УДК 316
DOI 10.18522/2227-8656.2020.3.19

ЗАЩИТА ИНВЕСТИЦИЙ В РАЗВИТИЕ БРЕНДОВ В ЭПОХУ ЦИФРОВИЗАЦИИ

PROTECTING INVESTMENT IN BRAND DEVELOPMENT IN THE AGE OF DIGITALIZATION

Ламинина Ольга Глебовна
Кандидат философских наук, доцент, кафедра информационной аналитики и политических технологий, Московский государственный технический университет имени Н.Э. Баумана, г. Москва, Россия,
e-mail: Olga.Laminina@gmail.com

Olga G. Laminina
Candidate of Philosophical Sciences, Associate Professor, Department of the Information Analytics and Political Technologies, Bauman Moscow State Technical University, Moscow, Russia,
e-mail: Olga.Laminina@gmail.com

Киберпространство – это цифровой мир, дающий новые возможности не только добропорядочным пользователям Сети, но и киберпреступникам, использующим все новые и максимально автоматизированные технологии. В данной статье анализируются основные риски и наиболее распространенные технологии, наносящие вред брендам. В связи с уязвимостью брендов перед лицом все увеличивающегося цифрового пространства раскрываются возможные проактивные средства для их защиты.

Ключевые слова: безопасность; мошенничество; информация; бренды; киберпреступник; домены; киберсквоттинг; фишинг-мошенничество.

Cyberspace is a digital world that gives new opportunities not only to legal users, but also to cybercriminals, who use all new and maximally automated technologies. This article analyzes the main risks and the most common technologies that harm brands. Due to the vulnerability of brands in the face of an ever-increasing digital space, possible proactive means to protect them are revealed.

Keywords: security; fraud; information; brands; cybercriminal; domains; cybersquatting; phishing fraud.

Введение

Развитие цифровых технологий и проникновение их во многие сферы жизнедеятельности человека являются важными элементами научно-технического прогресса. Процесс становления цифровой экономики в современном мире идет стремительными темпами. Однако отношение членов общества к данному технологическому прорыву далеко не во всем позитивное. Особенно это относится к созданию модели цифрового общества и дальнейшего его воплощения в жизнь (Ковалев, 2019). Так, в числе наиболее существенных рисков выявлены и называются следующие:

- риск снижения контроля в сфере цифровых сервисов, а также рост возможностей для мошенничества, обусловленные расширением спектра и индивидуализацией цифровых услуг населению;
- риск утечки информации, требующий значительных дополнительных инвестиций в информационную безопасность;
- риск роста и организованности киберпреступности;
- угроза массовой безработицы (Савина, 2018).

Цифровой мир брендов

В условиях цифровизации доменные имена и бренды начали использовать по-новому – в основном как средство индивидуализации. Но не сайтов в сети Интернет как совокупности программ для ЭВМ и иной информации, а юридических лиц, товаров, работ, услуг и предприятий (Косицкий, 2018).

Интеллектуальная собственность вообще и доменное имя и бренд в частности являются специфическими категориями, порожденными глобальным информационным пространством. Интеллектуальная собственность представляет собой информацию, на владение которой имеет право лицо, называемое ее собственником. Сегодня можно говорить о наличии глобального международного рынка обращения интеллектуальной собственности и информации, в частности брендов (Кривин, 2017).

По данным недавно опубликованного отчета, сделанного по результатам исследования, которое было проведено консалтинговым агентством Interbrand, широко известные организации, входящие в список 500 крупнейших компаний, ежегодно публикуемый журналом Fortune, осуществляют значительные инвестиции для построения собственных брендов, а также тратят немалые средства на их защиту.

Расширение цифрового сервиса, индивидуализация многих видов

услуг повышают угрозу мошенничества при снижении контроля со стороны пользователей или провайдеров. В настоящий момент киберугрозы и ущерб от киберпреступников вышли на второе место в мире после техногенных катастроф (Удалов, 2018).

Бренды, как крупные, так и мелкие, сталкиваются с новым миром, полным угроз и рисков ввиду того, что интеллектуальная собственность становится более уязвимой перед лицом все увеличивающегося цифрового пространства. Бренды все время осаждаются со стороны как киберпреступников, так и представляющих угрозу лиц, использующих возможности новых интернет-технологий для получения незаконной прибыли с одновременным снижением целостности и ценности зарекомендовавшего себя бренда.

«Мошенничество в отношении брендов» – это широкий собирательный термин, используемый для охвата большого ряда угроз, которые обходятся владельцам брендов в сотни миллиардов долларов каждый год (Филиппова, 2016).

Некоторые из наиболее распространенных технологий включают киберсквоттинг (покупка и регистрация доменного имени, который может быть торговой маркой, с целью последующей его перепродажи), продажу подделок брендовых товаров, целевое фишинг-мошенничество и кражу доменов. Тем не менее при использовании соответствующих инструментов для расследования и мониторинга организации могут заблаговременно защитить себя от убытков, поддерживать соответствующий уровень доверия со стороны клиентов, а также сохранить самый ценный бриллиант в короне интеллектуальной собственности – бренды (Цзин Ли, 2020).

Четыре наиболее распространенные технологии, наносящие вред брендам

С развитием технологий происходит изменение тактик, применяемых киберпреступниками для выявления и использования потенциальных уязвимостей. В отношении брендов количество проблем увеличивается в силу их комплексности, так как приходится выделять много ресурсов для выявления и преследования злоумышленников. Далее приводится описание четырех наиболее распространенных технологий Brand Abuse (наносящих вред брендам), которые должны быть хорошо известны тем, кто обеспечивает защиту инвестиций в бренды в долгосрочной перспективе:

1. **Киберсквоттинг** может реализовываться в двух основных форматах:

– **непосредственные опечатки.** Прямые опечатки – регистрация сквоттером намеренно неправильно написанных доменных имен при-

знанных брендов (например, amazan.com). Если неправильный домен ввести в веб-браузер, то пользователь будет перенаправлен на сайт с рекламой конкурента или на сайт с различными опросами, при этом мошенники могут использовать брендовое оформление и элементы логотипа amazon.com на странице для придания ей легитимности. Конечно же, любой человек, перенаправленный на такой сайт, в действительности пытался найти amazon.com и в итоге будет ужасно недоволен, а это негативно сказывается на бренде Amazon, не говоря о том, что клиенты не смогут найти сайт и получить услуги, на которые изначально рассчитывали;

– **сайты с негативными отзывами**, как, например, amazonsucks.com. Такие сайты зачастую регистрируются недовольными клиентами или конкурирующими компаниями, а также используются в качестве информационных досок для анонимных информационных атак на бренд компании (Форси, 2019).

2. **Фальсификация** является продолжением тактики киберсквоттинга. При использовании доменов с неправильно указанными именами или доменов, связанных с целевым брендом, мошенник или мошенническая организация будут пытаться продавать контрафактную продукцию, делая ставки на доверие пользователей и ценность бренда, чтобы не возникали сомнения в подлинности сайта.

3. **Фишинг** – это высокообъемный спам, специально нацеленный на клиентскую базу бренда. Используя сквоттированные домены, фишинг-мошенники стараются заставить клиента ввести свои учетные данные, чтобы получить номера кредитных карт и прочую ценную информацию, которая может находиться в учетной записи пользователя бренда/сайта.

Целевое фишинг-мошенничество представляет собой особенно вредоносную форму фишинга, в рамках которого мошенником направляются электронные письма с корпоративного домена, имеющего довольно правдоподобный вид, большому количеству сотрудников компании с просьбой о вводе логина и пароля или осуществлении других действий, которые позволили бы мошеннику получить доступ к данным и системам, которые можно было бы украсть или нанести вред. На первый взгляд данного рода мошенничество больше относится к вопросам кибербезопасности, но берет свое начало от атак Brand Abuse на уровне домена.

4. **Кража доменов.** В отдельных случаях кибермошенники могут попытаться украсть ваше доменное имя у вашего регистратора или как минимум взломать вашу учетную запись и изменить имена серверов,

данные DNS или данные службы Whois. Именно это произошло с сайтами twitter.com и newyorktimes.com, когда они были атакованы сирийской электронной армией в конце августа 2013 г. Защита от данного рода кибератак начинается на уровне регистратора и реестров.

Проактивные средства для защиты брендов

Не существует идеального рецепта, который обеспечил бы полную защиту вашего бренда. Вместо этого компании, занимающиеся данным вопросом, очень эффективно используют основные процессы, гарантирующие, что их бренд защищается проактивным и всеобъемлющим образом. Основные средства для защиты брендов можно разделить на три части.

Обнаружение

Генератор опечаток. В футболе говорят, что лучшая атака начинается с хорошей защиты. В сфере защиты брендов это означает, что компании должны сами регистрировать на себя домены с опечатками. Некоторые организации воспримут в штыки необходимость затраты средств на регистрацию доменов, которые они никогда не будут использовать. Однако намного лучше контролировать домены с опечатками, чем если это сделает за вас кто-то еще. В среднем стоимость составляет 500−800 рублей в год за домен, и это довольно дешевая страховая политика (Кокинг, 2019).

Многие компании, занимающиеся защитой брендов, предлагают бесплатный инструмент − генератор опечаток. Он используется для получения списка наиболее распространенных опечаток, которые возможны при написании вашего бренда. Данный инструмент рекомендуется использовать до запуска нового бренда, таким образом можно получить максимум информации о наиболее распространенных опечатках по бренду.

Поиск брендов. Необходимо найти зарегистрированные домены по всему миру, содержащие название бренда. Это позволит выявить почти все существующие или зарегистрированные ранее домены, которые используют название бренда как часть собственных доменов. Можно использовать функцию расширенного поиска, чтобы ограничить зону поиска доменами верхнего уровня, также это позволит сократить число ложных срабатываний с помощью функции И/НЕ и привязать строки бренда к определенной области внутри доменного имени.

Скриншоты. В случае если компания стала жертвой атаки на бренд, необходимо делать скриншоты вредоносных доменных имен. Скриншоты также могут быть важной частью доказательной базы при подаче иска или использоваться в качестве существенного аргумента для убеждения сторон передать управление доменами, которым был нанесен ущерб.

Получение данных о злоумышленнике

Службы Whois и Whois History. Эти инструменты используются для поиска информации о владельцах доменов, с помощью которых бренду был нанесен ущерб. Данные, предоставляемые службой Whois, помогут установить лицо или организацию, пытавшихся произвести манипуляции в своих интересах.

Технология изменения IP и сервера имен Reverse IP и Reverse NS

После выявления домена − источника вредоносной активности полезно найти другие домены, расположенные на одном и том же ресурсе. Это можно сделать с помощью технологии Reverse IP совместно с недавно появившимся инструментом последовательного поиска серверов имен Reverse Name Server, они позволят найти все остальные домены, расположенные по данному IP-адресу, или указать на соответствующий сервер имен.

Служба Reverse Whois. Reverse Whois − высокопроизводительный инструмент идентификации, позволяющий проводить поиск по всем записям службы Whois для выявления других доменов, находящихся в собственности одного и того же владельца. Можно вести поиск как среди зарегистрированных на настоящий момент доменов, так и среди ранее зарегистрированных. Искать можно по имени, адресу электронной почты, названию организации или другим связанным данным, указанным в записи службы Whois. Во многих случаях можно начать просто с одной записи Whois и получить в результате список из тысяч доменов с опечатками, находящихся в собственности одного и того же владельца.

Мониторинг. Многие компании предлагают услуги мониторинга.

Возможность мониторинга брендов. Ежедневно проводятся поиск всех новых зарегистрированных доменов и оповещение клиента в случае выявления любого содержащего установленные текстовые строки бренда. Это простой и дешевый способ предотвратить любого рода вредоносную доменную активность. Знания – си-

ла, а такие сведения позволят сорвать планы любых мошенников-кибersквоттеров.

Мониторинг доменов. Мониторинг доменов моментально уведомляет об изменениях любого рода в регистрационных данных вашего домена в службе Whois. Это довольно простой и незамысловатый способ создания дополнительного уровня защиты от краж доменов или предотвращения ситуации случайного истечения срока использования домена (Устел, 2019).

Мониторинг серверов имен и IP. Он позволит получать уведомления об активности определенных интернет-ресурсов, направленной на ваши домены. В результате можно получить список доменов или диапазоны IP-адресов, служащих хостом для вредоносных сайтов, а это позволит вам быть всегда на шаг впереди, изучая любую активность, исходящую от таких ресурсов.

Мониторинг владельцев регистрации. Мониторинг владельцев регистрации позволит не упускать из виду лица или организации, когда-либо замешанные в кибермошенничестве. После получения идентифицирующего имени, адреса электронной почты, алиаса или уникального маркера в записи по вредоносной активности службы Whois можно провести мониторинг владельцев регистрации для выявления любых новых доменных регистраций, связанных с такими идентификационными атрибутами. При этом приходят уведомления о любой последующей доменной активности со стороны таких лиц или организаций и появляются дополнительные доказательства для проводимой деятельности по обеспечению безопасности брендов.

Заключение

Борьба за обеспечение безопасности брендов и интеллектуальной собственности в интернет-пространстве будет становиться все более ожесточенной. Передовые линии защиты в такой борьбе находятся на уровне доменных имен и DNS. В то время как внимание, необходимое в этой области, минимально по сравнению с другими фронтами в этой войне, с другой стороны, беспечность может обойтись очень дорого, в первую очередь привести к репутационным рискам, потери прибыли и брендов. Избежать подобных ситуаций просто − надо воспользоваться бесплатными или относительно недорогостоящими службами и перевести свою осведомленность о новых и потенциальных киберугрозах на принципиально новый, более высокий уровень.

Литература

Ковалев В.Н. Риски цифровизации общества // Черноморская конференция : сб. материалов III Черноморской междунар. науч.-практ. конф. МГУ / под ред. О.А. Шпырко, В.В. Хапаева, С.И. Рубцовой, Ю.Л. Ситько. Севастополь : Филиал МГУ в г. Севастополе, 2019.

Кокинг С. Как защитить интернет-идентичность вашего бренда от конкурентов в 2020 году. 2019. Режим доступа: https:// irishtechnews.ie/protect-brands-online-identity-from-competitors.

Косицкий А.О. Доменное имя – что это для российской правовой системы? // Эволюция российского права : материалы XVI Междунар. науч. конф. молодых ученых и студентов. Екатеринбург : Уральский государственный юридический ун-т, 2018. С. 151–152.

Кривин Д.В. Доменное имя как средство индивидуализации юридического лица // Российское право: образование, практика, наука. 2017. № 1. (97). С. 60–61.

Савина Т.Н. Цифровая экономика как новая парадигма развития: вызовы, возможности и перспективы // Финансы и кредит. 2018. Т. 24, № 3. С. 579–590.

Удалов Д.В. Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1 (30). С. 12–18.

Устел С. Стратегия защиты бренда как проактивный подход. Режим доступа: https://www.ustels.com/keynote/proactive-brand-protection-strategy/.

Филиппова С.Ю. Право доступа к ресурсам интернет-сайта: проблемы гражданско-правовой квалификации // Информационное право. 2016. С.20-25.

Цзин Ли. Как правильно выбрать решение для защиты бренда. 15 мая 2020 г. Режим доступа: https:// blog.redpoints. com/en/choose-brand-protection-solution.

Форси К. Управление репутацией: как защитить свой бренд онлайн в 2020 году. 2019. Режим доступа: https:// blog. hubspot.com/marketing/reputation-management.

References

Kovalev, V.N. (2019). The risks of digitalization of society. *Black Sea Conference. The collection of materials of the III Black Sea International Scientific and Practical Conference of Lomonosov MSU.* In O.A. Shpyrko, V.V. Hapaeva, S.I. Rubcova, Yu.L. Sit'ko (Eds.). Sevastopol: Filial MGU v g. Sevastopole. (in Russian).

Cocking, S. (2019). How to protect the Internet identity of your rend from competitors in 2020. Available at: https:// irishtech-news.ie/protect-brands-online-identity-from-competitors/. (in Russian).

Kosickij, A.O. (2018). Domain name - what is it for the Russian legal system? *Evolution of Russian Law: Materials of the XVI International Scientific Conference of Young Scientists and Students*. Yekaterinburg: Ural'skij gosudarstvennyj yuridicheskij universitet, 151-152. (in Russian).

Krivin, D.V. (2017). The domain name as a means of individualization of a legal entity. *Rossiyskoye pravo: obrazovaniye, praktika, nauka,* 1 (97), 60-61. (in Russian).

Savina, T.N. (2018). Digital economy as a new development paradigm: challenges, opportunities and prospects. *Finansy i kredit,* 24, 3, 579-590. (in Russian).

Udalov, D.V. (2018). Threats and challenges of the digital economy. *Ekonomicheskaya bezopasnost' i kachestvo,* 1 (30), 12-18. (in Russian).

Ustel, S. Brand protection strategy as a proactive approach. Available at: https:// www.ustels.com/keynote/proactive-brand-protection-strategy/. (in Russian).

Filippova, S.Yu. (2016). The right of access to the resources of the website: problems of civil law qualifications. *Informatsionnoye pravo,* 20-25. (in Russian).

Jing, Li. How to choose the right solution for brand protection. May 15, 2020. Available at: https:// blog.redpoints.com/en/choose-brand-protection-solution. (in Russian).

Forsy, K. (2019). Reputation management: how to protect your brand online in 2020. Available at: https:// blog.hubspot.com/ marketing/reputation-management. (in Russian).

Поступила в редакцию ***29 апреля 2020 г.***