интереса к себе. Ему важен бурный рост просмотров, как позитивных, так и негативных комментариев. Чем их больше, тем внушительнее его потенциальный заработок.

Однако здесь стоит привести простой пример: человек красит волосы в яркий цвет, чтобы выделиться, привлечь к себе внимание. Да, это вызовет заинтересованность окружающих, заставит их улыбнуться. Но получишь ли признание и уважение с помощью нового цвета волос? Конечно, нет. Так и с пранкерством. Получишь две-три сотни комментариев, тебя пообсуждают какое-то время, и все. Розыгрыши через короткое время будут забыты, а репутацию свою ты точно подпортишь.

Безусловно, качественные и безобидные пранки вызывают море смеха, а смех, как известно, продлевает жизнь. Однако во всем нужно знать меру.

И в этой связи призываю подумайте о личной информационной безопасности.

Список использованной литературы:

1. Пранкерство. [Электронный источник]. URL: https://med-info.ru/content/view/5307 (дата обращения: 26.05.2021).

2. Что означает пранкер. [Электронный источник]. URL: https://top10mebel.ru/plumbing/chto-oznachaet-pranker-chto-takoe-prank-kto-takie-prankery-i-chem-oni/ (дата обращения: 26.05.2021).

3. Кто такой пранкер Вован? Доля правды: кто такие пранкеры и как находят телефоны звезд и политиков? Кто такой пранкер. [Электронный источник]. URL: https://biathlonmordovia.ru/electrical-components/kto-takoi-pranker-vovan-dolya-pravdy-kto-takie-prankery-i-kak-nahodyat/ (дата обращения: 26.05.2021).

4. Кто такие пранкеры? [Электронный источник]. URL: http://chtooznachaet.ru/prankery.html (дата обращения: 26.05.2021).

5. Что такое пранк и кто такие пранкеры. [Электронный источник]. URL: https://ktonanovenkogo.ru/voprosy-i-otvety/prank-chto-ehto-takoe-prankery.html (дата обращения: 26.05.2021).

6. Кто такие пранкеры. [Электронный источник]. URL: https://nationmagazine.ru/events/kto-takie-prankery-i-kak-oni-dozvanivayutsya-do-prezidentov/ (дата обращения: 26.05.2021).

7. Умереть от смеха. [Электронный источник]. URL: https://rg.ru/2014/11/12/prankery.html (дата обращения: 26.05.2021).

8. Российские пранкеры разыграли премьера Канады. [Электронный источник]. URL: https://mir24.tv/news/16436621/greta-tunberg-na-provode-rossiiskie-prankery-razygrali-premera-kanady (дата обращения: 26.05.2021).

9. Кто такой пранкер. [Электронный источник]. URL: https://nevacrossfit.ru/water/kto-takoi-pranker-prank-chto-eto-takoe-opredelenie-znachenie/ (дата обращения: 26.05.2021).

10. Пранкеры разбушевались. [Электронный источник]. URL: https://bloknot-stavropol.ru/news/privivka-ot-prankera-bezobidny-li-publichnye-priko-1186831?sphrase_id=1181252 (дата обращения: 26.05.2021).

11. «Я просто пошутил». Как суды наказывают пранкеров в России и мире. [Электронный источник]. URL: https://takiedela.ru/news/2020/02/19/prankery/ (дата обращения: 26.05.2021).

12. Пранкеров из Челябинска наказали за «расстрел пациента с коронавирусом». [Электронный источник]. URL: https://www.chel.kp.ru/daily/27092/4165473/ (дата обращения: 26.05.2021).

13. Что такое эффект Бузовой и когда шутка перестает быть шуткой: тюменский психолог – о пранкерстве. [Электронный источник]. URL: https://72.ru/text/gorod/2020/01/13/66437335/ (дата обращения: 26.05.2021).

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ - БУДУЩАЯ НОВЕЙШАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ИНТЕРНЕТА

Дворянкин Олег Александрович,
старший преподаватель кафедры информационной безопасности
Учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя
кандидат юридических наук

SOCIAL ENGINEERING - THE FUTURE OF THE LATEST INTERNET INFORMATION TECHNOLOGY

Oleg A. Dvoryankin,
candidate of legal sciences,
lecturer at the chair of information security of
the Moscow MUR RS Kikot university.

АННОТАЦИЯ

В статье представлена информация о социальной инженерии, как о новой информационной технологии сети Интернет. Однако в ходе исследования установлено, что технология имеет глубокие исторические корни. В настоящее время с учетом появления Интернета социальная инженерия получила новое дыхание и развитие. В статье изучены виды и их особенности, а также представлен ряд советов о том, как обнаружить их атаки правонарушителей, использующих методы и формы социальной инженерии.

Кроме отражены характеристики человека, которые способствуют развитию и совершенствованию настоящей технологии.

ABSTARCT

The article presents information about social engineering as a new information technology of the Internet. However, the study found that the technology has deep historical roots. Currently, with the advent of the Internet, social engineering has received a new breath and development. The article examines the types and their features, as well as provides a number of tips on how to detect their attacks by offenders using methods and forms of social engineering. In addition, the characteristics of a person that contribute to the development and improvement of this technology are reflected.

Ключевые слова: социальная инженерия, Интернет, информационная безопасность, компьютер, слабости человека, мошенник, мошенничество, обучение

Keywords: social engineering, Internet, information security, computer, human weaknesses, fraudster, fraud, training

«Миром правят данные», «данные – новая нефть».

Эти выражения отражают сегодняшнюю картину отношения к информации.

У бизнеса – как в IT-сфере, так и любой другой сфере – информация часто имеет очень высокую ценность и от нее зависит успешность компании, ее развитие, безопасность клиентов и репутация, но при этом в любой системе, которая связана с получением, хранением, обработкой данных, всегда участвует человек. И пока другие методы защиты справляются с сохранением конфиденциальных данных в тайне, человеческий фактор становится тем ключом, который открывает двери мошенникам [1].

Люди зачастую оказываются очень доверчивыми и сами предоставляют мошенникам конфиденциальную информацию. С помощью специальных практик мошенникам добыть необходимую информацию намного проще, нежели получить ее путем взлома системы безопасности. Этим они и пользуются.

Таким образом на лидирующие (передовые) места в современном обществе выходит социальная инженерия.

Социальная инженерия – это способ получения конфиденциальной информации с помощью психологического воздействия на человека. Основной целью социальной инженерии является получение выгоды через доступ к паролям, банковским данным и другим защищенным системам. Кибермошенников, которые используют эти приемы на практике, называют социальными инженерами.

Сейчас социальная инженерия приобрела прочную связь с киберпреступностью, но на самом деле это понятие появилось давно и изначально не имело выраженного негативного оттенка [2].

Люди использовали социальную инженерию с древних времен.

Например, в Древнем Риме и Древней Греции очень уважали специально подготовленных ораторов, способных убедить собеседника в его «неправоте» или привлечь противников на свое сторону, а соратников убедить в правильности выбранного ими пути. Эти люди участвовали в дипломатических переговорах и работали на благо своего государства.

В средние века социальная инженерия также активно проявила себя, в ходе подготовки к различным боевым сражениям, дипломатических баталиях и т.д.

В последующем она стала активно развиваться, когда мировое сообщество стало входить в капиталистическое мироустройство, в котором люди стали становиться индивидуалами и на которых стало легко воздействовать методом манипулирования.

Наибольшее развитие социальная инженерия получила в послевоенные годы, после 1945 года, в США и Великобритании, прежде всего в контексте обеспечения реализации проектов американских и британских спецслужб, в рамках которых новое научное направление начало приобретать масштабный прикладной характер. Целью социальной инженерии стала разработка технологий манипуляции сознанием людей.

В результате к началу 1960-70-х годов с всеобщим развитием телефонии в СССР стали появляться телефонные хулиганы, нарушавшие покой граждан просто ради шутки. «Информационные телефонные эксперты» сообразили, что так можно достаточно легко получать важную информацию. И уже к концу 70-х XX века бывшие телефонные хулиганы превратились в профессиональных социальных инженеров и их стали называть синжерами, способных мастерски манипулировать людьми, по одной лишь интонации определяя их комплексы и страхи [3].

В конце 90-х годов XX века, когда же появились компьютеры, большинство инженеров сменило профиль, став социальными хакерами, а понятия «социальная инженерия» и «социальные хакеры» стали синонимичны.

Иллюстрацию того, на что способен умелый социальный инженер можно найти в кинематографе. Так, в фильме «Поймай меня, если сможешь», основанный на реальных событиях – на истории легендарного мошенника Фрэнка Уильяма Абигнейла-младшего. За пять лет преступной деятельности его фальшивые чеки на общую сумму 2,5 миллионов долларов оказались в обращении 26 стран мира [4]. Скрываясь от уголовного преследования, Абигнейл проявил удивительные способности в перевоплощении, выдавая себя за пилота авиалиний, профессора социологии, врача и адвоката.

Еще один пример – кража у американской технологической компании «The Ubiquiti Networks» 40 млн долларов США в 2015 году. Никто не взламывал операционные системы и не крал данные – правила безопасности нарушили сами сотрудники. Мошенники прислали электронное письмо от имени топ-менеджера компании и попросили, чтобы финансисты перевели большую сумму денег на указанный банковский счет. Мошенники попросили – финансисты перевели [5].

В 2007 году одна из самых дорогих систем безопасности в мире была взломана – без насилия, без оружия, без электронных устройств.

Злоумышленник просто забрал из бельгийского банка «ABN AMRO» алмазы на 28 млн долларов США благодаря своему обаянию. Мошенник Карлос Гектор Фломенбаум, человек с аргентинским паспортом, украденным в Израиле, завоевал доверие сотрудников банка еще за год до инцидента. Он выдавал себя за бизнесмена, делал подарки, иначе говоря – налаживал коммуникацию. Однажды сотрудники предоставили ему доступ к секретному хранилищу драгоценных камней, оцененных в 120 000 каратов [5].

Еще один яркий пример, как знаменитый мошенник, аферист Виктор Люстиг не просто заполнил США фальшивыми купюрами и оставил «в дураках» американского гангстера Аль-Капоне, а еще продал достояние Парижа (Франция) – Эйфелеву башню. Все это стало возможным с помощью социальной инженерии.

Все эти реальные примеры социальной инженерии говорят о том, что она легко адаптируется к любым условиям и к любой обстановке. Играя на личных качествах человека или отсутствии профессиональных (недостаток знаний, игнорирование инструкций и так далее), киберпреступники буквально «взламывают» человека.

Таким образом, самое слабое звено защиты любой системы – сами пользователи.

В этой связи возникает вопрос: «Почему человека считают самым слабым звеном в информационной безопасности?»

Однозначного ответа нет, но эксперты по этой теме указывают на качества, свойственные большинству из нас, т.е. эмоции, испытываемые многими – это страх, доверие, алчность и желание помочь ближнему.

Профессор психологии Роберт Чалдини в своем бестселлере «Психология влияния» (1984 г.) описал шесть принципов влияния, которые применяют социальные инженеры:

– взаимность: предпочитаем платить добром за добро;

– последовательность: придерживаемся убеждений, соответствующих нашим ценностям;

– социальное доказательство: соглашаемся с тем, что делает большинство;

– власть и авторитет: готовы идти за людьми, которым доверяем и которых уважаем;

– симпатия: с удовольствием выполняем просьбы людей, которые нам нравятся;

– дефицит: желаем того, что нам недоступно [6].

Социальные инженеры пользуются тем, что психологические манипуляции не требуют больших затрат и специфических знаний (кроме нескольких психологических приемов), их можно применять в течение длительного времени, а еще их сложно обнаружить. Люди, которые владеют ценной информацией или имеют к ней доступ, сравнимы с доступным плодом: они на виду и до них очень легко дотянуться.

Таким образом, социальная инженерия направлена не на компьютерную технику, а на ее пользователя. Интерес представляют все платежеспособные лица, а также пользователи, обладающие ценной информацией, сотрудники предприятий и государственных учреждений.

Метод применяется с целью выполнения финансовых операций, взлома, кражи сведений (например, клиентских баз, персональных данных) и другого несанкционированного доступа к информации. Социальная инженерия помогает конкурентам осуществлять разведку, выявлять слабые стороны организации, переманивать сотрудников.

Все типы социальной инженерии опираются на слабые стороны человеческой психологии. Мошенники пользуются человеческими эмоциями, чтобы манипулировать и обманывать своих жертв. Людской страх, жадность, любопытство и даже готовность помогать другим, обращаются против них различными способами [7].

На сегодняшний день социальная инженерия может принимать разные виды.

1. **Фишинг** – это вид мошенничества, основная суть которого завладение логинами и паролями от важных сайтов, аккаунтов, счетов в банке и другой конфиденциальной информацией путем рассылки писем с ссылками на мошеннический сайт, внешне очень похожий на настоящий. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести на поддельной странице свои логин и пароль, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

2. **Фарминг** – при фарминге на персональный компьютер жертвы устанавливается вредоносная программа, которая меняет информацию по IP-

адресам (уникальным идентификаторам компьютера в сети Интернет), в результате чего обманутый пользователь перенаправляется на поддельные сайты без его ведома и согласия.

3. **Вишинг** – метод, который заключается в том, что злоумышленники, используя телефонную коммуникацию и, играя определенную роль (сотрудника банка, покупателя и т.д.), под разными предлогами выманивают у держателя платежной карточки конфиденциальную информацию или стимулируют его к совершению каких-то действий со своим счетом или банковской платежной картой [8].

3. **Взлом социальных сетей** – взламывается страница пользователя и от его имени идут сообщения его друзьям, чаще всего с просьбой «скинь денег на карточку». Тот, кого взломали, может понять об этом, когда не сможет войти в свой аккаунт, так как пароль уже изменен.

4. **СМС-атаки** – мошенник создает фейковый (поддельный) аккаунт в социальных сетях либо регистрируется, к примеру, в мессенджере Viber, с сим-карты, которая оформлена не на него, а на кого-то другого. Далее высылает объявление: «Помогите на лечение ребенку», размещая фото и реквизиты. Если это действительно реальный человек, то реквизиты легко проверяются. Но, к сожалению, люди не часто проверяют такую информацию.

5. **Претекстинг** – набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон, электронная почта и т. п. Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника, должность, название проектов, с которыми он работает, дату рождения). Используя такую информацию, он входит в доверие и получает необходимые ему данные [9].

6. **Кви про кво** (в английском языке это выражение обычно используется в значении «услуга за услугу») – злоумышленник представляется, например, сотрудником технической поддержки и информирует о возникновении каких-то проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое вредоносное программное обеспечение на компьютере жертвы. Эта техника предполагает обращение злоумышленника к пользователю, как правило, по электронной почте или корпоративному телефону.

7. **Обратная социальная инженерия** – создается такая ситуация, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, мошенник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте со злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные [10].

Методов мошенничества, которые используют социальную инженерию, – множество. Перечисленные – это всего лишь их часть. Самые распространенные для нашей страны – фишинг, взлом социальных сетей и вишинг.

Большинство методов социальной инженерии не требуют особых технических знаний со стороны злоумышленников, а значит использовать эти методы может кто-угодно – от мелких злоумышленников до опытных киберпреступников.

В этой связи встает вопрос: «Как избежать атаки с использованием социальной инженерии?»

Однозначного ответа нет.

Социальным инженерам особенно сложно противодействовать, поскольку они используют особенности человеческой натуры – любопытство, уважение к властям, желание помочь другу. Но есть ряд советов о том, как обнаружить их атаки.

1. **Проверять источник.**

Следует задуматься о том, откуда исходит сообщение, – не доверять слепо. На вашем столе неизвестно откуда появилась флешка? Вам внезапно позвонили и сообщили, что вы получили в наследство 5 млн долларов США? Ваш руководитель просит в письме предоставить ему массу данных об отдельных сотрудниках? Все это выглядит очень подозрительно, поэтому и действовать следует с осторожностью.

Проверить источник нетрудно. Например, посмотреть на заголовок электронного письма и сравнить его с другими письмами того же отправителя. Проверить, куда ведут ссылки, – поддельные гиперссылки легко выявить, просто наведя на них курсор (только не нужно при этом нажить на ссылку). Также следует проверить орфографию: в банках над перепиской с клиентами работают целые отделы квалифицированных специалистов. Письмо с явными ошибками, вероятно, подделка [11].

Если все же остаются сомнению, следует перейти на официальный сайт, связаться с представителем и попросить подтвердить или опровергнуть сообщение.

2. **Выяснить, что им известно.**

Знает ли тот, кто звонит или пишет, всю соответствующую информацию – например, ваше полное имя? Сотрудник банка уж точно должен иметь перед глазами все данные о собеседнике и обязательно спросит проверочное слово, прежде чем разрешит ему вносить изменения в свой счет. Если этого не произошло, с большой долей вероятности письмо, сообщение или звонок – подделка.

3. **Остановиться и подумать.**

Социальные инженеры часто используют иллюзию срочности в расчете на то, что жертва не будет особо задумываться о происходящем. Всего минута размышлений может помочь выявить и предотвратить атаку.

Не следует спешить сообщать данные по телефону или переходить по ссылке. Лучше перезвонить по официальному номеру или перейти на официальный сайт, также можно использовать другой способ связи, чтобы проверить благонадежность источника [12]. Например, если друг в электронном письме просит перечислить ему деньги, лучше написать или позвоните ему по телефону, чтобы убедиться, что письмо действительно от него.

4. **Требовать данные, удостоверяющие личность.**

Социальному инженеру проще всего проникнуть в охраняемое здание, неся в руках коробку или кипу папок. Кто-нибудь обязательно придержит для него дверь. Не нужно попадаться на эту удочку: всегда необходимо требовать удостоверение личности.

То же правило действует и в других ситуациях. Если запрашивают информацию – нужно уточнить имя и номер звонящего или его непосредственного руководителя. Затем просто проверить эту информацию в Интернете или справочнике прежде, чем сообщать какие-либо персональные данные.

5**. Использовать надежный спам-фильтр.**

Если ваш почтовый клиент недостаточно тщательно фильтрует спам или не помечает письма как подозрительные, попробуйте изменить настройки. Хорошие спам-фильтры используют разнообразную информацию для распознавания нежелательных писем [13].

Они могут выявлять подозрительные файлы или ссылки, заносить в черный список ненадежные IP-адреса или сомнительных отправителей и анализировать содержимое писем, чтобы обнаруживать фальшивки.

6. **Определить, насколько правдоподобна текущая ситуация.**

Некоторые социальные инженеры рассчитывают на то, что вы не станете вдумываться. Попробуйте оценить, насколько реалистична ситуация, – так можно избежать атаки мошенников.

Например: Если бы ваш друг действительно застрял в Китае, он бы вам скорее написал на почту, позвонил или написал SMS? Насколько вероятно, что нигерийский принц оставил вам в наследство миллион долларов? Стал бы банк по телефону узнавать данные вашего счета?

Атаки с использованием социальной инженерии крайне опасны, поскольку происходят в совершенно обыденных ситуациях.

Однако, полностью понимая их механизм и принимая элементарные меры предосторожности, человек гораздо меньше рискует стать их жертвой [14].

В большинстве случаев мошенник не станет рисковать, осознав, что эффект неожиданности пропал, а для него – эффект неожиданности самое важное в противозаконной деятельности.

Таким образом, социальная инженерия пытается использовать присущие людям слабости, например торопливость, алчность, альтруизм или страх перед официальным учреждением, в целях получения конфиденциальной информации и последующего доступа в систему.

Социальная инженерия нематериальна, ее невозможно физически устранить. Самый эффективный способ не стать жертвой социальной инженерии – не терять бдительности и не позволять злоумышленникам себя провести.

Ввиду того, что методы социальной инженерии разработаны профессионалами своего дела, распознать сразу обман порой не под силу даже «опытным» специалистам.

Атаки с использованием социальной инженерии – высокоэффективная и недорогая методика. Концептуально преступники преследуют цели, аналогичные целям легального бизнеса – они стремятся получить максимальную прибыль при одновременном сокращении операционных расходов. А благодаря множеству вариантов - атаки с использованием социальной инженерии идеально подходят для достижения этих целей.

Успешные атаки, в основе которых лежат методы социальной инженерии, направлены против базовых эмоциональных реакций людей. Когда человека переполняют такие чувства, как страх или сочувствие, он часто может принимать необдуманные решения.

В социальной инженерии все строится вокруг слабостей человека. С одной стороны, это личностные качества: сопереживание, наивность, доверчивость, лояльность к чужим слабостям, страх. С другой – качества профессиональные: недостаток знаний, неумение применять их на практике, игнорирование инструкций и должностных обязанностей. Поэтому социальную инженерию часто называют «взломом» человека.

На практике каждый взлом может иметь серьезные последствия, в первую очередь, для простого человека, которых расстается со своими финансовыми активами (деньгами) или для компании, в которой работает человек. Самый основной способ защиты от социальной инженерии – это обучение, поэтому тот, кто предупрежден, тот вооружен.

И главное думайте о своей личной информационной безопасности.

Список использованной литературы:

1. Осторожно, это ловушка: что такое социальная инженерия. [Электронный источник]. URL: https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/ (дата обращения: 16.05.2021).

2. Социальная инженерия. [Электронный источник]. URL: https://www.eset.com/ua-ru/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/ (дата обращения:

16.05.2021).

3. Что такое социальная инженерия? [Электронный источник]. URL: http://fingramota.by/ru/guide/practical/breaking-into/ (дата обращения: 16.05.2021).

4. Социальная инженерия – как не стать жертвой. [Электронный источник]. URL: https://efsol.ru/articles/social-engineering.html/ (дата обращения: 16.05.2021).

5. Социальная инженерия [Электронный источник]. URL: https://www.anti-malware.ru/threats/social-engineering/ (дата обращения: 16.05.2021).

6. Социальная инженерия. [Электронный источник]. URL: https://www.avast.ru/c-social-engineering (дата обращения: 16.05.2021).

7. Как понизить роль социальной инженерии в угрозе проникновения. [Электронный источник]. URL: https://itglobal.com/ru-ru/company/blog/kak-ponizit-rol-soczialnoj-inzhenerii-v-ugroze-proniknoveniya/ (дата обращения: 16.05.2021).

8. Как избежать атаки с использованием социальной инженерии. [Электронный источник]. URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения: 16.05.2021).

9. Социальная инженерия. [Электронный источник]. URL: https://www.stekspb.ru/blog/it/socialnaya-inzheneriya/ (дата обращения: 16.05.2021).

10. Методы социальной инженерии, или атаки на человеческий фактор. [Электронный источник]. URL: https://www.a1qa.ru/blog/sotsialnaya-inzheneriya-ili-ataki-na-chelovecheskiy-faktor/ (дата обращения: 16.05.2021).

11. Как социальная инженерия открывает хакеру двери в вашу организацию. [Электронный источник]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering/ (дата обращения: 16.05.2021).

12. Социальная инженерия: актуальная угроза и меры защиты. [Электронный источник]. URL: https://safe-surf.ru/users-of/article/642870/ (дата обращения: 16.05.2021).

13. Социальная инженерия – главное оружие киберпреступников. [Электронный источник]. URL: https://www.if24.ru/sotsialnaya-inzheneriya-glavnoe-oruzhie-kiberprestupnikov/ (дата обращения: 16.05.2021).

14. Что такое Социальная Инженерия? [Электронный источник]. URL: https://academy.binance.com/ru/articles/what-is-social-engineering (дата обращения: 16.05.2021).