УДК 304.444

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ЯВЛЕНИЕ, ИНСТРУМЕНТЫ, СВОЕВРЕМЕННОЕ ПРЕДУПРЕЖДЕНИЕ

**Ю.А. Бондарев**
бакалавр
**О.Н. Гнездечко**
доцент

*Владивостокский государственный университет экономики и сервиса*
*Владивосток. Россия*

*В статье рассматривается явление социальной инженерии как проявление способности человека к преобразованию материального и социального миров. Раскрывается определение понятия «социальная инженерия», выявляются психологические факторы проявления инженерии и внедрения социокультурных инноваций. Автор предлагает практические рекомендации по своевременному предупреждению последствий социальной инженерии.*

***Ключевые слова и словосочетания**: инженерия, социальная инженерия, конфиденциальная информация, кража информационных данных, своевременное предупреждение.*

# SOCIAL ENGINEERING: PHENOMENON, TOOLS AND BEFORE-THE-FACT PREVENTION

*The paper discusses the issues of social engineering as a particular presentation of the hu-man ability to develop material and social worlds. Revealed here is the notion of social engineering phenomenon. The author discusses psychological prerequisites of engineering implementing social and cultural innovation. The paper suggests a number of practical implications for before-the-fact prevention of social engineering consequences.*

***Keywords:** engineering, social engineering, sensitive information, data theft, before-the-fact prevention.*

Основная ***цель*** данной работы – раскрыть суть понятия «социальная инженерия» в аспекте определения обозначаемого явления. Кроме того, в статье *выявлены психологические факторы* проявления инженерии в любой человеческой деятельности и сознательной технической инженерии. Последовательная инженеризация социальной жизнедеятельности является объективно необходимым требованием для успешного развития общества [1, с.96].

«*Инженерия* <...> есть применение научных, экономических, социальных и практических знаний для того, чтобы изобретать, проектировать, строить, поддерживать и улучшать структуры, машины, приборы, системы, материалы и процессы» [7].

Изобретение нового знания вряд ли возможно без применения творчества и фантазии. Эти коннотации неявно выделяются в семантике глагола «изобретать» и включаются в описание явления *инженерии*. Методы и инструменты технической инженерии, её достижения способствуют выявлению её составляющих в любой человеческой *новаторской деятельности*. Очевидно, что инженерные методы и инструменты имеют громадный потенциал внедрения в теорию и практику сознательной социальной инженерии.

Немногочисленные работы отечественных социологов в области социальной инженерии свидетельствуют о непонимании прикладного характера социальной инженерии как отдельного вида инновационной деятельности [3, 2]. В этом и состоит ***актуальность*** рассматриваемой проблематики. В России явление социальной инженерии до настоящего времени плохо теоретически отрефлексировано и ещё хуже воплощено в практику. Мы определяем социальную инженерию как осознанную целенаправленную, *атрибутивную грань* человеческой деятельности. ***Объект*** нашего исследования − социальная инженерия − трактуется нами в широком понимании как проявление *способности человека создавать новые или творчески преобразовывать уже существующие процессы материального и социального миров*.

Однако в узких профессиональных кругах и сообществах термин «социальная инженерия» приобрёл специальное значение *кража информационных данных* [5]. Текущий статус термина «социальная инженерия» связан с манипулированием общественным сознанием и поведением отдельно взятого человека. Это в свою очередь может вызывать негативное отношение социума к

социальной инженерии, которая проявляется в применении специальных методов и инструментов. Именно они служат ***предметом*** нашего исследования.

Возникший в прошлом столетии этот новый вид деятельности существует в осознанно-организованным модусе [2, с.96]. Исторически меняется лишь уровень организованности социальной инженерии.

При этом неизбежным сегодня остаётся влияние человеческого фактора на все производственные структуры и процессы, включая защиту конфиденциальной информации. *Социальная инженерия* − это «искусство» манипулировать поведением человека с целью сломать защитные системы безопасности потенциальной жертвы, даже не подозревающей о том, что ею манипулируют. Основная цель социальной инженерии − получить доступ к конфиденциальной информации пользователя, их банковским данным и всему, что может принести финансовые или репутационные потери. Чаще всего этот метод используется через Интернет как незаконный с целью получить конфиденциальную информацию путём обмана и различных форм психологического давления. Другими словами, этот метод извлекает выгоду из человеческих слабостей, а именно поэтому очень эффективен.

Хотя термин «социальная инженерия» появился относительно недавно, в определенной форме это явление использовалось в Древнем Риме и Древней Греции [8], а также спецслужбами [9] для получения доступа к секретной информации. К началу 1970-х стали появляться телефонные хулиганы, позднее превратившиеся в профессиональных социальных инженеров, способных мастерски манипулировать пользователями, используя их слабости, комплексы и страхи.

Одним из самых известных социальных инженеров в истории является Кевин Митник. Всемирно известный хакер и консультант по информационной безопасности, К.Митник, является автором многочисленных книг по компьютерной безопасности, в которых основное внимание уделяется социальной инженерии и методам психологического воздействия на человека. В 2001 году под его авторством была издана книга «Искусство обмана», рассказывающая о реальных историях применения методов и инструментов социальной инженерии. К. Митник утверждает, что вскрыть пароль намного проще, чем пытаться взломать систему безопасности. Если вы все еще думаете, что социальная инженерия не заслуживает особого внимания, прочитайте о таких известных социальных инженерах, как Виктор Люстиг (который дважды продал Эйфелеву башню) или Робин Сейдж (с помощью фальшивого аккаунта в Facebook получивший доступ к секретной информации американских спецслужб) [9; 6].

Чтобы защититься от психологического давления социальных инженеров, необходимо понять, как работают инструменты социальной инженерии. Рассмотрим основные её виды и методы защиты от них [6], поскольку в настоящее время злоумышленник может получать информацию о своей цели даже путем сбора конфиденциальных данных через социальные сети, которые пользуются широкой популярностью.

Так, методы социальной инженерии включают в себя претекстинг, атаки через заражение сайта, фишинг, шпионаж и т.д. [8]. Претекстинг -−выдача себя за другого человека с целью получения информации, которая может быть предоставлена этому человеку, а для мошенника, занимающегося претекстингом, является недоступной. В результате, потенциальная жертва раскрывает конфиденциальную информацию, выполняя внушаемые ей действия. Этот тип психологической атаки обычно осуществляется по телефону. Чаще всего эта техника включает в себя больше, чем просто ложь, она связана с предварительными исследованиями (например, выяснения имени сотрудника, должности, которую он / она занимает либо название проектов, над которыми он / она работает), чтобы обеспечить доверие к цели. *Атака через заражение сайта* оказывается стратегией компьютерной атаки, в которой жертва представляет определенную группу (организацию, отрасль). При этой атаке злоумышленник отслеживает, какие веб-сайты посещает пользователь или группа, заражая один или несколько из них вредоносным ПО.

Мошенники посредством таких атак обычно собирают важные данные о пользователе. Различные фишинг техники направлены на мошенническое получение конфиденциальной информации. Обычно злоумышленник отправляет на адрес электронной почты поддельное письмо из банка или платежной системы, требуя «проверки» определенной информации или совершения определенных действий. Это письмо обычно содержит ссылку на фальшивую веб-страницу, имитирующую официальную с фирменным логотипом и контентом. В письме содержится форма, требующая ввода конфиденциальной информации, начиная с домашнего адреса и заканчивая PIN-кодом, учетной записью мобильного банкинга пользователя. Шпионаж подразумевает получение конфиденциальной информации без разрешения владельца. Основная цель техники – следить за потенциальной жертвой и секретностью их действий. Все, что нужно мошенникам, – это отслеживать

движения пальцев пользователей. Мошенничество в сфере социальной инженерии – это широкий термин, который подразумевает манипулирование и обман, связанный с инженерией.

Таким образом, социальная инженерия располагает огромным арсеналом методов и инструментов кражи информационных данных [6; 8].

Какие меры предупреждения может предпринять пользователь в целях своевременного предупреждения негативных проявлений социальной инженерии? Какие протоколы безопасности может установить пользователь для предотвращения кражи конфиденциальных данных? Программный каркас для средств эксплуатации уязвимостей подразумевает создание основ доверия на уровне сотрудника / персонала. Протоколы безопасности в отношении безопасных каналов связи, которые могут предотвратить утечку важных данных и/ или доступ к информации извне, со стороны мошенников. Сотрудников компании предупреждают об опасности разглашения личной информации и информационных данных компании, а также о способах своевременного предупреждения утечки данных. Каждый сотрудник компании, в зависимости от подразделения и должности, должен быть осведомлён, как и на какие темы можно общаться с клиентами, какую информацию можно предоставлять службе технической поддержки, как и что должен выполнять сотрудник компании.

Исходя из всего перечисленного, каждый пользователь должен быть осведомлен не только об опасностях раскрытия *информационных данных*, но и о мерах своевременного предупреждения утечки данных.

В наше время социальная инженерия нашла широкое распространение во всех сферах жизнедеятельности человека. Принимая во внимание уровень угрозы информационной безопасности, каждый может оказаться жертвой изощрённых проявлений социальной инженерии. Наиболее уязвимыми для всех видов компьютерного мошенничества является кража интеллектуальной собственности, в частности, разработки проектов, онлайн-курсов и т.п. Например, техническая разработка стандартов дистанционного обучения [4, с.89-94] может быть рассмотрена как интеллектуальная собственность, которая может быть украдена и использована не по назначению.

Особый интерес для злоумышленников представляют интеллектуальные разработки. Злоумышленники с помощью инструментов социальной инженерии могут украсть источники данных или исказить их для собственных целей, незаконно использовать для сторонних разработок, игнорируя авторское право в соответствии с личными потребностями.

Поэтому следует применять простые, но эффективные методы защиты личных данных и прав интеллектуальной собственности при обработке данных. К ним относятся: 1) использование безопасных протоколов передачи данных; 2) хранение идентификационных данных в секрете; 3) игнорирование подозрительных электронных писем и использование браузеров (Google, Chrome, Opera и т.д.) со встроенной проверкой безопасности сайта.

Таким образом, социальная инженерия – это способ, с помощью которого злоумышленники могут получить доступ к информационным данным компании или конфиденциальным данным пользователя, не будучи экспертом в этой области. Злоумышленник может использовать множество инструментов и тактик, чтобы обмануть жертву или получить информацию без их ведома. Любой вид социальной инженерии почти всегда используется со злым умыслом. Некоторые люди, конечно, упоминают о его преимуществах, указывая на то, что с его помощью можно решить социальные проблемы, а социальные институты могут адаптироваться к меняющимся условиям. Несмотря на это, методы социальной инженерии наиболее успешно используются для: 1) привлечения пользователей с целью получения конфиденциальной информации; 2) манипулирования сознанием людей; 3) дестабилизации работы компаний с целью их последующего уничтожения; 4) кражи базы данных; 5) финансового мошенничества; 6) промышленной разведки.

Все описанные правила своевременного предупреждения информационного воровства достаточно просты, однако большинство пользователей зачастую их игнорируют: 1. Защитите свои конфиденциальные данные; 2. Не забывайте соблюдать простые правила информационной безопасности; 3. Анализируйте шаги и действия хакеров, чтобы своевременно предупреждать атаки манипуляторов; 4. Никому не сообщайте информацию об учётных данных, номерах банковских счетов, карт, пин-кодах и т.п.

Важно помнить, что социальный инженер владеет искусством манипулирования и отслеживания действий других пользователей. Но гораздо важнее научиться распознавать проявления и инструменты социальных инженеров, чтобы не стать жертвой он-лайн мошенничества. Сознательная социальная инженерия должна осваивать инженерность на том же уровне, что и техническая. Иначе мы будем постоянно сталкиваться с негативными проявлениями сознательной социальной инженерии.

Таким образом, в статье мы раскрыли суть определения «социальная инженерия»; выявили предполагаемые психологические факторы её проявления в любой сфере человеческой деятельности; рассмотрели инструменты социальной инженерии. Сформулированы и предложены практические рекомендации по своевременному предупреждению негативных последствий социальной инженерии.

1. Волков Е.Н. Социальная инженерия: явление и его концептуализация // Вестник Нижегородского университета им. Н.И. Лобачевского. Сер.: Социальные науки. – 2014. – №3 (35). – С. 96–101.

2. Моисеева А.П. Генезис социальной инженерии в контексте междисциплинарности // Известия Томского политехнического университета. – 2012. – Т.320. – №6. – С. 64–69.

3. Резник Ю.М. Социальная инженерия: предметная область и границы применения // Социологические исследования. – 1994. – №2. – С. 87–96.

4. Соловов А.В. Организационные аспекты электронного дистанционного обучения // Высшее образование в России. – 2007. – № 12. – С. 89–94.

5. Социальная инженерия: сайт [Электронный ресурс].– URL: http://ru.wikipedia.org/wiki/ Социальная_ инженерия (дата обращения 27.03.2020).

6. Социальная инженерия – как не стать жертвой [Электронный ресурс]. – URL: http://efsol.ru/articles/social-engineering.html (дата обращения 28.03.2020).

7. Engineering [Электронный ресурс]. – URL: http://en.wikipedia. org/wiki/Engineering (дата обращения 10.04.2020).

8. The Social-Engineer Podcast [Электронный ресурс]. – URL: https://www.social-engineer.org/ (дата обращения 05.04.2020).

9. Wikipedia. The Free Encyclopedia [Электронный ресурс]. – URL: https://en.wikipedia.org (дата обращения 07.04.2020).