И. Р. Бегишев,
доктор юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Д. Д. Берсей,
кандидат юридических наук, доцент,
Северо-Кавказский федеральный университет

ГЕНЕЗИС КРИМИНАЛЬНОЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. В статье рассмотрены основные определения, а также этапы развития понятия «социальная инженерия». Определено, что на разных исторических этапах сущность данного понятия претерпевала изменение под влиянием тех или иных факторов, соответственно, объем понятия постепенно изменялся и расширялся. Установлено, что социальная инженерия заключена в применении различных технологий, позволяющих злоумышленнику организовать незаконное вторжение в информационную систему и завладеть необходимой цифровой информацией. Утверждается, что социоинженерные атаки стали настолько сложными, что могут сравниться по степени внедрения с техническими типами атак.

Ключевые слова: социальная инженерия, злоумышленник, социоинженерная атака, фишинг, киберпреступление, уголовное право, кибератака

THE GENESIS OF CRIMINAL SOCIAL ENGINEERING

Abstract. The article discusses the main definitions, as well as the stages of development of the concept of “social engineering”. It is determined that at different historical stages the essence of this concept underwent a change under the influence of various factors, respectively, the scope of the concept gradually changed and expanded. It is established that social engineering consists in the use of various technologies that allow an attacker to organize an illegal intrusion into an information system and seize the necessary digital information. It is argued that socioengineering attacks have become so complex that they can be compared in terms of the degree of implementation with technical types of attacks.

Keywords: social engineering, attacker, socioengineering attack, phishing, cybercrime, criminal law, cyberattack

Введение. На современном этапе ключевым фактором обеспечения работы любой компании выступает информационная безопасность. Информационная безопасность – это защита информации от широкого спектра угроз в целях обеспечения устойчивости и работоспособности бизнеса, минимизации бизнес-рисков и максимизации прибыли [1]. В этой связи руководству компаний необходимо регулярно инвестировать в технологии информационной безопасности, так как злоумышленники постоянно анализируют возможности организации информационной защиты крупных и средних организаций с целью получить несанкционированный доступ к тому или иному массиву информационных данных.

Однако необходимо учитывать, что не только посредством организации эффективной системы информационной защиты можно обезопасить конфиденциальные данные. Достаточно важно обеспечить такую защиту и с учетом человеческого фактора, который считается самым слабым звеном в информационной системе и в системе безопасности [2].

Одной из основных угроз информационной безопасности организации является рост числа инцидентов, связанных с применениями социоинженерных технологий – криминальной социальной инженерии.

Социальная инженерия заключена в применении различных социальных технологий, позволяющих социальному инженеру организовать незаконное вторжение в информационный массив жертвы [3]. Данная технология позволяет избежать технических манипуляций, связанных со взломом системы безопасности.

Основная часть. Уже к концу 2007 года методы социальной инженерии широко использовались инсайдерами для совершения электронных преступлений, при этом пользователи, выступившие «проводниками» к данным, не до конца осознали свою роль в этом процессе.

Согласно Оксфордскому словарю английского языка, термин «социальная инженерия» имеет два различных значения [4]. Во-первых, это «использование централизованного планирования в попытке управлять социальными изменениями и регулировать будущее развитие и поведение общества». Во-вторых, это «использование обмана для того, чтобы побудить человека разгласить частную или другую информацию и невольно обеспечить несанкционированный доступ к компьютерной системе или сети».

В обоих определениях имеет место индивид, который индуцирует поведение со стороны других, однако, если первое определение чаще может использоваться в области политического и экономического управления, то второе используется исключительно в сфере киберпространства.

Следующие определения социальной инженерии иллюстрируют, что не существует единого, широко принятого определения. В частности, данное понятие в разных источниках определяется следующим образом:

– «социально-психологический процесс, с помощью которого индивид может получить информацию от человека о целях организации» [5];

– «вид нападения на человеческий элемент, в ходе которого нападающий психологически склоняет потерпевшего разглашать информацию» [6];

– «использование социальных маскировок, культурных уловок и психологических трюков, чтобы заставить пользователей компьютеров помогать хакерам в их незаконном вторжении или использовании компьютерных систем и сетей» [7];

– «искусство получения доступа к защищенным объектам путем использования человеческой психологии без взлома информационной системы» [8];

– «атака, в которой злоумышленник использует человеческое взаимодействие для получения информации об организации или ее компьютерной системе» [9];

– «процесс, в котором злоумышленник пытается получить информацию о сети и компьютерной системе с помощью социальных средств» [10];

– «метод обмана, используемый хакерами для получения информации или данных о компании» [11];

– «нетехнический вид вторжения, который в значительной степени зависит от человеческого взаимодействия и часто связан с обманом других людей, цель которого – нарушить обычные процедуры безопасности» [12];

– «хакерская манипуляция человеческой склонностью доверять другим людям для получения информации, которая позволит осуществлять несанкционированный доступ к системам» [13];

– «наука искусного маневрирования людьми для получения личной информации» [14];

– «под социальной инженерией в контексте информационной безопасности имеется в виду искусство манипулирования людьми с целью совершения действий, связанные с получением или разглашением конфиденциальной информации» [15];

– «акт манипулирования человеком или людьми с целью совершения какого-либо действия с информацией» [16].

Также социальная инженерия была определена как «наука об использовании социальных взаимодействий, цель которых – убедить индивида выполнить конкретное задание злоумышленника, при этом, диалог осуществляется посредством социальных сетей» [17]. Есть мнение, что социальная инженерия – это техника, которая используется для взаимодействия с людьми с целью получения информации для достижения той или иной цели. На практике социальная инженерия может быть мощным инструментом в руках человека, который знает, как использовать ее методы наиболее эффективно [18]. Социальная инженерия бросает вызов безопасности всем людям сети, независимо от надежности их брандмауэров, методов криптографии, способов обнаружения вторжений в систему и антивирусных программных комплексов [19].

Впервые термин «социальный инженер» появился в книге 1842 г. под названием «эффективный инженер». Британским экономистом Дж. Греем было написано «лекарство от бедственного положения народов».

В 1891 г. норвежско-американский экономист Т. Веблен опубликовал эссе под названием «Некоторые забытые моменты в теории социализма», где он предпринял попытку найти ответ на вопрос, является ли современная экономика перспективной, и можно ли ее перестроить в соответствии с идеями экономистов-социалистов.

Т. Веблен отметил, что эта возможность является практическим вопросом «конструктивного характера», некоей «социальной инженерией», а не изначально логическим или теоретическим соображением, и по этой причине выразил свой глубокий скептицизм по поводу его успеха [20]. Самому термину «социальная инженерия» Т. Веблен не посчитал нужным дать определение. Тем не менее из контекстного употребления термина Т. Вебленом следует, что в основе социальной инженерии лежат социальные манипуляции.

Дж. Аддамс, американский социальный работник, активист, общественный деятель и реформатор, применил термин «социальная инженерия» в 1914 г. к попыткам европейских правительств принять политику социального страхования и бирж труда в рамках борьбы с безработицей [21].

Подобно Т. Веблену, Дж. Аддамс подчеркивала взаимосвязь между знанием и эффективностью политики, отмечая, что с женщинами следует консультироваться, прежде чем приступать к публичным выступлениям. Она приводит пример, иллюстрирующий прения в британском парламенте, в котором принимают участие исключительно представители мужского пола по поводу того, следует ли сделать незаконным производство детской пижамы из якобы легковоспламеняющегося материала, тогда как любая женщин того времени, как сардонически замечает Дж. Аддамс, могла бы сказать участникам прений, что таких пижам не существует [22].

К 1929 г. эта концепция привлекла внимание юристов [23], в то время как Великая Депрессия и эпоха нового курса обеспечили ее динамичное развитие среди научного сообщества в целом. Например, в 1937 г. Дж. Дэвис высказал мнение, что «социальную инженерию» необходимо считать новой академической дисциплиной на том основании, что прикладные социологи смогут «обуздать социальные приливы и отливы», используя растущий объем статистических данных и применяя передовые технологии в сочетании с социальными научными методами [24]. Дж. Дэвис писал: «Я вижу признаки необходимости применения результатов исследований социальных инженеров, которые не только планируют и исполняют, но разрабатывают конструктивные планы для успешного исполнения, а также социальных врачей, которые будут не только выписывать и лечить, но и реально лечить социальные болезни» [25]. Как и врачи, утверждал Дж. Дэвис, эти социальные инженеры обладают специализированными знаниями, необходимыми для манипулирования обществом различными способами.

Также в рассматриваемый период этнографы использовали этот термин для описания властных отношений между завоевателем и покоренными племенами в Африке. Например, в 1938 г. британский антрополог М. Рид использовала термин «социальная инженерия» для описания того, как завоеватели Нгони из Ньясаленда (ныне Малави) подчинили себе, а затем принудили их к исполнению своих обязанностей. М. Рид отметила, что эта социальная инженерия включает в себя значительное количество манипуляций в области государственного строительства, планирования и модификации социальных институтов, которая находилась под эгидой Нгони.

До начала 1940 гг. концепция социальной инженерии уже эксплицитно содержала две фундаментальные идеи, сохраняемые в ней и по сей день. Первая из них – это эпистемическая асимметрия, которая происходит от греческого слова эпистема (ἐπιστήμη) – «знание». Эпистемическая асимметрия возникает, когда один человек или группа наслаждается значительным преимуществом знаний над другим человеком или группой в пределах определенной области. Дж. Грей, Т. Веблен, Дж. Аддамс подчеркивали, что специализированные знания необходимы для успешной социальной инженерии в области экономики и планирования. Однако они по-разному оценивали успех применения таких знаний, но это было вызвано не несовместимыми представлениями о том, что требуется для социальной инженерии, а тем, что необходимо для ее осуществления.

Второй стала идея технократического доминирования, которая тесно связана с вышеупомянутой асимметрией. Технократ обычно обладает техническими

знаниями или навыками в той или иной области, например, в экономическом планировании или стоматологии. Технократическое доминирование возникает, когда лицо или группа, обладающие высокой степенью технических знаний, используют эти знания для осуществления изменения в поведении других людей, когда такое поведение ставит затронутых в положение снижение власти или авторитета по отношению к первому в пределах затронутой области.

Дж. Дэвис высказывал мнение о том, что технократы как в государственном, так и в частном секторах могут вылечить болезни общества с помощью реализация политики в отношении ничего не подозревающих (но, надеюсь, благодарных) граждан.

После успеха Манхэттенского проекта (1942–1946 гг.) динамичное развитие получили различные разработки в области кибернетики, которое связывалось с управлением процессами в живом организме или в машине. Это движение принесло с собой растущий оптимизм в успехе, связанном с развитием политики социальной инженерии и основанном на представлении о человечестве, которое было специально создано для амбициозных форм социального планирования.

Человеческий разум понимался как машина Тьюринга, с двумя «роботизированными механизмами обратной связи», что позволяло выполнить теоретико-игровой анализ человеческого поведения. В этом контексте социальная инженерия является просто технологией разработки правил игры, чтобы вызвать к жизни желаемую человеческую реакцию. Указанный оптимизм распространялся далеко за пределы планирования государственной политики [26].

В 1954 году социальная инженерия получила развитие в связи с выходом работы Рона Хаббарда «Введение в Саентологию». В данном труде рассматриваемое понятие получило уже прикладное значение, однако его основные элементы остались неизменными. Это произошло в рамках внедрения субкультуры «телефонного фрикинга», которую многие специалисты считают началом современной хакерской культуры. Телефонные фрикеры использовали свои растущие технические знания о возможностях управления сетями телефонной системы (схемах, переключателях, реле, тональных сложностях и пр.). Знание возможностей управления телефонными сетями давало фрикерам возможность захватить телефонную систему и использовать ее в своих собственных целях. При этом они могли подключиться к иностранным конференц-звонкам или получить доступ к рассматриваемым областям сети, где запрещено использование обычных телефонных протоколов.

Так, один из родоначальников телефонного фрикинга, Дж. Дрейпер отмечал, что часто он и его друг, и коллега, Деннис Дэн, использовали методы социальной инженерии, чтобы получить необходимую информацию от ничего не подозревающих сотрудников Bell Telephone.

Дрейпер описал социальную инженерию как «способность входить и разговаривать с людьми внутри телефонной компании ... они верят, что вы работали на телефонную компанию».

Телефонные фрикеры изменили понятие социальной инженерии, однако основные элементы понятия они не изменили. Перед телефонным фрикингом термин

«социальная инженерия» применялась только к деятельности влиятельных политических планировщиков, которые выступали за применение социальной инженерии для лечения социальных болезней.

В 1960-е и 1970-е гг. имело место бурное технологическое развитие вычислительной техники и технология. Интерактивные вычисления, совместное использование времени, аутентификация пользователя, общий доступ к файлам через иерархический файл, структуры и прототипы компьютерных утилит – все это было частью волны технических инноваций в мире.

Наряду с этой волной появились относительно простые инструменты безопасности, такие как контроль доступа и пароли. Следующее десятилетие ознаменовалось появлением локальных вычислительных сетей (LANs), пакетные сети (ARPANET) и объектно-ориентированного проектирования, криптографических приложений, такие как криптография с открытым ключом, криптографии и криптографического хэширования. Это повысило осознание безопасности как необходимой характеристики информационных систем, что привело к применению математических моделей безопасности и первым демонстрациям доказуемо безопасных систем [27].

По мере того, как эти технические меры безопасности становились все более изощренными, хакеры, которые были естественным порождением сообщества телефонных фрикеров, стали больше использовать нетехнические манипуляции.

В 1984 г. термин «социальная инженерия» появился в анонимной статье в начале XX в. Статья была названа «Жизненно важные ингредиенты: коммутационные центры и операторы», в ней присутствовало описание социальной инженерии как технологии, способной посредством убеждений заставить кого-то раскрыть ту или иную информацию. Однако автор негативно отзывался о таких возможностях социальной инженерии и называл это явление абсурдом.

В конце 80-х-начале 90-х гг. XX в. оптимизм по поводу успеха социального планирования пошел на убыль, концепция же применения социальной инженерии стала пользоваться популярностью в обществе. В этот период исследователи проявляли высокий интерес к категории «социальная инженерия» и описывают попытки применить в рамках этого понятия разнообразные техники манипулирования [28].

Рост количества атак в рамках социальной инженерии породил плодотворные научные исследования и позволил обобщить основные принципы социальной инженерии на основе поведения и восприимчивости из его участников [29]. Такая работа была основана на методах экспериментальной психологии для выявления факторов, повышающих вероятность социального успех инженера против жертвы. Например, классические принципы Р. Чалдини – взаимность, приверженность и последовательность, социальное доказательство, симпатия, авторитет и дефицит – действуют как независимые переменные, которые индивидуально или через их взаимодействие объясняют склонность индивида позволить эксплуатировать себя человеком-манипулятором. Особенно уязвимыми в данной связи являются доверчивые личности, позиционирующие манипулятора как как авторитет и готовые ему подчиниться. Такие психологические объяснения были разумны, когда

парадигмой была социальная инженерия от человека к человеку. Однако с развитием искусственного интеллекта получает развитие автоматизированная социальная инженерия, и попытки объяснить аспекты социальной инженерии только возможностью успешного контакта человека с человеком утратят актуальность. В частности, применение ботов, которые активно изменяют среду социальных сетей без участия человека-злоумышленника, – это одно их новых направлений развития социальной инженерии [30].

В 2000-е гг. XX в. возникло мнение, что социальная инженерия может позиционироваться как тактика, которая разыгрывается по-разному в зависимости от конкретной формы, принимаемой атакой. Это позволяет отграничить такие атаки между собой.

В частности, олицетворение может быть использовано в попытке собрать аутентификационную информацию (например, имена пользователей и пароли) для получения доступа к целевой сети [31]. Так, используя приложение смартфона, злоумышленник может связаться с жертвой, которая идентифицирует его с сотрудником IT-отдела, проводящего опрос сотрудников из-за недавнего взлома имени пользователя и пароля, над которым работает компания. Пользуясь доверием жертвы, социальный инженер получает доступ к ее идентификационным данным.

Авторизация третьей стороны происходит, когда аутентификационные данные украдены или переданы пользователю [32]. Однажды эта сторона может ложно аутентифицировать себя в сети, и пока не приняты меры по ее удалению, хакеры могут использовать дополнительную социальную инженерию или другие средства и методы для повышения внутри системы своих привилегий пользователя. Конечная цель – это получение прав администратора в сети, что позволяет преступнику получить полный доступ к любым ценным данным, хранящимся в ней.

Фишинговые электронные письма направлены на обман получателя, их цель – заставить его выполнить какое-то действие, обычно нажав на ссылку или загрузив вложение, маскируясь под законные запросы на получение информация, предупреждение безопасности или обычные электронные письма от друзей или коллег [33]. Фишинговые атаки могут иметь серьезные последствия для их жертв, такие, как потеря интеллектуальной собственности и конфиденциальной информации о клиентах, финансовые потери и угрозы национальной безопасности [34].

Фишинговые атаки несут в себе серьезную опасность, так как основаны на психологической уязвимости атакуемого лица и учитывают все его слабости [35]. Это одна из самых сложных тактик социальной инженерии, так как изощренные злоумышленники часто могут создавать электронные письма, которые выглядят почти идентичными законным.

Угрозы, которые несет с собой социальная инженерия, становятся все более реальными. Транснациональные корпорации все чаще становятся жертвами целенаправленных атак на их информационные системы.

Другие типы атак социальной инженерии включают:

– тактику, использующую всплывающие окна;

– сбор информации с помощью погружения в мусорные контейнеры;

– плечо серфинга, позволяющее контролировать чьи-то учетные данные или другую конфиденциальную информацию;

– личные атаки, такие как олицетворение на месте или просто использование чьего-то свободного компьютерного терминала;

– атаки, использующие преимущества социальных сетей и другой общедоступной информации;

– атаки, которые подчеркивают или нацеливают жертвы, признанные нетехнически подкованными или вообще лишенными технической осведомленности;

– различные нефишинговые технические атаки, которые не связаны с взаимодействие человека с человеком, включая автоматизированные методы [36].

Несмотря на это многообразие, данный список остается открытым.

Социальная инженерия требует, чтобы жертва находилась в асимметричном отношении к окружающему миру. Злоумышленник, который использует эту асимметрию для установления технократического контроля над своей жертвой, как правило, пользуется одним или несколькими методами, описанными выше. Наконец, сохраняя этот контроль, нападающий заменяет поведенческие цели жертвы своими собственными.

Соответственно, можно заключить, что социальная инженерия включает две составляющие:

1. Компьютерный или технологический обман: технологический подход заключается в том, чтобы обмануть пользователя, полагая, что он взаимодействует с реальным компьютером система и заставить его предоставить конфиденциальную информацию.

2. Человеческий обман: это делается путем обмана, используя невежество жертвы и естественную человеческую склонность быть полезным и понравилось [37].

Социальная инженерия – это использование ментальных манипуляций для обмана компьютера в результате которой пользователи получают доступ к компьютерам, определенной информации или базе данных. Это может быть наиболее опасным по следующим причинам:

– социальная инженерия является одной из самых успешных по сравнению с другими техническими;

– специалисты по информационной безопасности, а также пользователи компьютеров мало что знают о риске применения технологий социальной инженерии;

– человеческие привычки и природа: люди склонны следовать определенным привычкам и действиям по умолчанию, не думая. Хороший нападающий может наблюдать эти привычки и использовать их для отслеживания людей или групп [38].

Рассмотрим основные стадии социальной инженерии.

Большинство хакеров используют определенные шаги, чтобы начать свою атаку и безопасно приблизиться к цели без каких-либо подозрений:

1. Сбор информации для социальной инженерии.

За последнее десятилетие некоторые из самых больших угроз безопасности исходили от использование социальных сетей. Стремительный рост этих технологий позволяет миллионам людей пользователи каждый день публикуют свои посты в социальных сетях. Такого типа информация, которую они публикуют, может

выглядеть не очень важной, но это очень важно для запуска успешной атаки, например, таким ключом может стать персональная информация, фотографии, информация о местоположении, информация о друзьях, деловая информация и пр.

Опасность предоставления такого объема информации заключается в том, что любопытный злоумышленник может собрать воедино эти источники и получить четкую картину личности или бизнес. После того, как сообщение опубликовано, его практически невозможно полностью удалить из социальной сети. Тем более, что оно уже могло быть переслан другим и перепечатано снова. Имея эту информацию в руках, злоумышленник может использовать социальную инженерию, чтобы создать фейк изучаемого лица или получить прибыль в бизнесе с помощью инсайдерской информации;

2. Развитие отношений и доверие с жертвой.

Развитие доверия может быть достигнуто с помощью использования инсайдерской информации. Человеческая природа основывается на доверии к другим, пока они не докажут, что им нельзя доверять. Если кто-то говорит нам, что он является определенным человеком, обычно это воспринимается как утверждение;

3. Эксплуатация отношений.

На этом этапе злоумышленник использует манипуляцию. Нападающий должен изучить эмоциональное состояние своей жертвы и определить, как ее можно использовать его в своих интересах. Эксплуатация может происходить путем разглашения кажущейся неважной информации или доступа, предоставленного / переданного злоумышленнику.

Заключение. Таким образом, социоинженерные атаки стали настолько сложными, что могут сравниться по степени внедрения с техническими типами атак. Кроме того, в атаке социальной инженерии люди – самое слабое место, однако при соответствующей подготовке они могут эффективно противостоять социальным инженерам.

Список литературы

1. Akila L., and Deviselvam. Intrusion Response System for Relational Database to Avoid Anomalous Request // I-manager's Journal on Software Engineering. 2022. Vol. 6(2). Pp. 41–45.

2. Majd Latah Detection of malicious social bots: A survey and a refined taxonomy // Expert Systems with Applications. 2021. Vol. 1511. Art. 113383.

3. Carver, Jeffrey C., Leandro L. Minku, and Birgit Penzenstadler. 2022. OED Online. March 2017. Oxford University Press.

4. Joseph M. Hatfield The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages // Computers & Security. 2022. Vol. 83. Pp. 354–366.

5. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2022. Vol. 55. Pp. 114–127.

6. Waldo Rocha Flores, Mathias Ekstedt Shaping intention to resist social engineering through transformational leadership, information security culture and awareness // Computers & Security. 2021. Vol. 59. Pp. 26–44.

7. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2022. Vol. 55. Pp. 114–127.

8. Mouton, F.a b, Leenen, L.a, Venter, H.S.b Social engineering attack examples, templates and scenarios // Computers and Security. 2021. Vol. 59. Pp. 186–209.

9. Kvedar, D., Nettis, M., Fulton, S. P.: The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition // Journal of Computing Sciences in Colleges. 2020. Vol. 26(2). Pp. 80–87.

10. McDowell, M.: Cyber security tip st04-0141, avoiding social engineering and phishing attacks. Technical report, United States Computer Emergency Readiness Team, 2013.

11. Cruz, J.A.A.: Social engineering and awareness training. Technical report, Walsh College, 2020.

12. Mills, D.: Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. In: Information Security Curriculum Development Conference/ Pp. 139–141.

13. Doctor, Q., Dulaney, E., Skandier, T.: CompTIA A+ Complete Study Guide. Wiley Publishing, Indianappolis, 2023.

14. Hamill, J., Deckro, R. F., Kloeber Jr., J.M.: Evaluating information assurance strategies // Decision Support Systems. 2021. Vol. 39(3). Pp. 463–484.

15. Joint Chiefs of Staff: Information assurance: Legal, regulatory, policy and organizational legal, regulatory, policy and organizational considerations. Technical Report Fourth Edition, Department of Defense, Pentagon, Washington, 1999.

16. Hamill, J. T.: Modeling information assurance: A value focused thinking approach. Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2020.

17. Braverman, M.: Behavioural modelling of social engineering-based malicious software. In: Virus Bulletin Conf. Towards an Ontological Model Defining the Social Engineering Domain 279.

18. Åhlfeldt, R. M., Backlund, P., Wangler, B., Söderström, E.: Security issues in health care process integration? a research-in-progress report. In: EMOI-INTEROP.

19. Granger, S.: Social engineering fundamentals, part i: Hacker tactics.

20. Schoeman, A., Irwin, B., Richter, J.: Social recruiting: a next generation social engineering attack. In: Uses in Warfare and the Safeguarding of Peace.

21. Hadnagy, C.: Social Engineering: The Art of Human Hacking. Wiley Publishing.

22. Espinhara, J., Albuquerque, U.: Using online activity as digital fingerprints to create a better spear phisher. Technical report, Trustwave SpiderLabs.

23. Nemati, H.: Pervasive Information Security and Privacy Developments: Trends and Advancements, 1st edn. Information Science Reference.

24. McQuade III, S. C.: Understanding and managing cybercrime. Prentice Hall, Boston.

25. Griffiths, David, and Timothy Goddard. «An Explanatory Framework for Understanding Teachers Resistance to Adopting Educational Technology» // Kybernetes. 2022. Vol. 44. Pp. 240–250.

26. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2019. Vol. 55. Pp. 114–127.

27. Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H. S. Venter Necessity for ethics in social engineering research // Computers & Security. 2019. Vol. 55. Pp. 114–127.

28. Slade, John A. Law and Psychology // The Journal of Abnormal and Social Psychology. 2020. Vol. 24. Pp. 212–216.

29. Davis, Beverly J. PREPARE: Seeking Systemic Solutions for Technological Crisis Management // Knowledge and Process Management. 2022. Vol. 12. Pp. 123–131.

30. Alistair S. Social Engineering in the Information Age // The Information Society. 2021. Vol. 21. Pp. 67–71.

31. Denning, Dorothy E. The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking // Communications of the Association for Computing Machinery. 2021. Vol. 34. Pp. 22–43.

32. Gragg, David. A Multi-Level Defense Against Social Engineering. SANS Institute InfoSec Reading Room, Pp. 1–21.

33. Huber, Markus, Martin Mulazzani, Gerhardt Kitzler, Sigrun Goluch, and Edgar Weippl. Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam // IEEE Internet Computing. 2021. Vol. 15. Pp. 28–34.

34. Reid, Jim. Plugging the Holes in Host-Based Authentication // Computers & Security. 2021. Vol. 15. Pp. 661–671.

35. Hancock, Bill. Simple Social Engineering // Network Security . 2021. Vol. 6. Pp. 13–14.

36. Heartfield, Ryan, George Loukas, and Diane Gan. You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks // IEEE Access Journal. 2023. Vol. 4. Pp. 910–928.

37. Gilliland K. Understanding the IM Security Threat // EDPACS. 2021. Vol. 33. Art. 2006.

К. М. Беликова,
доктор юридических наук, профессор,
Московский государственный юридический
университет имени О. Е. Кутафина

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ НЕВЗАИМОЗАМЕНЯЕМЫХ ТОКЕНОВ (NFT)

Аннотация. В статье в контексте применения новых цифровых технологий, стоящих или способных встать на службу права интеллектуальной собственности, и с позиции российского и зарубежного опыта, в том числе: нормативных актов, рекомендательных инициатив, имеющих характер актов саморегулирования, доктрины – рассматривается современное состояние и перспективы правовой регламентации технологии невзаимозаменяемых токенов (NFT); делаются предложения по совершенствованию отечественного законодательства.

Ключевые слова: право, цифровые технологии, права интеллектуальной собственности, невзаимозаменяемые токены, технология блокчейн, смарт-контракты, финансовые акты