УДК 614.8+002.6:004.89
doi:10.15217/issn1684-8853.2016.4.77

МОДЕЛЬ ПРОФИЛЯ КОМПЕТЕНЦИЙ ЗЛОУМЫШЛЕННИКА В ЗАДАЧЕ АНАЛИЗА ЗАЩИЩЕННОСТИ ПЕРСОНАЛА ИНФОРМАЦИОННЫХ СИСТЕМ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК

М. В. Абрамов[а, б, в], *аспирант*
А. А. Азаров[а], *канд. техн. наук*
Т. В. Тулупьева[а, б, г], *канд. псих. наук, доцент*
А. Л. Тулупьев[а, б], *доктор физ.-мат. наук, профессор*
[а]*Санкт-Петербургский государственный университет, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*
[в]*Московский педагогический государственный университет, Москва, РФ*
[г]*Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте РФ, Санкт-Петербург, РФ*

Постановка проблемы: *возросшая сложность компьютерных сетей и механизмов защиты, увеличение количества уязвимостей пользователей, а также возможностей по реализации атак обусловливает необходимость разработки мощных автоматизированных средств (систем) анализа защищенности. В аппаратном и программно-техническом срезе эти проблемы решаются, существуют разработки систем анализа защищенности, в то же время эти средства, как правило, не учитывают или учитывают частично поведение пользователей. В последнее время существенная часть инцидентов нарушения информационной безопасности происходит с применением методов социальной инженерии. Общее направление исследований заключается в построении оценки защищенности персонала информационных систем от социоинженерных атак.* ***Цель:*** *предложить формальную модель злоумышленника и входящую в нее модель профиля его компетенций, на основании которых будет построена многофакторная оценка вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя.* ***Результаты:*** *описана формальная модель злоумышленника, состоящая из профиля компетенций, представляющего собой набор пар компетенция — выраженность компетенции; ресурсов, доступных злоумышленнику; начальных знаний об архитектуре системы; пользователей, к которым злоумышленник имеет доступ до момента начала атаки; целей злоумышленника. В свою очередь на основе данной модели предложен способ расчета многофакторной оценки вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя за счет агрегирования широкого круга факторов, характеризующих их.* ***Практическая значимость:*** *разработанные модели позволят оценивать защищенность информационной системы от социоинженерных атак, выявлять наиболее уязвимые звенья системы и своевременно предпринимать необходимые меры по обеспечению защиты информации.*

Ключевые слова *— социоинженерные атаки, защита пользователей, информационная безопасность, профиль компетенции злоумышленника.*

Введение

Компьютерные системы, хранящие и обрабатывающие информацию, активно используются во многих отраслях производства и в сфере услуг. Столь широкое распространение информационных технологий заставляет уделять все более заметное внимание вопросам информационной безопасности (ИБ). В последнее время атаки на информационные системы происходят чаще, приносят большие убытки и требуют больше ресурсов и времени для установления виновных в подобных преступлениях. Исследование 2014 г. с участием компаний из США показало, что средний размер убытков американских компаний от киберпреступлений вырос более чем на 9 % по сравнению с 2013 г., до 12,7 млн дол. Среднее время, необходимое для расследования атаки на информационные системы, также выросло и составило 45 дней в 2014 г. по сравнению с 32 днями в 2013 г. [1].

В настоящее время большая часть исследований в области обеспечения сохранения конфиденциальности информации посвящена усовершенствованию технической базы, осуществляющей контроль ИБ [2–8]. В этом направлении вопросы ИБ достаточно хорошо изучены, разработано большое количество средств, позволяющих снизить вероятность успеха программно-технической атаки злоумышленника. Хотя термин «информационная безопасность» определяется по-разному, в большинстве случаев основное внимание уделяется защите информации с использованием программных, аппаратных и программно-аппаратных решений [9]. В то же время пользователь информационной системы, к данным которой злоумышленник пытается получить доступ, является одним из ее самых уязвимых мест [10]. Согласно исследованию Лаборатории Касперского [11], наиболее распространенные инциденты ИБ так или иначе связаны с действиями пользователей систе-

мы. Одним из наиболее эффективных видов атак на ИБ является корпоративный шпионаж, которому подвергаются более четверти компаний, и почти 80 % из них успешно [11].

Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить ее безопасность (конфиденциальность, целостность или доступность) [12, 13]. В исследовании В. С. Веденеева и И. В. Бычкова [14] отмечается, что санкционированный пользователь информационной системы, вероятно, знаком с рядом сотрудников, обслуживающих и администрирующих информационную систему; имеет ряд разрешений на доступ к документам, хранящимся в информационной системе; может знать аутентификационные данные коллег; обладает физическим доступом к некоторым компьютерам. В связи с этим взаимодействие пользователей информационной системы со злоумышленниками может нанести серьезный ущерб компании. В частности, в России средний ущерб для компаний СМБ-сегмента (сегмент среднего и малого бизнеса) от серьезного инцидента составляет 780 000 руб., для крупных предприятий эта сумма может достигать 20 млн руб. [11].

Таким образом, проблемы ИБ и защиты пользователей от социоинженерных атак, т. е. атак, направленных в первую очередь на персонал, в настоящее время весьма актуальны. Исследования в этой области помогут в создании многоуровневых систем безопасности, более устойчивых к атакам злоумышленников. Под защитой пользователя от социоинженерной атаки в данной статье понимается деятельность по повышению устойчивости защищаемого пользователя к социоинженерным воздействиям на него заинтересованным субъектом в целях нарушения целостности, доступности и конфиденциальности защищаемой информации. В свою очередь под устойчивостью пользователя понимается способность не изменять свое поведение под воздействием злоумышленника.

Общее направление исследований заключается в построении оценки защищенности персонала информационных систем от социоинженерных атак. Под защищенностью персонала понимается степень его устойчивости к социоинженерным атакующим воздействиям злоумышленника. Цель настоящей работы — предложить формальную модель злоумышленника и входящую в нее модель профиля компетенций злоумышленника (ПКЗ), на основании которых будет построена многофакторная оценка вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя. Указанная цель достигается за счет агрегирования сведений о более широком круге факторов, влияющих на оценку вероятности успеха социоинженерного атакующего воздействия злоумышленника, и развития моделей комплекса «информационная система — персонал — критичные документы». Оценка позволит выявлять наиболее уязвимые звенья системы и своевременно предпринимать необходимые меры по обеспечению защиты информации.

Возросшая сложность компьютерных сетей и механизмов защиты [6], увеличение количества уязвимостей пользователей, а также возможностей по реализации атак обусловливает необходимость разработки мощных автоматизированных средств (систем) анализа защищенности. Эти системы призваны выполнять задачи по обнаружению уязвимостей пользователей информационной системы, информированию служб безопасности, выявлению возможных трасс атакующих действий нарушителей, определению критичных сетевых ресурсов и выбору адекватной угрозам политики безопасности, которая задействует наиболее подходящие в заданных условиях защитные механизмы. Уязвимость пользователя определяется по аналогии с программно-технической уязвимостью и заключает в себе некоторую характеристику пользователя, которая делает возможным успех социоинженерного атакующего действия злоумышленника [15].

Решение этих задач позволит существенно повысить защищенность пользователей информационных систем, т. е. уменьшить вероятность успеха атаки злоумышленника на информационную систему. Для увеличения точности данной оценки предлагается расширить модель комплекса «информационная система — персонал — критичные документы» (ИСПКД) за счет включения ПКЗ и перехода к более полной модели, а именно «критичные документы — информационная система — персонал — злоумышленник» (КДИСПЗ). В статье наиболее подробно рассмотрен подход к моделированию злоумышленника в рамках данной парадигмы и идея формирования профиля компетенций, включенного в модель.

Комплекс «информационная система — персонал — критичные документы»

В работе [16] были представлены компоненты, входящие в комплекс ИСПКД. Информационная система в этом комплексе включает в себя программно-технические устройства. В качестве таких устройств могут выступать [12]:

— ПК и различные периферийные устройства;

— сетевые адаптеры для ПК и сетевые кабели;

— сетевое оборудование, такое как концентраторы и коммутаторы, которые соединяют между собой ПК и принтеры.

С каждым из таких устройств ассоциированы информационные объекты (критичные докумен-

ты — материальные объекты с зафиксированной на них информацией в виде текста, звукозаписи или изображения, имеющие ценность для компании), которые хранятся на этих устройствах или могут быть доступны через них.

Также в комплекс включен персонал информационной системы. Пользователи системы имеют некоторые характеристики, такие как права доступа, должности и др. Ключевое отличие модели информационной системы с персоналом от информационной системы без персонала заключается в недетерминированности реакции пользователя на воздействие злоумышленника. Иными словами, успех социоинженерного атакующего воздействия злоумышленника на пользователя информационной системы носит недетерминированный вероятностный характер. Для вычисления оценок вероятности успеха таких воздействий был введен профиль уязвимостей пользователей (ПУП) [17, 18]. Кроме того, злоумышленник, как правило, не всесилен. Он обладает ограниченными ресурсами, неполными знаниями, и набор его компетенций не универсален. Это ограничение может быть отражено с помощью ПКЗ, описываемого в данной статье.

Если удалось построить указанные выше модели и затем идентифицировать их параметры, пусть с использованием оценок различной степени точности, то на их основе, в свою очередь, уже можно строить оценки, показатели, индексы или характеристики степени защищенности как отдельных пользователей информационных систем, а также, при определенных допущениях, и отдельных критичных документов, так и системы и персонала в целом. При этом расчеты сведутся к вычислению вероятности сложных событий и на их основе математических ожиданий целевых величин (например, математического ожидания ущерба от социоинженерных атакующих воздействий злоумышленника либо вероятности того, что критичный документ не будет поражен) по аналогии с работой [6].

Комплекс «критичные документы — информационная система — персонал — злоумышленник»

В работе [16] были предложены две модели имитации социоинженерных атак злоумышленника на пользователей информационной системы: на социальном графе пользователей и в комплексе ИСПКД. Данные модели дают оценку защищенности пользователей от социоинженерной атаки злоумышленника на основе связей между пользователями, в то же время в данных моделях не учитывается ПКЗ. Предлагается рассмотреть комплекс «критичные документы — информационная система — персонал — злоумышленник» вместо комплекса ИСПКД, который позволит увеличить точность оценки защищенности пользователей информационных систем от социоинженерных атак за счет вероятностных оценок действий злоумышленника. Профиль компетенций злоумышленника имеет большое значение наравне с ПУП для оценки успешности атакующего воздействия.

Важность изучения особенностей двух сторон взаимодействия: того, кто влияет, и того, на кого влияют, — подчеркивается в научной литературе. Известный специалист в области психологии влияния Роберт Чалдини в своей монографии [19] отмечал, что изучать психологию уступчивости он начал с серии экспериментов, позволяющих выяснить, какие принципы и особенности лежат в основе податливости в отношении просьб или требований, но вскоре понял, что нужно изучать и вторую сторону данного процесса. Он назвал людей, способных принудить других к выполнению тех или иных просьб, «профессионалами уступчивости», поскольку они хорошо знают, как построить взаимодействие, чтобы собеседник уступил и выполнил просьбу или требование. «Они знают, что срабатывает, а что — нет <...>. Такие люди стараются, во что бы то ни стало, заставить окружающих уступить, от этого зависит их успех в жизни. Те, кто не знает, как вынудить людей сказать «да», обычно терпят поражение; те же, кто знает, — процветают» [19]. Р. Чалдини в результате своих наблюдений вывел шесть основных принципов влияния: принцип последовательности, принцип взаимного обмена, принцип социального доказательства, принцип авторитета, принцип благорасположения, принцип дефицита. Однако в число главных принципов не было включено правило «личного материального интереса», которое автор рассматривает как «некоторую аксиому, которая заслуживает признания, но не подробного описания».

Модель пользователя в рамках данного исследования может быть представлена в виде $U=<C, Z, \mathrm{PV}, L>$, где C — критичные документы, к которым пользователь имеет доступ; Z — контролируемые зоны (т. е. помещения, в которых пользователь может физически присутствовать, например, серверная, отдел маркетинга и пр.); PV — ПУП; L — матрица взаимоотношений между пользователями.

Рассмотрим подробнее некоторые компоненты модели пользователя. PV представлен в работе [20]. C и Z — это столбцы из соответственно l и m элементов. $c_1..c_l$ — элементы столбца C, которые характеризуют уровень доступа пользователя к соответствующему критическому документу и могут иметь значения: 0 — данный пользователь не имеет доступа к документу, 1 — имеет доступ

к чтению, 2 — имеет доступ к редактированию и удалению. $z_1..z_m$ — элементы столбца Z, которые характеризуют наличие доступа пользователя к соответствующей контролируемой зоне и могут принимать значения 0 — данный пользователь не имеет доступа к контролируемой зоне или 1 — имеет доступ к контролируемой зоне.

Модель злоумышленника представим в виде $M=<R, S_0, U_0, P, G>$, где R — ресурсы, доступные злоумышленнику (например, время, деньги или личностные особенности злоумышленника); S_0 — начальные знания нарушителя об архитектуре системы (ее сотрудниках, их уязвимостях, доступных им критичных документах, взаимоотношениях персонала в контролируемых зонах); U_0 — пользователи, к которым злоумышленник имеет доступ до момента начала атаки; P — ПКЗ (будет представлен ниже); G — цели злоумышленника (например, получение доступа к той или иной информации).

Начальные знания нарушителя об архитектуре системы, S_0, представляют собой набор U_i: $i=1..n$, при этом информация, которая злоумышленнику неизвестна, представляется значением (–1). То есть, например, элементы столбца C — $c_1..c_l$ — будут принимать также значения: 0 — если злоумышленник знает, что пользователь не имеет доступа к документу; 1 — если злоумышленник знает, что пользователь имеет доступ к чтению; 2 — если злоумышленник знает, что пользователь имеет доступ к редактированию и удалению документа, и (–1) — если злоумышленник не знает, какие права доступа у пользователя по отношению к документу.

Далее рассмотрим ПКЗ, P. Он может быть охарактеризован известными злоумышленнику социоинженерными атакующими воздействиями и навыками их осуществления. Опираясь на опыт исследований аппаратных и программно-технических аспектов информационной безопасности и адаптируя его к области социоинженерных атак, можно ожидать, что для построения и регулярного последующего пополнения списков атакующих воздействий, ресурсов и прочих параметров, входящих в ПКЗ, а также подходов к их оценке потребуется отдельное и непрерывно длящееся междисциплинарное исследование при участии специалистов по психологии, социологии, информатике и математике. Чем полнее будут данные списки, тем более точные оценки можно получить. В предположении, что некая версия списков доступна, например, как в работе [21], продолжим дальнейшее развитие концепции.

Так, ПКЗ может быть представлен в виде $P=((K_1, D(K_1)), ..., (K_q, D(K_q)))$, где K_i — социоинженерное атакующее воздействие, а $D(K_i)$ — степень владения злоумышленником данным атакующим воздействием. Это один из факторов, влияющих на оценку успешности атаки, выражающий некоторое умение злоумышленника. Заметим, что оценка этого фактора может быть получена путем обратного моделирования от критичного документа к злоумышленнику. Например, пусть злоумышленник получил доступ к критичному документу; необходимо оценить наиболее вероятную или минимальную конфигурацию компетенций, которыми он должен обладать. Возможны иные подходы, например, оценка по серии специально организованных экспериментов или оценка по методике, составленной экспертами, или оценка, построенная с помощью статистического анализа социоинженерных атакующих воздействий, ставших известными.

Каждой модели злоумышленника сопоставлен свой ПКЗ, т. е. свой набор степеней владения различными типами атакующих воздействий. Таким образом, для каждого злоумышленника j ПКЗ будет состоять из социоинженерных атак и степеней владения ими: $P_j=((R_1, D_j(K_1)), ..., (R_q, D_j(K_q)))$. Формализовав таким образом ПКЗ, можно в простейшем случае, без учета ПУП, перейти к огрубленным оценкам вероятности успеха социоинженерных атакующих воздействий злоумышленника p_{ij}, которые представляются следующим образом: $p_{ij}=f(D_j(K_i), T_i)$, где $D_j(K_i)$ — степень владения атакующим воздействием K_i у злоумышленника j; T_i — максимально возможная степень владения атакующим воздействием, а p_{ij} — вероятность успеха социоинженерного атакующего воздействия j-го злоумышленника с использованием i-й атаки. Конечная структура функции f не выработана, однако одним из примеров может быть следующий ее вид:

$$p_{ij}=f(D_j(K_i),\ T)=\frac{D_j(K_i)}{T_i}.$$

Таким образом, происходит переход от степени владения атакующим воздействием, применяемым злоумышленником, к вероятности успеха социоинженерного атакующего воздействия на пользователя, и ПКЗ приобретает вид $p_{1j}, ..., p_{qj}$.

Отметим, что в статье рассматриваются простейшие социоинженерные атаки злоумышленника на пользователя, например, предложение зарегистрироваться на каком-то ресурсе или отправка письма с «полезным для пользователя приложением». Кроме того, будем считать, что злоумышленники действуют индивидуально, не используют ресурсы, знания и навыки друг друга и не пользуются результатами деятельности друг друга. Не менее интересным представляется исследование данной темы для модели, в которой задействованы группы злоумышленников, действующих в сговоре, но в текущей статье ограничимся комплексом, включающим только одного злоумышленника.

Стоит отметить, что модели пользователя информационной системы сопоставлен ПУП, в который входят степени выраженности уязвимостей пользователя, на их основании строятся вероятностные оценки успешности того или иного социоинженерного атакующего воздействия злоумышленника. Под выраженностью уязвимости пользователя понимается степень его подверженности социоинженерным атакующим воздействиям, которая зависит от его личностных психологических характеристик, уровня компетенций и иных факторов. Предполагается, что рассмотрение ПКЗ позволит сделать более точными вероятностные оценки защищенности пользователей информационных систем от социоинженерных атак.

Таким образом, при имитации социоинженерных атакующих воздействий, исходящих от злоумышленников, обладающих разными компетенциями, могут быть получены различные вероятностные оценки успеха социоинженерных атакующих воздействий. Успех социоинженерного атакующего воздействия j-го злоумышленника будет определяться степенью владения им различными социоинженерными атакующими воздействиями и выраженностью уязвимостей атакуемого пользователя информационной системы. Функция расчета вероятности успеха социоинженерного атакующего воздействия при заданных ПКЗ и ПУП в простейшем варианте может быть представлена в виде зависимости от ряда параметров:

$$p_{ij}^{lq} = g(D_j(K_i),\ T_i,\ S_q(V_l,\ K_i),\ B_l),$$

где $D_j(K_i)$ — степень владения социоинженерным атакующим воздействием K_i у злоумышленника j; $S_q(V_l, K_i)$ — выраженность уязвимости V_l, на которую можно воздействовать с помощью атаки K_i, у пользователя q; T_l — максимально возможная степень владения атакующим воздействием K_i; B_l — максимальная выраженность уязвимости V_l; p_{ij}^{lq} — вероятность успеха социоинженерного атакующего воздействия j-го злоумышленника с использованием его i-го ресурса на l-ю уязвимость k-го пользователя. Одним из возможных примеров данной функции будет являться

$$p_{ij}^{lq} = g(D_j(K_i),T_i,S_q(V_l,K_i),B_l) = \frac{D_j(K_i)S_q(V_l,K_i)}{T_i B_l}.$$

Важно отметить, что одно и то же атакующее воздействие можно использовать для оказания влияния на разные уязвимости пользователя. Так, например, финансовые ресурсы можно использовать как для подкупа пользователей информационной системы, так и для формирования внешнего образа, способствующего установлению соответствующих связей с жертвой. В простейшем случае рассматривается только влияние одного ресурса злоумышленника на одну уязвимость пользователя.

Введем еще одну функцию, которая будет заключать в себе оценку вероятности успешности атаки при использовании злоумышленником определенного атакующего воздействия на определенную уязвимость пользователя. Рассмотрим табличное задание данной функции на примере. В работе [17] было выявлено пять элементарных уязвимостей пользователя: техническая неосмотрительность, слабый пароль, техническая халатность и установка на получение личной выгоды, техническая неопытность, техническая безграмотность. Атакующее воздействие, заключающееся, например, в предложении зарегистрироваться на каком-то привлекательном сайте, вероятнее всего, будет иметь отклик у пользователей с сильно выраженными уязвимостями: технической неосмотрительностью, технической халатностью и установкой на получение личной

■ Атакующие воздействия злоумышленника и уязвимости пользователя

Уязвимости пользователя	Атакующие воздействия						
	Предложение зарегистрироваться на каком-то привлекательном сайте	Отправка письма с «полезным» для пользователя приложением	Виртуальное знакомство с пользователем в сети	Взлом	Подсматривание	Подкуп	Предложение помощи в решении компьютерных дел
Техническая неосмотрительность	1	0,9	0,8	0	0	0	0
Слабый пароль	0	0	0	1	0,9	0	0
Техническая халатность и установка на получение личной выгоды	0,9	0	0	0	0	1	0
Техническая неопытность	1	0,9	0,8	0	0	0	0
Техническая безграмотность	1	0,9	0	0	0	0	0,9

выгоды, технической неопытностью, технической безграмотностью. В то же время данное атакующее воздействие вряд ли приведет к успеху с пользователем, у которого вышеперечисленные уязвимости мало выражены, но имеет место использование слабого пароля.

Формализуя описанное выше, введем функцию следующего вида: $\varphi_{il}(K_i, V_l)$, где K_i — это тип атакующего воздействия, а V_l — уязвимость. Значения функции будут лежать на отрезке [0;1], причем 0 означает, что злоумышленник с использованием данного атакующего воздействия не сможет повлиять на уязвимость, 1 — злоумышленник добьется успеха, используя данную компетенцию для воздействия на уязвимость.

Значения для данной функции с учетом выявленных в работе [21] атакующих воздействий злоумышленника и элементарных уязвимостей пользователя могут быть представлены следующим образом (таблица).

Таким образом, итоговая формула примет следующий вид:

$$p_{ij}^{lq} = g(D_j(K_i), T_i, S_q(V_l, K_i), B_l)\varphi_{i,l}(K_i, V_l),$$

где функция $g(D_j(K_i), T_i, S_q(V_l, K_i), B_l)$ будет характеризовать факторы, связанные с выраженностью уязвимостей пользователя и компетенций злоумышленника, а $\varphi_{il}(K_i, V_l)$ — аспекты выбранной злоумышленником стратегии атаки, влияющей на ее успех.

Заключение

В статье приведен подход, позволяющий сделать оценку защищенности персонала информационных систем от социоинженерных атак, агрегирующей более широкий круг факторов по сравнению с подходами, рассмотренными в работе [16]. Это достигается за счет учета особенностей злоумышленника, находящих отражение в профиле его компетенций. Как следствие комплекс «информационная система — персонал — критичные документы» дополнен моделью злоумышленника. Представлен комплекс «критичные документы — информационная система — персонал — злоумышленник». Приведены модели пользователя и злоумышленника. Предложен подход к формализации профиля компетенций злоумышленника и расчету вероятности успеха социоинженерного атакующего воздействия злоумышленника на пользователя с использованием определенного типа атаки и уязвимости. Оценка степени защищенности в конце концов нацелена на достижение возможности выявить наиболее уязвимые звенья системы и своевременно отреагировать на возникающие вызовы по обеспечению защиты информации.

Дальнейшая работа по развитию изложенного подхода связана с выводом точной формулы вероятности успеха атакующего воздействия злоумышленника, поиском новых уязвимостей пользователей и компетенций злоумышленника, а также оценкой зависимости уязвимостей и компетенций. Кроме того, важной задачей представляется разработка, реализация и поддержание в актуальном состоянии базы данных атакующих воздействий, ресурсов и прочих параметров, входящих в профиль компетенций злоумышленника, а также базы данных уязвимостей пользователя.

Статья содержит материалы исследований, частично поддержанных грантами РФФИ 14-07-00694-а, 14-01-00580-а, 15-01-09001-а.

Литература

1. Убытки от киберпреступлений продолжают расти. http://www.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/index.html (дата обращения: 04.03.2015).
2. **Distefanoa S., Puliafitob A.** Information Dependability in Distributed Systems: The Dependable Distributed Storage System // Integrated Computer-Aided Engineering. 2014. N 21. P. 3–18.
3. **Goo J., Yim M. S., Kim D. J.** A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate // Professional Communication, IEEE Transactions on. 2014. Vol. 57. N 4. P. 286–308.
4. **James C.** Information Systems User Security: A Structured Model of the Knowing–Doing Gap // Computers in Human Behavior. 2012. Vol. 28. Iss. 5. P. 1849–1858.
5. **Trčcek D., Trobec R., Pavešsić N., Tasič J.F.** Information Systems Security and Human Behaviour // Behaviour & Information Technology. 2007. Vol. 26. Iss. 2. P. 113–118.
6. **Котенко И. В., Степашкин М. В.** Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Тр. ИСА РАН. 2007. Т. 31. С. 126–207.
7. **Котенко И. В., Степашкин М. В.** Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49. № 3. С. 3–8.
8. **Котенко И. В., Юсупов Р. М.** Перспективные направления исследований в области компьютерной безопасности//Защита информации. Инсайд. 2006. № 2. С. 46.
9. **Дорохов В. Э.** О рисках потери репутации организации вследствие инцидентов информационной безо-

пасности // Безопасность информационных технологий. 2014. № 2. С. 80–82.
10. **Сапронов К.** Человеческий фактор и его роль в обеспечении информационной безопасности. http://www.interface.ru/home.asp?artId=17137 (дата обращения: 05.03.2015).
11. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 30.04.2015).
12. **Сергиевский М.** Сети — что это такое // КомпьютерПресс. 1999. № 10. С. 3–9.
13. **Суворова А. В.** и др. Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения/ А. В. Суворова, А. Л. Тулупьев, А. Е. Пащенко, Т. В. Тулупьева, Т. В. Красносельских // Компьютерные инструменты в образовании. 2010. № 4. С. 30–38.
14. **Веденеев В. С., Бычков И. В.** Средства поиска инсайдеров в корпоративных ИС // Безопасность информационных технологий. 2014. № 1. С. 9–13.
15. **Бычек В., Ершова Е.** Социальная инженерия в интеллектуальной битве «добра» и «зла» // Защита информации. Инсайд. 2006. № 6. http://www.aladdin-rd.ru/company/pressroom/articles/11475/ (дата обращения: 28.06.2016).
16. **Азаров А. А.** Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищенности персонала информационных систем от социоинженерных атак: дис. ... канд. техн. наук. — СПб.: СПИИРАН, 2013. — 232 с.
17. **Тулупьев А. Л., Азаров А. А., Пащенко А. Е.** Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Тр. СПИИРАН. 2010. Вып. 2 (13). С. 143–155.
18. **Тулупьева Т. В., Тулупьев А. Л., Азаров А. А., Пащенко А. Е.** Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак // Тр. СПИИРАН. 2011. Вып. 18. С. 74–92.
19. **Cialdini R. B.** Influence: Science and practice. 5th ed. — Boston: Allyn & Bacon, 2009.
20. **Ванюшичева О. Ю.** и др. Количественные измерения поведенческих проявлений уязвимостей пользователей, ассоциированных с социоинженерными атаками/ О. Ю. Ванюшичева, Т. В. Тулупьева, А. Е. Пащенко, А. Л. Тулупьев, А. А. Азаров // Тр. СПИИРАН. 2011. Вып. 19. С. 34–47.
21. **Тулупьев А. Л., Тулупьева Т. В., Азаров А. А., Григорьева О. Ю.** Психологические особенности персонала, предрасполагающие к успешной реализации социоинженерных атак // Науч. тр. Северо-Западного института управления РАНХиГС. 2012. Т. 3. Вып. 3 (7). С. 256–266.

UDC 614.8+002.6:004.89
doi:10.15217/issn1684-8853.2016.4.77

Model of Malefactor Competencies Profile for Analyzing Information System Personnel Security from Social Engineering Attacks

Abramov M. V.[a,b,c], Post-Graduate Student, mva16@list.ru
Azarov A. A.[a], PhD, Tech., artur-azarov@yandex.ru
Tulupyeva T. V.[a,b,d], PhD, Psych., Associate Professor, tvt100a@mail.ru
Tulupyev A. L.[a,b], Dr. Sc., Phys.-Math., Associate Professor, alexander.tulupyev@gmail.com
[a]Saint-Petersburg State University, 7–9, Universitetskaia Nab., 199034, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line V.O., 199178, Saint-Petersburg, Russian Federation
[c]Moscow Pedagogical State University, 1/1, M. Pirogovskaya St., 119991, Moscow, Russian Federation
[d]Northwest Institute of Management of the Russian Academy of National Economy and Public Administration under the President of the Russian Federation, 57/43, Srednii Pr. V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: The increased complexity of computer networks and security mechanisms, the growing number of users' vulnerabilities and various ways to organize attacks cause the need to develop powerful automated tools and systems for vulnerability analysis. The technical (software and hardware) problems are mostly solved; there are many software systems for security analysis. However, these systems usually do not include or include only partially the users' behavior analysis, while an essential part of information security violations are caused now by social engineering attacks. The general purpose of the current research is to estimate the rate of information system personnel protection from social engineering attacks. **Purpose:** A formal model of a malefactor should be developed, including a model of malefactor's competencies profile. It will be a basis for multifactorial estimates of the probability of a success of malefactor's attack on the user. **Results:** A formal model of a malefactor was developed in this article. It consists of the profile of malefactor's competencies in paired format (a competence and its intensity), resources available for the malefactor, his/her basic knowledge about the system architecture, the set of users vulnerable for the attack, and malefactor's goals. On the basis of this model, a method of multi-factor assessment of malefactor's attack success probability was proposed. **Practical relevance:** The developed model allows you to evaluate how well information systems are protected from social engineering attacks, to identify the most vulnerable parts of the system and to promptly take necessary measures to ensure information security.

Keywords — Social Engineering Attacks, User Protection, Information Security, Malefactor Competencies Profile.

References

1. *Ubytki ot kiberprestuplenii prodolzhaiut rasti* [Losses from Cybercrimes Continue to Grow]. Avaible at: http://www.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/index.html (accessed 4 March 2015).
2. Distefanoa S., Puliafitob A. Information Dependability in Distributed Systems: The Dependable Distributed Storage System. *Integrated Computer-Aided Engineering*, 2014, no. 21, pp. 3–18.
3. Goo J., Yim M. S., Kim D. J. A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *Professional Communication, IEEE Transactions on*, 2014, vol. 57, no. 4, pp. 286–308.
4. James C. Information Systems User Security: A Structured Model of the Knowing–Doing Gap. *Computers in Human Behavior*, 2012, vol. 28, iss. 5, pp. 1849–1858.
5. Trčcek D., Trobec R., Pavešsić N., Tasič J.F. Information Systems Security and Human Behaviour. *Behaviour & Information Technology*, 2007, vol. 26, iss. 2, pp. 113–118.
6. Kotenko I. V., Stepashkin M. V. Security Analysis of Computer Networks Based on Modeling by Malefactors Actions and Constructing Attack Graph. *Trudy ISA RAN*, 2007, vol. 31, pp. 126–207 (In Russian).
7. Kotenko I. V., Stepashkin M. V. Systems Imitators: the Appointment, Functions, Architecture and Implementation Approach. *Izvestiia vuzov. Priborostroenie*, 2006, vol. 49, no. 3, pp. 3–8 (In Russian).
8. Kotenko I. V., Iusupov R. M. Perspective Directions in the Field of Computer Security Research. *Zashchita informatsii. Insaid*, 2006, no. 2, p. 46 (In Russian).
9. Dorokhov V. E. Reputation Risks Through Information Security Incidents. *Bezopasnost' informatsionnykh tekhnologii*, 2014, no. 2, pp. 80–82 (In Russian).
10. *Chelovecheskii faktor i ego rol' v obespechenii informatsionnoi bezopasnosti* [The Human Factor and its Role in Ensuring Information Security]. Avaible at: http://www.interface.ru/home.asp?artId=17137 (accessed 05 March 2015).
11. *Informatsionnaia bezopasnost' biznesa. Issledovaniia tekushchikh tendentsii v oblasti informatsionnoi bezopasnosti biznesa* [Business Information Security. Studies of Current Trends in Business Information Security]. Avaible at: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (accessed 30 April 2015).
12. Sergievskii M. Networks — what is it. *Komp'iuterPress*, 1999, no. 10, pp. 3–9 (In Russian).
13. Suvorova A. V., Tulupyev A. L., Pashchenko A. E., Tulup'eva T. V., Krasnosel'skikh T. V. Analysis of Granular Data and Knowledge in Research Problems Socially Significant Behaviors. *Komp'iuternye instrumenty v obrazovanii*, 2010, no. 4, pp. 30–38 (In Russian).
14. Vedeneev V. S., Bychkov I. V. Tool for Insider Threat Detection in Corporative Information Systems. *Bezopasnost' informatsionnykh tekhnologii*, 2014, no. 1, pp. 9–13 (In Russian).
15. Bychek V., Ershova E. Social Engineering in the Intellectual Battle of "good" and "evil". *Zashchita informatsii. Insaid*, 2006, no. 6. Avaible at: http://www.aladdin-rd.ru/ company/ pressroom/ articles/ 11475/ (accessed 28 June 2016).
16. Azarov A. A. *Veroiatnostno-reliatsionnye modeli i algoritmy obrabotki profilia uiazvimostei pol'zovatelei pri analize zashchishchennosti personala informatsionnykh sistem ot sotsioinzhenernykh atak.* Dis. kand. tehn. nauk [Probabilistic Relational Models and Algorithms for Processing User Profiles Vulnerabilities in the Analysis of Security of Information Systems Personnel from Socio-Engineering Attacks. PhD tech. sci. diss.]. Saint-Petersburg, SPIIRAN Publ., 2013. 232 p.
17. Tulupyev A. L., Pashchenko A. E., Azarov A. A. Information Model of the Use, who may be under the threat of Socio-engineering Attack. *Trudy SPIIRAN*, 2010, iss. 2(13), pp. 143–155 (In Russian).
18. Tulupyeva T. V., Tulupyev A. L., Azarov A. A., Pashchenko A. E. Psychological Defence as a Factor of User's Vulnerability in a Socio-Engineering Attacks Context. *Trudy SPIIRAN*, 2011, iss. 3(18), pp. 74–92 (In Russian).
19. Cialdini R. B. *Influence: Science and practice.* 5th ed. Boston, Allyn & Bacon, 2009.
20. Vaniushicheva O. Iu., Tulupyeva T. V., Pashchenko A. E., Tulupyev A. L., Azarov A. A. Quantitative Measurements of Behavioral Displays of User's Vulnerabilities Associated with Socio-Engineering Attacks. *Trudy SPIIRAN*, 2011, iss. 4(19), pp. 34–47 (In Russian).
21. Tulupyev A. L., Tulupyeva T. V., Azarov A. A., Grigor'eva O. Iu. Psychological Features of Personnel, Predisposes to the Successful Implementation of Socio-Engineering Attacks. *Nauchnye trudy Severo-Zapadnogo instituta upravleniia RANKhiGS*, 2012, vol. 3, iss. 3(7), pp. 256–266 (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.