УДК 338.2+343.35

ЦИФРОВИЗАЦИЯ ПРОТИВ КОРРУПЦИИ. ВОЗНИКНОВЕНИЕ Е-КОРРУПЦИИ

© 2019 Д.Н. Мухамадиева*

Рассматривается роль цифровизации, электронного правительства и электронно-сетевых общественных благ в снижении уровня коррупции. Высокие технологии и инновационные методы государственного управления в совокупности дают высокие результаты в борьбе с казнокрадством. В то же время с развитием науки и техники в условиях цифровизации экономики создается благоприятная среда для возникновения нового вида преступлений - е-коррупции, которая проявляется не только через получение политической ренты посредством госзаказов, но и с помощью вмешательства в государственное программное обеспечение. Переход к электронным данным имеет ряд существенных преимуществ, однако этот процесс все чаще становится мишенью злоумышленников. Вследствие е-коррупции ежедневно происходят многочисленные кибератаки на программное обеспечение разных уровней.

Ключевые слова: общественные блага, электронное правительство, электронные госуслуги, электронно-сетевые общественные блага, цифровая экономика, коррупция, е-коррупция.

Основные положения:

- эффективное государственное управление с помощью цифровой среды позволяет сокращать уровень коррупции, так как взаимодействие населения и госслужащих все чаще происходит через электронную площадку;
- процесс цифровизации экономики имеет не только положительные результаты, но и отрицательные в виде появления новой формы коррупции - е-коррупции;
- е-коррупция заключается в превышении госслужащими их полномочий в ходе работы с информационными системами высокого уровня и с электронным правительством.

Введение

Проблема коррупции существует практически в каждом государстве. Борьба с ней ведется различными методами, расходуются значительные средства. Коррупция способна разрушить любую страну. Исторически сложилось так, что данный процесс эволюционирует наряду с развитием общества, техники и технологий. Поэтому антикоррупционная политика также должна соответствовать времени и технологическим нововведениям.

Методы

Современные технологии, внедряемые в государственные структуры, позволяют более эффективно осуществлять государственное управление. Цифровизация взаимоотношений госслужащих и потребителей государственных услуг стала возможной благодаря системе электронного правительства, одной из положительных черт деятельности которого является то, что госуслуги технически усложняют применение коррупционных механизмов. Таким образом, электронное правительство и сопутствующие электронно-сетевые общественные блага можно рассматривать в качестве инструментов антикоррупционной политики.

Совершенствование проекта электронного правительства в России входит в приоритетные направления развития страны и активно поддерживается политическим курсом, а также способствует повышению эффективности управленческого аппарата, усиливает контроль за действиями госслужащих и противодействует коррупции.

Результаты

По словам Генсека ООН Антонио Гутерриша, мировая экономика ежегодно теряет более 5% мирового ВВП (2,6 трлн долл. США) от преступлений, связанных с коррупцией[1].

По данным Генеральной прокуратуры Российской Федерации, с 2015 по 2017 г.

* Мухамадиева Динара Назифовна, преподаватель Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации. E-mail: 89264279061@mail.ru.

ущерб от коррупционных действий для государства составил 130 млрд руб., а в первом полугодии 2018 г. - 3,8 млрд руб.[2]

По мнению многих экспертов международных организаций, таких как ООН, МВФ и др., деятельность электронного правительства способствует снижению уровня коррупции в странах, так как информационно-коммуникационные технологии позволяют высокоэффективно бороться с подобным процессом, поскольку они препятствуют принятию "удобных" решений чиновников, а технологически сложная система круглосуточно фиксирует и мониторит действия госслужащих.

Всемирная организация по борьбе с коррупцией Transparency International ежегодно исследует антикоррупционную ситуацию в мире. Для оценки стран по уровню коррупции проанализируем данные отчетов "Индекс восприятия коррупции" (табл. 1).

Таблица 1

Рейтинг стран по уровню коррупции*

Рейтинг 2017 г.	Страна	Индекс 2017 г.	Индекс 2016 г.	Индекс 2015 г.
1	Новая Зеландия	89	90	91
2	Дания	88	90	91
3	Финляндия	85	89	90
3	Норвегия	85	85	88
3	Швейцария	85	86	86
135	Россия	29	29	29

* Составлено автором по: Transparency International Corruption Perceptions Index 2017 // Transparency International - 2017. URL: https://www.transparency.org/news/feature/corruption_perceptions_index_2017 (accessed date: 23.12.2018).

Максимальный уровень коррупции - 0 баллов, отсутствие коррупции - 100 баллов.

В рейтинге стран по низкому уровню коррупции в 2017 г. лидируют Новая Зеландия, а также европейские страны (Дания, Финляндия, Норвегия), в которых традиционно высокий уровень цифровизации и развития электронного правительства. По представленным данным, Россия занимает 135-ю позицию в рейтинге из 180 исследуемых стран, где за период 2012-2014 гг. индекс коррупции составил 28-27 баллов, а в 2015-2017 гг. данный показатель был оценен в 29 баллов, что свидетельствует о стабильно низком проценте эффективности внедряемых органами власти мер, направленных на решение проблемы коррупции. Поскольку одной из таких мер является проект электронного правительства, которое начало свою работу с 2010 г., можно утверждать, что на данный момент это нововведение пока еще не справляется в полной мере с поставленной задачей. В соответствии с одной из распространенных точек зрения, основная проблема столь медленного характера изменений заключается в наличии низкого уровня информатизации государственных услуг.

Цифровая среда, с одной стороны, является инструментом борьбы с коррупцией, а с другой - причиной возникновения новой формы правонарушений - е-коррупции, которая заключается в превышении госслужащими их полномочий в ходе работы с информационными системами и электронным правительством.

Примером такого вида коррупции является крупный скандал, который разразился в 2011 г. из-за проверки правоохранительными органами выполнения госзаказа "Ростелекома" и Минкомсвязи РФ в рамках развития программы "Электронная Россия". В данный госзаказ входили мероприятия по проведению научно-исследовательских работ и поставка программно-технических средств. По итогам расследования выяснилось, что высокопоставленные чиновники вышеупомянутых организаций состояли в сговоре и посредством мошеннической схемы нанесли ущерб государству, оценивающийся в 280 млн руб.[3]

Вышеописанное показывает, что использование "выгодного" положения на госслужбе, даже в целях развития госпрограмм, может быть источником получения политической ренты.

В качестве другого примера проявления е-коррупции можно привести такую госуслугу, как электронное голосование. Данный процесс, по мнению экспертов, подвержен получению необъективных результатов, так

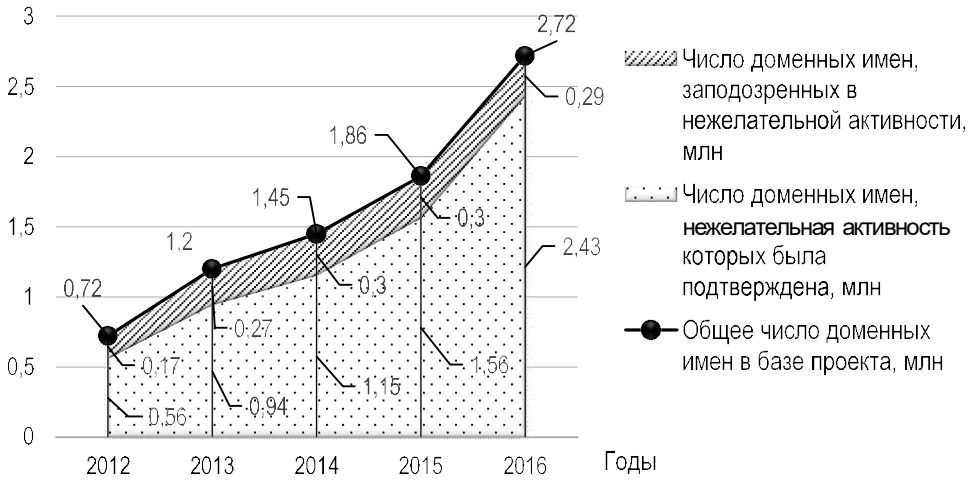

Рис. 1. **Число кибератак в России***

* Составлено автором по: Цифровая экономика России 2017: аналитика, цифры, факты // Российский интернет-форум 2017. URL: https://www.shopolog.ru/metodichka/analytics/cifrovaya-ekonomika-rossii-2017-analitika-cifry-fakty (дата обращения: 23.12.2018).

как имеется высокий риск фальсификации итогов голосования из-за давления пролоббированного начальства на работников, контролирующих цифровые процессы. Поэтому сегодня необходимо разрабатывать технологии и методы борьбы с развивающейся коррупцией в электронном пространстве на совершенно новом, инновационном уровне, а также вести активную социально-экономическую политику, пропагандирующую порицание казнокрадства.

Обсуждение

С каждым годом все больше людей вовлекается в цифровое пространство. Доступ в Интернет постоянно улучшается, территориальный охват им все увеличивается. По данным сайта интернет-статистики (Internet World Stats), ко второму полугодию 2018 г. общее количество интернет-пользователей в мире превысило 4,2 млрд чел.[4] По данным РАЭК, к 2020 г. три четверти россиян - 86,7 млн чел. - станут пользователями глобальной сети[5].

В данной связи проблема несанкционированного вмешательства в программное обеспечение любого уровня с целью выгоды становится все более актуальной.

Согласно данным исследования, проведенного аналитиками РАЭК, 31% компаний в России сталкивались с DDOS-атаками[6]. На рис. 1 представлено число кибератак за 2012-2016 гг.

Из приведенной иллюстрации видна увеличивающаяся тенденция нежелательной активности в цифровом пространстве. С 2012 по 2016 г. более чем в 4 раза - с 560 тыс. до 2,43 млн - возросло число доменных имен, нежелательная активность которых была подтверждена.

По данным компании Positive Technologies, анализирующей уровень безопасности сетей и приложений, мировой ущерб от различного рода атак за 2017 г. составил более 2,5 млрд долл. США (табл. 2).

Таблица 2

Ущерб миру от киберугроз, 2017 г.*

Ущерб	Сумма, долл. США
От атак с использованием вредоносного ПО	Более 1,5 млрд
От атак методом социальной инженерии	Более 250 млн
От компрометации учетных данных	Более 100 млн
От атак с использованием веб-уязвимостей	Более 390 млн
От атак с использованием уязвимостей ПО	Более 280 млн
От DDoS-атак	Не установлено

* Составлено автором по: Актуальные киберугрозы - 2017 // Positive Technologies. 2017. URL: https://www.cybersecurity_threatscape-2017_A4.RUS.0003.03.APR.06.2018 (дата обращения: 23.12.2018).

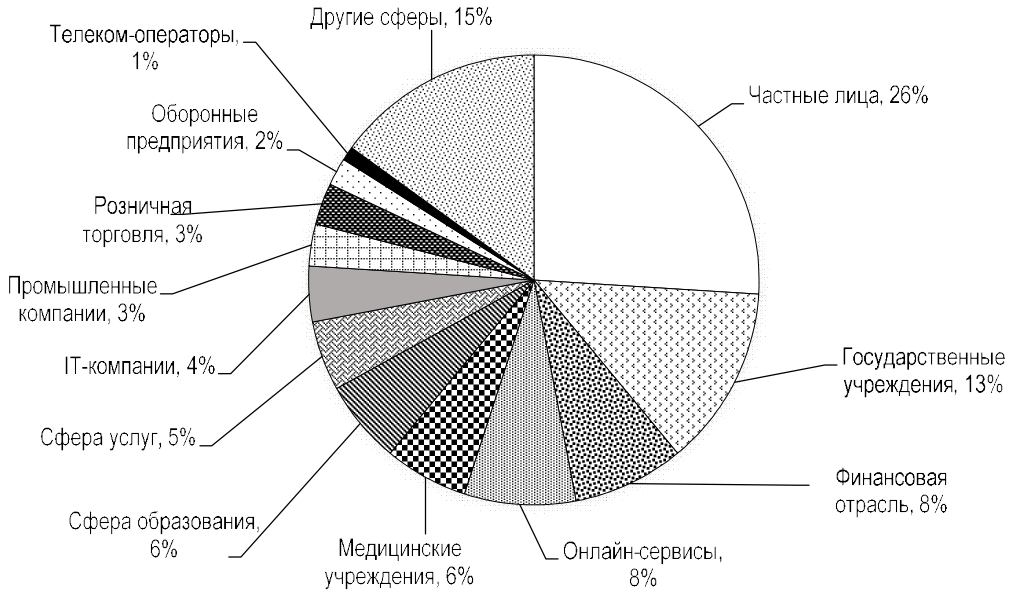

Рис. 2. **Категории пострадавших от кибератак в 2017 г.***

* Составлено автором по: Актуальные киберугрозы - 2017 // Positive Technologies. 2017. URL: https://www.cybersecurity_threatscape-2017_A4.RUS.0003.03.APR.06.2018 (дата обращения: 23.12.2018).

Семь из десяти атак злоумышленники совершали для извлечения финансовой выгоды, а 23% для получения данных[7]. На рис. 2 представлены категории лиц и объектов, пострадавших от киберзлоумышленников.

Больше всего киберугроз пришлось на частных пользователей (26%), на втором месте оказались государственные объекты (13%), а на третьем - банки и онлайн-сервисы (по 8%).

Борьба с кибератаками находится в активной фазе. Для защиты информации создаются институты, ведется научная работа. Специалисты данной сферы обучаются теории и практике цифровой безопасности. Однако знать и применять меры защиты личной информации в глобальной сети необходимо уже каждому пользователю.

Например, для борьбы с деятельностью хакеров в конце 2016 г. Госкорпорация "Ростех" открыла специальный центр противодействия киберугрозам. Ежедневно центр защищает от атак более 700 госпредприятий, входящих в "Ростех"[8].

Заключение

Цифровая среда формирует новую реальность, в которой деятельность человека переносится в виртуальное пространство. Поэтому, с одной стороны, с помощью инновационных технологий многие процессы становятся прозрачнее, быстрее, дешевле и эффективнее, а с другой стороны, могут проявляться побочные эффекты, такие как развитие е-коррупции и киберугрозы.

Таким образом, общество сталкивается с необходимостью увеличения уровня информационной безопасности и эффективной социально-экономической политики для устранения проблем, возникших вследствие негативных явлений цифровизации экономики.

---

[1] 9 декабря - Международный день борьбы с коррупцией / Центр новостей ООН. URL: http://www.un.org/russian/news/story.asp?NewsID=12791 (дата обращения: 23.12.2018).

[2] О результатах работы органов прокуратуры Российской Федерации за первое полугодие 2018 г. по возмещению ущерба, причиненного актами коррупции / Генпрокуратура РФ. URL: https://genproc.gov.ru/smi/news/genproc/news-1431928 (дата обращения: 23.12.2018).

[3] "Цифровая" коррупция / Антикоррупц. комитет по Свердлов. обл. URL: http://a-komitet.ru/smi_o_korrupcii/18508 (дата обращения: 23.12.2018).

[4] World Internet Usage and Population Statistics // Internet World Stats. 2018. June 30. URL: https://www.internetworldstats.com/stats.htm (access date: 23.12.2018).

[5] Программа "Цифровая Экономика РФ" представлена Президенту 5 июля 2017 года: комментарии и оценки аналитиков РАЭК / Ассоц. электрон. коммуникаций (РАЭК). URL: https://raec.ru/live/position/9547 (дата обращения: 23.12.2018).

[6] Цифровая экономика России 2017: аналитика, цифры, факты // Российский интернет-форум 2017. URL: https://www.shopolog.ru/metodichka/analytics/cifrovaya-ekonomika-rossii-2017-analitika-cifry-fakty (дата обращения: 23.12.2018).

[7] Актуальные киберугрозы - 2017 // Positive Technologies. 2017. URL: https://www.cybersecurity_threatscape-2017_A4.RUS.0003.03.APR.06.2018 (дата обращения: 23.12.2018).

[8] Ростех создает мощную защиту от кибератак. URL: http://rt.vk34.ru/blog/post/news/rosteh-sozdaet-moshnuyu-zashitu-ot-kiberatak (дата обращения: 23.12.2018).

Поступила в редакцию 13.01.2019 г.

DIGITALIZATION AGAINST CORRUPTION. EMERGENCE OF E-CORRUPTION

© 2019 D.N. Muhamadieva*

The role of digitalization, e-government and electronic network public goods in reducing corruption is considered. High technologies and innovative methods of public administration in the aggregate give high results in the fight against embezzlement. At the same time, with the development of science and technology under economy digitalization, a favorable environment is created for the emergence of a new type of crime - e-corruption, which manifests in obtaining political rent through government orders, but also in intervention in government software. The transition to electronic data has a number of significant advantages. However, this process is increasingly becoming the target of intruders. Due to e-corruption, numerous cyber attacks at different software levels occur every day.

Keywords: public goods, e-government, e-government services, e-network public goods, digital economy, corruption, e-corruption.

Highlights:

- effective public administration through the digital environment allows reducing the level of corruption, since the interaction of the population and civil servants is increasingly taking place through the electronic platform;
- the process of economy digitalization has not only positive results, but also negative ones in the form of the emergence of a new form of corruption - e-corruption;
- e-corruption is the abuse by state officials of their authority in working with high-level information systems and e-government.

Received for publication on 13.01.2019

* Dinara N. Mukhamadieva, a lecturer of Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation. E-mail: 89264279061@mail.ru.