DOI 10.22394/1726-1139-2021-8-97-107

Модель социального влияния в анализе социоинженерных атак*

Тулупьева Т. В.[1, *], *Абрамов М. В.*[2], *Тулупьев А. Л.*[3]

[1]Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация; *tulupeva-tv@ranepa.ru
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук, Санкт-Петербург, Российская Федерация
[3]Санкт-Петербургский государственный университет, Санкт-Петербург, Российская Федерация

РЕФЕРАТ

Целью данного исследования является модернизация модели социоинженерной атаки злоумышленника на пользователя, учитывающая более широкий круг факторов, влияющих на успех социоинженерной атаки, ассоциированных с принципами социального влияния. **Методы.** Для достижения поставленной цели были проанализированы подходы к социальному влиянию и составляющие социального влияния. Построена интегральная схема социального влияния, приземленная на контекст социоинженерных атак. **Результаты.** Предложена модель социального влияния, построенная в контексте социоинженерной атаки злоумышленника на пользователя. Предложено новое толкование термина уязвимость пользователя в контексте защиты информации. **Выводы.** Полученный результат формирует потенциал наполнения моделей пользователя и злоумышленника конкретными уязвимостями и компетенциями, что приведет к уточнению оценок успеха социоинженерной атаки злоумышленника на пользователя, за счет агрегации сведений из произошедших инцидентов.

Ключевые слова: социальное влияние, социоинженерные атаки, уязвимость пользователя, атакующее воздействие

Для цитирования: *Тулупьева Т. В., Абрамов М. В., Тулупьев А. Л.* Модель социального влияния в анализе социоинженерных атак // Управленческое консультирование. 2021. № 8. С. 97–107.

Model of Social Influence in Analysis of Socio-engineering Attacks

Tatyana V. Tulupieva[1, *], *Maxim V. Abramov*[2], *Alexander L. Tulupiev*[3]

[1]Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management, Branch of RANEPA), Saint-Petersburg, Russian Federation; *tulupeva-tv@ranepa.ru
[2]Saint-Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint-Petersburg, Russian Federation
[3]Saint-Petersburg State University, Saint-Petersburg, Russian Federation

ABSTRACT

The purpose of this study is to study the modernization of the model of an attacker's social engineering attack on a user, taking into account a wider range of factors influencing the success of a social engineering attack associated with the principles of social influence. **Methods.** To achieve this goal, the approaches to social influence and the components of social influence were analyzed. An integrated circuit of social influence is built, grounding in the context of socio-engineering attacks. **Results.** A model of social influence is proposed, built in the context of an attacker's social engineering attack on a user. A new interpretation of the term

*Работа выполнена в рамках проекта по государственному заданию СПБ ФИЦ РАН СПИИРАН № 0073-2019-0003; поддержана Санкт-Петербургским государственным университетом, проект № 73555239; при финансовой поддержке Фонда развития научных исследований и прикладных разработок СЗИУ РАНХиГС, РФФИ, проект № 20-07-00839.

user vulnerability in the context of information security has been proposed. **Conclusion.** The result obtained forms the potential of filling the user and attacker models with specific vulnerabilities and competencies, which will lead to a more accurate assessment of the success of the attacker's social engineering attack on the user, due to the aggregation of information from incidents that have occurred.

Keywords: social impact, socio-engineering attacks, user vulnerability, attack impact

For citing: Tulupieva T. V., Abramov M. V., Tulupiev A. L. Model of Social Influence in Analysis of Socio-engineering Attacks // Administrative consulting. 2021. N 8. P. 97–107.

Введение

По статистике[1] доля социоинженерных атак в общем объеме киберпреступлений в 2020 г. на юридические лица составила 45–67%, на частные лица — 51–76% (сводная информация за три квартала). Вместе с тем возрос размер ущерба компаний от такого рода воздействий. Наиболее распространенным способом оценки защищенности пользователей информационных систем от социоинженерных атак продолжает оставаться прямое тестирование, когда совершается атака на пользователей и дается заключение об уязвимости системы[2]. Такой анализ обладает рядом недостатков, связанных с отсутствием учета контекста проведения атаки, особенностей пользователя, подвергаемого воздействию. Одна и та же социоинженерная атака, которая не прошла в момент тестирования, может состояться в другой момент, просто потому что поменялись какие-то обстоятельства, у пользователя поменялось настроение или по иным причинам. Кроме того, сам факт тестирования может негативно сказываться на социально-психологическом климате в коллективе. В связи с этим актуальным видится подход к анализу защищенности пользователей информационных систем через оценку выраженности уязвимостей пользователя, то есть оценку степени его подверженности разным видам социоинженерных атак. Подверженность социоинженерной атаке, в свою очередь, связывается с выраженностью у пользователя различных психологических особенностей, психического состояния и другими факторами. Поиск и рассмотрение факторов, влияющих на успех атаки, является важной задачей в контексте обеспечения защищенности пользователей информационных систем от социоинженерных атак.

Социоинженерная атака — совокупность действий злоумышленника, направленных на другое лицо (или группу лиц) с целью достижения желаемого результата, в частности, нарушения безопасности информации (организации доступа к информации, передача ее другому лицу и т. п.) [15].

Данная статья посвящена рассмотрению термина уязвимости пользователя, выработке подхода, согласующегося с ГОСТом по защите информации[3], новому под-

[1] Актуальные киберугрозы: I квартал 2020 года // Positive Technologies. 2020. 16 июня [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/ (дата обращения: 12.02.2021); Актуальные киберугрозы: II квартал 2020 года // Positive Technologies. 2020. 16 июня [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/ (дата обращения: 12.02.2021); Актуальные киберугрозы: III квартал 2020 года // Positive Technologies. 2020. 16 июня [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/ (дата обращения: 12.02.2021).

[2] Социотехническое тестирование: какое лучше выбрать в 2021 году? // Group-IB — Хабр. 2020. 29 декабря [Электронный ресурс]. URL: https://m.habr.com/ru/company/group-ib/blog/535092/ (дата обращения: 12.02.2021).

[3] Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. — взамен ГОСТ Р 50922-96; введ. 01.02.2008 // СПС КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 12.02.2021).

ходу к социоинженерной атаке как к схеме социального влияния, где злоумышленник — это агент влияния, а пользователь информационной системы — реципиент. Теоретическая и практическая значимость полученного результата заключается в формировании потенциала наполнения моделей пользователя и злоумышленника конкретными уязвимостями и компетенциями, что приведет к уточнению оценок успеха социоинженерной атаки злоумышленника на пользователя, за счет агрегации сведений из произошедших инцидентов.

Подходы к социальному влиянию

Феномен социального влияния вызывает повышенный интерес у специалистов различных областей, имеющих дело с человеком в его социальном окружении, — психологов, социологов, психотерапевтов, социальных работников, врачей, педагогов, политиков и многих других. В таких направлениях психологической науки, как социальная психология, психология массовых коммуникаций, психология пропаганды, политическая психология, психология обучения и воспитания, психология малых и больших групп, психологическое консультирование и психотерапия социальное влияние находится в центре внимания и занимает ключевое место. При запросе в поисковых сервисах словосочетания «социальное влияние» Яндекс демонстрирует 5 млн результатов, Google — 38 млн.

Е.И. Середа в своей работе «Социальное влияние как предмет психологического исследования» выделяет несколько подходов к исследованию социального влияния: американский, европейский, российский и кросс-культурный [13]. Сравнение этих подходов можно представить в виде таблицы.

В соответствии с множественностью подходов к социальному влиянию разные исследователи предлагают свои определения социального влияния [7; 8; 9; 14; 16]. Обобщая имеющиеся определения для целей данной статьи, под социальным влиянием мы будем понимать воздействие на эмоциональную, интеллектуальную и/или поведенческую сферу другого человека с целью изменения в этих сферах. В данной статье мы сосредоточимся на межличностном влиянии вида «агент влияния — объект влияния». Другими словами, в поле нашего внимания войдет пятый и шестой уровень влияния по Г. Гарднеру [4], а первые четыре останутся за рамками рассмотрения. Если говорить о конечной цели социального влияния, особенно в контексте данной статьи, то ею является изменение социального поведения, а изменения в эмоциональной и интеллектуальной сферах являются лишь промежуточным этапом, подготовкой, основой для изменения поведения.

Составляющие социального влияния

При рассмотрении процесса социального влияния выделяют силы влияния, способы, виды, «мишени», источники влияния. Краткий анализ этих компонентов социального влияния позволит создать основу для разработки интегральной модели, объединяющей разрозненные направления.

Н.И. Семечкин рассматривает агента влияния (то есть, человека, который старается осознанно или неосознанно изменить поведение другого) и определяет, чем должен обладать субъект, чтобы оказывать социальное воздействие [12]. Для успешности социального влияния агент должен обладать или продемонстрировать одну или несколько сил влияния. Важно, что демонстрации прямой или косвенной (даже не обладания) силы влияния бывает достаточно для получения результата.

К силам влияния относятся [12]:

- возможность наказания или вознаграждения;
- экспертное влияние;

Таблица

Основные подходы к исследованию социального влияния [13]
Table. Basic approaches to the study of social influence

Подход	Особенности	Основные представители
Американский	Преимущественно индивидуально-центрированный и лабораторный. Наиболее длительный и обширный	Э. Аронсон, Дж. Брайант, Х. Брейкер, Г. Говард, Ф. Зимбардо, Т. Уилсон, Р. Чалдини, К. Штайнер, С. Аш, М. Шериф, С. Милгрэм
Европейский	Социоцентрированный подход. Придается особое значение социальному и культурному контекстам, в которых осуществляется тот или иной вид влияния, человек анализируется в контексте реальной жизни	С. Московичи, Э. Авермает, М. Домс, Дж. М. Левин, Ф. Йон, К. Йонас, Ж. Монмолен, Г. Петерс-Кюлингер, Ж. Пэшле, М. Хьюстон, В. Штребе
Российский	Находится на стыке двух подходов, американского и европейского, вследствие этого выделяются несколько направлений изучения социального влияния: информационное и межличностное воздействие и информационно-психологическая безопасность; межличностное влияние; влияние группы и субкультур на ценности и поведение молодежи	Г. А. Андреева, Т. А. Берсенева, Г. С. Грачев, Т. С. Кабаченко, И. К. Мельник, В. П. Пугачев, В. А. Рычкова, О. В. Москаленко, Е. Л. Доценко, М. Р. Душкина, Д. Е. Львов, Е. В. Сидоренко, Н. Ю. Синягина

- референтное влияние;
- нормативное влияние; сила власти и закона.

Помимо сил социального влияния Эдвард Джонс и Тейт Питтман [19] говорят о способах социального влияния, которые они связывают со стратегиями самопрезентации. К ним относятся: лесть и заискивание, самоназидательность, угрозы и запугивания, самовосхваление (самореклама), обвинение, просительность, демонстрация слабости, вызывание жалости. несмотря на то, что данные стратегии различны по своей сути, некоторые из них даже разнонаправлены друг другу, но у них есть общий компонент — вызвать эмоции, которые делают человека более подверженным влиянию, произвести нужное выгодное в данный момент впечатление.

Е. В. Сидоренко на основе работ Е. Л. Доценко, C. M. Steiner, E. E. Jones предлагает выделять виды влияния: аргументация, манипуляция, внушение, заражение, пробуждение импульса к подражанию, формирование благосклонности, просьба, игнорирование, принуждение [14]. При сравнении способов и видов социального влияния легко заметить совпадение и пересечение.

Для успешности и результативности социального влияния мало только иметь силы влияния, нужно, чтобы у объекта влияния или реципиента были определенные особенности, которые лежат в основе подверженности влиянию. Некоторые авторы называют эти особенности слабостями [6; 17] или мишенями. Под слабостями или мишенями подразумевают личностные структуры, определенные психические образования человека [5; 11] или «те особенности личности, ее слабости, потребности и желания, на которые воздействует инициатор, и в результате этого объект при-

нимает нужное инициатору решение» [7]. Мы в данной статье будем пользоваться понятием уязвимость. Далее мишени, слабости и уязвимости будут употребляться как синонимы. Д. В. Ольшанский [10] среди таких уязвимостей отмечал наличие большого количества автоматизмов в деятельности человека, которые существенно экономят психическую энергию и время, но при должном воздействии на них служат прекрасной платформой для манипулирования, поскольку выключают рефлексирующую составляющую, то есть критическое осмысление, из процесса деятельности. Г. Грачев и И. Мельник к мишеням относят пять групп психических образований [5]:

- побудители активности человека;
- регуляторы активности человека;
- когнитивные структуры;
- операциональный состав деятельности;
- психические состояния.

В. П. Шейнов к мишеням относит потребности, слабости, пристрастия и привычные ритуалы [17]. Никакую мишень реципиента нельзя рассматривать изолированно, в отрыве от других особенностей. Наличие мишени еще не обеспечивает успешность социального влияния и социоинженерной атаки, знание мишеней является необходимым условием, но не достаточным. Например, мы знаем, что у сотрудника организации существует потребность в деньгах. Это мишень, но из этого не следует однозначно, что он при первом же предложении продаст секретную информацию организации. Он может выбрать другие варианты удовлетворения своей потребности, и у него возникнут другие мотивы, запускающие иную деятельность для получения результата. Да и нужно, чтобы у агента влияния в распоряжении было то, что является важным и значимым для реципиента, чтобы социальное влияние было успешным.

Интегральная модель социального влияния

Следовательно, социальное влияние нужно рассматривать не как отдельно силы агента влияния, отдельно слабости реципиента и отдельно виды влияния, а как сложный комплекс, состоящий из возможностей и компетенций агента влияния (в которые включается владение способами и видами влияния), а также потребности, личностные особенности, психические свойства и состояния реципиента. Обобщая все рассмотренные подходы, мы предлагаем интегральную модель социального влияния в контексте социоинженерных атак (рис. 1).

Предлагаемая модель объединяет в общую картину различные компоненты социального влияния. Агент влияния, обладая определенными силами воздействия, выбирает, в соответствии с уязвимостями пользователя и учитывая контекст, то или иное воздействие, усиливает его способами влияния (или стратегиями самопрезентации) для получения желаемого результата. Усилением атакующего воздействия будет действие, направленное на изменение эмоционального (психического) состояния. Самим атакующим воздействием будет действие, направленное на совершение жертвой действия.

Отдельно в контексте социального влияния важно рассмотреть понятие уязвимости пользователя в контексте информационной безопасности. ГОСТ Р 50922-2006 определяет уязвимость (информационной системы), брешь как «свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации»[1]. Уязвимость пользователя может быть определена как

[1] Защита информации. Основные термины и определения: ГОСТ Р 50922-2006 — взамен ГОСТ Р 50922-96; введ. 01.02.2008 // СПС КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 20.02.2021).

конфигурация степени выраженности психологических особенностей, психических состояний и иных факторов, влияющих на успех социоинженерной атаки и характеризующих пользователя, которые в совокупности создают возможность реализации угроз атакующих воздействий злоумышленника.

Атакующим воздействием в данной модели будет выступать вид влияния (просьба, убеждение, поручение/приказ, манипуляция, описание желаемой модели). Атакующее воздействие усиливается контекстом: демонстрация слабости, игнорирование, угроза/запугивание, самовосхваление, вина, похвала, аргументы.

Разберем такой пример. Руководитель компании желает повысить уровень профессионализма своих подчиненных, но они не хотят тратить свое личное время и усилия на повышение квалификации. Чтобы изменить ситуацию, руководитель вводит премию за успешное повышение квалификации. В таких условиях увеличивается число сотрудников, повышающих свой профессиональный уровень. Здесь руководитель обладает силой вознаграждения и, используя просьбу («Я прошу вас пройти курсы повышения квалификации»), убеждения («Повышать свою квалификацию полезно») или поручение («Поручаю вам выбрать и пройти один из образовательных курсов онлайн»), получает нужный результат. Само воздействие он может усилить, используя похвалу («Вы самый опытный работник и лучше всех понимаете важность обучения»), или аргументацию («По статистике работник, регулярно повышающий квалификацию, в среднем получает зарплату выше, чем остальные»), или другой способ усиления воздействия. Конечно, выбранная стратегия будет действовать на тех сотрудников, у которых есть потребность в деньгах.

Эта схема социального влияния хорошо ложится в основу схемы социоинженерной атаки, где злоумышленник — это агент влияния, а пользователь информационной системы — реципиент. Подходы к описанию профиля злоумышленника были предприняты в ряде работ [1; 3; 18]. Модель злоумышленника [18] включает в себя ресурсы, доступные злоумышленнику (в частности, это подразумевает возможность вознаграждать и наказывать), профиль компетенций злоумышленника (который позволит ему использовать экспертную или референтную силу влияния), умение использовать вид атакующего действия (т. е. правильно подбирать вид воздействия и способы его усиления), знания злоумышленника о системе (в частности, о тех потребностях, особенностях, слабостях, которые есть у пользователя) (рис. 2).

Рассматривая модель пользователя, говорят о профиле уязвимостей [2]. В построение профиля уязвимостей пользователя существенный вклад может внести его психологический профиль, отражающий уровень выраженности психологических особенностей. Здесь мы можем говорить о его потребностях, ценностях, слабостях, присущих реципиенту в модели социального влияния. К слабостям можно отнести и общий уровень подверженности манипулятивному воздействию, о котором говорят авторы. Поскольку у реципиента может быть несколько источников или мишеней, то у пользователя несколько уязвимостей, степень их выраженности может различаться, и в этом случае целесообразно рассматривать профиль уязвимостей как модель системы всех уязвимостей пользователя. Соответственно, упомянутые в модели социального влияния потребности, ценности, слабости (то есть психологические особенности пользователя) лежат в основе формирования уязвимостей и при правильно подобранном воздействии агента влияния или злоумышленника могут спровоцировать вредоносные действия. Взаимосвязь между психологическими особенностями, уязвимостями и вредоносными действиями пользователя представлены на рис 3.

На рис. 3 введены следующие обозначения: ПС — психическое состояние, ПО — психологическая особенность, ДП — деструктивное поведение, УП — уязвимость пользователя.

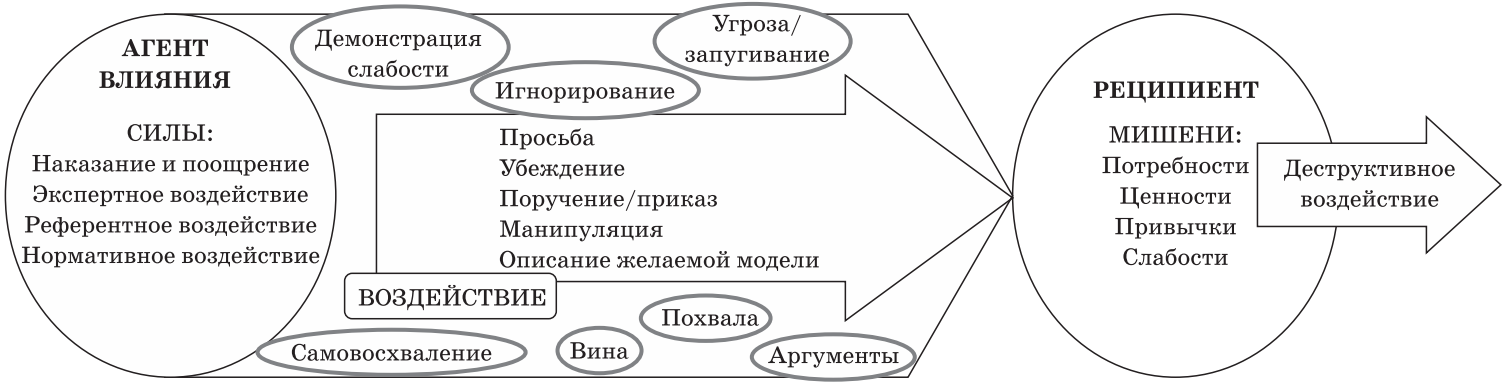

Рис. 1. Интегральная модель социального влияния
Fig. 1. Integral model of social influence

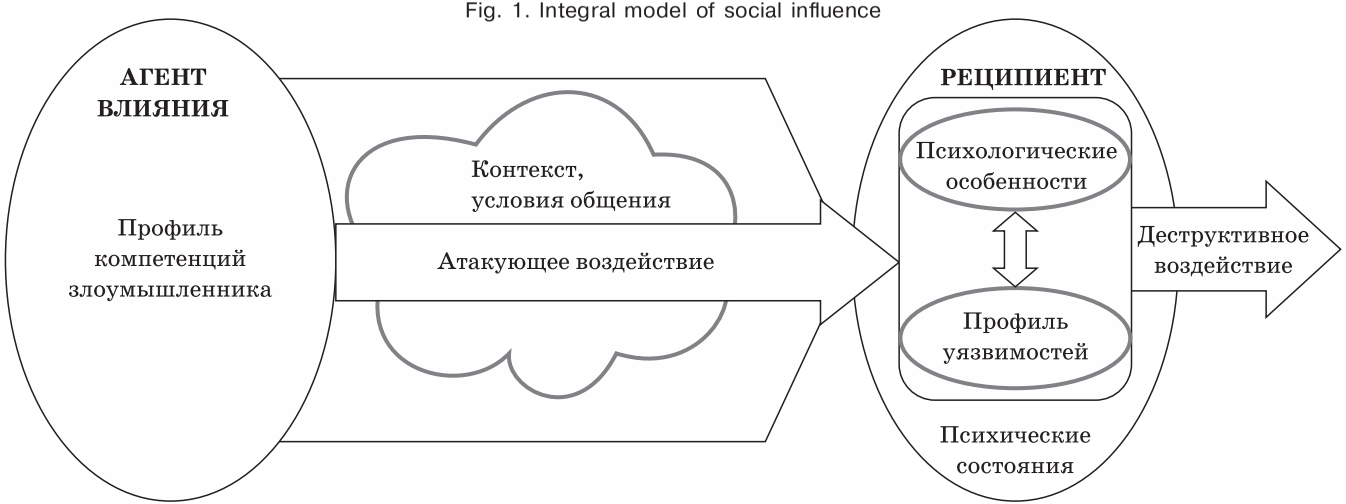

Рис. 2. Схема социоинженерной атаки
Fig. 2. Socio-engineering attack scheme

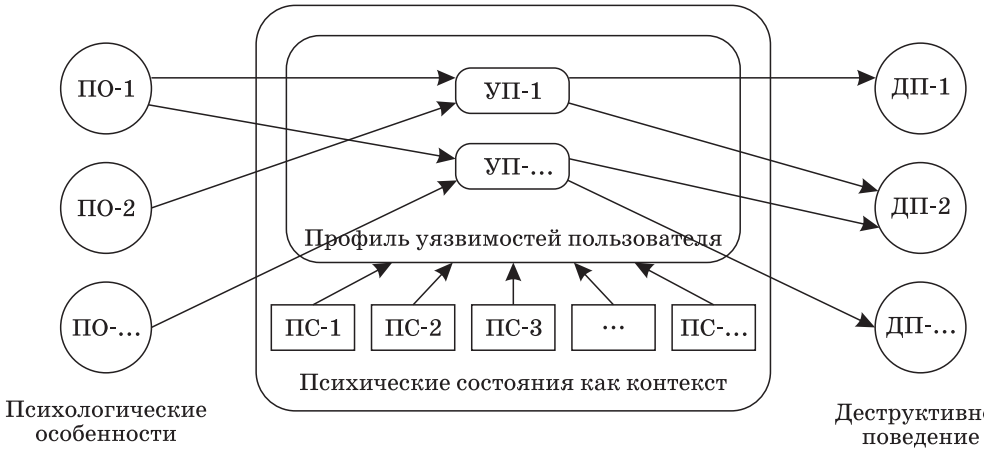

Рис. 3. Система «профиль психологических особенностей — профиль уязвимостей — деструктивное поведение» (приводится по: [2])
Fig. 3. The system "profile of psychological characteristics — profile of vulnerabilities — destructive behavior"

Анализ социоинженерной атаки с использованием модели социального влияния

Рассмотрим следующую социоинженерную атаку, которая является достаточно типичной и выполнена с использованием вредоносной ссылки.

«В 2015 г. клиенты одной почтовой системы получили электронные письма, в которых говорилось: “В связи с недавним обновлением нашего SSL-сервера и для улучшения обслуживания вы должны обновить свои данные для входа в систему. Для этого вам необходимо выполнить обновление по ссылке ниже”. Также было прислано предупреждение, что если не активировать ссылку в течение 48 часов, учетная запись Yahoo будет приостановлена или деактивирована» [21].

Агент влияния: использует силу вознаграждения (улучшение обслуживания) и экспертного влияния (Известное имя почтовой системы).

Вид воздействия: поручение (вам необходимо).

Усиление: угроза — «если не активировать ссылку в течение 48 часов, учетная запись будет приостановлена или деактивирована».

Особенности пользователя: потребность оставаться на связи, потребность пользоваться более качественным продуктом, страх остаться без электронной почты, отсутствие понимания возможных мошеннических действий.

Этот пример показателен тем, что рассылка была массовой: силы влияния, вид воздействия и способ усиления были одинаковы для всех. Но успешной эта социоинженерная атака оказалась только на тех пользователей, которые обладали всеми перечисленными «источниками».

Выводы

Схема социального влияния, объединяющая в общую картину агента влияния, обладающего определенными силами воздействия и усиливающими их способами влияния, хорошо ложится в основу модели социоинженерной атаки. Новый подход позволяет произвести качественное продвижение в построении усовершенствованных моделей пользователя и злоумышленника, а также оценки успеха социо-

инженерной атаки. Агентом влияния выступает злоумышленник, сила воздействия может быть рассмотрена как ресурс, само воздействие — как применение компетенции, а усиление — как степень выраженности компетенции. Потребности или мишени реципиента можно рассматривать как его уязвимости.

Заключение

Таким образом, в данной статье представлена интегральная модель социального влияния, предложено новое толкование термина уязвимости пользователя, выработан подход, согласующегося с ГОСТом по защите информации. Предложена новая модель социоинженерной атаки как схемы социального влияния, где злоумышленник — это агент влияния, а пользователь информационной системы — реципиент. Теоретическая и практическая значимость полученного результата заключается в формировании потенциала наполнения моделей пользователя и злоумышленника конкретными уязвимостями и компетенциями, что приведет к уточнению оценок успеха социоинженерной атаки злоумышленника на пользователя, за счет агрегации сведений из произошедших инцидентов.

Литература

1. *Абрамов М. В.* Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак / М. В. Абрамов, А. А. Азаров, Т. В. Тулупьева, А. Л. Тулупьев // Информационно-управляющие системы. 2016. № 4. С. 77–84.
2. *Абрамов М. В., Тулупьев А. Л., Тулупьева Т. В.* Психологические особенности, психические состояния пользователя и профиль его уязвимостей в контексте социоинженерных атак // Психология психических состояний : сб. статей студентов, магистрантов, аспирантов и молодых ученых. Казань, 2019. С. 312–317.
3. *Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л.* Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб. : ГУАП, 2018. 266 с.
4. *Гарднер Г.* Искусство и наука влияния на взгляды людей. М., 2008. 247 с.
5. *Грачев Г., Мельник И.* Манипулирование личностью. М., 2003. 376 с.
6. *Доценко Е. Л.* Психология манипуляции: феномены, механизмы и защиты. М. : ЧеРо, Издательство МГУ, 1997. 344 с.
7. *Зимбардо Ф., Ляйпе М.* Социальное влияние. СПб., 2001. 448 с.
8. *Кабаченко Т. С.* Методы психологического воздействия: учеб. пособие. М. : Педагогическое общество России, 2000. 544 с.
9. *Львов Д. Е.* Психология межличностного влияния : уч.-метод. пособие. Ижевск, 2005. 110 с.
10. *Ольшанский Д. В.* Психология масс. СПб. : Питер, 2001. 363 с.
11. *Пую Ю. В.* Истоки и генезис феномена манипулирования // Известия Российского государственного педагогического университета им. А. И. Герцена. 2009. № 90. С. 138–143.
12. *Семечкин Н. И.* Психология социального влияния. СПб. : Речь, 2004. 304 с.
13. *Середа Е. И.* Социальное влияние как предмет психологического исследования // Вестник Псковского государственного университета. Сер.: Социально-гуманитарные науки. 2009. № 9. С. 124–129.
14. *Сидоренко Е. В.* Тренинг влияния и противостояния влиянию. СПб. : Речь. 2002. 225 с.
15. *Социоинженерные* атаки. Проблемы анализа / А. А. Азаров, Т. В. Тулупьева, А. В. Суворова, А. Л. Тулупьев и др. СПб. : Наука, 2016. 352 с.
16. *Тернер Дж.* Социальное влияние. СПб., 2003. 256 с.
17. *Шейнов В. П.* Скрытое управление человеком. М. : АСТ. 2005. 816 с.
18. *Abramov M. V., Tulupyev A. L.* Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnurabilities and malefactor competencies in the attacking impact success prediction // Artificial Intelligence and Natural Language. 2019. P. 47–58.
19. *Jones E. E., Pittman T. S.* Toward a General Theory of Strategic Self-Presentation // Psychological Perspectives on the Self / ed. J. Suls, 1982. Vol. 1. Erlbaum, Hillsdale. P. 231–262.

20. *Michael A., Eloff J.* Discovering “Insider IT Sabotage” based on human behaviour // Information and Computer Security. 2020. Vol. 28. N 4. P. 575–589.
21. *Rubia F., Affan Y., Lin L., Wang J. at al.* Data for: Are the Con Artists Back? Deciphering Social Engineering Attacks. 2019. 04 августа [Электронный ресурс]. URL: https://data.mendeley.com/datasets/yw2djp4vdg/1 (дата обращения: 12.02.2021).

Об авторах:

Тулупьева Татьяна Валентиновна, доцент факультета государственного и муниципального управления Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), кандидат психологических наук, доцент; tulupeva-tv@ranepa.ru

Абрамов Максим Викторович, руководитель лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского Федерального исследовательского центра Российской академии наук (Санкт-Петербург, Российская Федерация), кандидат технических наук; mva@dscs.pro

Тулупьев Александр Львович, профессор кафедры информатики Санкт-Петербургского государственного университета (Санкт-Петербург, Российская Федерация), доктор физико-математических наук, профессор; alt@dscs.pro

References

1. Abramov M. V. Model of the profile of the attacker’s competencies in the task of analyzing the security of information systems personnel from socioengineering attacks / M. V. Abramov, A. A. Azarov, T. V. Tulupyeva, A. L. Tulupyev // Information and control systems [Informatsionno-upravlyayushchie sistemy]. 2016. No. 4. P. 77–84. (In rus)
2. Abramov M. V., Tulupiev A. L., Tulupyeva T. V. Psychological features, mental states of the user and profile of his vulnerabilities in the context of socioengineering attacks // Psychology of mental states: collection of articles of students, undergraduates, graduate students and young scientists. Kazan, 2019. P. 312–317. (In rus)
3. Abramov M. V., Tulupyeva T. V., Tulupyev A. L. Socioengineering attacks: social networks and assessments of user security. St. Petersburg: GUAP, 2018. 266 p. (In rus)
4. Gardner H. The Arts And Human Development: translation from English. M., 2008. 247 p. (In rus)
5. Grachev G., Melnik I. Manipulation of personality. M, 2003. 376 p. (In rus)
6. Docenko E. L. Psychology of manipulation: phenomena, mechanisms and defenses. M.: CheRo, Moscow State University Publishing House, 1997. 344 p. (In rus)
7. Zimbardo F., Leipe M. Social influence. St. Petersburg, 2001. 448 p. (In rus)
8. Kabachenko T. S. Methods of psychological impact: teaching manual. M.: Pedagogical Society of Russia, 2000. 544 p. (In rus)
9. Lvov D. E. Psychology of interpersonal influence: teaching method. allowance. Izhevsk, 2005. 110 p. (In rus)
10. Olshansky D. V. Psychology of the masses. St. Petersburg: Piter, 2001. 363 p. (In rus)
11. Puyu Yu. V. Origins and the genesis of the phenomenon of manipulation // News of the Russian Herzen State Pedagogical University [Izvestiya Rossiiskogo gosudarstvennogo pedagogicheskogo universiteta im. A. I. Gertsena]. 2009. No. 90. P. 138–143. (In rus)
12. Semechkin N. I. Psychology of social influence. St. Petersburg: Speech, 2004. 304 p. (In rus)
13. Sereda E. I. Social influence as a subject of psychological research // Bulletin of Pskov State University. Series: Social and Humanities Sciences [Vestnik Pskovskogo gosudarstvennogo universiteta. Ser.: Sotsial’no-gumanitarnye nauki]. 2009. No. 9. P. 124–129. (In rus)
14. Sidorenko E. V. Training influence and opposition to influence. St. Petersburg: Speech. 2002. 225 p. (In rus)
15. Socioengineering attacks. Problems of analysis / A. A. Azarov, T. V. Tulupyeva, A. V. Suvorova, A. L. Tulupyev, M. V. Abramov, R. M. Yusupov. St. Petersburg: Science, 2016. 352 p. (In rus)
16. Turner J. Social influence. St. Petersburg, 2003. 256 p. (In rus)
17. Sheynov V. P. Hidden human control. M.: AST. 2005. 816 p. (In rus)
18. Abramov M. V., Tulupyev A. L. Soft estimates of user protection from social engineering attacks: fuzzy combination of user vulnurabilities and malefactor competencies in the attacking impact success prediction // Artificial Intelligence and Natural Language. 2019. P. 47–58.
19. Jones E. E., Pittman T. S. Toward a General Theory of Strategic Self-Presentation // Psychological Perspectives on the Self / ed. J. Suls, 1982. Vol. 1. Erlbaum, Hillsdale. P. 231–262.

20. Michael A., Eloff J. Discovering “Insider IT Sabotage” based on human behaviour // Information and Computer Security. 2020. Vol. 28. N 4. P. 575–589.
21. Rubia F., Affan Y., Lin L., Wang J. at al. Data for: Are the Con Artists Back? Deciphering Social Engineering Attacks. 2019. 04 августа [Electronic resource]. URL: https://data.mendeley.com/datasets/yw2djp4vdg/1 (date of the address: 12.02.2021).

About the authors:

Tatyana V. Tulupieva, Associate Professor of the Faculty of State and Municipal Management of North-West Institute of Management, Branch of RANEPA (St. Petersburg, Russian Federation), PhD in Psychology, Associate Professor; tulupeva-tv@ranepa.ru

Maxim V. Abramov, Head of the Laboratory of Theoretical and Interdisciplinary Problems of Informatics of the St. Petersburg Federal Research Center of the Russian Academy of Sciences (St. Petersburg, Russian Federation), PhD in Technical Science; mva@dscs.pro

Alexander L. Tulupiev, Professor of the Department of Informatics of St. Petersburg State University (St. Petersburg, Russian Federation), Doctor of Science (Physics and Mathematics), professor; alt@dscs.pro