М. В. Петрович, д-р экон. наук, профессор
БГЭУ, Минск (Беларусь)

Хакинг социального поведения: сущность и методы реализации

Современный человек живет в хаосе событий, лавинообразной информации, мнений и утверждений, понять и рационально осознать которые невозможно. Одно и то же, казалось бы, очевидное событие, услуга или материальное благо может подаваться для потребления, пониматься и трактоваться по-разному в зависимости от источника события и его интерпретатора. Подобные массовые явления характерны для многих сфер социальной жизни – ритейла, сервисных систем, здравоохранения, политики, государственного и корпоративного управления.

Основа этого – асимметричность информации и возникающие на этой основе несовершенные коммуникации. Теорию информационной асимметрии во второй половине XX века разработали Дж. Акерлоф, М. Спенс и Дж. Стиглиц (Нобелевская премия по экономике в 2001 году) в рамках информационной экономики на основе анализа рынков и управления финансами корпораций [1].

В деловых средах имеется множество участников, главные из которых государство, потребители и производители, а также сервисные структуры (банки, транспорт, реклама и др.). Объективно то, что производитель по сравнению с другими имеет больше информации о качестве произведенного продукта, продавец о состоянии спроса, банкир о стоимости денег на рынке, перевозчик о специфике транспортной логистики. Внутри каждой организации также имеется информационное неравенство между уровнями управления, территориальными подразделениями.

Асимметричные ситуации могут рождать внутренние, и межгрупповые, личные и профессиональные конфликты, что объективно рождает необходимость активного вмешательства в ход этих процессов социальных институтов с применением соответствующих технологий. Широкую известность в этой связи в начале XXI века получили технологии управляемого выбора, основанные на так называемой теории мягкого подталкивания, разработанной Р.Талером и К.Санстейном (Нобелевская премия 2017 г.). Эти технологии предполагают использование не всегда очевидных инструментов и косвенных коммуникаций. Инструменты данных технологий – «это любой элемент архитектуры выбора, который меняет поведение человека предсказуемым способом, не ограничивая при этом его возможности выбора или не меняя в значительной степени его экономические стимулы» [2].

В арсенале технологий управляемого выбора все большее место занимают методы социальной инженерии и социального программирования, которые часто называют методами социального взлома или хакинга. Эти инструменты применяются во многих сферах человеческих отношений, в том числе и в маркетинговых системах. Получение нужной информации о тактике и стратегии товаропроизводящих и сервисных корпораций, их ценовой и маркетинговой политике, о работе с конкурентами и потребителями – некоторые из задач, решаемых с применением названных методов и технологий. Чтобы защититься от таких технологий в современном сложном мире, нужно знать их суть и правила применения.

Социальную инженерию можно определить как манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации. Объектом социальной инженерии является не компьютер или его программное обеспечение, а человек рядом с компьютерными системами. В более широком понимании социальная инженерия направлена на человека и его внутренний мир для получения нужной информации и желаемой модели поведения. Считается, что социальная инженерия – это, в общем-то, игра на пороках и слабостях людей. Среди чувств, к которым обычно взывают мошенники, выделяют четыре основных: любопытство, жалость, страх, жадность. Практически все методы социальной инженерии имеют отрицательную направленность и очень часто конфликтуют с нормами морали и этики. Проблема актуальна и потому, что применение социальной инженерии не требует значительных финансовых вложений и досконального знания компьютерных технологий.

Скрытая социальная инженерия не предполагает прямого воздействия на человека. В этом случае его ни к чему не принуждают, но искусственно создается ситуация, когда человек сам обращается, не подозревая, что становится объектом манипулирования.

Нужно знать, что социальная инженерия проводится по некоторым общим правилам, которые можно назвать инструментами социального взлома.

1. В процессе манипулирования первостепенное значение придается форме, а не содержанию. Дело в том, что очень много людей смотрят только на внешнюю атрибутику и не смотрят на суть. Это одно из основных правил социальной инженерии.

2. Социальные хакеры убеждены, что большинство людей переоценивают свою значимость. Такие люди отрицательно зависимы от своего чувства собственной значимости и поэтому могут быть хорошей мишенью для атаки. Считается, что у такого человека слабая «взрослая» компонента или в терминологии Фрейда слабое СуперЭго. Ему достаточно лишь чуть-чуть польстить, и "он что и не знал, расскажет, и что не мог, сделает" [3].

3. Третье правило социальной инженерии основано на утверждении, что ***многие люди нетерпеливы в своих желаниях и ленивы.*** Они хотят, чтобы все хорошее, что только с ними в жизни может произойти, произошло как можно быстрее и желательно с минимальными усилиями с их стороны. Поэтому социальные хакеры всячески потакают таким слабостям и не разочаровывают их в ожиданиях. Примеры действия этого правила можно найти в кредитных договорах с банками, с микрофинансовыми организациями, с операторами мобильной связи, с застройщиками, в торговых сетях при скидках и массовых распродажах и т.д.

4. Четвертое правило: ***играйте на слабости человека к деньгам – один из основных приемов в социальной инженерии.*** Применяется в разных вариациях: от банального подкупа до "писем счастья", в которых сказано, что "если перечислите на этот счет два доллара, то через месяц получите двадцать" [3].

В современном информационном пространстве основными инструментами социального взлома являются следующие приемы.

1. Фишинг (англ. fishing – рыбалка) на сегодняшний день один из самых распространенных видов социальной инженерии. По сути, фишинг это кибер-преступление, чаще всего направленное на получение информации для доступа к банковским счетам доверчивых пользователей. "Фишеры" используют поддельные электронные письма, якобы присылаемые банком, с просьбой подтвердить пароль или уведомление о переводе крупной суммы денег. Самое важное в том, что жертва совершает все эти

действия абсолютно добровольно. В настоящее время существуют различные виды фишинга – почтовый фишинг, уэйлинг (атака на руководство компаний), вишинг (атака по телефону от имени какой-то организации), фишинг в социальных сетях (Facebook, Instagram и Twitter) и другие [4].

2. Фарминг. Этот прием сводится к автоматическому перенаправлению пользователей на фальшивые сайты. Фарминг гораздо более опасен, чем фишинг, так как в отличие от фишинга этот метод хищения данных не требует отсылки писем потенциальным жертвам и соответственно их ответа на них.

3. Кража баз данных – это одна из основных областей применения социальной инженерии. В современном деловом мире имеется множество баз данных: в органах внутренних дел, в бизнес-структурах, в социальных фондах, в ритейле, в банковских учреждениях, в образовательной сфере и т.д. Характерно, что примерно в 80 случаях из 100 информацию воруют не по техническому каналу, а по социальному. Увольнение обиженного системного администратора вместе с базой данных, подкуп работающего сотрудника, или приход специалиста по ремонту компьютера – некоторые из примеров. Это сильно усложняет задачу защиты информации [**5].**

4. Еще один социоинженерный инструмент получения информации – ***участие в различных выставках, презентациях и т. д.*** Представитель компании, который стоит у стенда, нередко выдает самые сокровенные секреты компании, которые ему известны, отвечая на любые вопросы.

5. Обольщение, игра на эгоизме и слабостях пола. Существуют даже агентства, которые содержат обольстительниц самого разного вида. Цель их существования – получение прибыли путем "развода" состоятельных лиц мужского пола. Здесь не нужны сложные и дорогостоящие комбинации. Нужна только информация о «мишени»: какую еду и вино предпочитает, какие книги, каких девушек, какие машины, какую музыку и т.д. Далее создается «случайная» встреча.

6. Информация из открытых источников. Существует мнение, что около 90% всей закрытой информации разведчики всех уровней получают из открытых источников[4]. Происходит это по причине отсутствия личных и корпоративных информационных фильтров, самоконтроля и ответственности.

7. Взять интервью – один из самых простых, но вместе с тем и самых привлекательных способов получить информацию об организации: какие маркетинговые планы, кто конкуренты, какие новинки нас ожидают и т.д. Извлечение полезной деловой информации из разговора с кем-то, кто не подозревает, что является объектом манипулирования, называется ***скрытым допросом.*** При этом хакеру рекомендуется слегка "задеть" профессиональное самолюбие или, наоборот, разыграть из себя "дурака", попросив объяснить ту или иную деталь. Это весьма действенный способ, который состоит из соответствующих правил и алгоритмов. Но в любом случае нужно иметь максимум информации о собеседнике, включая его сильные и слабые стороны, знать психологические приемы манипулирования.

Социальное программирование отличается от социальной инженерии. Если социальная инженерия – это атака на конкретного человека, манипулирование им с целью получения нужной информации и/или соответствующей модели поведения, то социальное программирование, во-первых, не всегда связано с социальным взломом поведения и среды отдельных людей, во-вторых, это не одноразовое действие как при социальной инженерии.

Социальное программирование – процесс реализации какой-то программы, плана, где в центре внимания находится как единичный человек, так и группы людей (толпы, митинги, собрания, общество в целом), а также организации. Социальное программирование выступает в следующих основных формах:

- воспитание;
- процесс обучения в различных учебных заведениях;
- формирование и соблюдение традиций, обычаев, норм, стереотипов и шаблонов поведения;
- реклама и разная пиар-информация в различных СМИ, интернете, книгах, музыке, кино и др.;
- государственная идеология и пропаганда;
- «обработка» человека в разных социальных структурах – религиозных, деловых, политических, спортивных, обучающих и других.

Все современные информационные войны не только в режиме открытых военных, политических и корпоративных конфликтов основаны на социальном программировании.

Социальное программирование нужно рассматривать на двух основных уровнях.

А. Социальное программирование рассматривается как некоторая функция общества и государства по формированию и распространению социально приемлемого набора норм, традиций, привычек, целей и действий. Любая государственная идеология и конкретная политика реализуется через социальное программирование. В данном случае социальное программирование является составной частью социальных технологий.

Б. Социальное программирование как целенаправленное воздействие на человека или группу людей по изменению и насаждению нужных для субъекта программирования ценностей, норм, принципов, целей и действий, не всегда согласующихся с распространенными и массовыми. В данном случае – социальное программирование то же, что и зомбирование. По сути, это модификация или изменение массовых стереотипов.

Социальное программирование очень подвижная категория как в историческом, так в конкретном ситуативном измерении. Одна и та же ситуация в зависимости от целей ее участников может подаваться как разная по критериям морали, нравственности, успешности и приемлемости.

Но социальное программирование не обязательно специально выстроенная для определенных целей программа. Это неотъемлемый атрибут всей человеческой жизни. Все инструменты воспитания, наказания, поощрения, приобщения, обучения представляют собой арсенал социального программирования.

Основная концепция социального программирования состоит в том, что многие поступки людей и их реакции на то или иное внешнее воздействие во многих случаях предсказуемы. Конкретными целями социального программирования может быть обуздание агрессивной толпы, обеспечение победы какого-либо кандидата на очередных выборах, создание черного пиара для кандидата, распространение паники вокруг банка с целью его разорения, создание ажиотажного спроса на какой-то продукт или услугу и т.д. Это имеет значение в маркетинге, политике, рекламе и других сферах человеческой жизни.

В социальном программировании разработка схемы воздействия идет с конца, т. е. от нужного итога. Например, заместитель хочет стать руководителем. Он знает слабости начальника к алкоголю и женскому полу и в рамках социального программирования

поведения руководителя стимулирует эти слабости. Программа таких действий закономерно приводит к нужному финалу – проблемы со здоровьем, незавидная репутация начальника, и его фиаско.

Социальное программирование, в отличие от социальной инженерии, имеет более обширную область применения, т. к. работает со всеми категориями людей, независимо от того, частью какой системы они являются. Социальная же инженерия всегда работает только с человеком, который является частью компьютерной системы, хотя методы в том и другом случае используются аналогичные. Если социальная инженерия связана с реализацией, как правило, отрицательного влияния на поведение людей, то социальное программирование же, как и любая область знания, имеет и положительную и отрицательную область применения.

В современных условиях эти технологии социального хакинга поведения человека эффективно реализуются через СМИ, в первую очередь массовое телевидение, а также через интернет. Потребитель такой информации не имеет объективных критериев оценки ее объективности. Более того, массовый потребитель, как правило, существует в асимметричной информационной среде (ходит в один магазин, смотрит один телевизионный канал, читает одну газету), что может приводить к ложным оценкам и убеждениям. Массовому потребителю практически невозможно отличить фейки от объективной реальности. О том, что такое воздействие на личное и массовое поведение эффективно, свидетельствуют жесткие ограничительные меры некоторых государств по предотвращению внешнего воздействия многих средств массового влияния на свое население (instagram, youtube, tik-tok и другие).

Примером социального программирования является так называемое «Убийство форумов» где, с помощью социального вмешательства создают антирекламу тому или иному проекту. Социальный программист с помощью явных провокаторских действий в одиночку разрушает форум, пользуясь при этом несколькими псевдонимами (nickname) для создания вокруг себя постоянных недовольных посетителей проекта. В результате подобных мероприятий на форуме становится невозможным продвижение товаров или идей [5].

Социальное программирование нужно рассматривать в более широком контексте: как набор инструментов социальной адаптации, образовательной деятельности, профилактики отклоняющегося поведения, формирования социально приемлемых навыков, нужных привычек, формирования спроса на нужные товары и услуги, а также других эффектов.

Список использованных источников:

1. Асимметричность информации. Электронный ресурс]. – 2022. – Режим доступа: https://ru.wikipedia.org/wiki. – Дата доступа: 15.03.2022г.

2. Талер Р., Санстейн К. Подталкивание: как улучшить наши решения насчет здоровья, благосостояния и счастья. Thaler R., Sunstein C. nudge: improving decisions about health, wealth, and happiness. – new Haven: Yale Univ.. Press, 2008. – 293 p [Электронный ресурс]. – 2022. – Режим доступа: .https://cyberleninka.ru/article/n/2012-01-021-taler-r-sansteyn-k-podtalkivanie-kak-uluchshit-nashi-resheniya-naschet-zdorovya-blagososto yaniya-i-schastya-thaler-r-sunstein-c- Дата доступа: 15.03.2022г.

3. Магия социального взлома. Социальная инженерия: тонкая игра на людских слабостях. [Электронный ресурс] .- 2022. – Режим доступа: http://166509288.livejournal.com/744063.html – Дата доступа: 15.03.2022 г.

4. 11 типов фишинга и их примеры из реальной жизни. [Электронный ресурс]. – 2022. – Режим доступа: https://club.cnews.ru/blogs/entry/11_tipov_fishinga_i_ih_primery_iz_realnoj_zhizni- Дата доступа: 15.03.2022г.

5. М. Кузнецов, И. Симдянов. Социальная инженерия и социальные хакеры. Издательство: БХВ – Петербург, 2007. [Электронный ресурс]. – 2022. – Режим доступа: https://kartaslov.ru. – Дата доступа: 15.03.2022г.