Доверие и безопасность в информационном обществе

ОСОБЕННОСТИ «ЧЕРНОГО РЫНКА» ПЕРСОНАЛЬНЫХ ДАННЫХ И СОЗДАВАЕМЫЕ ИМ ПРОБЛЕМЫ

Статья рекомендована к публикации председателем редакционного совета Ю.Е. Хохловым 28.12.2020.

Алигулиев Расим Магамед оглу

Доктор технических наук, профессор
Институт информационных технологий НАНА
Баку, Азербайджанская Республика
r.alguliev@gmail.com

Махмудов Расим Шариф оглу

Институт информационных технологий НАНА
Баку, Азербайджанская Республика
rasimmahmudov@gmail.com

Аннотация

В статье исследуются сущность и особенности «черного рынка» персональных данных. Рассмотрены являющиеся предметом купли-продажи на «черном рынке» виды информации и услуг, технологии и их ценовая политика, а также цели, для которых используются персональные данные, приобретенные на «черном рынке». Кроме того, отмечены проблемы, связанные с незаконным приобретением и продажей персональных данных с точки зрения личных, корпоративных и национальных интересов.

Ключевые слова

личная жизнь, персональные данные; «черный рынок» персональных данных; стоимость персональных данных; кража персональных данных

Введение

Базы данных, которые из-за их стратегической важности называют «валютой XXI века», по своей значимости сравнивают с запасами нефти. Развитие в мире инновационных инициатив, информационной экономики и экономики знаний также резко увеличивает спрос на персональные данные. В «Отчете о цифровой экономике» UNCTAD (United Nations Conference on Trade and Development), представленном в 2019 году, говорится: «Основу цифровой экономики составляют цифровые данные. А основу цифровых данных – персональные данные.» [1].

Очевидно, что по мере роста ценности и важности персональных данных растет и спрос на них. Из-за наличия норм юридической ответственности и ограничений на использование персональных данных спрос на их использование в незаконных деловых и криминальных целях способствует формированию «черного рынка» в этой сфере.

Применение современных технологий и инструментов информационной безопасности в основном обеспечивают защиту от стандартных кибератак. Поэтому киберпреступники постоянно ищут новые возможности и методы обхода существующих систем безопасности. Одним из таких методов является получение персональных данных посредством «черного рынка» [2].

На «черном рынке» могут быть проданы любые персональные данные, которые люди хотят сохранить в секрете от других, например, удостоверение личности, водительские права, страховое свидетельство, кредитная карта, карта здоровья, банковский счет, ИНН, информация о мобильном телефоне, адрес электронной почты, домашний или рабочий адрес и т. д. Киберпреступники используют эту информацию для мошенничества, шантажа и вымогательства, применяя методы социальной инженерии. Хотя исследователи предсказывали формирование рынка персональных данных еще в 1990-х годах, представители научного и юридического сообществ в то время относились к этой идее весьма осторожно. Они считали, что право на неприкосновенность частной

жизни и существующие механизмы для его реализации не позволят персональным данным стать предметом торговли [3].

Многие эксперты по-прежнему считают неприкосновенность частной жизни неотъемлемым правом человека. Хотя технологии конфиденциальности нацелены на защиту этих прав, рынок персональных данных развивается в другом направлении. Многие эксперты предсказывают, что «черный рынок» персональных данных будет продолжать расти. Этот быстрорастущий «черный бизнес» поддерживается мировым сообществом хакеров и разработчиков вредоносных программ. Таким образом, «черный рынок» персональных данных также стимулирует развитие рынка вредоносного и криминального программного обеспечения [4].

В Соединенных Штатах к товарам «черного рынка» проявляют большой интерес. В 2019 году страна потратила на персональные данные 15,2 миллиарда долларов. Самый крупный «черный рынок» персональных данных в мире находится в США – около 60% мирового рынка. Китайский рынок персональных данных с 2,4 миллиардами долларов является вторым по величине в мире. Следующие три места занимают Великобритания, Канада и Франция соответственно [5].

В статье исследуются сущность и особенности «черного рынка» персональных данных. Рассмотрены виды информации и услуг, технологии и их ценовая политика, которые являются предметом торговли на «черном рынке», определена цель использования персональных данных, приобретенных на «черном рынке». Кроме того, отмечены проблемы, связанные с незаконным приобретением и продажей этих данных с точки зрения личных, корпоративных и национальных интересов.

1. Подходы к сущности личной жизни и персональных данных

Персональные данные являются важной составляющей личной жизни. Другими словами, обеспечение конфиденциальности личной жизни требует защиты персональных данных. Поэтому, чтобы лучше понять суть персональных данных, целесообразно рассматривать их через призму личной жизни [6].

Благодаря практическому применению статьи 8 «Европейской конвенции о защите прав и свобод человека» (1950 г.), дано точное нормативное объяснение термина «личная жизнь». Так, в заявлении Европейского суда по правам человека (1992 г.) говорится: «Личная жизнь – это широкая категория, которую невозможно полностью описать. Каждый человек волен развивать эту концепцию и придавать ей определенный смысл. Недопустимо ограничивать это понятие «внутренним кругом» и исключать внешний мир, не принадлежащий этому кругу. Таким образом, понятие «личная жизнь» отражает необходимость развития права на взаимодействие с другими людьми и внешним миром» [7].

Общим эквивалентом термина «неприкосновенность частной жизни» и термина «privacy», используемого в международных документах, является латинское выражение «конфиденциальность». Его смысл – свобода, секретность, одиночество, собственность, личная жизнь, частная жизнь, неприкосновенность, неприкосновенность частной жизни, идентичность, межличностные отношения.

Персональные данные можно разделить на две категории в зависимости от отношения к ним людей, к которым они относятся [2]:

- «нейтральные» персонализированные данные, факт обнародования и распространения которых субъект этих данных игнорирует;
- данные, распространение которых субъект этих данных хочет ограничить.

Данные, относящиеся ко второй категории, называются «персональными данными», а несанкционированный доступ и использование этих данных классифицируются в международном праве как «нарушение прав субъекта данных».

2. Основные особенности и услуги «черного рынка»

«Черный рынок» традиционно определяется как место незаконного обмена товарами и услугами. Очевидно, что существуют такие виды товаров и услуг, продажа которых разрешается законом. Однако в некоторых случаях этот процесс осуществляется без официального оформления (без получения лицензии, без учета налогов или без соблюдения других необходимых требований). В этом случае покупка и продажа товаров и услуг попадает в категорию «черного рынка». Есть также товары и услуги, продажа которых вообще запрещена законом (например, наркотики, торговля

людьми и т. д.). Закон не разрешает покупку и продажу персональных данных без разрешения владельцев. Следовательно, незаконная покупка и продажа такой информации также попадает в категорию «черного рынка».

Следует отметить, что купля-продажа персональных данных – это новый вид бизнеса, который становится все более актуальным в связи с развитием Интернета и других информационных технологий, электронных сервисов, виртуальных отношений. Персональные данные тогда становятся предметом торговли, когда определенная категория людей заинтересована в их использовании для бизнеса и других целей.

Одна из основных причин широкого использования персональных данных на «черном рынке» заключается в том, что эта сфера пока не регулируется законодательством. Пока что законодательство ни одной страны не признает какую-либо информацию, в том числе персональные данные, предметом продажи. Поэтому такие выражения, как «покупка и продажа персональных данных», «кража персональных данных» юридически описать сложно.

На данный момент только закон «О защите персональных данных потребителей», принятый штатом Калифорния и вступивший в силу 1 января 2020 года, предусматривает куплю-продажу персональных данных [8]. Согласно этому закону, продажа персональных данных – это предоставление компанией персональных данных потребителя в коммерческих целях третьей стороне в устной, письменной, электронной или других формах за плату. В данном случае речь идет о продаже персональных данных, собранных компанией от потребителей, которых она обслуживает, третьему лицу, которое желает использовать эту информацию в коммерческих целях для получения дохода. То есть этот закон не регулирует прямые отношения между владельцами персональных данных и их получателями. Эксперты прогнозируют, что такой правовой механизм в будущем будет применяться на всей территории США, а также в других странах.

Термин «кража персональных данных» как юридическое понятие в настоящее время отражен только в законодательстве США и Великобритании [9]. «Кража персональных данных» означает захват такого типа информации другими лицами различными скрытыми способами в коммерческих, мошеннических или других преступных целях без разрешения самого владельца персональных данных. В законодательствах многих странах такие действия, как кража персональных данных, описывается как «нарушение неприкосновенности личной жизни», «несанкционированный доступ к компьютерной информации» и т. д.

Однако, несмотря на то, что эти юридические вопросы еще не решены, персональные данные как предмет купли-продажи уже давно пользуются большим спросом для целей Big Data. Отметим, что Big Data – это одна из основных технологических и экономических тенденций в мире.

Одна из основных характеристик персональных данных – это их ценность. Ценность персональных данных определяется целью человека, который ее ищет. Как и в случае с другими предметами торговли, рыночный закон спроса и предложения играет важную роль в определении ценности персональных данных.

Цена при продаже персональных данных на «черном рынке» зависит от социального статуса и финансовых возможностей людей. Для формирования кадрового состава этого «черного рынка труда» организуются специальные хакерские курсы. В большинстве случаев оплата на «черном рынке» производится в криптовалюте, что очень затрудняет борьбу с подобной киберпреступностью. На формирование цен персональных данных на черном рынке влияют 4 основных фактора. Во-первых, как и в нормальной экономике, на «черном рынке» действуют законы спроса и предложения. Вторым фактором является остаток на счете – если на кредитной карте доступная сумма в достаточном количестве, то и цена будет высокой. Третий фактор – это высокий бал стабильности карт лояльности (loyalty cards), что также увеличивает их ценность. Наконец, ценность персональных данных может зависеть от их повторного использования. То есть возможность повторного использования увеличивает ценность этих данных. Например, клиенты «черного рынка» платят больше за многоразовую кредитную карту, чем за одноразовую подарочную карту.

Незаконная продажа персональных данных часто осуществляется в Интернете. Для оказания подобных незаконных услуг широко используется скрытая сеть DarkNet. Доступ к этой сети возможен с помощью специального программного обеспечения. Анонимность членов этой сети защищена, и они обязаны осуществлять куплю-продажу посредством биткойна и других криптовалют [10].

На «черном рынке» корпоративные данные обычно более ценны, чем персональные. Поэтому преступники больше нацелены на персональные данные, которые собираются и хранятся на предприятиях и в организациях, что делает их более уязвимыми.

Киберпреступники сортируют и инвентаризируют любую незаконно изъятую информацию без разрешения владельца, прежде чем выпустить ее на рынок. Данным, которые считают ценными, они назначают более высокую цену. А то, что, по их мнению, менее ценно, они собирают и массово продают за небольшую плату.

Хакеры и посредники с «черного рынка» пытаются по возможности быстро провести процесс купли-продажи украденных персональных данных, потому что их владельцы стараются принять ответные меры, как только узнают о краже.

Если какие-либо персональные данные являются актуальными, надежными и полными, то они считаются ценным ресурсом для бизнеса. Персональные данные, обладающие всеми этими свойствами, пользуются большим спросом на «черном рынке». Однако, поскольку такого рода информация приобретается нелегальным путем, проверить ее невозможно.

На «черном рынке» персональных данных предлагаются следующие услуги [10]:

- местонахождение мобильного абонента в режиме реального времени;
- идентификация лиц, находящихся в зоне охвата мобильного абонента в режиме реального времени;
- список лиц, с которыми абонент общается по мобильному телефону и другая информация;
- информация о географическом местоположении, времени и траекториях движения человека;
- информация о личном имуществе человека, его банковских счетах и т. д.;
- персональные данные, собираемые на серверах провайдеров при использовании интернет-сервисов и т.д.

3. Почему персональные данные покупают на «черном рынке»?

На «черном рынке» персональные данные покупают для различных видов деятельности. Но в большинстве случаев конечная цель одна – получить прибыль. Есть разные способы незаконного заработка денег с помощью персональных данных. Рост количества компаний, специализирующихся на аналитике Big Data, разработке программного обеспечения для автоматизации маркетинговых процессов, быстро увеличивает спрос на персональные данные на «черном рынке». В цифровом маркетинге существует наибольший спрос на информацию, которая служит следующим целям [11]:

- повышение эффективности интернет-компаний;
- точный таргетинг рекламных кампаний;
- анализ профилей и интересов пользователей;
- разработка наилучших продуктов и услуг.

На основе анализа полученных персональных данных коммерческие компании определяют целевую аудиторию, применяют индивидуализированные, адресные рекламные технологии. Таким образом, когда люди используют различные поисковые системы, социальные сети, онлайн-сервисы в Интернете, собирается информация об их желаниях, потребностях, образе жизни, увлечениях, которая становятся очень полезной для рекламной и маркетинговой деятельности.

Одно из самых распространенных преступлений –– это кража финансовой информации чужих кредитных карт, банковских счетов и т. д. и присвоение их денег. Для получения такой информации используются различные технологии, характерные для физической и виртуальной среды.

В некоторых случаях персональные данные необходимы для создания и продажи поддельных документов. В других случаях – вымогают деньги, шантажируя людей после изъятия их персональных данных. Кроме того, криминальные группы, получив информацию о наличии у кого-то ценного имущества, пытаются заполучить его. Персональные данные также могут быть предметом политической борьбы. Так, политические оппоненты получив незаконным путем персональные данные другой стороны, могут использовать их для снижения ее политического престижа.

Персональные данные также могут использоваться иностранными спецслужбами в политических и идеологических целях. В этом случае персональные данные становятся объектом национальной безопасности.

4. Проблемы, создаваемые «черным рынком»

Формирование и развитие «черного рынка» персональных данных создают ряд проблем для государства, граждан, предприятий и организаций. Во-первых, персональные данные, попадающие на «черный рынок», приобретаются незаконным путем, преступными методами, с причинением вреда юридическим и физическим лицам. Во-вторых, во многих случаях персональные данные используются в злонамеренных целях.

Кража персональных данных может иметь ряд негативных последствий для их владельцев. Согласно опросу, 40% людей, чьи персональные данные были украдены, заявили, что не могут нормально спать по ночам, 65% испытывали чувство нервозности, 69% – чувство опасности и страха. 7% респондентов заявили, что почти дошли до самоубийства, 15% жертв кражи продали свои личные вещи для покрытия убытков, а 7% взяли для из-за этого ссуду [12].

Кража персональных данных наносит больший ущерб бизнесу. Факты показывают, что это постоянный риск для компаний и к подобным негативным ситуациям всегда нужно быть готовым. Для компаний, столкнувшихся с утечками данных, самая большая финансовая потеря – это потеря репутации. После таких случаев компании должны принять необходимые меры для восстановления доверия клиентов и снижения долгосрочных отрицательных финансовых последствий.

Большинство утечек данных – это результат кибератак. На расследование и выявление подобных инцидентов уходит много времени. Компании признают, что чем больше времени требуется на обнаружение и предотвращение утечек данных, тем дороже это стоит. Объем таких расходов растет с каждым годом. Для выявления и предотвращения подобных угроз необходимо использовать личный опыт и увеличивать инвестиции в технологии [4].

В усиленно регулируемых областях, таких как здравоохранение и финансовые услуги, утечка данных обходится дороже, потому что уровень и вероятность потери репутации и клиентов в результате подобных инцидентов в этих сферах выше.

Если персональные данные попадут в руки внешней разведки через «черный рынок», то могут возникнуть серьезные проблемы для национальной безопасности. Так, с помощью технологий Big Data можно проанализировать большой объем персональных данных, из которых можно извлечь различную полезную информацию, интересующую иностранные спецслужбы. Эта информация может отражать отношение, взгляды, подходы граждан к любому вопросу в любой стране или их материальное, моральное, психологическое состояние и состояние здоровья. Кроме того, эта информация может быть использована спецслужбами для совершения любых провокаций против страны.

Другой преступной целью получения персональных данных через «черный рынок» является использование их для вымогательства посредством шантажа и запугивания. В этом случае шантажируемые чиновники вынуждены подчиняться требованиям шантажиста из опасения нанести ущерб своей карьере и распада семейных отношений [6].

Заключение

Для эффективной борьбы с «черным рынком» персональных данных важно усовершенствовать соответствующее законодательство и усилить меры по борьбе с киберпреступностью.

С технологической точки зрения ответственность за решение важных задач ложится на учреждения, реализующие государственную политику по усилению защиты персональных данных, а также предприятия и организации, оказывающие различные услуги гражданам.

Сами граждане должны заботиться о своих персональных данных, правильно обращаться с ними, учитывать особенности виртуальной среды. Особое внимание следует уделить формированию у них культуры информационной безопасности.

Кроме того, чтобы эффективно использовать персональные данные для нужд Big Data, необходимо разработать и внедрить механизмы их анонимности.

В настоящее время функционирующие в этой сфере международные юридические органы обсуждают создание соответствующих юридических механизмов, позволяющих людям пользоваться своими персональными данными, получая при этом доход. Для этого, прежде всего, важно, чтобы каждый получил право на собственность своих персональных данных.

Незаконный доступ к персональным данным может стать серьезной угрозой национальной безопасности. Таким образом, защиту персональных данных следует рассматривать как неотъемлемую часть национальной безопасности.

Следует отметить, что большие данные, в которых персональные данные имеют особый вес, сравниваются с запасами нефти с точки зрения их стратегической важности и преимуществ. Следовательно, необходимо сделать так, чтобы и права людей на неприкосновенность частной жизни, и национальная безопасность были обеспечены на высоком уровне, а также чтобы была возможность использовать персональные данные в полезных целях.

Литература

1. UNCTAD. Digital Economy Report (2019), United Nations, 2019, 194 p.
2. Alguliyev R., Mahmudov R. Sensitivity of personal data in the context of national mentality and issues of ensuring their security // Problems of Information Society, 2019, № 2, pp. 117-128.
3. Samuelson P. Privacy as intellectual property? // Stanford Law Review, 2000, pp. 1125–1173.
4. Nuncic M. The Black Market for Data. https://www.ontrack.com (дата обращения: 15.09.2020).
5. Fontinelle A. How Black Markets Work. 2019. https://www.investopedia.com (дата обращения: 23.09.2020).
6. Alguliyev R., Mahmudov R., The place of personal data in the national mentality and the problems of their protection / V Republican Conference "Actual multidisciplinary scientific-practical problems of information security", Baku, November 29, 2019, pp. 21-24.
7. Красотенко О. Понятие «частная жизнь» в решениях Европейского Суда по правам человека / Сборник тезисов 68-й научно-практической конференции студентов, магистрантов и аспирантов факультета международных отношений БГУ. Минск, 27 апреля 2011, с. 51-53.
8. Dayman D. CCPA Sell Definition, 29 September, 2020. https://www.osano.com/articles/ccpa-definition-sell (дата обращения: 18.09.2020).
9. Oxford English Dictionary. https://www.oxfordlearnersdictionaries.com (дата обращения: 10.11.2020).
10. Armor. The Black Market Report, 2018, 16 p.
11. Spiekermann S., Böhme R., The challenges of personal data markets and privacy // Electronic Markets, June 2015, https://www.eprofing.springer.com/journals/printpage (дата обращения: 06.10.2020).
12. Cook G. How Much Is My Identity Worth on the Black Market? https://www.findreviews.com (дата обращения: 08.10.2020).

FEATURES OF THE "BLACK MARKET" OF PERSONAL DATA AND THE PROBLEMS CREATED BY THEM

Aliguliyev, Rasim M.

Doctor of technical sciences, professor
Institute of Information Technologies of ANAS
Baku, Azerbaijan
r.alguliev@gmail.com

Mahmudov, Rasim Sh.

Institute of Information Technologies of ANAS
Baku, Azerbaijan
rasimmahmudov@gmail.com

Abstract

The article examines the essence and features of the "black market" of personal data. The types of information and services, technologies and their pricing policy, as well as the purposes for which personal data purchased on the black market are used, are considered. In addition, the problems associated with the illegal acquisition and sale of personal data from the point of view of personal, corporate and national interests were noted.

Keywords

personal life, personal data; "black market" of personal data; the cost of personal data; theft of personal data

References

1. UNCTAD. Digital Economy Report (2019), United Nations, 2019, 194 p.
2. Alguliyev R., Mahmudov R. Sensitivity of personal data in the context of national mentality and issues of ensuring their security // Problems of Information Society, 2019, № 2, pp. 117-128.
3. Samuelson P. Privacy as intellectual property? // Stanford Law Review, 2000, pp. 1125–1173.
4. Nuncic M. The Black Market for Data. https://www.ontrack.com (accessed: 15.09.2020).
5. Fontinelle A. How Black Markets Work. 2019, https://www.investopedia.com (accessed: 23.09.2020).
6. Alguliyev R., Mahmudov R., The place of personal data in the national mentality and the problems of their protection / V Republican Conference "Actual multidisciplinary scientific-practical problems of information security", Baku, November 29, 2019, pp. 21-24.
7. Krasotenko O. Ponyatiye "chastnaya zhizn" v resheniyakh Evropeyskogo Suda po pravam cheloveka / Sbornik tezisov 68-y nauchno-prakticheskoy konferentsii studentov, magistrantov i aspirantov fakulteta mezhdunarodnykh otnosheniy BGU. Minsk. 27 aprelya 2011. s. 51-53.
8. Dayman D. CCPA Sell Definition, 29 September, 2020, https://www.osano.com/articles/ccpa-definition-sell (accessed: 18.09.2020).
9. Oxford English Dictionary, https://www.oxfordlearnersdictionaries.com (accessed: 10.11.2020).
10. Armor. The Black Market Report, 2018, 16 p.
11. Spiekermann S., Böhme R., The challenges of personal data markets and privacy // Electronic Markets, June 2015, https://www.eprofing.springer.com/journals/printpage (accessed: 06.10.2020).
12. Cook G. How Much Is My Identity Worth on the Black Market? https://www.findreviews.com (accessed: 08.10.2020).