников;

- если организация не имеет торговой маркой (товарного знака), то зарегистрировать торговую марку (товарного знака), совпадающие с выбранным доменным именем;

- проработать административную процедуру, в частности должностные обязанности администратора домена, обеспечивающие безопасность логина и пароля, в частности запретить передавать их по электронной почте;

- проводить замену логина и пароля при смене работника, осуществляющего администрирование домена;

- поскольку, домен с течением времени может являться значительным, а иногда и единственным активом организации, необходимо прописать в Уставе порядок совершения и одобрения сделок, связанных с ним.

Для того, чтобы избегнуть судебных разбирательств, рекомендуется при регистрации доменного имени:

- выбирать доменное имя, совпадающее с фирменным наименованием компании, а еще лучше с его торговой маркой (товарным знаком);

- проверить по базе Роспатента, что данное доменное имя, не входит в качестве элемента в зарегистрированный товарный знак какой- либо организации ;

- провести предварительную регистрацию домена;

- поскольку, домен с течением времени может являться значительным, а иногда и единственным активом организации, необходимо Устав организации дополнить пунктами о порядке совершения сделок (как было указано выше продажа домена является сделкой) с данным доменным именем;

- не использовать на сайте информацию о тех товарах и услугах по МКТУ, по которым существуют охраняемые в РФ товарные знаки, сходные до степени смешения с данным доменом;

- для юридических лиц и ИП, использующих домен для размещения рекламных сайтов и реализации посредством сайта, размещенного на данном домене, товаров или услуг, необходимо разработать и зарегистрировать товарный знак по соответствующим классам Международной классификации товаров и услуг;

- позаботиться о безопасности сайта заранее: установить технические средства защиты от веб-атак и взлома, проработать организационные меры защиты и технику безопасности при работе с сайтом;

- провести предварительную регистрацию доменных имен сходных до степени смешения с имеющемся доменным именем;

- оценить трафик по доменным именам и оставить только посещаемые домены;

- подготовить нотариально заверенный протокол осмотра сайта (распечатка интернет-страницы).

Нотариально заверенный протокол осмотра сайта составляется на основании письменного запроса на имя нотариуса, в котором указываются:

-цель: удостоверить факт нарушения исключительных прав;

- адрес страницы в сети Интернет;

-реквизиты документа;

-заголовок и его месторасположение на интернет-странице;

- цитаты, которые будут указаны в судебном иске и их месторасположение на интернет-странице.

В протоколе необходимо указать последовательность действий, которые совершил нотариус для получения Prtscr интернет- страницы.

Возможна на основании того, что «заключено соглашение о передаче доменного имени…»[31] передача прав на доменное имя другому юридическому лицу для ведения совместной хозяйственной деятельности.

Продажа доменного имени-это передача права администрирования доменного имени от одного администратора (физического или юридического лица) к другому (физическому или юридическому лицу).

Продажа доменного имени может осуществляться двумя способами:

1). Путем заключения договора

-Администратор домена и лицо, намеревающееся использовать домен, заключают между собой гражданско-правовой договор, в соответствии с действующим законодательством Российской Федерации, описав все то, что стороны посчитают необходимым (договор купли-продажи, дарения и проч.). Договор заключается как в обычной письменной форме, так и нотариально заверенной;

- Администратор домена и Получатель направляют регистратору соответствующие заявления.

2). Путем соответствующих заявлений регистратору, составленных по определенной регистратором форме.

Передача прав на домен проводиться в следующем порядке:

-прежний администратор направляет регистратору соответствующее заявление, по утвержденной регистратором форме, которым подтверждает свой отказ на права администрирования домена;

---

[31]Постановление Президиума ВАС РФ от 11.11.2008 N 5560/08 по делу N А56-46111/2003

- новый администратор направляет регистратору заявление, в котором подтверждает свое согласие на получение прав администрирования домена.

Данные заявления на регистратора являются фактом заключения сделки по передаче прав администрирования доменным именем от одного администратором к другому.

В соответствии с Правилами регистрации доменов в доменах .RU и.РФ передача прав по администрированию домена невозможна в следующих случаях:

1. В течении тридцати календарных дней с момента передачи прав администрирования домена .RU или .РФ от одного администратора к другого;

2. Закончился срок регистрации домена .RU, .РФ или .SU.

3. В течении 30 дней с момента смены регистратора, осуществляющего поддержку доменного имени;

4. В течении шестидесяти календарных дней после получения администратором домена прав администрирования домена .SU и доменов третьего уровня.

5. Доменное имя совпадает с включенным в стоп-лист.

6. Документы на передачу доменного имени неверно оформлены или не предоставлен их полный комплект.

7. Передающая права на домены .RU, .РФ и .SU сторона не известна.

8. По доменному имени проходят аукционные торги.

9. Администратор доменане предоставил в установленный срок дополнительные сведения запрашиваемые регистратором в соответствии с п. 9.2.5−9.2.7 Правил регистрации доменных имен в доменах .RU и .РФ и доменов третьего уровня.

Убедиться, что передача прав на доменное имя произошла, можно используя сервис Whois.

Поскольку передача доменного имени, как было указано выше, является сделкой, как любая сделка, она может быть признана судом недействительной на основании ст. 168– 179 ГК РФ.

При оспаривании сделки по передаче домена нужно иметь ввиду, что:

- сделка может оспаривается одной из сторон по сделке;

- сделка оспаривается не сторонами по сделке, а другим заинтересованным лицом.

Однако, в любом случае требование о признании сделки по передаче доменного имени недействительной должно предъявляться к предыдущему и ли настоящему владельцам доменного имени, но ни в кое случае не к регистратору.

Регистратор доменных имен, являющихся предметом судебного разбирательства, может привлекаться к участию в деле лишь как третье лицо, не заявляющее самостоятельные требования на предмет спора.

Это вытекает из Правил регистрации доменных имен в домене .RU и.РФ, на основании которых регистратор обязан:

- предоставить суду информацию о владельце доменного имени;
- предоставить суду информацию о наличии доменного имени у его администратора;
- предоставить суду «историю» домена;
- заблокировать домен на время судебного разбирательства.

Таким образом он, на основании решение суда, реализует досрочное прекращение права администрирования в интересах права истца, выигравшего судебное разбирательство.

В исковых требованиях истец должен:

1. если у истца имеется договор купли–продажи доменного имени, то истец должен просить суд признать указанный договор недействительным.

2.если у истца нет документов, на основании которых право администрирования доменным именем перешло к конкретному

администратору, он, в соответствии с Правилами должен получить у регистратора:

- сведения об администраторе домена;

- копии документов, на основании которых администратор получил права на домен.

- сформулировать требования о применении последствий недействительности сделки по передаче доменного имени, заключающееся в передаче прав на доменное имя предыдущему администратору.

В соответствии с Правилами регистрации доменных имен в доменах .RU и.РФ регистратор имеет право прекратить возможность управления доменным именем конкретному администратору на основании, вступившего в законную силу решения суда.

Истец может добиться исполнения решения суда, если добровольное исполнение Получателем не произведено следующими способами:

1) с помощью исполнительного производства (судебные приставы);

2) с помощью регистратора; в соответствии с Правилами вступившее в законную силу решение суда об удовлетворении иска- основание для передачи регистратором права администрирования доменным именем предыдущему администратору.

Если домен, представляет собой значительную коммерческую ценность, то возникают судебные споры, связанные с наследованием доменов.

Здесь необходимо рассмотреть следующие случаи:

1). администратор домена- физическое лицо умер;

2). администратор домена- коммерческая компания ликвидируется, передается по наследству, кто-то из учредителей выходит из компании.

С юридической точки зрения:

1). администрирование домена — это услуги, и согласно ч.1 ст. 1112 ГК РФ «В состав наследства входят принадлежавшие наследодателю на день открытия наследства вещи, иное имущество, в том числе имущественные

права и обязанности. Не входят в состав наследства права и обязанности, неразрывно связанные с личностью наследодателя, в частности право на алименты, право на возмещение вреда, причиненного жизни или здоровью гражданина, а также права и обязанности, переход которых в порядке наследования не допускается настоящим Кодексом или другими законами. Не входят в состав наследства личные неимущественные права и другие нематериальные блага» данные услуги в наследственную массу не входят.

2). В соответствии с ч.2 ст. 418 ГК РФ «1. Обязательство прекращается смертью должника, если исполнение не может быть произведено без личного участия должника либо обязательство иным образом неразрывно связано с личностью должника.

2. Обязательство прекращается смертью кредитора, если исполнение предназначено лично для кредитора либо обязательство иным образом неразрывно связано с личностью кредитора», обязательства Регистратора прекращается после смерти администратора домена.

Хотя в Правилах регистрации доменных имен в домене RU, смерть администратора не обозначена в перечне случаев прекращения управления доменом, в ГК РФ, имеющем большую юридическую силу по сравнению с Правилами, содержится прекращение обязательств в случае смерти кредитора, после получения неопровержимых доказательств смерти кредитора. В соответствии с документами Координационного центра, нотариально заверенная копия свидетельства о смерти гражданина является достаточным доказательством.

На основании изложенного выше регистратор может:

-аннулировать регистрацию сразу после получения копии свидетельства о смерти гражданина, являющегося администратором домена;

- аннулировать регистрацию после окончания срока действия регистрации;

- разработать свои правила по передаче прав администрирования домена наследникам или третьим лицам.

Хотя регистратор имеет достаточно большие права в этой ситуации, необходимо учитывать, что сегодня доменные имена могут стоить достаточно дорого и неоднозначная трактовка правил регистратора создает повод для претензий третьих лиц

Если администратор домена- юридическое лицо то возможна:

1). продажа права администрирования домена и соответственно:

- включения полученной суммы в наследственную массу;
- учет ее при ликвидации компании.

2). оценка его стоимости, исходя из рыночных условий и включение ее в расчет при определении доли того или иного учредителя, наследника.

Если доменное имя зарегистрировано для сайта с помощью которого ведется коммерческая деятельность возможна его продажа другой компании-посреднику, с необходимостью вернуть при определенных условиях.

Следует отметить, что этот вопрос с течением времени будет все более актуальным, и необходимо внесение дополнений, не только в правила регистрации доменных имен, но и в законодательные нормы.

Большое практическое значение имеет вопрос о подсудности данной категории споров.

После принятия Президиумом ВАС РФ постановления от 8 декабря 2009 года, доменные споры о нарушениях исключительных прав на товарный знак в доменном имени с участием физических лиц, не зарегистрированных в качестве индивидуальных предпринимателей, подлежат разрешению в арбитражных судах, а не в суд общей юрисдикции.

Это обосновывается экономическим характером спора, а в соответствии со статьей 22 ГПК РФ экономические споры исключены из категорий дел, подлежащих разрешению судами общей юрисдикции, и отнесены к ведению арбитражных судов.

Апелляционные жалобы на судебные акты по доменным спорам рассматривают арбитражные апелляционные суды.

Кассационные жалобы по данным спорам касаются, как правило товарных знаков, т.е., интеллектуальной собственности, поэтому такие судебные дела подлежат рассмотрению в Суде по интеллектуальным правам, который является специализированным арбитражным судом, рассматривающим дела по спорам, связанным с защитой интеллектуальных прав, в качестве суда первой и кассационной инстанций.

Доменные споры не подпадают по категорию дел, которые Суд по интеллектуальным правам рассматривает в качестве суда первой инстанции, в силу экономического характера спора.

«Рассмотрение Судом по интеллектуальным правам в качестве суда кассационной инстанции доменных споров, рассмотренных арбитражными судами субъектов Российской Федерации, арбитражными апелляционными судами, осуществляется «в судебном заседании коллегиальным составом судей…»[32], а не Президиумом Суда по интеллектуальным правам.

Вступившие в законную силу судебные акты по доменным спорам:

- арбитражных судов;

–апелляционных арбитражных судов;

- Суда по интеллектуальным правам,

могут быть пересмотрены Высшим Арбитражным Судом Российской Федерации.

3.3 Совершенствование процедуры обеспечительных мер при доменных спорах

Основное противоречие заключается в том, что передать(продать) доменное имя, согласно Правилам регистрации доменных имен в домене. РФ Координационного центра доменов RU/РФ, можно другому администратору за три дня, а рассмотрение судебного дела, включая получение судебного решения длится, как правило несколько месяцев. Поэтому необходимо

[32]Арбитражный процессуальный кодекс Российской Федерации" от 24.07.2002 N 95-ФЗ (ред. от 25.12.2018) (ПринятГД 14.06.2002) ч. 1 Ст. 284

проверить «не предпринимались ли ответчиком попытки продать или иначе передать доменное имя…»[33].

«В целях предотвращения причинения значительного ущерба заявителю обеспечительные меры могут быть направлены на сохранение существующего состояния отношений (status quo) между сторонами» пункт 9 постановления Пленума Высшего Арбитражного Суда Российской Федерации от 12.10.2006 № 55 “О применении арбитражными судами обеспечительных мер”.

При этом продажа доменного имени может быть осуществлена:

- до подачи иска;

-сразу после того, как администратор домена, он же ответчик, узнает отом, что к нему предъявлен иск;

- во время рассмотрения судебного дела;

- после получения судебного решения,

при этом администратор домена, он же ответчик может передать домен, как без смены фирмы регистратора, так и со сменой фирмы регистратора.

Такие же последствия наступают в случае, если у регистратора будет аннулирована аккредитация.

В первом случае необходимо подготовить все документы и доказательства, на нового ответчика. При этом нужно учитывать, что доказать факт нарушения новым ответчиком прав истца будет невозможно, особенно, если домен фактически не использовался.

Избежать данной ситуации позволит мониторинг сайтов регистраторов, на которых отражаются домены находящиеся в стадии регистрации иинформационного сервиса WHOIS до того момента, когда судом будут приняты обеспечительные меры.

[33]Постановление Президиума ВАС РФ No. 1192/00 от 16.01.2001 г. по делу № А40-25314/99-15-271

В других случаях необходимо получить решение суда обобеспечительных мерах, направленных к регистратору данного доменного имени и ответчику.

Юридической основой, в данной ситуации являются предварительные обеспечительные меры, в соответствии со ст. 91 АПК РФ и ст. 99 АПК РФ.

В соответствии с статьей 91 АПК РФ, обеспечительными мерами могут быть «запрещение ответчику и другим лицам совершать определенные действия, касающиеся предмета спора», следовательно, возможен запрет совершения названных действий для регистратора, в функции, которого входит функция по распределению доменных имен администраторам следующего уровня.

В соответствии с статьей 92 АПК РФ

1) «Заявление об обеспечении имущественных интересов, подписанное усиленной квалифицированной электронной подписью в порядке, установленном законодательством Российской Федерации, может быть подано в арбитражный суд посредством заполнения формы, размещенной на официальном сайте арбитражного суда в информационно-телекоммуникационной сети "Интернет"».

2). Заявитель должен обосновать причины обращения с требованием о применении обеспечительных мер.

В соответствии с статьей 99 АПК РФ:

1). Указанные меры могут быть приняты судом еще до подачи искового заявления.

2). В то же время при рассмотрении заявления о предварительных обеспечительных мерах согласно ч. 4 ст. 99 АПК РФ предоставление встречного обеспечения является обязательным условием удовлетворения такого ходатайства.

3). ч. 7ст. 99 АПК РФ «Исковое заявление подается заявителем в арбитражный суд, который вынес определение об обеспечении имущественных интересов, или иной суд. Заявитель сообщает арбитражному

суду, вынесшему определение об обеспечении имущественных интересов, о направлении претензии (требования), а также о подаче искового заявления в иной суд».

4). ч. 8 ст. 99 АПК РФ «Если заявителем не были представлены арбитражному суду, вынесшему определение об обеспечении имущественных интересов, доказательства направления претензии (требования) либо подачи искового заявления в срок, установленный в определении арбитражного суда об обеспечении имущественных интересов, обеспечение отменяется тем же арбитражным судом. Об отмене обеспечения имущественных интересов выносится определение. Копии определения направляются заявителю и иным заинтересованным лицам не позднее следующего дня после дня вынесения определения».

Процессуальные вопросы по обеспечительным мерам, позволяющим исключить передачу прав администрирования на спорные домены, нашли свое отражение в Постановлении Президиум Суда по интеллектуальным правам «Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору» от 15 октября 2013 года.

В постановление дается определение понятия доменного спора.

«Под доменным спором в настоящей справке понимаются дела о правомерности использования доменного имени, сходного с результатом интеллектуальной деятельности или средством индивидуализации, принадлежащим заявителю, в которых заявлено требование о понуждении к совершению либо о воспрещении каких-либо действий, подлежащее принудительному исполнению»[34].

В соответствии, с Постановлением:

1. Должна быть конкретно указана та обеспечительная мера, которую просит применить истец.

[34]Постановление Президиума Суда по интеллектуальным правам от 15 октября 2013 г. № СП-23/3 “Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору”//СПС КонсультантПлюс.

2. «В обеспечении иска может быть отказано, если отсутствуют предусмотренные статьей 90 Кодекса основания для принятия соответствующих мер,обоснованности доводов заявителя о необходимости принятия обеспечительных мер».

3. Согласно пункт 10 постановления Пленума Высшего Арбитражного Суда Российской Федерации от 12.10.2006 № 55 “О применении арбитражными судами обеспечительных мер” суд рассматривает «насколько истребуемая заявителем конкретная обеспечительная мера связана с предметом заявленного требования, соразмерна ему»[35].

4. В п. 2 справки указано, что «резолютивная часть определения о применении обеспечительных мер по доменному спору может предусматривать запрет администратору совершать какие-либо действия с доменом, включая отчуждение, отказ, смену регистратора, а также запрет регистратору аннулировать доменное имя и передавать права его администрирования другому лицу»[36].

Для принятия указанных обеспечительных мер истцу необходимо предоставить регистратору подтверждение предъявления судебного иска в связи с спорным доменным именем, в форме копии искового заявления с отметкой суда о его принятии, после чего регистратор обязан будет произвести действия не позволяющие администратору:

- отказаться от доменного имени;

- передать поддержку доменного имени другомуадминистратору или регистратору.

Необходимо иметь в виду, что:

- ограничение, предусмотренные Правилами, хотя и действует до момента пока администратор не представит регистратору доказательства окончания судебного разбирательства, но не более сорока пяти календарных

[35]Постановление Пленума ВАС РФ от 12.10.2006 N 55 (ред. от 27.06.2017) "О применении арбитражными судами обеспечительных мер"//СПС КонсультантПлюс.
[36]Постановление Президиума Суда по интеллектуальным правам от 15 октября 2013 г. № СП-23/3 “Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору”//СПС КонсультантПлюс.

дней. После истечении этого срока, согласно Правилам, администратор вправе передать права администрирования другому лицу или отказаться от доменного имени. Учитывая то, что судебное разбирательство по доменным спорам могут длиться дольше чем 45 дней, то к моменту его окончания администрирование спорного домена может перейти к другим лицам;

- обеспечительные меры, принятые судом в отношении регистратора спорного доменного имени, могут оказаться недостаточными если регистратор передаст поддержку сведений о доменном имени другому регистратору или утратит аккредитацию[37];

Поэтому, истцу необходимо добиваться, чтобы обеспечительная мера, направленная на исключение возможности передачи поддержки спорного доменного имени другому регистратору, должна быть принята судом в отношении: администратора, регистратора, и Координационного центра национального домена сети Интернет[38].

- после окончания судебного разбирательства, истцам необходимо самостоятельно отменять принятые по их заявлению обеспечительные меры, своевременно обращаясь для этого в суд (ст. 95 АПК РФ).

Особое внимание истцу следует уделить доказательствам нарушения его прав.

В соответствии с пунктом 10 постановления Пленума Высшего Арбитражного Суда Российской Федерации от 12.10.2006 № 55 “О применении арбитражными судами обеспечительных мер», достаточными доказательствами являются:

«- наличия у него права на результат интеллектуальной деятельности или средство индивидуализации;

- факта нарушения и обоснования причины обращения с требованием о применении обеспечительных мер» [39].

---

[37] ГерцеваЕ. Н., ГринкевичА. П.. Доменные споры. Судебная практика в России: Эксмо; Москва; 2014 С. 368

[38] Там же. С. 370

[39] Постановление Пленума Высшего Арбитражного Суда Российской Федерации от 12.10.2006 № 55 “О применении арбитражными судами обеспечительных мер»//СПС КонсультантПлюс.П. 10

Таким образом в данной главе разработаны усовершенствованные процедуры выбора и регистрации доменного имени, процедуры разрешения гражданско-правовых споров по доменным именам, усовершенствованные процедуры обеспечительных мер при доменных спорах.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет сделать следующие выводы:

1.Проведенный анализ показывает, что одним из центральных вопросов гражданско-правового регулирования в области информационной безопасности является регулирование прав на доменное имя, в силу того, что:

- затрагивает все три базовых принципаинформационной безопасности: «конфиденциальность» — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов; «целостность» — свойство сохранения правильности и полноты активов;«доступность» — свойствобыть доступным и готовым к использованию по запросу авторизованного субъекта.

- оборот доменных имен присутствует практически в большинстве проблем, связанных синформационной безопасностью и правовоеурегулированиеэтоговопроса позволит во многом успешно разрешать и большинство других проблем;

- судебная практика свидетельствует о большом количестве судебных дел, продолжающихся длительное время в судах разных инстанций.

2. В исследованиях в специалистов содержатся различные подходы к сущности понятия «доменное имя» и к его правовому статусу, поэтому необходимовключение доменных имен в перечень объектов гражданского оборота и определение правового порядка регулирования возникающих правоотношений.

3.Принесомненно важнейших функциях адресной и идентификационной, сегодня все большее значение приобретет коммерческая стоимость доменного имени (стоимость отдельных доменов доходит до 14 миллионов долларов) и с течением времени, в силу экспоненциального характера увеличения объемов информации в мире, будет только возрастать.

Поэтому доменное имя все больше будет приобретать свойства товарного знака, а значит свойства интеллектуальной собственности, что необходимо учитывать при разработке законодательных актов.

4.Степенью доверия к регистратору со стороны клиента: насколько можно быть уверенным в том, что у компании-регистратора не возникнет серьезных проблем, в результате которых клиент может лишиться своего домена, в большой степени, определяет выбор регистратора.

5. При выборе регистратора необходим анализ рейтинга регистраторов.

6.Степенью уверенности в том, что у компании-регистратора не возникнет серьезных проблем возрастает при учете следующих рекомендаций:

-использовать услуги по аренде DNS, предоставляемые крупными регистраторами или хостинг-провайдерами;

- одновременно использовать нескольких DNS-серверов, находящихся у разных провайдеров;

- страна, где зарегистрирована компания- Россия;

- как давно оказывает подобные услуги;

- количество клиентов;

- какой % рынка занимает;

-где территориально расположены сервера – наиболее предпочтительный вариант- Россия;

- существует и какой тестовый период;

- стоимостная политика;

-существует ли техническая поддержка;

- наличие положительных отзывов.

7.Необходимо предусмотреть в законодательстве меры по тому, кто принимает на себя ответственность за дальнейшее поддержание домена в случае прекращения деятельности регистратора и в какие сроки.

8.При регистрации доменного имени ранее существовавшего, но затем прекратившего существование и имеющего плохую репутацию.

Первый способ, которым вы можете воспользоваться, — это специальный инструмент проверки истории у официального регистратора.

Второй способ, связан с использованием специальных сервисов.Необходимо сделать проверку домена сервисы безопасного поиска Яндекса и Google, Базы Роскомнадзора и брать домены только с нулевой или хорошей историей.

Третий способ- предварительная заявка на регистрацию домена в зоне РФ.

9.Во избежание такой ситуацииневерного делегировании полномочий но управлению корпоративным доменом организации юридическим лицам следует:

- выбирать доменное имя, совпадающее с фирменным наименованием компании, а еще лучше с его торговой маркой (товарным знаком);

-убедиться в отсутствии зарегистрированного ранее товарного знака, в котором используется обозначение тождественное или сходное до степени смешения с доменом, а также поданных в Роспатент ранее заявок на регистрацию такого товарного знака. Это можно проверить по базе Роспатента;

- провести предварительную регистрацию домена;

- проверить доменное имя, как указано в разделе 3.1 на его « репутацию»;

- регистрировать домены на саму организацию, а не на ее сотрудников;

- если организация не имеет торговой маркой (товарного знака), то зарегистрировать торговую марку (товарного знака), совпадающие с выбранным доменным именем;

- проработать административную процедуру, в частности должностные обязанности администратора домена, обеспечивающие безопасность логина и пароля, в частности запретить передавать их по электронной почте;

- проводить замену логина и пароля при смене работника, осуществляющего администрирование домена;

- поскольку, домен с течением времени может являться значительным, а иногда и единственным активом организации, необходимо прописать в Уставе порядок совершения и одобрения сделок, связанных с ним.

10. Существующая на сегодня ситуация, когда можно зарегистрировать доменное имя, одинаковое или сходное до степени смешения с зарегистрированным на другую организацию товарным знаком, и не использовать, является благоприятной для возможных нарушителей, поскольку у последних сохраняется возможность заблокировать использование доменного имени владельцем товарного знака и, таким образом, заставить его выкупить доменное имя.

11. Для предотвращения судебных разбирательств с правообладателями, рекомендуется при регистрации или использовании домена:

- выбирать доменное имя, совпадающее с фирменным наименованием компании, а еще лучше с его торговой маркой (товарным знаком);

-убедиться в отсутствии зарегистрированного ранее товарного знака, в котором используется одинаковое или сходное до степени смешения с доменом сочетание символов, по базе Роспатента;

- провести предварительную регистрацию домена;

- поскольку, домен с течением времени может являться значительным, а иногда и единственным активом организации, необходимо предусмотреть в Уставе организации порядок совершения сделок с ним;

- не размещать на сайте, находящихся по данному доменному адресу информацию о тех товарах и услугахпо МКТУ, по которым существуют зарегистрированные в РФ товарные знаки;

- для юридических лиц и ИП, в случае намерения использования домены для своей коммерческой деятельности, необходимо зарегистрировать товарный знак по классам своей деятельности;

- позаботиться о безопасности сайта заранее: установить технические средства защиты от веб-атак и взлома, проработать организационные меры защиты и технику безопасности при работе с сайтом;

- провести предварительную регистрацию доменных имен сходных до степени смешения с имеющемся доменным именем;

- оценить трафик по доменным именам и оставить только посещаемые домены;

- подготовить нотариально заверенный протокол осмотра сайта (распечатка интернет-страницы).

9.В случае продажи доменного имени, осуществляется передача права администрирования доменного имени.

10. С точки зрения российского законодательства регистрация доменного имени — это услуга, оказываемая юридическим лицом физическому или юридическому лицу. То есть администратор не покупает домен — он лишь получает право администрирования домена, а соответственно право на управление доменом нельзя наследовать.

11. В настоящий момент наиболее удобным способом передачи доменов по наследству являются:

- продажа права администрирования домена и соответственно включения полученной суммы в наследственную массу;

- оформление права администрирования домена на юридическое лицо, владельцем которого является тот, кто заинтересован в корректном переводе доменов на наследников. В таком случае наследники унаследуют домены вместе с юридическим лицом: наследование долей в компаниях более четко регулируется законодательством.

- оценка его стоимости, исходя из рыночных условий и включение ее в расчет при определении доли наследника.

12. При разделе имущества обанкротившейся компании с доменными именами также возникают серьезные трудности. Если владельцев бизнеса несколько, раздел доменного имени между ними может оказаться весьма

проблематичной задачей. Одним из подходов здесь может служить продажа домена и включение его в общую стоимость разделяемого имущества.
Другой подход заключается в оценке его стоимости, исходя из рыночных условий и включение ее в расчет при определении доли того или иного учредителя, наследника.

13. Необходимо внесение поправок в законодательство или в правила регистрации доменных имен в случае наследования.

14. Исполнения судебного решения о запрете ответчику использовать в доменном имени, идентичное или совпадающее до степени смешения с товарным знаком фирмы- истца обозначение, правами на которое обладает истец может столкнуться с трудностями.Основное противоречия заключается в том, что передать(продать) доменное имя можно другому администратору за 3 дня, а рассмотрение судебного дела, включая получение судебного решения длится, как правило несколько месяцев.

При этом продажа доменного имени может быть осуществлена:

- до подачи иска;

-сразу после того, как администратор домена- ответчик, узнает отом, что к нему предъявлен иск;

- во время рассмотрения судебного дела;

- после получения судебного решения,

при этом администратор домена, он же ответчик может передать домен, как без смены фирмы регистратора, так и со сменойфирмы регистратора.

Аналогичные последствия наступают в случае утраты регистратором аккредитации.

Особенность доменных споров состоит в том, что администратору доменного имени требуется очень мало времени для того, чтобы передать права администрирования домена иному администратору, что послужит основанием для отказа истцу в удовлетворении заявленных им требований о запрете предыдущему администратору использовать спорное доменное имя.

15.Юридической основой обеспечительных мер являются предварительные обеспечительные меры, предусмотренные ст. 91 АПК РФ и ст. 99 АПК РФ и Постановление Президиума Суда по интеллектуальным правам «Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору» от 15 октября 2013 года.

16. При регистрации доменного именидоменное имя должно:

- быть достаточно просто запоминаемым;

-отражать по возможности, содержательнуюсоставляющую информационных ресурсов, которые предполагается размещать по этому адресу;

- не должно противоречить общественным интересам, принципам гуманности и морали;

- не должно совпадать с специализированными обозначениями, доменных имен, сходство с которыми может вводить в заблуждение;

- быть «свободным».

17. После принятия Президиумом ВАС РФ постановления от 8 декабря 2009 года, доменные споры о нарушениях исключительных прав на товарный знак в доменном имени с участием физических лиц, не зарегистрированных в качестве индивидуальных предпринимателей, подлежат разрешению в арбитражных судах.

18.Апелляционные жалобы на судебные акты по доменным спорам рассматривают арбитражные апелляционные суды.

19. В соответствии с законом Суд по интеллектуальным правам является специализированным арбитражным судом, рассматривающим в пределах своей компетенции дела по спорам, связанным с защитой интеллектуальных прав, в качестве суда первой и кассационной инстанций.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

Нормативные правовые акты

1. «Конвенция по охране промышленной собственности» (Заключена в Париже 20.03.1883) (ред. от 02.10.1979)// СПС КонсультантПлюс.

2.«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ) // СПС КонсультантПлюс.

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»(принят ГД РФ 14.07.2006)// СПС КонсультантПлюс.

4. Федеральный закон от 11 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (принят ГД РФ 25.03.2011)// СПС КонсультантПлюс.

5.Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет")// СПС КонсультантПлюс.

6. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"// СПС КонсультантПлюс.

7. Постановление Правительства Российской Федерации от 30 июня 2004 г. № 320 «Об утверждении Положения о Федеральном агентстве связи»// СПС Консультант Плюс.

8. Постановление Правительства Российской Федерации от 23 января 2006 г. № 32 «Об утверждении Правил оказания услуг связи по передаче данных»// СПС Консультант Плюс.

9. Гражданский кодекс Российской Федерации от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018) (принят ГД 24.11. 2006) // СПС Консультант Плюс.

10. Арбитражный процессуальный кодекс Российской Федерации" от 24.07.2002 N 95-ФЗ (ред. от 25.12.2018) (принят 14.06.2002)// СПС Консультант Плюс.

Специальная литература

11.ГерцеваЕ. Н., ГринкевичА. П. Доменные споры. Судебная практика в России: Эксмо; Москва, 2014.

12. Дашян М.С. Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет– М.:"Волтерс Клувер", 2007.

13.Звягин В.А. Проблемы правового регулирования использования исключительных прав на фирменные наименования и прав на доменные имена: Автореф. Дис. на соиск. уч. степ. канд. юрид. наук.М., 2011.- 24 с.

14. МикаеваА. С. Проблемы правового регулирования в сети Интернет и их причины / А. С. Микаева //Актуальные проблемы российского права. 2016. № 9 (70) с.67-74.

15. Правила регистрации доменных имен в доменах .RU , утв. Решением Координационного центра национального домена сети Интернет от 17.06.2009 №2009-08/53)// СПС Консультант Плюс.

16. Попцов А. В. Правовое регулирование доменного имени в Российской Федерации: Автореф. дис. на соиск. уч. степ. канд. юрид. наук.М., 2009.- 36 с.

17. Серго А. Г. Правовой режим доменных имен и его развитие в гражданском праве: Автореф. дис. на соиск. уч. степ. д-ра юрид. наук.М., 20011.- 59 с.

18. Серго А. Г. Доменные имена в свете нового законодательства М.: ГОУ ВПО РГИИС, 2010.

Источники на иностранном языке

19. Anderson, J. M. Why we need a new definition of information security // Computers & Security. — 2003. — Vol. 22, no. 4. — P. 308–313. — DOI:10.1016/S0167-4048(03)00407-3.

20. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014.

21. Belinda Isaac. Personal Names and the UDRP: A Warning to Authors and Celebrities // Entertainment Law Review. Vol. 12, No. 2. 2001. pp. 43-52.

22. Department of Defense Tristed Computer System Evaliatin Criteria-Dod 520028-STD,Desember 26, 1985.

23. Duncan Curley. Cybersquatters Evicted Protecting Names Under the UDRP // Entertainment Law Review. Vol. 12, No. 3. 2001. pp. 91-94.

24. Emerson H. Tiller. ICANN's Uniform Domain Name Dispute Resolution Policy: An Overview and Critique // Internet Law & Business. Vol. 1, No. 8. June 2000. pp. 589-602.

25.Sebastian Baum. Domain Name Conflicts in Germany — An Economic Analysis of the Federal High Court’s Recent Decisions// European Business Organization Law Review, Vol 4, Issue 1, March 2003 pp 137–170.

Материалы судебнойпрактики

26. Постановление Президиума ВАС РФ от 08.12.2009 N 9833/09 по делу N А40-53937/08-51-526// СПС Консультант Плюс.

27. Постановление Президиума Суда по интеллектуальным правам от 15 октября 2013 г. № СП-23/3 “Об утверждении справки о некоторых вопросах, связанных с процессуальным порядком применения обеспечительных мер по доменному спору”// СПС Консультант Плюс.

28. Постановление Пленума ВАС РФ от 12.10.2006 N 55 (ред. от 27.06.2017) "О применении арбитражными судами обеспечительных мер"// СПС Консультант Плюс.

29.Постановление Президиума ВАС РФNo. 1192/00от 16.01.2001 г. по делу № А40-25314/99-15-271// СПС Консультант Плюс.

30. Постановление Президиума ВАС РФот 11.11.2008 N 5560/08 по делу N А56-46111/2003// СПС Консультант Плюс.

31. Постановление ФАС Московского округа от 13.07.2010 N КГ-А40/7026-10 по делу N А40-100094/09-110-663// СПС Консультант Плюс.