Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2022. Т. 22, вып. 2. С. 152–159
Izvestiya of Saratov University. Economics. Management. Law, 2022, vol. 22, iss. 2, pp. 152–159
https://eup.sgu.ru https://doi.org/10.18500/1994-2540-2022-22-2-152-159

Научная статья
УДК 004.738.5+004.62+343.7

Проблемы обеспечения безопасности экономического следа личности в интернете

О. Ю. Красильников

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, Россия, 410012, г. Саратов, ул. Астраханская, д. 83

Красильников Олег Юрьевич, доктор экономических наук, профессор кафедры экономической теории и национальной экономики, ok-russia@yandex.ru, https://orcid.org/0000-0002-2211-4370

Аннотация. ***Введение.*** В статье рассматриваются проблемы обеспечения безопасности экономической информации частных лиц в интернете. Исследованы понятие и формы экономического интернет-следа личности. ***Теоретический анализ.*** Мошеннические действия в виртуальной среде, направленные против частных лиц, занимают значительную долю от общего количества киберпреступлений. Основным мотивом правонарушений является получение финансовой выгоды, а методом – распространение и использование вредоносного программного обеспечения. Проанализировано противоречие формальных институтов обеспечения экономической кибербезопасности и неформальных институтов виртуального мошенничества, а также представлены способы его разрешения: ужесточение контроля и организация гармоничного взаимодействия экономических агентов. Исследованы формы институциональной координации субъектов на основе рыночных отношений: введение периода охлаждения при осуществлении финансовых операций; определение минимального объема средств, после которого транзакция подлежит обязательному контролю со стороны финансовых структур и надзорных органов; установление суммы денежных средств, которую банки должны возвращать в упрощенном и безусловном порядке клиентам – физическим лицам, ставшим жертвами кибермошенников; внедрение технологии блокчейн. Особое внимание уделено вопросу формирования финансовой грамотности населения. Отмечено увеличение случаев кибермошенничества в период пандемии коронавируса. ***Результаты.*** Делается вывод о слабости государственных и рыночных институтов защиты экономического интернет-следа личности. Предлагается разработать соответствующую государственную стратегию повышения безопасности использования экономической информации частных лиц в интернете.

Ключевые слова: интернет-след, кибермошенничество, кибербезопасность, формальные и неформальные институты, противоречие, финансовая грамотность

Для цитирования: *Красильников О. Ю.* Проблемы обеспечения безопасности экономического следа личности в интернете // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2022. Т. 22, вып. 2. С. 152–159. https://doi.org/10.18500/1994-2540-2022-22-2-152-159

Article

Problems of ensuring the security of an individual's economic trace on the Internet

O. Yu. Krasilnikov

Saratov State University, 83 Astrakhanskaya St., Saratov 410012, Russia

Oleg Yu. Krasilnikov, ok-russia@yandex.ru, https://orcid.org/0000-0002-2211-4370

Abstract. ***Introduction.*** 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. ***Theoretical analysis.*** Fraudulent actions in a virtual environment directed against individuals account for a significant proportion of the total number of cybercrimes. The main motive of the offenses is to obtain financial benefits, and the method is the distribution and use of malicious software. 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 organization of harmonious interaction of economic agents. The forms of institutional coordination of subjects on the basis of market relations are investigated: the introduction of a cooling-off period during financial transactions; the determination of the minimum amount of funds after which the transaction is subject to mandatory control by financial structures and supervisory authorities; the establishment of the amount of funds that banks must return in a simplified and unconditional manner to customers – individuals who have become victims of cybercriminals; the introduction of blockchain technology. Special attention is paid to the formation of financial literacy of the population. The author notes an increase in cases of cyberbullying during the coronavirus pandemic. ***Results.*** The conclusion is made

about the weakness of state and market institutions to protect the economic Internet trace of the individual. It is proposed to develop an appropriate state strategy to improve the security of the individuals' economic information use on the Internet.

Keywords: internet trace, cyberbullying, cybersecurity, formal and informal institutions, contradiction, financial competence

For citation: Krasilnikov O. Yu. Problems of ensuring the security of an individual's economic trace on the Internet. *Izvestiya of Saratov University. Economics. Management. Law*, 2022, vol. 22, iss. 2, pp. 152–159 (in Russian). https://doi.org/10.18500/1994-2540-2022-22-2-152-159

Введение

Развитие информационно-коммуникационных технологий (ИКТ), в первую очередь интернет, 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 «Artificial Intelligence Journey 2021», посвященной искусственному интеллекту, президент РФ В. В. Путин заявил: «Государство должно взять на себя ответственность за хранение критически важной информации. Речь уже идет не о том, чтобы обеспечить кибербезопасность самого человека, но и его виртуального двойника – аватара внутри формирующихся метавселенных» [1]. При использовании киберпространства все чаще возникают вопросы о защите личных данных и цифровых платежей, противодействии манипуляциям с потребительскими предпочтениями, интересами и поступками граждан.

Нас, прежде всего, интересует экономический интернет-след личности, который 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;

– данные, содержащие информацию о денежных переводах и платежах по банковским картам, товарным покупкам, выдаче и погашению кредитов, заказам транспортных средств;

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

– данные, содержащие информацию о благотворительных пожертвованиях, спонсорских перечислениях, выигрышах в виртуальных лотереях и казино, роялти, выплатах за рекламу;

– информация о потребительских предпочтениях индивидов.

Теоретический анализ

Многие действия людей в интернете сопровождаются экономическим следом, связанным с движением денежных средств, товаров и услуг. Поэтому они содержат потенциальный риск утраты материальных и нематериальных ценностей. Не случайно в последнее время 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.

По статистике МВД России, 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, по данным Генеральной прокуратуры, в России раскрывается меньше 25% киберпреступлений [2]. 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 меньше 250 млн руб. [3].

Как следует из приведенной ниже таблицы, мошеннические действия в виртуальной среде, направленные против частных лиц, занимают значительную долю от общего количества киберпреступлений. При этом, даже если кибератаки нацелены на те или иные учреждения или предприятия, в значительной степени они касаются конкретных людей, руководителей или работников данных организаций. Основным мотивом киберпреступлений является получение финансовой выгоды, а методом – распространение и использование вредоносного программного обеспечения (ВПО).

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. Все это создает реальную угрозу национальной безопасности страны.

Распределение киберинцидентов по мотивам, методам, объектам и сферам атак в 2020 г. (единиц) [4]
Table. **Distribution of cyber incidents by motives, methods, objects and spheres in 2020 (units) [4]**

Распределение киберинцидентов		Госучреждения	Финансовые организации	Промышленность	Медицинские учреждения	IT-компании	Наука и образование	Торговля	Другие	Без привязки к отрасли	Частные лица
Всего атак		359	126	239	178	115	128	124	417	260	325
Объект	Компьютеры, серверы и сетевое оборудование	290	103	220	144	94	92	63	278	171	116
	Веб-ресурсы	51	12	8	14	11	16	60	102	37	19
	Люди	230	77	178	118	51	82	40	152	144	225
	Мобильные устройства	2	–	–	–	–	–	–	4	2	79
	IoT-устройства	–	–	1	–	–	–	–	–	8	4
	Другие	5	4	–	–		7	3	20		9
Метод	Использование ВПО	255	82	212	121	75	78	52	204	156	191
	Социальная инженерия	230	77	178	118	51	82	40	152	144	225
	Подбор учетных данных	10	5	3	17	5	9	6	29	23	18
	Хакинг	71	27	50	38	44	24	24	131	60	23
	Эксплуатация веб-уязвимостей	34	5	6	6	2	11	50	77	25	4
	Другие	23	13	7	4	13	9	4	33	8	8
Мотив	Получение данных	103	48	87	101	49	67	27	172	72	98
	Финансовая выгода	210	89	200	112	77	56	111	241	160	234
	Хактивизм	58	10	7	9	17	26	5	59	29	22
	Кибервойна	5	1	–	1	1	3	–	6	20	3
	Неизвестен	11	–	4	2	–	2	–	10	3	–

На наш взгляд, в экономике России и других государств вполне сформировались специфические институты виртуального мошенничества. Они включают в себя набор неформальных норм и правил, позволяющих кибермошенникам незаконно проникать в защищенные информационные системы и использовать их в целях обогащения. Кроме того, сюда же относятся 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.

Таким образом, складывается объективное противоречие формальных институтов обеспечения экономической кибербезопасности и неформальных институтов виртуального мошенничества [5, с. 22]. Данное противоречие может разрешаться как минимум двумя основными способами:

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

2) на основе гармоничного рыночного взаимодействия экономических агентов (рис. 1).

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. При этом издержки внелегальности будут заведомо меньше, чем затраты на безопасность. Действительно, функционирование неформальных институтов виртуального жульничества не тре-

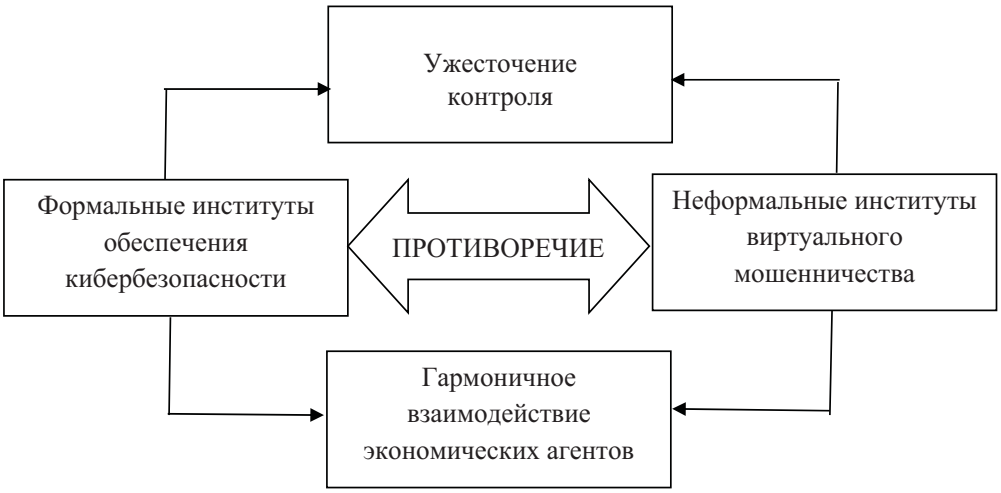

Рис. 1. Институциональное противоречие экономического интернет-следа личности и способы его разрешения

Fig. 1. Institutional Contradiction of an Individual's Economic Internet Trace and ways to resolve it

бует регистрации, лицензирования, содержания большого числа штатных работников, уплаты налогов и социальных взносов.

Так, по оценкам аналитиков авторитетной консалтинговой компании «Deloitte» (США), сегодня в мире среднемесячные затраты на самые простые средства взлома составляют порядка 34 долл. США, 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. США в год [6]. При таком разрыве в транзакционных издержках необходимо многократно увеличить затраты на обеспечение информационной безопасности.

Однако рост подобных затрат неизбежно будет снижать эффективность бизнеса. Но еще бо́льшие потери предприниматели могут понести, возмещая убытки по искам со стороны недовольных или обманутых клиентов. Поэтому представители бизнеса также должны будут решать нелегкую задачу оптимизации 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 деле 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) [7].

Определенные шаги со стороны государства в деле 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 законодательство внесены поправки об использовании 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 [8].

Поэтому гораздо более эффективным, на наш взгляд, является организация действенного контроля за экономическими транзакциями в интернете со стороны соответствующих государственных органов, в первую очередь МВД, ФСБ и Роскомнадзора. Так, наряду со специальным управлением «К», существующим в структуре МВД и занимающимся компьютерной безопасностью, объявлено о создании особых подразделений киберполиции во всех регионах страны [2]. В качестве примера успешной борьбы с киберпреступниками можно привести задержание в январе 2022 г. ФСБ России членов организованной хакерской группировки «REvil»

после соответствующего обращения спецслужб США. Объектами кибератак хакеров в основном были крупные иностранные компании, однако члены преступной группы не гнушались и вымогательством, а также воровством денежных средств со счетов иностранных граждан. Сотни американских компаний и знаменитостей пострадали от действий киберпреступников, в частности бывший президент США Д. Трамп, у которого злоумышленники вымогали деньги за неразглашение компроментирующей информации [9].

Значительную роль в обеспечении экономической безопасности граждан в интернете играет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Так, одним из направлений подобной деятельности является выявление так называемых фишинговых сайтов (по-другому – сайтов-клонов), которые создают и используют кибермошенники, чтобы выманивать у пользователей данные онлайн-кабинетов финансовых организаций, 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 [10].

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

Как было указано ранее, вторым способом разрешения институционального противоречия экономического интернет-следа личности является гармоничное рыночное взаимодействие субъектов хозяйственных отношений, когда исчезает сам интерес к осуществлению киберпреступлений. В этом случае транзакционные издержки подготовки и осуществления кибермошенничества значительно превышают выгоду от его реализации. Из теории известно, что формальные институты изменяются дискретно на основе постоянной эволюции неформальных. Поэтому желательным трендом развития является непротиворечивое взаимодействие данных институтов.

Можно выделить несколько форм подобной институциональной координации на основе 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 [3]. 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 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» подобная сумма определена в размере 600 тыс. рублей. В связи с участившимися случаями кибермошенничества, возможно, существует необходимость скорректировать данную сумму в сторону понижения.

3. Установление суммы 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 уведомления от банка о проведенной операции. Одновременно с установлением суммы возврата ЦБ РФ предлагает значительно изменить процедуру подтверждения банками операций, если они видят признаки того, что транзакция совершается в целях мошенничества [3].

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 [5, с. 12].

5. Повышение финансовой грамотности населения, особенно его наиболее уязвимой части – людей преклонного возраста. Финансовая гра-

мотность 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» [11]. Важными целями указанной стратегии являются: формирование знаний граждан о рисках на финансовом рынке, выработка способности распознавать признаки финансового мошенничества, а также умений отстаивать свои законные права как потребителя финансовых услуг.

В рамках Стратегии выделяются следующие группы населения:

– граждане, склонные к рискованному типу финансового поведения в сложных жизненных обстоятельствах; к таковым Правительство РФ относит людей с низкими и средними доходами;

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

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

И если в образовательных организациях повсеместно вводятся обязательные курсы по основам финансовой грамотности, то две первые группы населения являются наиболее уязвимыми с точки зрения осуществления кибермошенничества. Основными факторами риска стать жертвами киберпреступления, характерными для указанных категорий граждан, являются:

– низкие доходы и отсутствие коммерческой собственности, когда индивиду, по существу, нечего терять в надежде быстро обогатиться;

– присущая с советских времен пожилому населению вера в государство, порождающая патерналистские настроения;

– высокая психологическая внушаемость людей зрелого возраста.

В целях наживы мошенники все чаще стали использовать виртуальные финансовые пирамиды, работающие по типу знаменитой МММ (по иронии судьбы WWW есть перевернутое МММ). Одним из последних нашумевших случаев стал лопнувший в 2021 г. финансовый пузырь компании «Финико». Все расчеты внутри фирмы производились во внутренней валюте – цифронах. Ее нужно было покупать за криптовалютные биткоины. Цифрон при этом оставался единственной единицей измерения внутри компьютерной интернет-платформы, а его цена контролировалась руководством компании. В итоге Центробанк РФ выявил у «Финико» признаки финансовой пирамиды и передал материалы по ней в правоохранительные органы [12].

В период пандемии коронавируса актуальность обеспечения безопасности экономического интернет-следа личности значительно возросла, так как во время удаленной работы 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 персональной информации и финансовая выгода. Среди сведений, украденных у частных лиц, лидировали учетные системные и личные данные, а также реквизиты платежных карт (рис. 2).

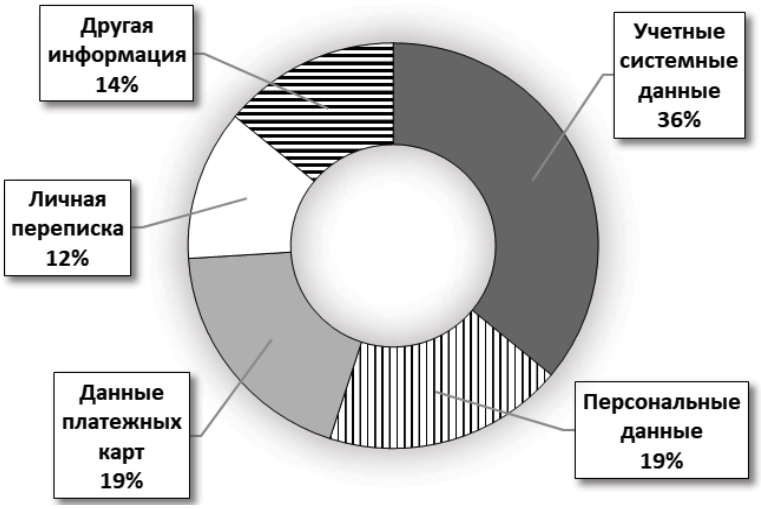

Рис. 2. Типы украденных кибермошенниками данных у частных лиц [4]
Fig. 2. Types of data stolen by cybercriminals from individuals [4]

В общем количестве кибератак на частных лиц лидируют такие способы мошенничества, как создание фишинговых сайтов и распространение вредоносного контента посредством электронной почты (рис. 3).

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 [4]. Попавшие в институциональную ловушку недофинансирования российские медицинские учреждения характеризуются низкой степенью компьютеризации, и в этом смысле они более устойчивы к хакерским кибератакам.

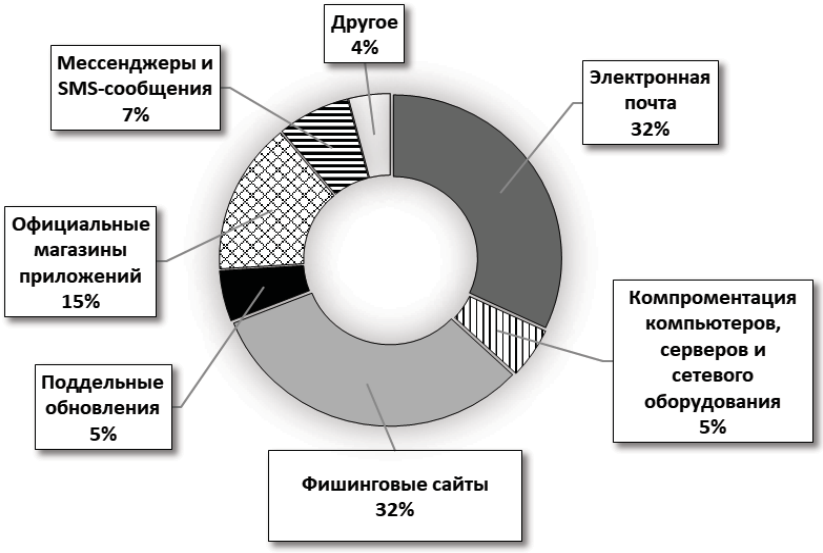

Рис. 3. Способы распространения вредоносного программного обеспечения в кибератаках на частных лиц [4]
Fig. 3. Ways to distribute harmful software in cyber attacks on individuals [4]

Результаты

В целом, необходимо отметить слабость государственных и рыночных институтов защиты экономического интернет-следа личности. Данный факт объясняется постоянным прогрессом ИКТ, появлением все более совершенных гаджетов и новых приложений. Государственные органы не успевают, а рынок не спешит реагировать на данные изменения. Это происходит из-за того, что чиновничий аппарат слабо мотивирован, а рыночные структуры неохотно идут на мероприятия, не предполагающие получение прибыли. Судебные институты также не готовы к интерпретации и рассмотрению не закрепленных в законодательной базе и правоприменительной практике новых видов киберпреступлений.

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

В то же время государству в рамках национального проекта развития цифровой экономики в России необходимо разработать комплексную стратегию защиты экономического интернет-следа личности. Важная роль в данном вопросе должна отводиться научному сообществу, представителям которого следует теоретически осмыслить, оценить и обосновать практические шаги по обеспечению кибербезопасности граждан.

Список литературы

1. Путин заявил о долге властей защищать аватары россиян в метавселенных // РБК. URL: https://www.rbc.ru/rbcfreenews/618ea97f9a794713ffa492fb (дата обращения: 15.01.2022).
2. Число киберпреступлений в России // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России (дата обращения: 15.01.2022).

3. Мошеннические переводы ложатся на банковские плечи // РБК. URL: https://www.rbc.ru/newspaper/2021/12/06/61a8d4639a79476b808c4eee (дата обращения: 15.01.2022).
4. Актуальные киберугрозы : итоги 2020 года // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 16.01.2022).
5. *Красильников О. Ю.* Неоинституциональная экономика. Саратов : Изд-во Саратовского ун-та, 2002. 104 с.
6. Как зарабатывают киберпреступники : дипфейк-боссы и цифровое вымогательство // ХАЙТЕК. URL: https://hightech.fm/2020/10/30/deep-fake-fishing (дата обращения: 15.01.2022).
7. Хакеры не нужны : как в Сбере воровали персональные данные на продажу // LIFE. URL: https://life-ru.turbopages.org/life.ru/s/p/1384457 (дата обращения: 15.01.2022).
8. Большинство россиян скептически настроены к идее сдачи биометрических данных для ЕБС // PIKABU. URL: https://pikabu.ru/story/bolshinstvo_rossiyan_skepticheski_nastroenyi_k_idee_sdachi_biometricheskikh_dannyikh_dlya_ebs_8155118 (дата обращения: 17.01.2022).
9. ФСБ поймала хакеров REvil. Они вымогали у Трампа $42 млн за «грязное белье» // Газета.ru. URL: https://www.gazeta.ru/social/2022/01/14/14419411.shtml (дата обращения: 18.01.2022).
10. Роскомнадзор намерен блокировать фишинговые сайты // Infostart.ru. URL: https://infostart.ru/journal/news/uchet-nalogi-pravo/roskomnadzor-nameren-blokirovat-fishingovye-sayty_1370292/ (дата обращения: 16.01.2022).
11. Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 годы. Принята распоряжением Правительства РФ от 25.09.2017 № 2039-р. Доступ из справ.-правовой системы «КонсультантПлюс».
12. Вторая после МММ : как работала финансовая пирамида «Финико» // Forbes. URL: https://www.forbes.ru/finansy-i-investicii/437501-vtoraya-posle-mmm-kak-rabotala-finansovaya-piramida-finiko (дата обращения: 18.01.2022).

References

1. Putin declared the duty of the authorities to protect the avatars of Russians in the metaverse. *RBC*. Available at: https://www.rbc.ru/rbcfreenews/ 618ea97f9a794713ffa492fb (accessed 15 January 2022) (in Russian).
2. The number of cybercrimes in Russia. *TAdviser*. Available at: https:// www.tadviser.ru/index.php/Stat'ja:Chislo_kiberprestuplenij_v_Rossii (accessed 15 January 2022) (in Russian).
3. Fraudulent transfers fall on bank shoulders. *RBC*. Available at: https://www.rbc.ru/newspaper/ 2021/12/06/61a8d4639a79476b808c4eee (accessed 15 January 2022) (in Russian).
4. Current cyber threats: results of 2020. *Positive Technologies*. Available at: https://www.ptsecurity.com/ru-ru/research/ analytics/cybersecurity-threatscape-2020/ (accessed 16 January 2022) (in Russian).
5. Krasilnikov O. Yu. *Neoinstitutsional'naia ekonomika* [Neo-institutional Economics]. Saratov, Saratov State University Publ., 2002. 104 p. (in Russian).
6. How Cybercriminals earn: Deepfake bosses and digital extortion. *HAITEK* (HIGHTECH). Available at: https://hightech.fm/2020/10/30/deep-fake-fishing (accessed 15 January 2022) (in Russian).
7. Hackers are not needed: How Sberbank stole personal data for sale. *LIFE*. Available at: https://life-ru.turbopages.org/ life.ru/s/p/1384457 (accessed 15 January 2022) (in Russian).
8. Most Russians are skeptical about the idea of submitting biometric data for EBS. *PIKABU*. Available at: https://pikabu.ru/story/bolshinstvo_rossiyan_ skepticheski_nastroenyi_k_idee_sdachi_biometricheskikh_dannyikh_dlya_ebs_8155118 (accessed 17 January 2022) (in Russian).
9. The FSB caught the REvil hackers. They extorted $42 million from Trump for "dirty laundry". *Gazeta.ru*. Available at: https://www.gazeta.ru/social/2022/01/14/14419411.shtml (accessed 18 January 2022) (in Russian).
10. Roskomnadzor intends to block phishing sites. *Infostart.ru*. Available at: https://infostart.ru/journal/news/uchet-nalogi-pravo/roskomnadzor-nameren-blokirovat-fishingovye-sayty_1370292/ (accessed 16 January 2022) (in Russian).
11. Strategy for improving financial literacy in the Russian Federation for 2017–2023. Adopted by the Decree of the Government of the Russian Federation of 25.09.2017 no. 2039-r. *ATP «Consultant»* [electronic resource] (in Russian).
12. Second after MMM: How the "Finico" pyramid scheme worked. *Forbes*. Available at: https://www.forbes.ru/finansy-i-investicii/437501-vtoraya-posle-mmm-kak-rabotala-finansovaya-piramida-finiko (accessed 18 January 2022) (in Russian).

Поступила в редакцию 20.01.2022; одобрена после рецензирования 05.02.2022; принята к публикации 10.02.2022
The article was submitted 20.01.2022; approved after reviewing 05.02.2022; accepted for publication 10.02.2022