ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭКОНОМИЧЕСКОГО ИНТЕРНЕТ-СЛЕДА ЛИЧНОСТИ

Красильников Олег Юрьевич

доктор экономических наук, профессор, профессор кафедры экономической теории и национальной экономики ФГБОУ ВО «Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского» (Саратов, Россия)

e-mail: ok-russia@yandex.ru[1]

Аннотация. *В статье рассматриваются проблемы обеспечения безопасности экономической информации частных лиц в Интернете. Исследованы понятие и формы экономического интернет-следа личности. Проанализировано противоречие между формальными институтами обеспечения экономической кибербезопасности и неформальными институтами виртуального мошенничества, а также представлены способы его разрешения: ужесточение контроля и гармонизация взаимодействия экономических агентов. В условиях слабости современных институтов защиты экономической информации частных лиц в Интернете предлагается разработать государственную стратегию повышения безопасности ее использования.*

Ключевые слова: *интернет-след; кибермошенничество; кибербезопасность; формальные и неформальные институты; финансовая грамотность; Россия.*

Для цитирования: Красильников О.Ю. Обеспечение безопасности экономического интернет-следа личности // Социальные новации и социальные науки: [электронный журнал]. – 2022. – № 1. – С. 161–170.

URL: https://sns-journal.ru/ru/archive/ DOI: 10.31249/snsn/2022.01.14

Рукопись поступила 11.01.2022.

Введение

Расширение использования информационно-коммуникационных технологий (ИКТ), в первую очередь Интернета, приводит к тому, что большинство людей вольно или невольно оставляют значимый информационный след во Всемирной паутине (социальных сетях, поисковых, почтовых и других серверах) в виде аватаров, аккаунтов, личных страниц и кабинетов на сайтах банков, онлайн-магазинов, маркетплейсов, агрегаторов и т.п.

На конференции, посвященной искусственному интеллекту «Artificial Intelligence Journey 2021», Президент РФ В.В. Путин заявил: «Государство должно взять на себя ответственность за хранение критически важной информации. Речь идет не только об обеспечении кибербезопасности самого человека, но и его виртуального двойника – аватара внутри формирующихся метавселенных» [Путин заявил …, 2021]. При использовании киберпространства всё чаще возникают вопросы о защите личных данных и цифровых платежей, противодействии манипуляциям потребительскими предпочтениями, интересами и поступками граждан.

Криминальное использование цифрового следа личности в Интернете

Многие действия людей в Интернете сопровождаются возникновением «экономического следа», связанного с движением денежных средств, товаров и услуг. Экономический интернет-след личности может существовать в различных формах:

– в виде личных кабинетов и электронных кошельков на сайтах банков, страховых и инвестиционных компаний, трейдеров и других финансовых организаций;

– в виде кабинетов и аккаунтов на сайтах интернет-магазинов, маркетплейсов, транспортных агрегаторов, компаний по продаже пассажирских и зрительских билетов;

– в качестве данных о денежных переводах и платежах по банковским картам, покупкам, выдаче и погашению кредитов, заказам транспортных средств;

– как информация о сделках купли-продажи иностранной валюты, кибервалюты и ценных бумаг;

– в качестве данных о благотворительных пожертвованиях, спонсорских перечислениях, выигрышах в виртуальных лотереях и казино, роялти, выплатах за рекламу;

– как информация о потребительских предпочтениях индивидов.

Возможность манипулирования этими сведениями создает потенциальный риск утраты материальных и нематериальных ценностей. Закономерно, что по мере расширения использования

цифровых технологий в последние годы участились случаи так называемого кибермошенничества, начиная с хакерских атак и заканчивая банальным воровством денег с банковских карт с помощью телефонного обзвона широкого круга вероятных жертв.

В период пандемии коронавируса актуальность обеспечения безопасности экономического интернет-следа личности значительно возросла, так как увеличился уровень киберугроз. В 2020 г. количество киберинцидентов выросло на 51% по сравнению с предыдущим годом. При этом в общем количестве кибератак 69% приходилось на частных лиц. Основными мотивами злоумышленников были получение данных и финансовая выгода. Среди сведений, украденных у частных лиц, на первом месте стояли учетные системные данные (36%). Далее идут: персональные данные (19%), данные платежных карт (19%), личная переписка (12%) и другая информация (14%) [Актуальные киберугрозы …, 2021].

В общем количестве кибератак на частных лиц лидируют такие способы мошенничества, как создание фишинговых сайтов (32%), поддельных мобильных приложений (15%), а также распространение вредоносного контента посредством электронной почты (32%), мессенджеров и SMS-сообщений (7%). В период пандемии в США и странах Евросоюза участились хакерские атаки на медучреждения, что негативно отразилось не только на финансовом положении, но и на физическом здоровье населения. Зачастую сотрудники больниц не могли получить доступ к результатам анализов пациентов и ранее сделанным назначениям, к заблокированным данным с диагностических приборов, а также оказать неотложную медицинскую помощь, поскольку все необходимые сведения хранились в электронном виде и оказались зашифрованы в результате кибератак [Актуальные киберугрозы …, 2021]. Попавшие в институциональную ловушку недофинансирования российские медицинские учреждения характеризуются низкой степенью компьютеризации, и в этом смысле они более устойчивы к хакерским кибератакам.

В России, по статистике МВД, за семь месяцев 2021 г. произошло почти 320 тыс. киберпреступлений. Это на 16% больше, чем за тот же период предыдущего года. Около 127 тыс. преступлений совершены с использованием мобильной связи, 104 тыс. – с применением банковских карт. При этом, согласно данным Генеральной прокуратуры, в стране раскрывается меньше 25% киберпреступлений [Число киберпреступлений, 2021]. Согласно другим оценкам, только за третий квартал 2021 г. мошенники похитили у клиентов кредитно-финансовых организаций путем несанкционированных денежных переводов почти 3,2 млрд руб. При этом банки вернули клиентам только 7,7% похищенных средств, или менее 250 млн руб. [Чернышова, 2021].

Подобные негативные тенденции тесно связаны с цифровизацией общественных отношений, а также с такими особенностями киберпространства, как доступность информации, охват широкой аудитории, анонимность и трансграничный характер. Игнорирование этих аспектов внедрения

цифровых технологий создает реальную угрозу как безопасности личности, так и национальной безопасности.

Противоречие правовых и противоправных институтов в Интернете

На наш взгляд, в России и других странах мира уже сформировались специфические структуры, специализирующиеся на преступлениях в киберпространстве (например, Anonymous). Они обладают некоторым набором неформальных норм и правил, что говорит об определенной институционализации виртуального мошенничества. Разработанные схемы позволяют кибермошенникам незаконно проникать в защищенные информационные системы и использовать их в целях обогащения. Кроме того, они включают электронные и вербальные информационно-коммуникативные методики обмана потенциальных жертв.

В свою очередь им противостоят институты обеспечения кибербезопасности. Это формальные нормы и правила, закрепленные на законодательном или корпоративном уровне, препятствующие виртуальному мошенничеству. Сюда же можно отнести институты формирования финансовой грамотности населения страны.

Между формальными институтами обеспечения экономической кибербезопасности и неформальными институтами виртуального мошенничества возникает объективное противоречие [Красильников, 2002, с. 22]. Данное противоречие может разрешаться как минимум двумя способами:

1) с помощью ужесточения контроля со стороны государства, банковского и предпринимательского сообщества;

2) на основе гармонизации взаимодействия экономических агентов (см. рис. 1).

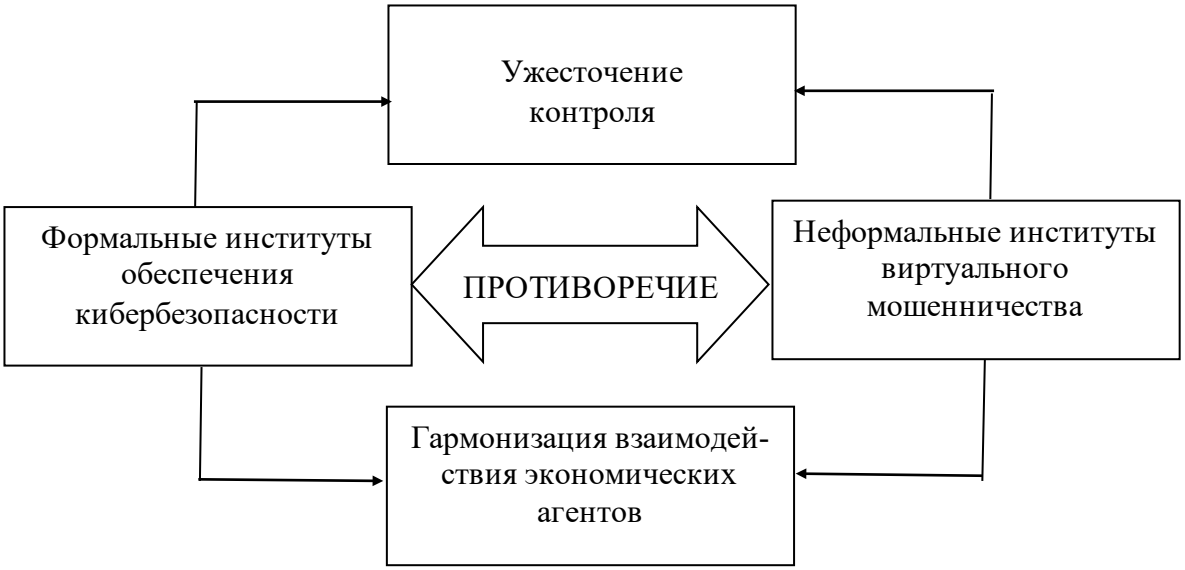

Рис. 1. Институциональное противоречие формальных институтов обеспечения экономической кибербезопасности и неформальных институтов виртуального мошенничества и способы его разрешения (составлено автором)

Рассмотрим указанные способы разрешения противоречия с применением теории транзакционных издержек, к которым, несомненно, относятся затраты на обеспечение экономической безопасности, с одной стороны, и на осуществление мошеннической деятельности – с другой.

Экономические издержки вне легальности заведомо меньше, чем затраты на безопасность. Функционирование неформальных институтов виртуального жульничества не требует регистрации, лицензирования, содержания большого числа штатных работников, уплаты налогов и социальных взносов. В условиях слабого контроля со стороны государства и хозяйствующих субъектов количество случаев кибермошенничества будет постоянно расти.

Введенные в период пандемии коронавируса карантинные ограничения увеличили объемы онлайн-заказов – от доставки еды из ресторанов, продуктов из супермаркетов до одежды и техники. Кибермошенники всё чаще стали подделывать порталы курьерской доставки. Кроме того, появились ресурсы, которые предлагали материальную помощь малому бизнесу, потребительские кредиты и займы гражданам – а на самом деле выманивали данные и средства пользователей. Что наиболее возмутительно, возникли даже сайты-клоны различных благотворительных фондов по оказанию материальной помощи больным детям и пенсионерам.

По оценкам аналитиков авторитетной консалтинговой компании «Deloitte» (США), сегодня в мире среднемесячные затраты на самые простые средства взлома составляют порядка 34 долл., тогда как доход от них превышает 25 тыс. долл. ежемесячно. При этом усредненные расходы на обеспечение кибербезопасности на одного штатного сотрудника в 2020 г. банки оценили в 2,7 тыс. долл. в год [Как зарабатывают …, 2020]. Как видно, огромный разрыв в транзакционных издержках предопределяет необходимость многократного увеличения затрат на информационную безопасность.

Однако рост подобных затрат неизбежно снижает эффективность бизнеса. Но еще большие потери предприниматели могут понести, возмещая убытки по искам со стороны недовольных или обманутых клиентов. Поэтому представители бизнеса вынуждены решать нелегкую задачу минимизации своих транзакционных издержек как со стороны обеспечения информационной безопасности, так и со стороны возмещения вреда клиентам, пострадавшим от действий кибермошенников.

Важную роль в данном вопросе должно играть государство, особенно в области защиты личных сведений о человеке. Согласно исследованию группы компаний «InfoWatch», только за 2020 г. в России количество утечек персональных данных в финансовом сегменте Интернета выросло на 36,5% (с 52 до 71 млн случаев) [Греков, Баязитова, 2021].

Определенные шаги со стороны государства в направлении обеспечения кибербезопасности уже сделаны. В 2006 г. принят Федеральный закон РФ «О персональных данных», в 2011 г. – Закон «Об электронной подписи». В 2020 г. в законодательстве урегулированы вопросы использова-

ния Единой биометрической системы (ЕБС), оператором которой является ПАО «Ростелеком». ЕБС позволяет идентифицировать человека по отпечатку пальца, голосу или посредством распознавания лица. С ее помощью можно взять кредит, открыть банковский счет, снять наличные в банкомате или дистанционно подписать финансовые документы. Не за горами создание единой государственной базы данных, объединяющей физические параметры человека и его виртуального двойника.

Как показывают данные социологического опроса, проведенного Аналитическим центром Национального агентства финансовых исследований (НАФИ), 52% россиян знают о существовании ЕБС, но только 19% уже сдавали свои данные, а из остальных сдавать данные готов только каждый пятый [Большинство россиян …, 2021].

Гораздо более эффективным способом, на наш взгляд, является организация действенного контроля за экономическими транзакциями в Интернете со стороны соответствующих государственных органов, в первую очередь МВД и Роскомнадзора. Так, наряду со специальным управлением «К», существующим в структуре МВД и занимающимся компьютерной безопасностью, объявлено о создании специальных подразделений киберполиции во всех регионах страны [Число киберпреступлений …, 2021].

Значительную роль в обеспечении экономической безопасности граждан в Интернете играет Роскомнадзор. Одним из основных направлений его деятельности является выявление так называемых фишинговых сайтов (сайтов-клонов), которые создают и используют кибермошенники, чтобы выманивать у пользователей данные их онлайн-кабинетов в финансовых организациях, реквизиты банковских карт и счетов, а также другие персональные сведения. Только за первые девять месяцев 2020 г. было обнаружено 14,8 тыс. таких сайтов, и их число постоянно увеличивается [Шестакова, 2021].

Представляется, что функционал и полномочия перечисленных контролирующих органов могут быть существенным образом усовершенствованы.

Как было указано ранее, вторым способом разрешения противоречия формальных институтов обеспечения экономической кибербезопасности и неформальных институтов виртуального мошенничества является гармонизация взаимодействия субъектов хозяйственных отношений. В случае, когда транзакционные издержки подготовки и осуществления кибермошенничества значительно превышают выгоду от его реализации, исчезает интерес в осуществлении киберпреступлений.

Из теории известно, что формальные институты изменяются дискретно, тогда как неформальные постоянно эволюционируют. Поэтому желательным ходом развития событий является периодическое обновление способов и норм формального взаимодействия хозяйствующих субъектов, защищающих от различных виртуальных киберпреступников.

Можно выделить несколько форм подобной институциональной координации рыночных отношений:

1. Введение так называемого периода охлаждения при осуществлении финансовых операций. Так, ЦБ РФ планирует дать банкам право списывать деньги по подозрительным транзакциям по истечении одного-двух рабочих дней, даже несмотря на согласие клиента. Банк России также предполагает наделить финансовые организации правом блокировать на пять рабочих дней все расходные операции по счету получателя средств, информация о котором содержится в базе данных (ее ведет сам ЦБ) при попытках осуществления переводов денежных средств без согласия клиента [Чернышова, 2021]. Подобные нововведения должны заметно снизить интерес к осуществлению мошеннических действий. Однако это может привести к значительным затруднениям для самих экономических субъектов, например, при осуществлении быстрых платежей.

2. Определение минимальной суммы, после которой транзакция подлежит обязательному контролю со стороны финансовых структур и надзорных органов. Сейчас в соответствии с Федеральным законом от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» подобная сумма определена в размере 600 тыс. руб. В связи с участившимися случаями кибермошенничества существует необходимость скорректировать эту сумму в сторону понижения.

3. Установление величины денежных средств, которую банки должны возвращать в упрощенном и безусловном порядке клиентам – физическим лицам, ставшим жертвами кибермошенников. Предполагается, что для этого гражданин должен уведомить банк о мошенничестве не позднее следующего дня после получения информации от банка о проведенной операции. Одновременно ЦБ РФ предлагает изменить процедуру подтверждения банками операций, имеющих признаки мошеннических транзакций [Чернышова, 2021].

4. Совершенствование способов осуществления финансовых операций, в частности внедрение технологии блокчейн. Применение метода построения цепочки взаимосвязанных блоков информации особенно актуально в тех случаях, когда у контрагентов нет полного доверия друг к другу и существует большая вероятность оппортунистического поведения сторон. Как известно, под оппортунизмом в экономике понимается поведение субъектов транзакции, не связанное с соображениями морали, к которому, несомненно, относится кибермошенничество[1] [Красильников, 2002, с. 12].

5. Повышение финансовой грамотности населения, особенно его наиболее уязвимой части – людей преклонного возраста. Финансовая грамотность предполагает наличие базового набора

[1] Как известно, под оппортунизмом в экономике понимается такое поведение субъектов транзакции, которое не ограничено соображениями морали и противоречит интересам других агентов. К ним, несомненно, относится кибермошенничество.

знаний, навыков и компетенций, позволяющего индивиду принимать разумные экономические решения и осуществлять действия в целях достижения личного материального благополучия.

Финансовая грамотность предполагает наличие базового набора знаний, навыков и компетенций, позволяющего индивиду принимать разумные экономические решения и осуществлять действия в целях достижения личного материального благополучия. В последнее время данному вопросу уделяется повышенное внимание.

В 2017 г. Правительством РФ была принята «Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 годы» [Стратегия …, 2017]. Целями, которые должны быть достигнуты в результате ее реализации, являются: знание граждан о рисках на финансовом рынке, способность распознавать признаки финансового мошенничества, умение отстаивать свои законные права как потребителя финансовых услуг.

В рамках стратегии выделяются следующие группы населения:

– склонные к рискованному типу финансового поведения в сложных жизненных обстоятельствах;

– испытывающие трудности при реализации своих прав на финансовое образование и их защиту, а именно: граждане пенсионного и предпенсионного возраста, а также лица с ограниченными возможностями здоровья;

– учащиеся образовательных организаций, учреждений профессионального образования и высших учебных заведений.

Основными факторами риска стать жертвами киберпреступления, характерными для указанных категорий граждан, служат:

– низкие доходы и отсутствие коммерческой собственности, когда индивиду по существу нечего терять при осуществлении надежды приобрести большее;

– патерналистские привычки, отсутствие навыков ответственного финансового поведения;

– высокий уровень психологической внушаемости.

Если в образовательных учреждениях повсеместно вводятся обязательные курсы по основам финансовой грамотности, то две первые группы населения остаются наиболее уязвимыми с точки зрения осуществления кибермошенничества.

Заключение

Можно констатировать слабость современных государственных и рыночных институтов защиты экономического интернет-следа личности. Данный факт объясняется опережающим прогрессом ИКТ, появлением все более совершенных гаджетов и новых приложений. Государственные органы не успевают, а рынок не спешит реагировать на имеющие место изменения. Это происходит из-за слабой мотивированности чиновничьего аппарата и низкой заинтересованности

рыночных структур в мероприятиях, не предполагающих получение прибыли. Судебные институты также не готовы к интерпретации и рассмотрению не закрепленных в законодательной базе и правоприменительной практике новых видов киберпреступлений.

В сложившейся ситуации индивид, по существу, остается один на один с кибермошенниками. Согласно постулату «защити себя сам», частному лицу необходимо повышать бдительность и финансовую грамотность, пользоваться антивирусными программами, критически оценивать соблазнительные финансовые предложения, чаще менять пароли к банковским кабинетам и т.д.

В то же время значимость вопросов безопасности экономической информации в Интернете для общества требует действий со стороны государства по ее обеспечению. Представляется, что в рамках национального проекта развития цифровой экономики в России необходимо разработать комплексную стратегию защиты экономического интернет-следа личности. Важная роль в данном направлении должна принадлежать научному сообществу, представителям которого следует теоретически осмыслить, оценить и обосновать практические шаги по обеспечению кибербезопасности граждан.

Список литературы

1. Актуальные киберугрозы: итоги 2020 г. // Positive Technologies. – 2021. – 28.04. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/?sphrase_id=98052 (дата обращения: 14.02.2022).
2. Большинство россиян скептически настроены к идее сдачи биометрических данных для ЕБС // PIKABU. – 2021. – 20.04. – URL: https://pikabu.ru/story/bolshinstvo_rossiyan_skepticheski_nastroenyi_k_idee_sdachi_biometricheskikh_dannyikh_dlya_ebs_8155118 (дата обращения: 14.02.2022).
3. Как зарабатывают киберпреступники: дипфейк-боссы и цифровое вымогательство // ХАЙТЕК. – 2020. – 30.10. – URL: https://hightech.fm/2020/10/30/deep-fake-fishing (дата обращения: 14.02.2022).
4. Красильников О.Ю. Неоинституциональная экономика. – Саратов : Изд-во Сарат. ун-та, 2002. – 104 с.
5. Чернышова Е. Мошеннические переводы ложатся на банковские плечи // РБК. – 2021. – 06.12. – URL: https://www.rbc.ru/newspaper/2021/12/06/61a8d4639a79476b808c4eee (дата обращения: 14.02.2022).
6. Путин заявил о долге властей защищать аватары россиян в метавселенных // РБК. – 2021. – 12.11. – URL: https://www.rbc.ru/technology_and_media/14/02/2022/6208c2f49a79470c3f893bae (дата обращения: 14.02.2022).
7. Шестакова К. Роскомнадзор намерен блокировать фишинговые сайты // Infostart.ru. – 2021. – 27.01. – URL: https://infostart.ru/journal/news/uchet-nalogi-pravo/roskomnadzor-nameren-blokirovat-fishingovye-sayty_1370292/ (дата обращения: 14.02.2022).
8. Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 гг. : распоряжение Правительства РФ от 25.09.2017 № 2039-р // КонсультантПлюс. – 2017. – URL: http://www.consultant.ru/document/cons_doc_LAW_278903/ (дата обращения: 14.02.2022).
9. Число киберпреступлений в России // Tadviser. – 2021. – 19.11. – URL: https://www.tadviser.ru/index.php/ (дата обращения: 14.02.2022).
10. Греков М., Баязитова А. Хакеры не нужны: как в Сбере воровали персональные данные на продажу // LIFE. – 2021. – 12.03. – URL: https://life.ru/p/1384457 (дата обращения: 14.02.2022).

ENSURING THE SECURITY OF THE ECONOMIC INTERNET PERSONALITY TRACE

Oleg Krasilnikov

Drs (Econ. Sci.), professor, Professor of the Department of Economic Theory and National Economics, Saratov National Research State University named after N.G. Chernyshevsky (Saratov, Russia)

Abstract. *The article deals with the problems of ensuring the security of economic information of individuals on the Internet. The concept and forms of the economic Internet trace of the individual are*

investigated. The contradiction between formal institutions of economic cybersecurity and informal institutions of virtual fraud is analyzed, and the ways of its resolution are presented: tightening control and harmonization of harmonious interaction of economic agents. Given the weakness of modern institutions for the protection of economic information of individuals on the Internet, it is proposed to develop a state strategy to improve the security of its use.

Keywords: *internet trace; cyberbullying; cybersecurity; formal and informal institutions; financial competence; Russia.*

For citation: Krasilnikov O.Yu. Ensuring the security of the economic internet personality trace // Social Novelties and Social Sciences : [electronic journal]. – 2022. – № 1. – Pp. 161–170.

URL: https://sns-journal.ru/ru/archive/ DOI: 10.31249/snsn/2022.01.14