УДК 351/354:004:304.444 EDN: ZHADGM

Бецан Д. О.
Донбасский государственный технический университет
E-mail: betsan.daria@yandex.ru

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ РИСКИ В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ: МЕРЫ ПРОТИВОДЕЙСТВИЯ И МИНИМИЗАЦИИ УГРОЗ

Статья посвящена определению роли социальной инженерии и информационных рисков в контексте цифровизации государственного управления. Раскрыта сущность цифровизации государственного управления, её роль в развитии государства. Определены и охарактеризованы ключевые риски и угрозы социальной инженерии, возникающие в процессе цифровизации государственного управления. Разработан комплексный подход мер противодействия и минимизации угроз социальной инженерии к обеспечению информационной безопасности в условиях цифровизации государственного управления.

Ключевые слова: *цифровизация, государственное управление, социальная инженерия, киберугрозы, информационная безопасность*

Проблема и её связь с научными и практическими задачами. В современном мире правительства многих государств всё больше стремятся к цифровизации государственного управления, что позволяет сделать реализацию административных процедур проще и доступнее. В целом цифровая трансформация государственного управления позволяет перейти к горизонтальной модели управления, основанной на прозрачности и открытости государственных данных, а также способствовать сотрудничеству с гражданским обществом при разработке государственной политики.

Использование цифровых платформ позволяет улучшить доступ к услугам и ускорить процессы. Однако вместе с этим возрастает количество угроз социальной инженерии — манипулятивного воздействия на граждан для получения конфиденциальной информации или доступа к системам. В контексте цифровизации государственного управления методы социальной инженерии представляют серьезную угрозу безопасности данных граждан и самих государственных структур. Возрастает актуальность необходимости разработки мер противодействия и минимизации угроз для обеспечения информационной безопасности государства.

На современном этапе развития государства стремятся к обеспечению более эффективного, безопасного и прозрачного государственного управления. Этой цели можно достичь путем цифровизации государственного управления. Многие ученые-теоретики и практики, понимая актуальность цифровизации государственного управления, посвятили свои труды данной теме.

Так, исследованию вопросов цифровой трансформации государственного и муниципального управления, реализации цифрового правительства посвящены научные труды таких авторов как Е. И. Добролюбова, А. Ю. Марченко, Н. Е. Дмитриева, Е. В. Васильева, В. А. Болдырева, И. Р. Гумеров, А. С. Киселёв, О. Л. Конюкова, С. А. Мартынова, О. В. Панина, В. Н. Южакова, А. И. Левин и др.

Исследованию угроз, возникающих в процессе цифровизации государственного управления посвящены исследования Е. А. Кипервар, Е. В. Мамай, М. С. Мизя, Н. И. Шашкова, В. А. Яковлева-Черныша и др.

Постановка задачи. ***Цель*** исследования заключается в раскрытии роли социальной инженерии и информационных рисков в

контексте цифровизации государственного управления.

Для достижения данной цели необходимо решить следующие ***задачи***:

– раскрыть сущность цифровизации государственного управления, её роль в развитии государства;

– определить и охарактеризовать ключевые риски и угрозы социальной инженерии, возникающие в процессе цифровизации государственного управления;

– разработать комплексный подход мер противодействия и минимизации угроз социальной инженерии к обеспечению информационной безопасности в условиях цифровизации государственного управления.

Предмет исследования **—** социальная инженерия как угроза для информационной безопасности государства. ***Объект*** **—** цифровое государственное управление.

Изложение материала. Под цифровизацией понимают процесс преобразования традиционных аналоговых процессов, услуг или продуктов в цифровой формат. Такие преобразования могут затрагивать множество сфер жизнедеятельности общества: бизнес, образование, культуру, здравоохранение и др.

Основой цифровизации выступает информация, которая обрабатывается, хранится и передается с помощью цифровых технологий. Активное и массовое распространение цифровых технологий и сопутствующие общественно-трансформационные процессы также оказывают влияние на сферу государственного управления, что проявляется в создании электронных форм взаимодействия между разными участниками общественных отношений, развитии электронного правительства.

Цифровизация государственного управления представляет собой особую форму организации государственного управления, направленную на применение информационно-коммуникационных технологий с целью повышения эффективности, открытости и прозрачности деятельности органов государственной власти и местного самоуправления [1].

В Российской Федерации процесс цифровизации государственного управления нормативно закреплен Указом Президента РФ от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [2]. Впоследствии распоряжением Правительства РФ от 28 июля 2017 года № 1632 разработана и утверждена национальная программа «Цифровая экономика Российской Федерации» [3]. В структуру национальной программы включен федеральный проект «Цифровое государственное управление». Указанный федеральный проект предусматривает мероприятия цифровой трансформации системы государственного управления, что будет способствовать повышению качества жизни граждан и развитию бизнеса.

Цифровизация государственного управления должна осуществляться с учетом соблюдения таких основных принципов, как «повышение открытости государственного аппарата, централизация данных и создание единого электронного правительства» [4].

Цифровое государственное управление играет существенную роль в развитии страны:

1) использование цифровых технологий способствует повышению эффективности деятельности государственных органов, позволяя автоматизировать и оптимизировать процессы, ускорить движение информации;

2) улучшает качество предоставления государственных услуг путем упрощения административных процедур, сокращения документооборота и временных затрат;

3) позволяет расширить возможности участия граждан в процессах принятия решений путем использования платформ обратной связи, общественных обсуждений, голосований в электронном формате;

4) способствует более прозрачному, открытому и доступному взаимодействию между государством и обществом;

5) расширяет возможности сбора, хранения и анализа больших объемов информации для принятия решений;

6) обеспечивает более оперативное реагирование и координацию действий в кризисных ситуациях, например, террористические угрозы, пандемия;

7) способствует сокращению расходов на обслуживание государственных структур [5].

Следует отметить, несмотря на существенное значение цифровизации государственного управления для развития страны, этот процесс сопровождается рядом рисков и угроз (рис. 1).

Рассмотрим представленные риски и угрозы подробнее.

1. Киберугрозы и утечка данных. Государственный сектор обрабатывает конфиденциальную информацию, такую как персональные данные, медицинские данные, финансовая информация. Цифровые решения в государственном управлении должны обеспечить безопасность и предотвратить нарушение целостности такой информации. Одним из векторов киберугроз является социальная инженерия и информационные риски.

2. Сложности взаимодействия с аналоговыми структурами. Переход к цифровому государственному управлению может вызвать сопротивление и сложности интеграции с традиционными структурами, которые существовали ранее.

3. Ограниченность ресурсов. Внедрение и реализация цифровых технологий в государственное управление требует значительного ресурсного обеспечения, которое не все страны или регионы могут гарантировать.

4. Потеря доверия общества. Недостаточная защищенность, ошибки в работе с конфиденциальной информацией могут стать причиной потери доверия общества к государственному аппарату.

5. Угроза сокращения рабочих мест. Развитие робототехники может привести к сокращению рабочих мест и исчезновению ряда профессий.

В контексте цифровизации государственного управления серьезную угрозу безопасности персональных данных граждан и самих государственных структур представляет такое явление, как социальная инженерия в контексте информационной безопасности.

Социальная инженерия — это «метод, который злоумышленники используют для манипулирования людьми, чтобы заставить их разглашать конфиденциальную информацию» [6, с. 55]. Методы социальной инженерии используются киберпреступниками, чтобы «обойти меры безопасности, получить доступ к конфиденциальным данным и скомпрометировать системы» [6, с. 55]. Существует несколько типов угроз социальной инженерии.

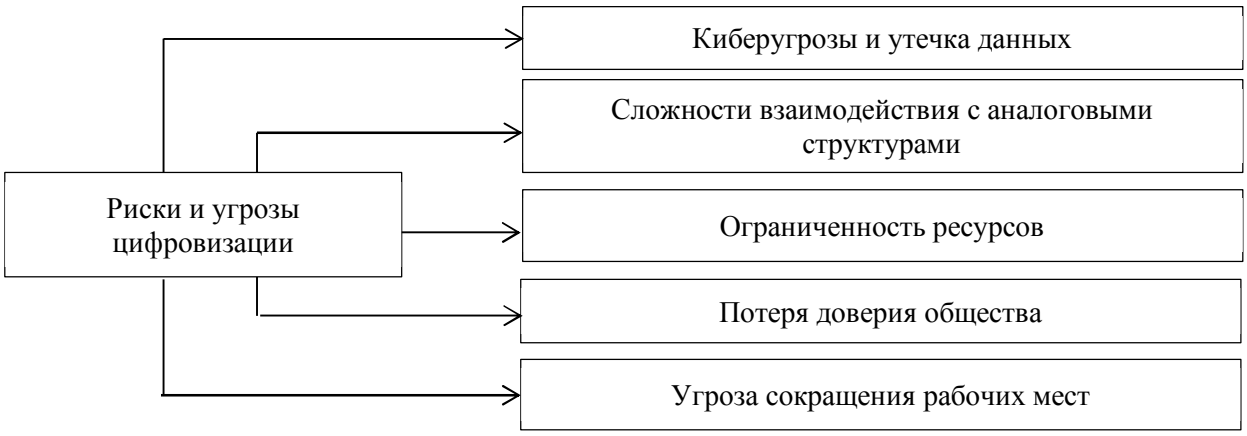

Рисунок 1 — Риски и угрозы, возникающие в процессе цифровизации государственного управления

Fhishing (фишинг) подразумевает, что злоумышленник через поддельное электронное письмо или сообщение выдает себя за представителя государственных служб, чтобы обманом заставить предоставить конфиденциальную информацию. Меры противодействия фишингу: проявлять бдительность при вводе логинов и паролей на сайтах, не открывать сомнительные файлы и/или ссылки в социальных сетях, мессенджерах и электронной почте.

Pretexting (приманка) как вид социальной инженерии заключается в том, что злоумышленник перед тем, как совершить атаку создаёт поддельный сценарий работы с жертвой. Например, может позвонить и представиться сотрудником государственной службы и запросить доступ к информации об учетной записи жертвы в ЕСИА. Основными способами защиты являются информирование населения через СМИ о возможных сценариях действий мошенников, создание черного списка номеров и их автоматическая блокировка, использование антифрод-платформ.

Baiting (травля) — злоумышленник предлагает жертве бесплатный подарок и вынуждает предоставить конфиденциальную информацию или перейти по вредоносной ссылке. Для борьбы с этим видом социальной инженерии рекомендуется информировать население об опасности заманчивых предложений и устройств, которые могут быть заражены вредоносным программным обеспечением, не переходить по подозрительным ссылкам.

Кви про кво (услуга за услугу) — злоумышленник предлагает жертве некую выгоду в обмен на конфиденциальную информацию. Например, бесплатная подарочная карта в обмен на данные от учетной записи пользователя банка.

Вредоносное программное обеспечение — пользователю представляются ложные сведения об угрозах компьютеру, чтобы побудить к установке вредоносного программного обеспечения.

Обратная социальная инженерия предполагает, что жертва проявляет доверие к незнакомому человеку и добровольно сообщает конфиденциальную информацию. Например, злоумышленник может представиться представителем техподдержки, а жертва, желая помочь, сама сообщает пинкоды, одноразовые пароли, которые будут использованы против нее.

В целом метод социальной инженерии отличается достаточной эффективностью, т. к. основан на человеческих эмоциях и склонностях, затрудняя выявление и обнаружение. Рассмотренный перечень типов угроз социальной инженерии не окончательный, существуют также плечевой серфинг, телефонный фишинг и фрикинг, смишинг, ловля «на живца», взлом электронной почты, троян и др. Методы социальной инженерии могут использоваться как по отдельности, так и в комплексе с другими методами. Таким образом с развитием информационных технологий увеличивается количество и совершенствуется качество угроз информационной безопасности как отдельного гражданина, так и общества, государства в целом.

Кроме угроз социальной инженерии существенную опасность в условиях цифровизации государственного управления представляют информационные риски. Под информационным риском следует понимать опасность возникновения ущерба, в результате применения информационных технологий.

К основным видам информационных рисков относятся: утечка персональных данных, нарушение конфиденциальности данных, экономические потери, угрозы национальной безопасности. Злоумышленники, получив доступ к персональным данным граждан (паспортные данные, сведения о доходах, имуществе и пр.), имеют возможность заниматься шантажом, вымогательством, побуждением к совершению жертвой действий, направленных против государства. В свою очередь, жертва будет нести не только финансовые потери, но и, возможно, уголовную ответственность.

В случае утечки конфиденциальных данных со стороны государственных структур,

возникает риск потери доверия со стороны граждан. Граждане будут опасаться пользоваться электронными услугами, что замедлит процесс цифровизации и снизит эффективность государственного управления.

Цифровые системы государственного управления могут содержать информацию стратегического значения. Если злоумышленники получат доступ к такой информации, это может нанести ущерб национальной безопасности страны. Атаки социальной инженерии могут привести к значительным экономическим потерям как для государства, так и для отдельных граждан. Мошеннические схемы, основанные на краже данных, могут привести к убыткам от несанкционированных транзакций или неправомерного использования финансовых ресурсов.

С целью предотвращения угроз социальной инженерии, а также минимизации информационных рисков необходимо реализовывать комплексный подход к обеспечению информационной безопасности в условиях цифровизации государственного управления.

Во-первых, информировать население и государственных служащих о принципах работы атак через социальную инженерию, обучать умению распознавать такие угрозы. Необходимо рассматривать примеры реальных случаев и прорабатывать алгоритмы поведения при подозрительных ситуациях.

Во-вторых, использовать многофакторную аутентификацию, которая позволяет защитить учетные записи при утечке паролей, путем запроса подтверждения личности (одноразовый код, биометрические данные и пр.).

В-третьих, осуществлять мониторинг и анализ поведения пользователей информационных систем, которые позволят предотвратить утечку данных и обнаружить потенциальные угрозы на ранних стадиях.

В-четвертых, использовать системы предотвращения утечек данных (Data Loss Prevention, DLP) — программные средства, процессы и методы защиты данных, которые помогают предотвратить несанкционированный доступ, неправильное использование или потерю конфиденциальных или критически важных данных. Применение DLP снижает вероятность того, что злоумышленник сможет использовать украденные данные для дальнейшего проникновения в систему.

В-пятых, внедрять современные стандарты шифрования данных с целью защиты информации от несанкционированного доступа.

В-шестых, регулярно осуществлять аудит и тестирование устойчивости систем и процессов, а также обновлять политики безопасности и адаптировать их под новые угрозы.

Предложенный комплексный подход подтверждает актуальность вопроса разработки мер противодействия и минимизации угроз информационной безопасности в условиях цифровизации государственного управления.

Заключение. Цифровизация государственного управления является одним из наиболее актуальных и важных направлений развития в современном мире. Внедрение цифровых технологий в функционирование государственного аппарата позволяет упростить и улучшить процессы взаимодействия государства и граждан, повысить эффективность работы органов власти, обеспечить более прозрачное и открытое управление.

Однако развитие цифровизации сопряжено с возникновением угроз социального инжиниринга и информационными рисками. Возникает реальная необходимость повышения осведомленности среди государственных служащих и населения о методах манипуляции и угрозах безопасности. В исследовании разработан комплексный подход мер противодействия и минимизации угроз социальной инженерии к обеспечению информационной безопасности в условиях цифровизации государственного управления. Реализация предложенных мер позволит снизить риски угроз социального инжиниринга. Тем не менее рекомендуется продолжать исследование и разработку мер противодействия угрозам, а также развитие систем быстрого реагирования на инциденты, связанные с утечкой данных.

Список источников

1. Цифровое государственное управление: вероятные риски и новые возможности / Е. А. Кипервар, Е. В. Мамай, М. С. Мизя, Е. А. Кипервар // Креативная экономика. 2020. Т. 14. № 10. С. 2223–2242. URL: https://elibrary.ru/item.asp?id=44385925 (дата обращения: 10.12.2024). DOI: 10.18334/ce.14.10.110882

2. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Российской Федерации от 09.05.2017 № 203. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687&rdk= (дата обращения: 10.12.2024).

3. Об утверждении программы «Цифровая экономика Российской Федерации» (утратило силу на основании распоряжения Правительства Российской Федерации от 12.02.2019 № 195-р) : распоряжение Правительства РФ от 28.07.2017 № 1632-р. URL: http://publication.pravo.gov.ru/Document/View/0001201708030016 (дата обращения: 10.12.2024).

4. Двоеглазова Е. А., Куракова Ч. М. Цифровизация государственного управления // Актуальные исследования. 2024. № 5 (187). Ч. I. С. 70–74. URL: https://apni.ru/article/8347-tsifrovizatsiya-gosudarstvennogo-upravleniya (дата обращения: 10.12.2024).

5. Шашкова Н. И. Цифровое государственное управление: роль, риски и новые парадигмы развития // Вестник экономики, права и социологии. 2023. № 3. С. 55–59. URL: https://rucont.ru/efd/891234 (дата обращения: 10.12.2024).

6. Козырь Н. С., Седых Н. В. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов. М. : Юрайт, 2024. 170 с. (Высшее образование). URL: https://urait.ru/bcode/544965 (дата обращения: 10.12.2024).

Рекомендована к печати к.э.н., доц. каф. менеджмента Кобзевой Е. В., начальником отдела молодежи и спорта Администрации городского округа город Брянка Грищенко А. Л.

Статья поступила в редакцию 15.03.2025.

СВЕДЕНИЯ ОБ АВТОРЕ

Бецан Дарья Олеговна, *старший преподаватель каф. менеджмента*
Донбасский государственный технический университет,
г. Алчевск, Россия,
e-mail: betsan.daria@yandex.ru

Betsan D. O. *(Donbass State Technical University, Alchevsk, Russia, e-mail: betsan.daria@yandex.ru)*

SOCIAL ENGINEERING AND INFORMATION RISKS IN THE PROCESS OF DIGITIZING PUBLIC ADMINISTRATION: MEASURES TO COUNTERACT AND MINIMIZE THREATS

The article is devoted to defining the role of social engineering and information risks related to digitizing public administration. The essence of digitizing public administration and the role it plays in developing the State is revealed. Identify and characterize the key risks and threats of social engineering that arise in the process of digitizing public administration. A comprehensive approach to countering and minimizing social engineering threats to information security in the context of digitizing public administration has been developed.

Key words: *digitization, public administration, social engineering, cyberthreats, information security.*

References

1. Kipervar E. A., Mamaj E. V., Mizya M. S., Kipervar E. A. Digital public gobernance: likely risks and new opportunities [Cifrovoe gosudarstvennoe upravlenie: veroyatnye riski i novye vozmozhnosti].

Creative Economy. 2020. Vol. 14. No. 10. Pp. 2223–2242. URL: https://elibrary.ru/item.asp?id=44385925 (date of treatment:10.12.2024). DOI: 10.18334/ce.14.10.110882

2. On the strategy for the development of information society in the Russian Federation for 2017–2030 : Decree of the President of the Russian Federation of 09.05.2017 No. 203. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687&rdk (date of treatment: 10.12.2024).

3. On Approval of the program "Digital economy of the Russian Federation" (lapsed on the basis of the order of the Government of the Russian Federation of 12.02.2019 No. 195-r) : Order of the Government of the Russian Federation of 28.07.2017 No. 1632-r. URL: http://publication.pravo.gov.ru/Document/View/0001201708030016 (date of treatment: 10.12.2024)

4. Dvoeglazova E. A., Kurakova Ch. M. Digitalization of public administration [Cifrovizaciya gosudarstvennogo upravleniya]. Actual researches. 2024. No. 5 (187). Part I. Pp. 70–74 URL: https://apni.ru/article/8347-tsifrovizatsiya-gosudarstvennogo-upravleniya (date of treatment: 10.12.2024).

5. Shashkova N. I. Digital public governance: role, risks and new development paradigms [Cifrovoe gosudarstvennoe upravlenie: rol', riski i novye paradigmy razvitiya]. The Review of Economy, the Law and Sociology. 2023. No. 3. Pp. 55–59. URL: https://rucont.ru/efd/891234 (date of treatment: 10.12.2024).

6. Kozyr' N. S., Sedyh N. V. Humanitarian aspects of information security : a textbook for universities [Gumanitarnye aspekty informacionnoj bezopasnosti : uchebnoe posobie dlya vuzov]. M. : Yurajt, 2024. 170 p. URL: https://urait.ru/bcode/544965 (date of treatment: 10.12.2024).

INFORMATION ABOUT THE AUTHOR

Betsan Daria Olegovna, *Senior lecturer of the Management Department*
Donbass State Technical University,
Alchevsk, Russia,
e-mail: betsan.daria@yandex.ru