6. Макарейко, Н. В. Государственное принуждение как средство обеспечения общественного порядка : дис. … канд. юрид. наук : 12.00.01 / Н. В. Макарейко. – Н. Новгород, 1996. – 249 л.

7. Мингес, А. В. Специальные меры административного пресечения: применение огнестрельного оружия, физической силы и специальных средств представителями исполнительной власти государства / А. В. Мингес ; МВД России ; Волгогр. юрид. ин-т. – Волгоград : Волгогр. юрид. ин-т МВД России, 1999. – 135 с.

8. Резвых, В. Д. Административно-правовая охрана социалистической собственности / В. Д. Резвых. – М. : Юрид. лит., 1975. – 168 с.

9. Тюрин, В. А. Проблемы применения мер пресечения в административном праве России : дис. … д-ра юрид. наук : 12.00.14 / В. А. Тюрин. – М. : ВНИИ МВД России, 2004. – 341 л.

10. Тюрин, В. А. Совершенствование законодательства о мерах административного пресечения / В. А. Тюрин // Соврем. право. – 2003. – № 3. – С. 25–29.

11. Ямпольская, Ц. Я. К методологии науки управления / Ц. Я. Ямпольская // Совет. государство и право. – 1965. – № 8. – С. 12–21.

Дата поступления в редакцию: 10.05.2022

УДК 342.9

М. В. Губич, *кандидат юридических наук, доцент, заместитель начальника кафедры информационного права факультета криминальной милиции Академии Министерства внутренних дел Республики Беларусь*
e-mail: gubichmv@yandex.by

ПРОБЛЕМНЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ СУЩНОСТИ И СОДЕРЖАНИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Представлен авторский концепт сущности и содержания социальной инженерии, аргументирована некорректность использования термина «социальная инженерия» для обозначения способа совершения хищений, характеризующегося применением злоумышленником информационно-коммуникационных технологий и технологий психологического воздействия на жертву для получения конфиденциальных сведений и (или) склонения жертвы к осуществлению действий, необходимых для завладения предметом преступного посягательства. Обоснована необходимость введения термина «скамминг», используемого для лексического обозначения преступлений, совершенных указанным способом.

Ключевые слова: социальная инженерия, угроза информационной безопасности, скамминг, скаммер, обеспечение национальной безопасности.

M. V. Gubich, *Candidate of Juridical Sciences, Associate Professor, Deputy Head of the Department of Information Law of the Faculty of Criminal Militia of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*
e-mail: gubichmv@yandex.by

PROBLEMATIC ASPECTS OF THE DEFINITION THE ESSENCE AND CONTENT OF SOCIAL ENGINEERING IN THE CONTEXT OF INFORMATION SECURITY

The author's concept of the essence and content of social engineering is presented, the incorrectness of using the term «social engineering» to denote a method of committing theft characterized by the use of information and communication technologies and technologies of psychological influence on the victim by the attacker to obtain confidential information and (or) incline the victim to perform actions necessary to seize the subject of criminal encroachment is argued. The necessity of introducing the term "scamming", used for lexical designation of crimes committed in this way, is substantiated.

Keywords: social engineering, threat to information security, scamming, scammer, ensuring national security.

Классический подход к построению системы защиты информации включает в себя правовые, организационные и технические меры, комплекс которых позволяет обеспечивать безопасность систем и информационных ресурсов. Однако в цепочке «человек – машина» слабым звеном

часто является человек. У машины нет эмоций, присущих человеку пороков и слабостей, у всех людей разные темперамент и интеллект. Наличие указанных и иных «уязвимостей» человека обусловило появление такого нового направления в обеспечении информационной безопасности, как противодействие социальной инженерии. Наукой и практикой до настоящего времени не выработаны единые подход и понимание социальной инженерии как угрозы информационной безопасности, что препятствует организации системного противодействия рассматриваемой деятельности. В этой связи полагаем актуальным представить авторский концепт сущности и содержания социальной инженерии.

Общеизвестно, что методы социальной инженерии в той или иной степени использовались в военных, политических и иных целях на протяжении всей истории человечества. Во все времена были востребованы люди, способные вести дипломатические переговоры, склонить собеседника на свою сторону или ввести в заблуждение. Однако в научном лексиконе данный термин закрепился сравнительно недавно. По мнению К. Поппера, одного из теоретиков социальной инженерии, рассматриваемый термин был впервые введен в 1922 г. Р. Паундом в работе «Введение в философию права» [6, с. 87]. При этом сам К. Поппер понимал социальную инженерию как «поэлементную» деятельность по проектированию новых и по перестройке и управлению уже существующими социальными институтами, осуществляемую путем частичных, постепенных реформ и изменений [5, с. 75–83].

В научной литературе периода СССР исследуемый термин начинает встречаться в начале 1970-х гг. в трудах с критикой западной социологии и социальной психологии. В 80-х гг. XX в. советские исследователи в своих работах используют аналогичные по смыслу термины – «социоинженерная деятельность» и «социальный инженеризм», полагая при этом, что социальная инженерия – это наука точных измерений, формул, чертежей, основанная на применении математических методов к изучению социальных, экономических, психофизиологических проблем производства. Следовательно, основной сферой прикладного применения достижений социальной инженерии в данный период являлось повышение эффективности производства, но не за счет усовершенствования орудий труда, а в результате повышения качества управления персоналом предприятия, достигаемого посредством внедрения инженерного подхода при применении социологических и психологических методов воздействия [4, с. 13].

В исследованиях западных ученых второй половины XX в. понятие «социальная инженерия» трактуется более широко – предлагается ее применение в управлении как отдельным предприятием, корпорацией, так и государством, а некоторыми учеными положения социальной инженерии разрабатываются применительно к достижению политических целей [8].

Однако и западные, и советские исследователи сходились в одном – управление социальной группой (работники предприятия, корпорации или целое государство) необходимо осуществлять комплексно, используя достижения как социологии и психологии, так и точных наук. Таким образом, термин «социальная инженерия» стал символическим выражением внедрения технического подхода в социальную область и им обозначалась особая деятельность, ориентированная на целенаправленное изменение и регулирование различных организационных структур (социальных институтов, формальных организаций и др.), определяющих человеческое поведение и обеспечивающих контроль за ним.

В сфере информационной безопасности социальная инженерия является собирательным термином и применяется для обозначения социопсихологических манипуляций, используемых злоумышленниками для получения доступа к защищенным системам с целью кражи информации, паролей, данных о банковских платежных карточках и т. п. При этом специалисты в сфере кибербезопасности таких злоумышленников называют социальными инженерами.

Представляется возможным подвергнуть критике применение терминов «социальная инженерия» и «социальный инженер» в указанном выше контексте. По нашему мнению, деятельность злоумышленников, направленная на завладение защищаемыми сведениями в целях личного обогащения, не может быть признана ни наукой, ни искусством. Да и самих злоумышленников в данном контексте называть социальными инженерами является некорректным.

Семантический анализ слова «инженерия» показал, что оно происходит от латинского слова ingeniosus – «искусный» [3], в «Толковом словаре русского языка» С. И. Ожегова, Т. В. Ефремовой указанное слово толкуется как инженерное дело, творческая техническая деятельность,

конструирование [2], в англоязычной лексике им обозначается область человеческой интеллектуальной деятельности, дисциплина, профессия, задачей которой является применение достижений науки, техники, использование законов физики и природных ресурсов для решения конкретных проблем, достижения целей и выполнения задач человечества. Инженерное дело реализуется через применение как научных знаний, так и практического опыта (инженерные навыки, умения) с целью создания (в первую очередь проектирования) полезных технологических и технических процессов и объектов, которые реализуют эти процессы [3].

Люди, которые постоянно и профессионально практикуют инженерию, называются инженерами. Инженер – это лицо, имеющее соответствующее образование и квалификацию, способное разработать и реализовать инженерную идею, которая выражается в создании некоего материального объекта. При этом для того чтобы стать, например, инженером-конструктором, необходимо пройти достаточно сложный путь, начиная с общеобразовательной подготовки (письмо, чтение, математика, физика, информатика и т. д.), получить знания в области черчения, разобраться в устройстве механизмов и уже только после этого освоить учебные дисциплины специализации подготовки инженера, чтобы далее на протяжении всей своей профессиональной деятельности самосовершенствоваться.

Деятельность злоумышленника направлена на получение личной выгоды за счет причинения вреда иным лицам. При этом его временны́е и интеллектуальные затраты, необходимые для осуществления злонамеренных действий, не идут ни в какое сравнение с подготовкой инженера (за исключением ничтожной доли действительно профессиональных преступников). Исследование материалов правоохранительных органов, касающихся лиц, подозреваемых в совершении преступлений, показывает, что в абсолютном большинстве случаев преступник неоднократно применял одну известную ему психологическую манипуляцию (которую, как правило, даже не сам придумывал, а узнал, общаясь в закрытых группах интернет-мошенников, или же купил соответствующую схему действий в даркнете), оказывая воздействие на жертву (при этом для применения манипуляции наличия у преступника высшего образования, а тем более инженерного, не требуется). Такая манипуляция, по своей сути, является технологией, которая может быть алгоритмизирована, расчленена на отдельные процедуры и операции, не требующие значительных затрат интеллектуального труда.

Таким образом, в качестве промежуточного итога представляется возможным заключить, что произошедшая диффузия использования термина «социальная инженерия» привела к размытию терминологической границы его применения. В этой связи, опираясь в том числе на исследования, посвященные динамике развития и возникновению новых научно-технических терминов [7], предлагаем ввести в научно-практический лексикон термин «скаммер» (от англ. scam – мошенничество, жульничество, обман), которым следует обозначать злоумышленника, использующего в преступных целях приемы психологических манипуляций, совершаемых с применением информационно-коммуникационных технологий. Способ совершения таких преступлений следует именовать скаммингом.

Высказанное предложение о введении в оборот данных англоязычных терминов не является категоричным и требует дальнейшего научного осмысления. Однако представляется необходимым лексическое выделение в самостоятельную категорию преступников-скаммеров и непосредственно скамминга. К тому же обзор публикаций и тематических форумов показал, что данные термины уже используются в профессиональном сленге сотрудников правоохранительных органов, специалистов в сфере обеспечения информационной безопасности и сами лица, вовлеченные в данный вид деятельности, называют себя скаммерами. Кроме того, предлагаемое выделение обусловлено потребностью разграничения «зон ответственности» и полномочий субъектов обеспечения информационной безопасности.

В целях раскрытия сущности скамминга и уточнения его отличий от социальной инженерии целесообразно кратко изложить особенности механизма совершения скамминг-преступлений, который включает в себя следующие значимые для целей настоящего исследования элементы: субъекта, совершающего заранее спланированные противоправные действия; дистанционные способы достижения преступного результата; обстановку преступления, образованную виртуальной средой; предмет преступного посягательства; потерпевшее лицо.

Личность скаммера характеризуется в первую очередь наличием определенных знаний и практических навыков в области психологии, использования информационно-коммуникационных технологий, в том числе технологий создания фишинговых сайтов, поиска персональных данных потенциальных жертв и иной конфиденциальной информации в открытых источниках, и др.

Способы достижения преступного результата постоянно совершенствуются. В этой связи невозможно представить их исчерпывающий перечень, но для целей исследования способы можно разделить на прямой скамминг и обратный. В первом случае деятельность злоумышленника направлена на введение жертвы в заблуждение и побуждение к выполнению необходимых для скаммера действий. Обратный скамминг также характеризуется активностью злоумышленника, однако она направлена на создание у жертвы таких обстоятельств (или их видимости), при которых она инициативно связывается со скаммером и выполняет действия в его интересах.

Обстановка совершения скамминг-преступлений образуется виртуальной средой и дистанционностью данных деяний. При этом как виртуальность среды, так и дистанционность определяются неотъемлемым признаком скамминга – использованием информационно-коммуникационных технологий, посредством которых создается виртуальный мир, где взаимодействие между преступником и жертвой осуществляется удаленно.

Истинный предмет посягательства скаммера совпадает с предметом хищений (различные материальные ценности во всем своем многообразии, наличные или безналичные деньги, товары и т. д.), однако непосредственным предметом посягательства могут выступать логины и пароли, проверочные слова, карты кодов, аккаунты, иная информация, необходимая злоумышленнику для завладения истинным предметом.

Результаты пилотного опроса сотрудников правоохранительных органов показали, что потерпевшими от скамминга становились лица вне зависимости от социального статуса, профессии, образования и возраста. В основном это излишне доверчивые и беспечные люди с низким уровнем финансовой и правовой грамотности, в отношении же других лиц обязательным условием достижения необходимого преступнику результата являлось создание у потерпевшего соответствующего психического состояния (спешка, нервозность и т. п.).

В этой связи сформулируем основные признаки скамминга. Это способ совершения ненасильственного преступления против собственности, характеризующийся применением злоумышленником информационно-коммуникационных технологий и технологий психологического воздействия на жертву с целью получения конфиденциальных сведений и (или) склонения жертвы к осуществлению действий, необходимых для завладения скаммером предметом преступного посягательства.

Вместе с тем применение социопсихологических средств воздействия, в том числе с использованием информационно-коммуникационных технологий, в целях склонения людей к осуществлению действий в интересах воздействующего субъекта, имеет место не только в общеуголовной практике. По нашему мнению, использование термина «социальная инженерия» более уместно в контексте социального конструирования, социального моделирования и проектирования как обозначение инструмента рационального воздействия на социальные явления и процессы. Иначе говоря, термин «социальная инженерия» следует использовать для обозначения значительно большей по своему масштабу деятельности, нежели скамминг.

Во-первых, социальная инженерия используется при осуществлении государственного управления, так как для достижения его целей все более значимыми становятся эффективность воздействия на личность и социальную группу. Это достигается использованием социально-психологических методов, в том числе посредством информационно-коммуникационных технологий [1]. С их помощью формируются социальные установки, ценностные ориентации, групповое сознание. В данном понимании социоинженерная деятельность сопряжена с реализацией всех традиционно выделяемых функций управления – планирования, программирования, организации, координации и контроля. Сфера ее применения не ограничивается подготовкой управленческих решений. Она включает в себя такие управленческие задачи, как выбор стратегии развития, экспертная оценка принимаемых решений, управленческое консультирование, контроль за внедрением социальных новшеств и др. [6, с. 90]. В этой связи использование термина «социоинженерная деятельность» в качестве инструмента государственного управления согла-

суется с классическим подходом к пониманию рассматриваемой деятельности представителями социологических и психологических наук.

Во-вторых, методы социальной инженерии могут применяться и в деструктивных целях. Так, в выступлениях глав государств, политиков и общественных деятелей звучат высказывания о применении посредством информационно-коммуникационных технологий методов манипулирования сознанием населения в целях формирования определенного, как правило, негативного, отношения к политике государства, в том числе и к правоохранительным органам. Эффективность таких воздействий подтверждается чередой событий, произошедших в недавней мировой истории: Бульдозерная революция (Югославия, 2000 г.), Революция роз (Грузия, 2003 г.), Оранжевая революция (Украина, 2004 г.), Революция тюльпанов (Кыргызстан, 2005 г.), Евромайдан (Украина, 2013–2014 гг.) и т. д. При этом технологии «цветных» революций так же, как и скамминга, постоянно совершенствуются, однако объекты, цели, средства и методы у субъектов рассматриваемых воздействий разнятся.

Среди направлений использования методов социоинженерной деятельности в деструктивных целях также можно выделить распространение идеологии экстремизма, расизма, АУЕ («арестантский уклад един» или «арестантское уркаганское единство»), навязывание искусственных ценностей, вовлечение в деструктивные культы и секты и т. д.

В противовес указанным и иным деструктивным воздействиям субъектами обеспечения национальной безопасности осуществляется комплекс ответных действий: информационное противоборство, контрпропаганда, правовое просвещение и морально-нравственное воспитание отдельных сегментов общества, что также следует причислить к социальной инженерии.

В связи с тем что перечисление всех направлений использования и возможного применения социоинженерных знаний не является целью настоящего исследования, представляется возможным изложить его основные выводы.

Анализ сущности и содержания термина «социальная инженерия» показал, что произошедшая диффузия его одновременного использования в сфере социопсихологических наук и в сфере обеспечения информационной безопасности привела к размытию терминологической границы его применения.

По нашему мнению, некорректным является использование термина «социальная инженерия» для обозначения способа совершения ненасильственных преступлений против собственности, характеризующегося применением злоумышленником информационно-коммуникационных технологий и технологий психологического воздействия на жертву для получения конфиденциальных сведений и (или) склонения жертвы к осуществлению действий, необходимых для завладения предметом преступного посягательства.

В целях лексического выделения в отдельную категорию данного способа совершения ненасильственных преступлений против собственности видится возможным использовать для его обозначения термин «скамминг», а преступника, осуществляющего преступные деяния данным способом, именовать скаммером.

Помимо решения теоретической задачи лексического определения указанного способа совершения преступлений введение в научно-практический лексикон терминов «скамминг» и «скаммер» обусловлено удобством их использования, в том числе при определении компетенций субъектов обеспечения информационной безопасности. Так, противодействие скаммингу является «зоной ответственности» органов внутренних дел, в то время как организация противодействия деструктивной деятельности (например, «цветным» революциям), осуществляемой с использованием социальной инженерии, входит в компетенцию иных субъектов обеспечения национальной безопасности.

Социальная инженерия как деятельность, заключающаяся в применении социопсихологических средств воздействия, в том числе с использованием информационно-коммуникационных технологий, в целях склонения людей к осуществлению действий в интересах воздействующего субъекта, может быть рассмотрена как позитивная и деструктивная. К позитивной социоинженерной деятельности следует относить ее осуществление в целях государственного управления, а также для достижения иных общественно значимых результатов. Деструктивным является использование методов социальной инженерии для достижения противоположных результатов, создающих угрозу национальной безопасности.

Процесс становления новой научной терминологии, обусловленный развитием информационно-коммуникационных технологий, требует к себе внимательного отношения. В этой связи представленный авторский концепт сущности и содержания социальной инженерии не претендует на окончательную завершенность и требует дальнейшего всестороннего изучения.

Список использованных источников

1. Воропаев, Д. А. Блогер как агент правовой социализации / Д. А. Воропаев // Вестн. Акад. МВД Респ. Беларусь. – 2021. – № 2. – С. 48–53.

2. Инженерия [Электронный ресурс] // GUFO.ME. – Режим доступа: https://gufo.me/dict/ozhegov/инженерия. – Дата доступа: 23.12.2021.

3. Инженерия [Электронный ресурс] // Словари и энциклопедии на Академике. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/940092. – Дата доступа: 23.12.2021.

4. Кравченко, А. И. Социальный инженеризм в эпоху советской власти (статья вторая) / А. И. Кравченко // Социология. – 2017. – № 2. – С. 3–14.

5. Поппер, К. Р. Нищета историцизма : пер. с англ. / К. Р. Поппер. – М. : Прогресс – VIA, 1993. – 187 с.

6. Резник, Ю. М. Социальная инженерия: предметная область и границы применения [Электронный ресурс] / Ю. М. Резник // Книгогид. – Режим доступа: https://knigogid.ru/books/1780483-socialnaya-inzheneriya-predmetnaya-oblast-i-granicy-primeneniya. – Дата доступа: 23.12.2021.

7. Романенко, В. Н. Динамика развития научно-технических терминов. Возникновение новых терминов / В. Н. Романенко, Г. В. Никитина // Вестн. СПбГУ. Сер. 12. – 2010. – Вып. 3. – С. 80–89.

8. Шарп, Д. От диктатуры к демократии: стратегия и тактика освобождения / Д. Шарп ; пер. с англ. Н. Козловской. – М. : Новое изд-во, 2005. – 84 с.

Дата поступления в редакцию: 03.01.2022

УДК 341

К. Д. Сазон*, кандидат юридических наук, доцент,*
начальник кафедры конституционного и международного права
Академии Министерства внутренних дел Республики Беларусь,
e-mail: KSazon@list.ru

КОНСТИТУЦИОННАЯ МОДЕРНИЗАЦИЯ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ РЕСПУБЛИКИ БЕЛАРУСЬ

Рассматриваются особенности обеспечения национальных интересов Республики Беларусь в контексте конституционной модернизации. На примере обновления положений Основного Закона, затрагивающих правовой статус Президента, Парламента, Совета Безопасности Республики Беларусь, обосновывается их значение для повышения эффективности функционирования государственного аппарата, предлагаются направления отраслевой юридизации конституционных нововведений.

Ключевые слова: Конституция, модернизация, национальные интересы, национальная безопасность, статус.

K. D. Sazon*, Candidate of Juridical Sciences, Associate Professor, Head of the Department*
of Constitutional and International Law of the Academy of the Ministry of Internal Affairs of the Republic of Belarus
e-mail: KSazon@list.ru

CONSTITUTIONAL MODERNIZATION IN THE CONTEXT OF ENSURING NATIONAL INTERESTS OF THE REPUBLIC OF BELARUS

The article examines the peculiarities of ensuring the national interests of the Republic of Belarus in the context of constitutional modernization. On the example of updating the provisions of the Constitution affecting the legal status of the President, Parliament, Security Council of the Republic of Belarus, their importance for improving the efficiency of the functioning of the state apparatus is substantiated, the directions of sectoral legalization of constitutional innovations are proposed.

Keywords: Constitution, modernization, national interests, national security, status