УДК 343.97; 343.918; 343.4; 316.42

[1]А. Л. Золкин, [2]М. С. Чистяков, [3]Д. И. Лукашина

[1] Поволжский государственный университет телекоммуникаций и информатики (ПГУТИ), г. Самара, email: alzolkin@list.ru

[1] Частное учреждение образовательная организация высшего образования «Медицинский университет «Реавиз» (Реавиз), г. Самара

[2] Владимирский филиал Российского университета кооперации, г. Владимир, email: shreyamax@mail.ru

[3] Владимирский филиал, ФГОБУ ВО «Финансовый университет при Правительстве РФ», г. Владимир

[3]ФКОУ ВО «Владимирский юридический институт Федеральной службы исполнения наказаний» (ВЮИ ФСИН России), г. Владимир, email: daha1995@list.ru

ЭЛЕКТРОННОЕ МОШЕННИЧЕСТВО КАК ФАКТОР НИВЕЛИРОВАНИЯ ИНСТИТУЦИОНАЛЬНОГО РАЗВИТИЯ МЕДИЦИНСКОГО СТРАХОВАНИЯ И ДОСТУПНОГО ЛЕКАРСТВЕННОГО ОБРАЩЕНИЯ В ПРОЕКЦИИ ОБЩЕСТВЕННОГО БЛАГА

Ключевые слова: электронное мошенничество, медицинское страхование, лекарственное обращение, информационная медицина, цифровая (информационная) экосистема.

Современное цивилизационное развитие в проявлении новых высоких технологий предполагает изучение не только экономических и технических возможностей, но и последствия применения технологий «Индустрии 4.0» представителями преступного мира. Поскольку цифровые технологии стали частью повседневной обыденности, преступления, совершаемые с их помощью, с каждым витком развития «Индустрии 4.0» приобретают особую актуальную значимость в целях противодействия данным деяниям.

[1]A. L. Zolkin, [2]M. S. Chistyakov, [3]D. I. Lukashina

[1] Volga Region State University of Telecommunications and Informatics (PGUTI), Samara, email: alzolkin@list.ru

[1] Private institution educational organization of higher education “Medical University” Reaviz “ (Reaviz), Samara

[2] Vladimir Branch of the Russian University of Cooperation, Vladimir, email: shreyamax@mail.ru

[3] Vladimir Branch, Financial University under the Government of the Russian Federation, Vladimir

[3]Vladimir Law Institute of the Federal Penitentiary Service (VUI of the Federal Penitentiary Service of Russia), Vladimir, email: daha1995@list.ru

Keywords: electronic fraud, health insurance, drug circulation, information medicine, digital (information) ecosystem.

Modern civilizational development in the manifestation of new high technologies involves the study of not only economic and technical opportunities, but also the consequences of the use of Industry 4.0 technologies by representatives of the underworld. Since digital technologies have become a part of everyday life, crimes committed with their help, with each round of the development of Industry 4.0, acquire particular relevance in order to counteract these acts.

В документе, предшествующему действующей Стратегии развития информационного общества, фиксировалось: «Развитие инновационных информационно-коммуникационных технологий выступает важным элементом политической модернизации страны. Итогом их внедрения становится формирование информационного общества, характеризующегося высоким уровнем развития информационных и телекоммуникационных технологий и их интенсивным использованием гражданами, бизнесом и органами государственной власти» (Стратегия развития

информационного общества в Российской Федерации, утвержденная Президентом Российской Федерации 07.02.2008 №Пр-112, документ утратил силу) [2].

Целью обзорного исследования является рассмотрение корыстного использования цифровых технологий в плоскости мошеннических действий в сегменте социально значимой деятельности общественного пространства – медицинского страхования и качественного лекарственного обеспечения населения.

В ходе аналитического обзора был использован метод позиционного сравнения, системный и другие методы анализа. Использованы материалы, в т.ч. справочного характера, являющиеся данными, опубликованными в научных изданиях, специализированных научных изданиях и информационно-коммуникационной сети «Интернет».

Новые реалии информационно-цифрового формата эволюции мирового социума вызваны постиндустриальным этапом технологического развития информационного общества, которые несут не только блага, но и множественные вариации угроз.

В развитии информационного общества зарождаются специфические отношения, определенные закономерности и структура [11].

Цифровая эволюция определенного сегмента народного хозяйства формирует специфический цифровой инструментарий, необходимый для данной сферы деятельности в условиях информационной трансформации. Это цифровые информационные массивы (базы); системы идентификации пользователя; определенные механизмы пополнения; извлечения и получения информации из этих баз; система «Умный город», «Безопасный город»; система геолокации м установления местонахождения объекта; технологи блокчейна и обработки больших массивов данных и прочее. Антиподом положительного воздействия данных инструментов на сферы жизнедеятельности социума являются возникающие условия их потенциального применения в коростных целях. Тем значительнее данная угроза, что посредством информационных технологий нивелируются границы между государствами и пространственные барьеры между людьми.

Одной из причин ускоренного развития мошенничества в информационного-коммуникационной среде является отставание государственно-правового регулирования взаимоотношений резидентов цифрового пространства, в том числе в социально значимых сферах народного хозяйства.

В обзоре данной статьи, посвященной цифровой безопасности, выделим частность применения информационных технологий в сфере медицинского страхования и обращения лекарственных препаратов.

Юридический задел проблематики мошенничества достаточно обширен. Теоретические основы заложены С.В. Познышевым, Н.С. Таганцевым, И.Я Фойницким (1871) и др. Социальная инженерия и границы ее применения как предметная область исследована Б.В. Быховцевым, Ю.М. Резником, М.В. Дан. Д.А. Никитиной изучен международный опыт исследований и практические рекомендации населению в период распространения новой коронавирусной инфекции (COVID-19). К.Г. Айрапетяном проведен анализ статистических данных интернет-мошенничества в период пандемии COVID-19. В работе Гарфина, Сильвера и Холмана приведены результаты исследования, в котором описываются события в средствах массовой информации (СМИ), связанные с коронавирусом [7].

Интернет в современных реалиях в деструктивном проявлении представляет собой одну из форм коррупционных сетей высокотехнологичного порядка с кланово-корпоративной структурой.

Российская Федерация находится в ряду государств, недостаточно защищенных от угроз информационно-агрессивного характера. Российская правовая система в целом и законодательство, в частности, слабо адаптированы к противостоянию киберпреступности и вызовам «цифровой эпохи» в силу недостаточного внимания к регламентации и координации охраны общественных отношений в информационно-коммуникационной плоскости. Данные обстоятельства привели к низкой резистентности национального законодательства к новым противоправным проявлениям с использованием информационно-коммуникационных технологий [21,126].

Информация, собранная в различных массивах и используемая в информационно-коммуникационном пространстве, с возможностью последующего сбора, анализа и аккумулирования информации, представляет собой ресурс не только потенциального блага, но и причинения вреда, в т.ч. при преступном умысле.

Обыватель, являющийся резидентом сетевого пространства, оставляет огромный информационный след. «Данные – это новая нефть. Описание, как люди «ходят» по сайту магазина одежды, – это BigData. Список клиентов с картами скидок – нет, это структурированная информация»

Мошенничество, совершаемое в информационно-цифровой среде, представляет собой деяние, при котором преступные элементы оставляют т.н. следовую информацию при использовании современных средств коммуникаций.

Кража данных СНИЛС (страховое свидетельство индивидуального лицевого счета) представляет особую угрозу манипуляций с персональными данными граждан. Одно из наиболее распространенных видов мошенничества в системе обязательного медицинского страхования представляет собой внесение недостоверных данных о застрахованном лице в соответствующую медицинскую документацию с целью последующего выставления страховой компании или территориальному фонду обязательного медицинского страхования (ТФОМС) счетов за оказание несуществующих медицинских услуг. Подобного рода преступных манипуляций с вовлечением информационных массивов и реестров при эмерджентной синергии с цифровой средой представляет собой угрозу для различных сторон государственного устройства, в т.ч. в институциональном обеспечении должного медицинского обслуживания, транспарентной высокотехнологичной медицины как общественного блага, гарантированного государством, поскольку финансовая нагрузка при ложных страховых случаях является угрозой и ингибитором формирования условий для доступности медицинских услуг.

Преступные деяния в сфере медицинского страхования подпадают в состав экономических преступлений (статья 159 УК РФ, статья 159.5 УК РФ) либо преступлений, совершенных должностными лицами (статья 285.2 УК РФ, статья 290 УК РФ). Отметим, что при распределении денежных средств как функции общественных отношений, всегда присутствовал соблазн похищения как коррупционный фактор, лицами, непосредственно участвующими в данном процессе. При этом к преступным деяниям, таким как приписка и использование недостоверных данных о пациенте и информации о медицинских манипуляциях, присовокупляются цифровые инструменты для мошенничества, которые, напротив, должны нести иную миссию – реализацию конституционных прав граждан.

Дальнейшее развитие контроля в здравоохранении на платформе цифровых технологий будет благоприятствовать формированию особой цифровой среды, способствующей снижению мошенничества в системе обязательного медицинского страхования (ОМС). А именно: меры профилактического цифрового контроля (появления сервиса на портале государственных услуг), позволяющие верифицировать перечень медицинских услуг, оказанных пациенту, и их стоимостью за определенный хронологический период.

Данной концепции будет способствовать ведение электронных медицинских карт (ЭМК), являющихся составной частью цифровизации медицинской сферы народного хозяйства страны. ЭМК позволят в автоматизированном режиме вести медицинскую документацию на каждого пациента с пошаговой детализацией течения болезни с последующей аналитической, экономической и иной работой по нахождению человека в статусе «клиента» ЛПУ, что позволит выявить преимущества и недостатки в каждом конкретном случае течения заболевания и процедур лечения. Данный алгоритм позволит выработать определенные шаблоны по различным ситуативным проявлениям в деятельности медицинской службы с поправкой на конкретный регион [22,409].

В свою очередь, информационная медицина позволит произвести ранжирование необходимой информации от сопутствующей, зачастую – ненужной [6,142].

Еще одной угрозой повсеместного распространения информационных технологий является присвоение персональных данных иными лицами. В данном случае назрела необходимость в новых реалиях повсеместно развивать цифровое удостоверение личности (цифровой идентификатор), что будет способствовать обеспечению политических, социальных и экономических процедур в эпоху «Индустрии 4.0» [24].

Прослеживается определенная взаимосвязь дистанционной продажи лекарственных препаратов посредством информационно-коммуникационного пространства с нелегальным и поддельным оборотом лекарственной продукции. Более чем 50% объема реализации лекарственных средств через Интернет, в т.ч. через нелегальные сайты, которые пользуются завуалированным адресом, приходится на поддельные лекарства.

Данная ситуация осложняется развитием международной торговли и транспарентными границами, что переводит лекарственное обращение в статус международного. Необходимо учитывать, что законодательство государств в данной сфере разнится и не коррелирует с международными правовыми актами, что затрудняет отслеживание и борьбу с незаконным обращением лекарственных средств в транснациональных масштабах.

В связи с возрастающей актуализацией проблематики оборота фальсифицированных и незаконных лекарственных средств, в т.ч. через Интернет, Совет Европы 1 декабря 2010 года принял Конвенцию MEDICRIME. Конвенция устанавливает уголовную ответственность за производство и распространение фальсифицированной медицинской продукции.

В настоящее время в практике оборота лекарственных средств в РФ происходят коренные изменения. Внедрена система мониторинга движения лекарственных средств, которая позволит упорядочить рынок лекарственного обращения и возвести на новый уровень контроль и надзор в данной социально значимой сфере народного хозяйства.

Однако, по различным оценкам, порядка 10% мирового оборота лекарственного производства приходится на фальсифицированные препараты [19]. Глобальные последствия новой коронавирусной инфекции (COVID-19) привели к изменению привычного образа жизни, например, к ускорению распространения интернет-торговли, в т.ч. лекарствами. Возрастает активность «теневого сектора» в данном сегменте фармацевтического оборота, в котором участники и ранее чувствовали свою безнаказанность.

Цифровая преступность является результатом отсутствия либо слабого развития социального контроля во Всемирной паутине. Отчасти данный механизм в синергии с государственным контролем, как особый вид социально-юридического купирования подобного рода криминальных угроз, находится на этапе своего становления. Провоцирующим фактором криминогенного характера является отсутствие должного уровня культуры «нахождения» в цифровом пространстве при все более возрастающем развитии информационно-информационных технологий, катализирующим правовой нигилизм с одной стороны, и незащищенность «сетевых обывателей» – с другой [18].

13 мая 2019 года на региональной площадке Legal Forum Live Петербургского международного юридического форума, А.И. Овчинников в своем докладе «Концепции цифровой безопасности в РФ: основные задачи, понятия и направления обеспечения безопасности личности, общества и государства» отметил, что застуживает отдельного анализа вопрос о цифровизации правового регулирования, государственного управления в связи с наличием большого количества рисков в этих процессах для общества и человека. По его мнению, развитие цифровых технологий может привести к глобальным деструктивным последствия для социума [17].

Современные процессы цифровизации характеризуются конвергенцией воздействия на сознание – как на личностное, так и на социальное целое, выраженное в транспарентных и латентных информационных войнах. Информация, которая имеет потенциал полезности применения, может нести угрозу для социума в корыстных «руках и умах злоумышленников». Данный аспект раз-

вития информационного общества является нравственным во взаимодействии и взаимоотношениях представителей мировой цивилизации и представляет собой этико-моральную основу ее существования.

Уровень информационной культуры социума во многом предопределено и опирается на информационно-цифровую компетентность носителей данных знаний в цифровой экосистеме.

Обратимся к дефиниции «цифровая (информационная) экосистема» для рассмотрения создания потенциальных условий для предотвращения формирования возможных угрожающих факторов как «обратной стороны» преимуществ цифровой экономики. Так, пп «с» п.4 Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [1] фиксируется, что «экосистема цифровой экономики – партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан».

В научном сообществе в т.ч. укоренился оборот экосистема информационного общества.

Если же рассматривать информационную экосистему как некоторое подобие окружающего средового фона, а информационное общество как «общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан» [1], то экосистему информационного общества возможно определить как информационную часть окружающей среды, интегрированную в информационное общество [5].

Сейчас многие компании выстраивают вокруг своих брендов собственные экосистемы. Создание глобальной цифровой экосистемы позволит минимизировать возможные риски развития «Индустрии 4.0». Цифровая (информационная) экосистема подразумевает верификационную основу цифровой идентификации совершаемых действий физического и юридического лица в данной системе.

Формирование цифровой экосистемы сопряжено не только с потенциальным нивелированием угроз повсеместной конвергенции цифрового пространства в повседневную жизнь, но и с возможными угрозами ее функционирования. Ее создание и развитие позволит нивелировать нарастающие угрозы цифрового эволюционного развития.

Развитие различных сегментов цифровой экосистемы позволит расширить трансфер персонализированной информации в особом защищенном статусе на платформе блокчейн.

Учитывая экономическую направленность данного издания, авторы не акцентируют более подробного внимания на сущности и функционировании цифровых экосистем. Но в заключение хотели бы отметить, эволюция основных информационных систем во благо социума позволит, с одной стороны – создать условия генерации новых перспективных возможностей для информационного общества и экономики знаний, а с другой – значительно снизить угрозу расширения вариаций мошеннических действий, возникающих под воздействием информационно-коммуникационных технологий.

Библиографический список

1. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ. 2017. №20. ст. 2901.

2. Абдряшитова А.И., Грачева Е.В., Казаков М.Ю., Лачинина Т.А., Чистяков М.С. Инструменты управления реализацией муниципальных функций в электронном виде: монография / отв. ред. Т.А. Лачинина. – М.: ИНФРА-М, 2018. – 251 с. – Научная мысль. – ISBN 978-5-16-013276-1.

3. Белл Д. Грядущее постиндустриальное общество. – М., 1999.

4. Быков В.А., Епишина Е.О., Семенова Ю.О. Коррупция как угроза экономической безопасности в сфере предпринимательства // сборник статей по итогам VI Межрегиональной научно-практической конференции научно-педагогических и практических работников «Наука и общество: проблемы и перспективы развития». – Москва: Московский финансово-юридический университет (МФЮА), 2019. – С. 257-264. ISBN 978-5-94811-303-6.

5. Гаврилов С.Н., Володина С.И. Информационная (цифровая) экосистема адвокатуры в контексте экосистемы цифровой экономики России // Актуальные проблемы российского права. – 2019. – №6(103). – С. 156-166. DOI: 10.17803/1994-1471.2019.103.6.156-166.

6. Губернаторов А.М., Лачинина Т.А., Чистяков М.С. Высокие технологии в формировании инновационной среды в сфере здравоохранения // Сборник научных трудов участников XI Международной Кондратьевской конференции «Возможные сценарии будущего России и мира: междисциплинарный дискурс. – Москва: Межрегиональная общественная организация содействия изучению, пропаганде научного наследия Н.Д. Кондратьева, 2020. С. 140-146. DOI: 10.46865/978-5-901640-34-0-2020-140-146.

7. Гусев О.Б., Завидов Б.Д., Коротков А.П., Слюсаренко М.И. Преступления против собственности: кража, мошенничество, присвоение или растрата, грабеж, разбой, вымогательство. – М.: Экзамен, 2001. –192 с.

8. Желудков М.А., Пузырева К.Ю. Новый взгляд на способы профилактики преступности в сфере обязательного медицинского страхования // Вестник Волжского университета имени В.А. Татищева. – 2020. – Т. 2. – № 4(97). – С. 114-122.

9. Иванов А.Л., Шустова И.С. Исследование цифровых экосистем как фундаментального элемента цифровой экономики // Креативная экономика. – 2020. – Том 14. – № 5. – С. 655-670. DOI: 10.18334/ce.14.5.110151.

10. Интернет-корпорации манипулируют нашим поведением. Как меняется жизнь, если вживить в руку биочип [Электронный ресурс]. URL: https://hi-tech.mail.ru/review/nami-manipuliruyut-s-pomoshchyu-bigdata/ (22.02.2021).

11. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. … канд. юрид. наук. – Пятигорск, 2010.

12. Конвенция Медикрим [Электронный ресурс]. URL: https://rm.coe.int/medicrimeconvention10qa-ru/1680993aaa (17.02.2021).

13. Лачинина Т.А., Чирков М.А., Чистяков М.С. О развитии менеджмента здравоохранения в посткоронавирусную эпоху эпидемиологической неопределенности // Философия хозяйства. – 2020. – №6(132). – С. 201-207.

14. Лекарства: поддельные/ложно маркированные/фальсифицированные/ контрафактные [Электронный ресурс]. URL: https://www.who.int/medicines/services/counterfeit/ru/ (15.02.2021).

15. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. – М., 1999.

16. Мунтян М.А. Постиндустриальное общество как концепция новой глобальной цивилизации // Безопасность Евразии. – М., 2001. – №2.

17. Овчинников А.И., Ахрамеева О.В., Воронцов С.А., Кожокарь И.П., Кравченко А.Г., Мамычев А.Ю., Мордовцев А.Ю., Шатковская Т.В. Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. // Вестник юридического факультета ЮФУ. – 2019. – Т.6. – №2. – С. 111-122. DOI: 10.23683/2313-6138-2019-6-2-18.

18. Осипенко А. Л. Сетевая компьютерная преступность. Теория и практика борьбы. Омск, 2009. 480 с.

19. Пасечная А.А. Проблемный аспект уголовного наказания за онлайн– продажу фальшивых лекарств // сборник научных трудов XIV Международной научно-практической конференции «Российское право на современном этапе». – Москва: Издательство «Знание-М», 2020. С. 415-418.

20. Рейнман Л.Д. Информационное общество и роль телекоммуникаций в его становлении // Вопросы философии. – М., 2001. – №3.

21. Чекушов А.А., Гордеевцев Е.И., Чирков М.А., Чистяков М.С. Преступность в цифровой среде, как фактор, ограничивавший развитие информационных технологий // Вестник Владимирского юридического института. – 2020. – №1(54). С. 125-133.

22. Чирков М.А., Чистяков М.С. Влияние цифровой среды на формирование современной архитектоники здравоохранения // Материалы XXIII Международной научно-практической конференции «Экономика и управление: современные вызовы, тенденции и перспективы развития» (Байкальские экономические чтения). – Улан-Удэ: Восточно-Сибирский государственный университет технологий и управления, 2019. С. 407-413.

23. Chirkov M.A., Abdryashitova A.I., Chistyakov M.S. Crime counteraction in the digital environment as a factor of the development of high technology // Proceedings of the 1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019). – ATLANTIS PRESS 29 AVENUE LAVMIERE, PARIS, 75019, FRANCE. P. 437-440. doi.org/10.2991/mtde-19.2019.85 ISBN 978-94-6252-721-8.

24. McKinsey Global Institute (2019), Digital identification. A key to inclusive growth, McKinsey Global Institute, April 2019. – www.mckinsey.com/mgi