3. Устройства 3D ввода [Электронный ресурс] / Режим доступа: http://rangevision.com/ - Дата доступа 17.03.2012

Григорьев В.С., Прохорчук А.Н.

БГЭУ, УЭФ, группы 11-ДЭГ-2 и 11-ДЭЗ, 1 курс

ПРОБЛЕМА КИБЕРСКВОТТИНГА В БЕЛАРУСИ, МЕТОДЫ ЕЕ РЕШЕНИЯ

Англ. «squatter» – поселившейся незаконно на незанятой земле. Регистрация доменных имен с целью их последующей перепродажи. Практикующие подобную деятельность – кибersквоттеры. Основные цели кибersквоттеров. Методы достижения поставленных целей. Получение доступа к статистике поисковых запросов популярных поисковых систем. Четыре типа кибersквоттинга. 1) Тайпсквоттинг. Наиболее безобидный, зарабатывание на имени компании без препятствий для ее деятельности. 2) Брендовый кибersквоттинг. Покупка доменных имен, невзирая на охрану посредством регистрации. 3) Защитный кибersквоттинг. Выкуп доменов, созвучных с оригиналом. 4) Бит-сквоттинг. Использование ошибок в модулях оперативной памяти DNS-серверов. Запись в двоичной системе практически соответствует подлинному имени домена. Причина: DNS-серверы работают с использованием ASCII-таблицы, в которой числовое значение соответствует определённому символу. Постепенное превращение доменов из потребительского товара в средство инвестирования.

Распространение кибersквоттинга на территории Беларуси. Массовое явление в стране. Цена вопроса в белорусском сегменте. Сравнение зоны .by с зонами .ru, .com, .org. Тридцатидневная блокировка домена при регистрации. Лазейка для кибersквоттеров. Постановление о лишении прав регистрации доменных имен компанией ООО “Открытый контакт”. Выбор нового технического регистратора доменов Право присваивания доменных имен белорусским сайтам - УП “Надежные программы”. Снижение стоимости

годового обслуживания. Либерализация законодательства в пользу брендовых имен. Выкуп захваченных имен без судебного разбирательства. Двоякое отношение со стороны компаний.

Две главные причины киберсквоттинга: пробелы в законодательстве и нерасторопность компаний. В правовых документах понятия «бренд» и «домен» используются недавно, законодательство в их отношении только формируется. Придание домену статуса товарного знака. Защита товарного знака, его длительная регистрация. Пример с организацией «Белшина». Прямой путь в антимонопольный орган.

Арбитражный центр (ICANN) при всемирной организации интеллектуальной собственности. Уникальность процедуры решения споров о доменах. Возможность распространения практики на территорию Байнета.

Возможность для компании регистрации сразу всех созвучных названий. Возможная регистрация с ошибками. Небольшие издержки по сравнению с судебными разбирательствами.

Как защититься от киберсквоттинга? Большая трудность в белорусских регионах. Отсутствие законодательного регулирования доменного имени как объекта гражданских прав. Отсутствие третейских процедур, которые защищают права владельца бренда от киберсквоттинга. Введение товарного знака в гражданский оборот. Территориальное ограничение законодательства о товарных знаках. Рассмотрение методов ICANN. Единая политика по разрешению споров, связанных с доменными именами. Правила для разрешения споров, связанных с доменными именами при выборе доменного имени. Минусы данной процедуры.

Регистрация латинского имени, имеющего нужное кириллическое значение. Добавление к имени домена ключевого слова, характеризующего деятельность. Регистрация имени в другой доменной зоне. Использование вспомогательных зон. Аналоговые зоны Республики Беларусь. Фиксирование всех ошибочных значений имени при быстром наборе домена, последующий их выкуп. Возможность регистрации доменного имени в качестве товарного знака

или знака обслуживания. Избегание созвучности имени с чужими брендами. Создание собственных методик.

Литература

1. Журнал «Компьютерные вести» № 17, 16.11.2011, стр. 3-5
2. Журнал «Главная Книга.by» №2, январь 2012, стр. 30-36
3. Википедия, ru.wikipedia.org/wiki/Киберсквоттинг
4. Газета «Хартия», 05.03.2012
5. Газета «Советская Белоруссия», 03.11.2010

Гринько Е.Ю.
БГЭУ, ФМБК, ДЯК-3, 1 курс

ЗАЩИТА ОС ANDRIOD ОТ МОБИЛЬНОГО БОТНЕТА

В 2008г. эксперты в области информационной безопасности считали, что уже в течение года злоумышленники могут попытаться сформировать мобильные ботнеты с целью проведения различного рода атак при помощи портативных устройств. Как сообщал CNET News, ожидать появления первых мобильных ботнетов стоило уже в 2009 году. Такие ботнеты злоумышленники теоретически могли использовать для рассылки спама абонентам сотовых операторов или для организации атак на беспроводные сервисы.

В феврале 2012г компанией Symantec было обнаружено вредоносное приложение для мобильных телефонов на платформе ОС Android - RootSmart, которое распространяется в альтернативных китайских каталогах программного обеспечения. В официальном Android Market такого пока не обнаружено. Программа RootSmart устанавливается вместе с обычными программами из каталога, но при этом передаёт на удалённый сервер информацию о заражённом устройстве: номер IMEI, номер IMSI, ID соты, location area code и код мобильной сети.

RootSmart является второй программой после GingerMaster, которая применила на практике известный рут-эксплоит GingerBreak (для Android OS