ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ, ПСИХИЧЕСКИЕ СОСТОЯНИЯ ПОЛЬЗОВАТЕЛЯ И ПРОФИЛЬ ЕГО УЯЗВИМОСТЕЙ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК[1]

USER'S PSYCHOLOGICAL TRAITS, MENTAL STATES, AND VULNURABILITIES PROFILE IN THE CONTEXT OF SOCIAL ENGENEERING ATTACKS

Абрамов М.В., Тулупьев А.Л., Тулупьева Т.В.
Abramov M.V., Tulupyev A.L., Tulupyeva T.V.

Аннотация. В статье представлены основы социальной манипуляции, как способа воздействия на пользователей информационной системы, к которой злоумышленник пытается получить доступ для нарушения информационной безопасности компании. Приведены примеры уязвимостей пользователя к социоинженерным атакам. Обозначена взаимосвязь между психологическими особенностями пользователя и его уязвимостями, а также неоходимость учета психического состояния при оценке последствий атакующего действия злоумышленника Полученные результаты составляют основу для математического моделирования профиля уязвимостей пользователя, построения иерархии моделей данного профиля. На их основе можно оценить вероятность успешной реализации атакующего воздействия злоумышленника на пользователя.

Ключевые слова. Социоинженерные атаки, социальные сети, уязвимости пользователей, информационная безопасность, психические состояния пользователя.

Abstract. The article presents the basics of social manipulation, as a means of influencing users of an information system, to which an attacker tries to gain access to violate the company's information security. Examples of user vulnerabilities to socioinnergive attacks are given. The relationship between the psychological characteristics of the user and his vulnerabilities is indicated, as well as the need to take into account the psychological state when assessing the consequences of the attacking action of the evil-intentioned user. On this basis, it is possible to estimate the probability of the successful implementation of the attacker's attack on the user.

Keywords. Social engineering attacks, social media, user vulnerabilities, information security, mental state of the user.

Введение

В настоящее время персонал, особенно, административное звено активно использует современные компьютерные технологии для организации производственного процесса, внешней и внутренней коммуникации и хранения информации. Для защиты информации

[1] Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2019-0003, при финансовой поддержке РФФИ, проект №18-01-00626– Методы представления, синтеза оценок истинности и машинного обучения в алгебраических байесовских сетях и родственных моделях знаний с неопределенностью: логико-вероятностный подход и системы графов; проект № 18-37-00323 – Социоинженерные атаки в корпоративных информационных системах: подходы, методы и алгоритмы выявления наиболее вероятных траекторий.

от внешнего вторжения службы информационной безопасности пытаются использовать различные современные программно-технические системы обеспечения защиты данных, препятствующие доступу злоумышленника к ним. Тем не менее, представленные сегодня системы защиты информации, несмотря на декларируемые эффективность, надежность, сложность структуры, не позволяют в полной мере решать вопросы обеспечения, поддержания и мониторинга информационной безопасности организации, поскольку, концентрируясь на программно-технической составляющей автоматизированных информационных систем, они упускают из рассмотрения пользователей как существенной компоненты, с которой связаны риски, изучаемые в сфере Human Reliability. В действительности же пользователь и, даже шире, сотрудник не редко оказывается самым уязвимым элементом в системе безопасности организации, в том числе и в системе ее информационной безопасности [14]. Любой сотрудник или клиент компании (как санкционированный пользователь информационной системы, так и несанкционированный), имеющий доступ к конфиденциальной информации или к устройствам, на которых эта информация хранится, может нарушить ее безопасность (в частности конфиденциальность, целостность или доступность) преднамеренно или случайно [1]. Именно поэтому требуется как изучать, выявлять и предотвращать социоинженерные атаки, направленные на пользователя, так и выявлять особенности самих пользователей, создающие благоприятный контекст для развития и успешной реализации социоинженерных атак. Иначе говоря, для выработки эффективных методик предотвращения социоинженерных атак необходимо выявить причину успешности осуществления этих атак, то есть, в частности, понять, чем они обусловлены или какой психологический контекст способствует их успеху; другими словами, обращаясь к классике – самым подробным образом отвечать на вопрос «почему хорошие люди делают плохие вещи» [16] в сфере информационной безопасности, выполняя свои рабочие функции

Под социоинженерной атакой будем понимать совокупность действий злоумышленника, направленную 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.) [4].

Основы социальной манипуляции

Злоумышленники, обладающие навыками социоинженеров, с легкостью могут повлиять на неподготовленного сотрудника, имеющего доступ к компьютеру, подключенному к корпоративной сети (корпоративной информационной системе), с целью получения именно той информации, которая им нужна. Для предотвращения этого необходимо научиться прогнозировать степени выраженности уязвимостей пользователей информационных систем, знать степень их подверженности технологиям социального манипулирования [9, 10, 15]. Мы предполагаем, что в построение профиля уязвимостей пользователя существенный вклад может сделать его психологический профиль, отражающий уровень выраженности психологических особенностей [2, 3, 4]. Вместе с тем, нельзя упускать из виду, что психологический профиль пользователя, к которому мы обратимся чуть позже, является важной, но не единственной информационной составляющей в построении профиля уязвимостей пользователя. Одной из перспективных составляющих в построении профиля уязвимостей пользователя представляется использование общего уровня подверженности

манипулятивному воздействию на пользователя [18]. Данный показатель может влиять на степень подверженности пользователя к социоинженерным атакующим воздействиям, которые используют именно такие характеристики пользователя, как доверчивость, лень, любезность и даже энтузиазм сотрудников организации.

Социальную манипуляцию рассматривают как вид психологического воздействия или психологического влияния [13, 17]. Если мы не рассматриваем социоинженерную атаку по рекомпенсационному типу, когда злоумышленник совершает ряд действий, показывающих его заинтересованность в информации и возможности получения вознаграждения лицами, предоставляющими такую информацию, то в остальных видах социоинженерных атак технологии социального манипулирования применяются активно.

Обратим внимание, что одних только сил влияния недостаточно для успешного осуществления социоинженерной атаки. Нужна еще соответствующая особенность другой стороны – сотрудника, – которую некоторые авторы называют слабостью [8] или мишенью [7, 12], а мы будем пользоваться понятием уязвимость.

Примеры уязвимостей пользователя.

В качестве мишеней выделяются личностные структуры, определенные психические образования человека [12]. Шейнов В.П. дает более конкретное описание мишеней – «те особенности личности, ее слабости, потребности и желания, на которые воздействует инициатор, и в результате этого объект принимает нужное инициатору решение» [18]. Классификация мишеней содержит пять групп психических образований [7]:

1) побудители активности человека: потребности, интересы, склонности;

2) регуляторы активности человека: групповые нормы, самооценка (в том числе, чувство собственного достоинства, самоуважение, гордость), субъективные отношения, мировоззрение, убеждения, верования, смысловые, целевые, операциональные установки и т. д.;

3) когнитивные (информационные) структуры (в том числе, информационно-ориентировочная основа поведения человека в целом) – знания об окружающем мире, о людях и другие разнообразные сведения, которые являются информационным обеспечением активности человека;

4) операциональный состав деятельности: способ мышления, стиль поведения и общения, привычки, умения, навыки и т. п.;

5) психические состояния: фоновые, функциональные, эмоциональные.

Представляется, что знание мишеней является необходимым условием для осуществления социоинженерной атаки, но не достаточным. Из того, что у сотрудника существует потребность в деньгах, не следует однозначно, что он при первом же предложении продаст конфиденциальную информацию организации. Для этого нужно, чтобы из всех возможностей удовлетворить свою потребность, он выбрал бы именно этот способ удовлетворения. А есть еще варианты, например, найти временную подработку, пересмотреть свои приоритеты и т.д., которые зависят от других особенностей личности. Следовательно, получается сложный комплекс, состоящий из потребности, личностных особенностей, психических свойств и состояний. При осознании предмета, который способен удовлетворить потребность, формируется мотив [11], который, в свою очередь запускает деятельность, нацеленную на получение определенного результата.

И здесь мы приходим к уточнению важного понятия – уязвимость. По ГОСТ Р. 56546-2015 уязвимость определяется как недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации [6]. Уязвимость пользователя – комплексное образование, основывающееся на психических феноменах (свойствах, процессах, состояниях), использование которого может привести к успешности социоинженерной атаки и инициировать вредоносные действия пользователя. У пользователя уязвимостей несколько, степень их выраженности может различаться, и в этом случае целесообразно рассматривать профиль уязвимостей как модель (разной степени полноты и завершенности) системы всех уязвимостий пользователя. В основе уязвимости может лежать несколько психологических особенностей, равно как и одна и та же психологическая особенность может обеспечивать различные уязвимости. Взаимосвязь между психологическими особенностями, уязвимостями и вредоносными действиями пользователя представлены на рис. 1.

На рис. 1 введены следующие обозначения: ПС – психологическое состояние, ПО – психологическая особенность ДП – деструктивное поведение, УП – уязвимость пользователя.

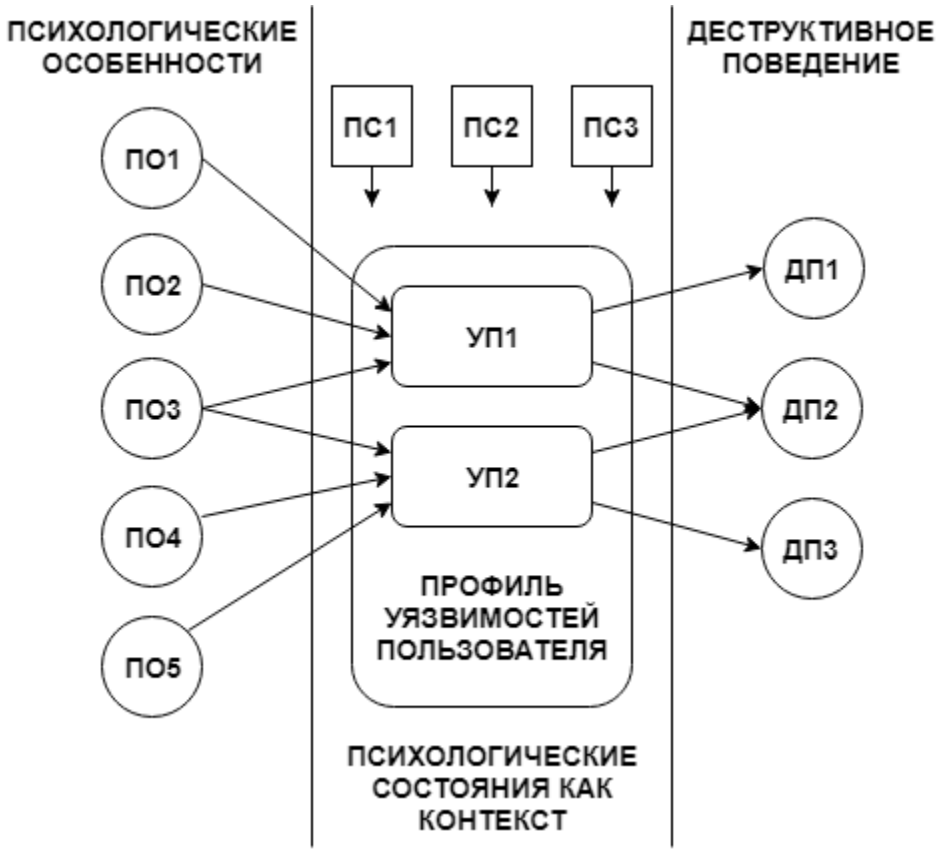

Рис. 1. Система «профиль психологических особенностей – профиль уязвимостей – деструктивное поведение»

Для определения уязвимостей авторами было проведено исследование [14], в результате которого выявилось пять факторов (в скобках указаны психологические особенности, с которыми они оказались связаны):

1) информационная неосмотрительность (низкая потребность в поиске новых ощущений, высокая общая самооценка, низкая самооценка внешности);

2) слабый пароль (психологическая защита по типу регрессия, подозрительность, самооценка уверенности в себе, недостаточная уровень слуховой памяти, выраженность меланхолических черт);

3) техническая халатность и установка на получение личной выгоды (уровень притязаний по практическим умениям, пониженный уровень притязаний по уверенности в себе, повышенная самооценка своего авторитета, пониженная самооценка умственных способностей, несклонность к мстительности, дипломатичность, несклонность к риску, психологическая защита по типу отрицания, подозрительность);

4) техническая неопытность (психологическая защита по типу вытеснение и рационализация, сдержанность, пониженная чувствительность, консерватизм, склонность к компромиссам, психологический возраст);

5) техническая безграмотность (психологическая защита по типу замещение, интеллект, эмоциональная нестабильность, расслабленность, высокая общая интернальность, низкая интернальность в области неудач и достижений, высокая интернальность в области межличностных отношений).

Заключение

В статье представлены основы социальной манипуляции, как способа воздействия на пользователей информационной системы, к которой злоумышленник пытается получить доступ для нарушения информационной безопасности компании. Приведены примеры уязвимостей пользователя к социоинженерным атакам. Обозначена взаимосввязь между психологическими особенностями пользователя, психическими состояниями и его уязвимостями. Полученные результаты составляют основу для математического моделирования профиля уязвимостей пользователя, построения иерархии моделей данного профиля. На их основе можно оценить вероятность успешной реализации атакующего воздействия злоумышленника на пользователя.

Список литературы

1. *Shaw E.,* The insider threat to information systems: The psychology of the dangerous insider / Shaw E., Ruby K., Post J. //Security Awareness Bulletin. – 1998. – Т. 2. – №. 98. – С. 1-10.
2. *Абрамов М.В.* Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений: в 2 т. / М.В. Абрамов, А.А. Азаров // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2017). Санкт-Петербург. – 2017. – Т. 1. – С. 130-133.
3. *Абрамов М.В*. Задача анализа защищённости пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей / Абрамов М.В., Тулупьев А.Л., Сулейманов А.А. // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – № 2. – С. 313-321.
4. *Азаров А.А.* Социоинженерные атаки. Проблемы анализа. / А.А. Азаров, Т.В. Тулупьева, А.В. Суворова, А.Л. Тулупьев, М.В, Абрамов, Р.М. Юсупов. – СПб.: Наука, 2016. – 352 с.
5. *Багрецов Г.И.* Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети: в 2 т. / Г.И. Багрецов, Н.А. Шиндарев, М.В. Абрамов, Т.В. Тулупьева // Труды VII всероссийской научно-практической конференции «Нечёткие системы, мягкие вычисления и интеллектуальные технологии» НСМВИТ–2017 (г. Санкт-Петербург, 3–7 июля, 2017 г.). – 1. СПб.: Политехника-сервис, 2017. С. 9-16.

6. ГОСТ Р. 56546-2015«Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» //М.: Стандартинформ. – 2015.

7. *Грачев Г.* Манипулирование личностью / Г. Грачев, И. Мельник. – М., 2003. – 376 с.

8. *Доценко Е.Л.* Психология манипуляции: феномены, механизмы и защиты/ Е.Л. Доценко – М.: 2000.

9. *Кузнецов М.В.* Социальная инженерия и социальные хакеры / М.В. Кузнецов , И.В. Симдянов – БХВ – Петербург. 2007. –250 с.

10. Митник К.Д. Искусство обмана / К.Д. Митник , В.Л. Саймон – М.: Компания АйТи, 2004. – 360 с.

11. *Молл Е.Г.* Менеджмент: Организационное поведение: Учебное пособие / Е.Г. Молл – М.: Финансы и статистика, 1998. – 160 с.

12. *Пую Ю.В.* Истоки и генезис феномена манипулирования / Ю.В. Пую // Известия Российского Государственного Педагогического Университета им. А.И. ГЕРЦЕНА – № 90. – 2009. – С. 138-143

13. *Сидоренко Е.В.* Тренинг влияния и противостояния влиянию / Е.В. Сидоренко – СПб.: Речь, 2004.

14. *Тулупьев А. Л.* Психологические особенности персонала, предрасполагающие к успешной реализации социоинженерных атак / А.Л. Тулупьев, Т.В. Тулупьева., А.А. Азаров, О.Ю Григорьева. //Научные труды Северо-Западного института управления. – 2012. – Т. 3. – №. 3 (7). – С. 256-266.

15. *Филиппов Г.Г.* Опыт классификации технологий социального манипулирования / Филиппов Г.Г. // Управленческое консультирование. Актуальные проблемы государственного и муниципального управления. – 2011. – №1. – С. 112-122.

16. *Холлис Дж.* Почему хорошие люди совершают плохие поступки: Понимание темных сторон нашей души / Дж. Холлис – Когито-Центр; Москва; 2011. – 330 с.

17. *Цымбал Е.А.* Феномен социального манипулирования (социально-философский анализ) / Е.А. Цымбал // Актуальные проблемы гуманитарных и естественных наук. – 2010 – № 11.– С. 161-165

18. *Шейнов В.П.* Скрытое управление человеком (психологи манипулирования) /В.П. Шейнов. – М.: ООО "Издательство АСТ", Мн.: Харвест, 2001. – 848 с.