УДК 614.8+002.6:004.89

Т.В. Тулупьева, А.Л. Тулупьев, А.Е. Пащенко,
А.А. Азаров, М.В. Степашкин

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ, ВЛИЯЮЩИЕ НА СТЕПЕНЬ УЯЗВИМОСТИ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ТОЧКИ ЗРЕНИЯ СОЦИОИНЖЕНЕРНЫХ АТАК

Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В. **Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинженерных атак.**
Аннотация. Настоящая статья посвящена обзору результатов исследований по психологии, относящихся к характеристике уязвимостей человека-пользователя, и формировании на его основе требований к информационной модели пользователя, которая в последствии будет интегрирована в информационную систему для анализа защищенности этой системы от социоинженерных атак. Рассмотрены намеренные и ненамеренные действия сотрудников, и на их основе сформированы требования к информационной модели пользователя, содержащей критичные свойства пользователя, которые больше других влияют на степень успеха предпринятой против него социоинженерной атаки. Полученные в ходе моделирования сведения помогут в дальнейшем прогнозировать (имитировать) реакцию пользователя в ответ на атакующие действия.
Ключевые слова: социоинженерная атака, особенности личности, потребности человека, информационная модель пользователя, действия пользователя.

Tulupyeva T.V., Tulupyev A.L., Paschenko A.E., Azarov A.A., Stepashkin M.V. **Social Psychological Factors That Influence the Information System Users Vulnerability Degree in Regard of Socio-Engineering Attacks.**
Abstract. Current paper is devoted to the review of the results of researches on psychology, concerned characteristics of person-user vulnerability, and forming demands, based on this researches, to informative model of the user, which can be integrated to the informative system for analyzing the protection of this system from socioengineering attacks. Intended and unintended actions of the user was examined, and on this base requirements to the informative model of the user has been made, which includes critical user properties, which influences more than others on the rate of success of socioengineering attack, made on this user. information gained from modeling will help to prognoses (imitate) reaction of the user like an answer to the attack action.
Keywords: socioengineering attack, features of the person, requirements of the person, informative model of the user, user actions.

1. Введение. Человеческий фактор играет существенную роль в системе обеспечения безопасности информации, и человек, являясь пользователем информационной системы, был и остается одним из самых уязвимых ее мест. Люди, работающие с информацией, могут рассматриваться как звено в цепочке механизма, который обеспечива-

ет работоспособность и безопасность всей системы [8].

Сотрудник компании (в том числе санкционированный пользователь информационной системы), имеющий доступ к конфиденциальной информации, может нарушить ее безопасность (в частности, конфиденциальность, целостность или доступность) преднамеренно или случайно. Поэтому все возможные действия сотрудника, результатом которых является нарушение безопасности информации (такие действия будем в дальнейшем называть атаками), можно условно разделить на две группы: намеренные (осознаваемые) и ненамеренные (неосознаваемые, случайные).

Цель настоящей работы состоит в формировании на основе обзора некоторых теорий и результатов исследований в области инженерной, общей и социальной психологии, относящихся к характеристике уязвимостей человека-пользователя, требований к информационной модели пользователя, которая предполагается к использованию в построении более широкой модели сцены или контекста, в котором может развиваться социоинженерная атака.

2. Намеренные (осознаваемые) действия сотрудников. Намеренные (осознаваемые) атаки, выполняемые сотрудниками, связаны с удовлетворением их потребностей (под потребностью понимается состояние человека, «создаваемое испытываемой им нуждой в объектах, необходимых для его существования и развития, и выступающее источником его активности»[7]). С определенной потребностью связан мотив (или несколько мотивов), который является «побуждением к деятельности, связанным с удовлетворением потребности субъекта» [7]. Однако некоторыми авторами, например А.Н. Леонтьевым или П.М. Якобсоном, предлагается выделять две категории мотивационных явлений: собственно мотивы личности, в их классическом понимании, и совокупность «динамических сил» и «психологических моментов», которые, наряду с мотивами, определяют целостное поведение человека [11]. Это идея является достаточно важной в контексте социоинженерных атак. По мнению П.М. Якобсона, мотивами могут быть политические или нравственные идеалы, достаточно сильное чувство, действенные моральные убеждения, привычки, подражание и др. [13] В настоящее время «любой фактор, влияющий на возникновение побуждения и принятие решения, объявляется мотивом» [4].

Таким образом, для выявления и классификации мотивов, свойственных сотрудникам, целесообразно рассмотреть основные потребностно-мотивационные теории.

Выделяют следующие классы потребностно-мотивационных тео-

рий [6]:

– содержательные, раскрывающие причины того или иного поведения людей (идентификация внутренних побуждений) и пытающиеся ответить на вопрос «Что?» (например, теории А. Маслоу, К. Альдерфера, Д. Мак Клелланда);

– процессуальные, пытающиеся ответить на вопрос «Как?» (например, теория ожидания или теория справедливости).

Среди потребностно-мотивационных теорий особого внимания (как наиболее известная и широко распространенная) заслуживает теория А. Маслоу, определяющая следующие иерархические уровни (пирамиду) потребностей [9]:

1) физиологические потребности (в воде, пище, сексуальные потребности и т.п.);

2) потребности в безопасности и уверенности в будущем (в физической и социальной безопасности, защите, стабильности);

3) социальные потребности (в общении, любви, принадлежность к группе и т.п.);

4) потребности в уважении и признании (в оценке другими, в престиже, уважении, признании профессиональной компетентности, привлекательности и т.п.);

5) потребности в самовыражении и саморазвитии.

Знание данной иерархии и учет особенностей потребностно-мотивационной сферы сотрудника (актуальные для него мотивы и потребности) позволяют получить качественное выполнение сотрудником своих должностных обязанностей, а злоумышленнику — подтолкнуть его к реализации противоправных действий, в том числе, направленных на нарушение безопасности информации.

Очевидно, что еще до реализации воздействия на сотрудника злоумышленнику необходимо определить следующее:

1) уровень иерархии, являющийся наиболее актуальным для данного сотрудника в настоящее время;

2) насколько сильно выражена выявленная потребность, насколько она реализована или может быть реализована [12] (чем сильнее выражена потребность, тем больше вероятность того, что сотрудник согласится на реализацию противоправных действий).

При решении первой задачи злоумышленник должен также учитывать, что:

1) уровни актуальных потребностей сотрудников различаются, у разных сотрудников могут быть различные потребности;

2) потребности сотрудника со временем изменяются — нельзя рассчитывать на то, что если данная мотивация 1 раз была эффективна, то она останется актуальной для данного сотрудника все время.

Таким образом, анализ пирамиды потребностей А. Маслоу позволяет определить первую группу сотрудников, способных реализовывать намеренные (осознаваемые) атаки, — сотрудников, испытывающих явную потребность в чем-то.

К. Альдерфер выделил три иерархических уровня потребностей:

1) потребности существования (физиологические и иные материальные),

2) связующие потребности (в межличностном взаимодействии, отношениях и оценке),

3) потребности роста (в развитии и саморазвитии).

К. Альдерфельд подверг критике утверждение А. Маслоу и отрицал необходимость строго последовательного удовлетворения потребностей. Теория К. Альдерфера вводит очень важное фрустрационно-регрессивное измерение: если удовлетворение более высокой потребности блокировано, возрастает стремление к более полному и частому удовлетворению низлежащей потребности, т. е. блокированная потребность делает более актуальной менее высокую потребность, которую индивид в состоянии удовлетворить [3].

Таким образом, вторую группу сотрудников, способных реализовывать намеренные (осознаваемые) атаки, составляют сотрудники, которым не удалось удовлетворить потребность более высокого уровня.

Теория Д. Мак Клелланда утверждает, что людям присущи три основные потребности:

1) власти;

2) достижений;

3) причастности (аффилиации).

Неудовлетворение любой из этих потребностей может подтолкнуть сотрудника к реализации намеренных (осознаваемых) атак или действий в ответ на социоинженерные атаки.

Теория справедливости Дж. Ст. Адамса устанавливает, что основную роль в выполнении работы и получении удовлетворения играет степень справедливости (или несправедливости), которую ощущают работники в конкретной ситуации на своей работе. Несправедливость возникает в ситуации, когда человек чувствует, что отношение отдачи, которую он получает, к его вкладу в выполнение работы не равно соответствующему отношению у других работников. Данный дисбаланс

вызывает психологическое напряжение, которое необходимо снять, т.е. восстановить справедливость. Дисбаланс может быть устранен сотрудником путем изменения следующих факторов:

— ситуации в корне (уволиться),

— уровня затрачиваемых усилий (работать медленнее и получать менее качественный результат),

— получаемого вознаграждения (попросить прибавки жалования или получить дополнительное вознаграждение за реализацию противоправных действий, направленных в том числе и на нарушение безопасности информации).

Таким образом, пока сотрудники не убедятся, что они получают справедливое вознаграждение за выполняемую работу, они будут стремиться уменьшить интенсивность труда или искать другие способы восстановления справедливости [6].

Подводя итог, можно выделить следующие группы сотрудников, способных намеренно (осознанно) реализовывать действия, направленные на нарушение безопасности информации:

1) сотрудники, испытывающие явную потребность в чем-то (например, потребность в деньгах, любви, уважении, признании и т.д.);

2) сотрудники, которым не удалось удовлетворить потребность более высокого уровня (по иерархии К. Альдерфера);

3) сотрудники с выраженной потребностью власти;

4) сотрудники с выраженной потребностью в достижениях;

5) сотрудники с выраженной потребностью в причастности (аффилиации);

6) сотрудники, считающие несправедливым распределение вознаграждения за потраченные усилия.

3. Ненамеренные (неосознаваемые) действия сотрудников. Наглядным примером ненамеренных (неосознаваемых) действий, приводящих к нарушению безопасности информации, является обработка сотрудниками (санкционированными пользователями информационной системы) почтовых вложений, получаемых из недоверенных источников. Большинство пользователей осознают опасность таких вложений, однако проведенный опрос показал, что только 55 % пользователей их игнорируют, а 45 % опрошенных открывают вложения по разным причинам (из любопытства — 29, по невнимательности — 10, из-за безалаберности — 4, прочее — 2 %).

В общем случае группу сотрудников, способных реализовывать ненамеренные (неосознаваемые) атаки, составляют те из них, которые не осознают последствий нарушения действующих в компании ин-

струкций и правил политики обеспечения безопасности информации. Данные сотрудники могут не осознавать истинной ценности информации (секретари, охрана и т.п.) или иметь особые привилегии доступа к конфиденциальной информации (техническая поддержка, системные администраторы, бухгалтерия, отдел кадров и т.п.).

К фактором, повышающим успешность воздействия злоумышленников на сотрудников, можно отнести:

– большую численность штата сотрудников;
– наличие филиалов компании;
– доступность информации о местонахождении сотрудников (например, на автоответчике);
– доступность информации о внутренних телефонных номерах сотрудников;
– поверхностное ознакомление (обучение) сотрудников с реализуемой в компании политикой обеспечения безопасности информации;
– отсутствие правил классифицирования информации (отнесения информации к классу конфиденциальной);
– отсутствие системы сообщения о произошедших нарушениях правил политики обеспечения безопасности информации.

При воздействии на сотрудников злоумышленники используют методы, направленные на их «слабые места» (в качестве которых выступают описанные выше потребности) таким образом, что сотрудник не замечает самого факта выполнения им действий, нарушающих безопасность информации. В таких методах в качестве основы выступают различные виды и силы социального влияния [10]:

– лесть и заискивание, угрозы и запугивание;
– самовосхваление (самореклама),
– самоназидательность и обвинение;
– просительность, демонстрация беспомощности, слабости, зависимости, вызывание жалости;
– экспертное, референтное и нормативное (сила власти и закона) влияния.

Учитываются также и потребности сотрудников. Кстати, любопытство можно рассматривать как потребность в получении дополнительной информации, что может быть составной частью потребности в общении (например, появляется новая тема для разговора), так и потребности во власти (дополнительная информация, как способ управления коллегами).

Основываясь на этом, можно выделить типичные методы воздей-

ствия злоумышленников на санкционированных пользователей (сотрудников) [17]:

- представляться другом-сотрудником (социальная потребность),
- представляться сотрудником поставщика, партнерской компании (социальная потребность, нормативное влияние), представителем закона (сила власти и закона),
- представляться кем-либо из руководства (сила власти и закона),
- представляться новым сотрудником, просящим о помощи (социальная потребность, потребность в самоуважении)
- представляться поставщиком или производителем операционных систем, звонящим, чтобы предложить обновление или патч (социальная потребность, нормативное влияние),
- предлагать помощь в случае возникновения проблемы, потом заставить эту проблему возникнуть, принуждая жертву попросить о помощи (социальная потребность, экспертное влияние),
- отправлять бесплатное ПО или патч жертве для установки (материальные потребности),
- использование фальшивого pop-up окна с просьбой аутентифицироваться еще раз, или ввести пароль (нормативное влияние),
- оставлять диск или дискету на столе у жертвы с вредоносным ПО (использование любопытства),
- использование внутреннего сленга и терминологии для возникновения доверия (потребность в принадлежности)
- предлагать приз за регистрацию на сайте с именем пользователя и паролем (материальные потребности).

4. Требования к информационной модели пользователя. Как отмечено выше, пользователи могут совершать различные противоправные действия в информационной системе и намеренно, и случайно. При этом указанные действия совершаются или не совершаются в зависимости от внутреннего состоянии пользователя. Соответственно, при построении информационной модели пользователя требуется выделить те существенные, «критичные» свойства пользователя, которые и будут влиять на его поведение в системе. Затем, обеспечив формализованное представление психологического профиля пользователя в рассматриваемой модели, можно будет приступить к имитации его действий в ответ на социоинженерные атакующие действия, что, в свою очередь, откроет возможность анализа степени защищенности

пользователя и автоматизированной информационной системы, к которой он имеет доступ [14].

В первую очередь, в информационной модели должны быть представлены сведения о правах пользователя, которыми он обладает в отношении программно-технических компонент информационной системы. Например пользователь может быть отнесен к группе администраторов или санкционированных пользователей. Как показывают исследования, основную угрозу представляют пользователи, имеющие навыки работы с компьютерами, т.е. разработчики, сотрудники службы поддержки [14]. Для подобных групп пользователей можно задать атомарные действия, которые может совершать на устройствах этот пользователь в ответ на атакующие воздействия или их серию. В силу того, что большинство пользователей обладает одинаковыми правами, их относят к группам пользователей, и уже этим группам (группе) приписывают все действия, которые может совершать пользователь.

Следующей особенностью, существенно влияющей на безопасность информационной системы, является наличие зон доступа и распределение прав доступа в эти зоны среди пользователей. Так, например, не всякий пользователь может попасть в серверную. Эта особенность должна быть представлена как свойство конкретного пользователя, а не группы пользователей, потому что обычными являются ситуации, когда в организации допуск в разные кабинеты (аудитории, офисы) открыт разным группам лиц, при этом обладающим одними и теми же правами доступа к устройствам.

Вместе с этим необходимо учесть следующее: несмотря на то, что учетные записи групп пользователей могут присутствовать на всех устройствах, у определенных пользователей может не быть доступа к некоторым устройствам, даже находящимся в той контролируемой зоне, к которым у этих пользователей есть доступ.

Наконец, одним из качеств (свойств) пользователя должна стать должность, занимаемая им в компании (или, возможно, набор из нескольких атрибутов, характеризующих позицию пользователя в иерархии организации). Так, например, пользователь может не иметь никакого доступа к компьютерам, но если его должность «директор», то он располагает колоссальными ресурсами, чтобы влиять на других пользователей, тем самым явно принуждая или скрыто побуждая их к противоправным действиям. При этом пользователи могут и не знать, что действия, которые они совершают под давлением вышестоящего руководства, могут оказаться или являются противоправными.

Перечисленные особенности, характеризующие пользователя, яв-

ляются существенными и наиболее очевидными; сведения о них, как правило, доступны и могут быть использованы без затруднений при построении информационной модели конкретного пользователя. Но этих сведений недостаточно, поскольку они не могут нести информации о причине, по которой или с использованием которой совершается та или иная социоинженерная атака. Опираясь на результаты обзора, предлагается выделить несколько основных параметров состояния пользователя, которые сильнее всего влияют на его поведение: нарциссизм, заинтересованность пользователя в деньгах, возможность запугать пользователя, возможность запугать пользователя. Кроме того, нельзя пренебречь влиянием на поведение пользователя его социальных и личностных расстройств и действий механизмов психологической защиты. Охарактеризуем подробнее перечисленные потенциальные уязвимости.

Нарциссизм. Многим людям присуще чувство нарциссизма. Они считают себя лучше других и не такими, как все, поэтому считают, что могут позволить себе больше, чем другие [14]. Кроме того, они хотят доказать окружающим, что они лучше их, поэтому могут попробовать взломать информационную систему и что-нибудь там испортить.

Заинтересованность пользователя в деньгах. Большинство людей считает что деньги, которые они получают за свою работу, не окупают затраченный на эту работу труд. Поэтому многие могут согласиться отдать кому-либо некоторую информацию, которую им не составит большого труда достать, за определенную сумму денег.

Возможность запугать пользователя. У каждого человека есть секреты. Порой люди не хотят, чтобы их секреты знали окружающие, в силу несоответствия этих секретов нравственным или правовым нормам. Злоумышленники могут воспользоваться нежеланием пользователя раскрывать конфиденциальную информацию личного характера и вынудить вместо нее отдать злоумышленникам необходимую им информацию служебного характера.

Социальные и личностные расстройства пользователя. Они также могут открывать (или образовывать) серьезную уязвимость (или даже набор уязвимостей) для совершения социоинженерных атак. Например люди, подверженные таким расстройствам, при возникновении проблем замыкаются в себе и не пытаются их решить. Таких проблем накапливается множество. И предложение злоумышленника решить их может вызвать очень серьезный позитивный отклик пользователя: он будет готов на многое, чтобы злоумышленники решили его проблемы. Кроме того, у подобного рода пользователей чаще возни-

кают противоречия с администрацией, что также может привести к желанию в качестве компенсации за какое-то действие руководителя нанести ущерб информационной системе компании.

Особо отметим роль психологической защиты в формировании поведения пользователя. С накоплением жизненного опыта у человека формируется специальная система, ограждающая от информации, нарушающей его внутреннее равновесие, — система защитных психологических барьеров [2]. Пока поступающая извне информация не расходится со сложившимся у человека представлением об окружающем мире, о себе, человек не испытывает дискомфорта [5]. Но как только намечается какое-либо расхождение, перед человеком встает проблема: либо изменить идеальное представление о самом себе, либо каким-то образом переработать информацию. Именно при выборе последней стратегии начинают действовать механизмы психологической защиты. Общая черта всех видов психологической защиты в том, что судить о ней можно только по косвенным проявлениям. Осознаются субъектом только некоторые из воздействующих на него стимулов, прошедшие через так называемый «фильтр значимости» [1], а отражается на поведении и многое из того, что было воспринято неосознаваемым образом. Когда человек получил неприятную информацию, отреагировать он на нее может различными способами. Он может уменьшить значимость информации, отрицать факты, которые другим кажутся совершенно очевидными или забыть «неудобную» информацию.

5. Выводы. Исходя из результатов, накопленных в области психологии и социальной психологии, представляется целесообразным включать в информационную модель пользователя, использующуюся при построении более «широких» моделей сцен (или контекстов), в которых может развиваться, осуществляться или имитироваться социоинженерная атака, три категории атрибутов:

— первая характеризует права пользователя относительно операций, которые он может осуществлять в автоматизированной информационной системе;

— вторая описывает позицию пользователя в организационной иерархии, раскрывая его возможности взаимодействия с другими пользователями;

— третья характеризует уязвимости пользователя, которые могут быть использованы при реализации атакующих действий.

Сведения о взаимосвязи указанных категорий атрибутов позволят прогнозировать (или имитировать) реакцию (серию действий) пользо-

вателя в ответ на атакующие действия. При этом следует учитывать, что такого рода взаимосвязи могут носить не только детерминированный, но также и стохастический характер, что должно стать предметом отдельного исследования.

Литература

1. *Бассин Ф.В.* Проблема бессознательного (О неосознаваемых возможностях высшей нервной деятельности). М.: Медицина, 1968. 468 с.
2. *Грановская Р.М., Крижанская Ю.С.* Творчество и преодоление стереотипов. СПб.: OMS, 1994. 180 с.
3. *Занковский А.Н.* Организационная психология: Учебное пособие для вузов по специальности «Организационная психология». 2-е изд. М.: Флинта, МПСИ, 2002. 648 с.
4. *Ильин Е.П.* Мотивация и мотивы. СПб.: Питер, 2000. 512 с.
5. *Коул М.* Культурно-историческая психология: наука будущего. М.: Когито-Центр, ИП РАН, 1997. 432 с.
6. *Молл Е.Г.* Менеджмент: Организационное поведение: Учебное пособие. М.: Финансы и статистика, 1998. 160 с.
7. Общая психология. Словарь // Психологический лексикон. Энциклопедический словарь в 6 т. / Ред.-сост. Л.А. Карпенко. Под общ. ред. А.В. Петровского. М.: ПЕРСЭ, 2005. 251 с.
8. *Сапронов К.* Человеческий фактор и его роль в обеспечении информационной безопасности. [электронный ресурс *http://www.interface.ru/home.asp?artId=17137*].
9. *Сартан Г.Н., Смирнов А.Ю., Гудимов В.В., Гудимов В.В.. Подхватилин Н.В., Алещунас М.Р.* Новые технологии управления персоналом. СПб.: Речь, 2003. 240 с.
10. *Семечкин Н.И.* Психология социального влияния. СПб.: Речь, 2004. 304 с.
11. *Сидоренко Е.В.* Мотивационный тренинг. СПб.: Речь, 2000. 324 с.
12. *Хьелл Л., Зинглер Д.* Теория личности. 3-е межд. изд. СПб.: Питер, 2002.
13. *Якобсон П.М.* Психологические проблемы мотивации поведения человека. М.: Просвещение, 1969. 317 с.
14. *Shaw E., Ruby K.G., Post J.M.* The Insider Threat to Information Systems The Psychology of the Dangerous Insider // Security Awareness Bulletin. 1998. N 2.
15. *Kotenko I.V., Stepashkin M.V.* Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life // Springer-Verlag Lecture Notes in Computer Science. 2005. Vol. 3685. P. 311–324.
16. *Kotenko I.V., Stepashkin M.V.* Network Security Evaluation Based on Simulation of Malefactor's Behavior // Proc. of the Intern. Conf. on Security and Cryptography (SECRYPT–2006), Setubal, 2006. P. 339–344.
17. *Mitnik K.* The Art of Deception. [электронный ресурс *http://bugtraq.ru/library/books/mitnick/*].

Тулупьева Татьяна Валентиновна — канд. психол. наук, доцент; с. н. с. лаборатории теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН), доцент кафедры информатики математико-механического факультета Санкт -Петербургского государственного университета (СПбГУ), доцент кафедры психологии управления и педагогики Северо-Западной академии государственной службы (СЗАГС). Область научных интересов: применение методов математики и информатики в гуманитарных исследованиях, информатизация организации и проведе-

ния психологических исследований, применение методов биостатистики в эпидемиологии, психология личности, психология управления. Число научных публикаций — около 70. TVT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Tulupyeva Tatiana Valentinovna — PhD in Psychology, associate professor; senior researcher, Theoretical and Interdisciplinary Computer Science Laboratory (TICS Lab), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), associate professor, Computer Science Department, Faculty of Mathematics and Mechanics, St. Petersburg State University (SPbSU), associate professor, Management Psychology and Pedagogic Department, North-West Academy of Public Administration (NWAPA). Research interests: application of mathematics and computer science in humanities, informatization of psychological studies, application of biostatistics in epidemiology, psychology of personality, management psychology. The number of publications — 70. TVT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Тулупьев Александр Львович — д-р физ.-мат. наук, доцент; заведующий лабораторией теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН), профессор кафедры информатики математико-механического факультета С.-Петербургского государственного университета (СПбГУ). Область научных интересов: представление и обработка данных и знаний с неопределенностью, применение методов математики и информатики в социокультурных исследованиях, применение методов биостатистики и математического моделирования в эпидемиологии, технология разработки программных комплексов с СУБД. Число научных публикаций — 210. ALT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Tulupyev Alexander Lvovich — PhD in Appl. Math. and CS, Dr. Sci. in CS, associate professor; head of laboratory, Theoretical and Interdisciplinary Computer Science Laboratory (TICS Lab), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), professor, Computer Science Department, Faculty of Mathematics and Mechanics, St. Petersburg State University (SPbSU). Research interests: uncertain knowledge and data representation and processing, application of mathematics and computer science in sociocultural studies, applications of biostatistics and mathematical modeling in modern epidemiology, software technologies and development of information systems with databases. The number of publications — 210. ALT@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Пащенко Антон Евгеньевич — м. н. с. научно-исследовательской группы междисциплинарных проблем информатики Учреждения Российской академии наук Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: математическая статистика, статистическое моделирование, применение методов биостатистики и математического моделирования в эпидемиологии. Число научных публикаций — 35. AEP@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Paschenko Anton Evgen'evich — junior researcher, Interdisciplinary Computer Science Research and Development Group, St. Petersburg Institute for Informatics and Automation of

the Russian Academy of Sciences (SPIIRAS). Research interests: mathematical statistics, statistical modeling, application of biostatistics and mathematical modeling in epidemiology. The number of publications — 35. AEP@iias.spb.su, www.tulupyev.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Степашкин Михаил Викторович — канд. техн. наук, н. с. лаборатории проблем компьютерной безопасности Учреждения Российской академии наук Санкт -Петербургский институт информатики и автоматизации РАН (СПИИРАН). Область научных интересов: методы и средства защиты информации от несанкционированного доступа, оценка уровня защищенности информационных систем, обнаружение вторжений, ложные информационные системы. Число научных публикаций — более 40. stepashkin@comsec.spb.ru, http://comsec.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450.

Stepashkin Mikhail Viktorovich — PhD, researcher of Laboratory of Computer Security Problems St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: methods and tools for information protection from unauthorized access, security level evaluation of information systems, intrusion detection, deception systems. The number of publications — more than 40. stepashkin@comsec.spb.ru, http://comsec.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-2642, fax +7(812)328-4450.

Азаров Артур Александрович — студент математико-механического и экономического факультетов Санкт-Петербургского государственного университета. Область научных интересов: автоматизация анализа защищенности информационных систем с учетом социоинженерных атак. Число научных публикаций — 2. artur-azarov@yandex.ru, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Azarov Artur Alexandrovich — student of Saint-Petersburg State University of the faculties of Mathematics and Mechanics and Economics. Research interests: the analyzing protection of informative systems concerning socioengineering's attacks. The number of publications — 2. artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Поддержка исследований. Настоящая работа частично поддержана грантом РФФИ (проект № 10-01-00640-а) и грантом СПбГУ (Мероприятие 2, 2011–2013 гг.).

Рекомендовано ТиМПИ СПИИРАН, зав. лаб. д-р физ.-мат. наук, доцент А.Л. Тулупьев.

Статья поступила в редакцию 20.11.2010.

РЕФЕРАТ

Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Степашкин М.В.
Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социо-инженерных атак.

Насколько бы ни была совершенной система обеспечения безопасности информации, с точки зрения технического обеспечения безопасности, человеческий фактор играет существенную роль, так как человек остается наиболее слабым звеном в этой системе. Любой сотрудник компании, имеющий достаточно прав для доступа к конфиденциальной информации, может нарушить ее целостность или предоставить эту информацию злоумышленнику, что в любом случае нанесет вред компании. Таким образом, появляется необходимость анализировать защищенность информационной системы при угрозах социо-инженерных атак. Для этого необходимо построить информационную модель пользователя, которая обладала бы определенным набором свойств, с помощью которого можно моделировать социоинженерные атаки.

Для решения этой задачи в статье рассмотрены действия, совершаемые сотрудником, которые влекут за собой нарушение безопасности информации. В ходе работ рассмотрены различные концепции и подходы инженерной, общей и социальной психологии, которые относятся к характеристикам уязвимости сотрудников компании. Таким образом получена классификация действий сотрудников, влияющая на защищенность информации. На основе этой классификации выделены критичные свойства пользователя, которые могут послужить основными причинами к совершению пользователем противоправных действий.

Выделено три категории атрибутов: права пользователя относительно операций, которые он может осуществлять в автоматизированной информационной системе, описана позиция пользователя в организационной иерархии, раскрыты возможности его взаимодействия с другими пользователями и уязвимости пользователя, которые могут быть использованы при реализации атакующих действий. Из полученных результатов стало понятно, что взаимодействие этих атрибутов и является предметом анализа защищенности информационных систем от социоинженерных атак. Кроме того, сделан вывод о необходимости ввода дополнительных информационных моделей. Таким образом, проблемы, поднятые в данной статье, могут стать предметом отдельного исследования.

SUMMARY

Tulupyeva T.V., Tulupyev A.L., Paschenko A.E., Azarov A.A., Stepashkin M.V.
Social Psychological Factors That Influence the Information System Users Vulnerability Degree in Regard of Socio-Engineering Attacks.

It does not matter how perfect security of information system, concerned to the technical part of the system, is, the human factor has a significant role, as it stays the weakest part of this system. Any employee of the company, who has proper rights to access private information, may break integrity of the information or give this information to the malefactor, all this can lead to the harmful effects to the company. In this case, it becomes essential to analyze the protection of the informative system in case of socioengineering attacks. To this it is needed to maintain informative model of the user, which includes special properties, which can help to model socio-engineering attacks.

For solving this problem, in the paper considered actions, which user can make, which can lead to the break of information protection. During work period, different concepts and solutions of engineering, common and social psychology were examined. This concepts are related to the characteristics of vulnerability of the employee of the company. In this case, classification on the users actions, which can influence on the information protection, were gained. On this base critical properties of the user, which can become main reasons for user to make an illegal actions, were highlighted.

Three categories of attributes were allocated: users rights concerning operations, which user can make in automatic informative system, description of the position of the user in the organization, showing his abilities to deal with other users and vulnerability of the user, which can be used for attack actions. To sum up, it is obvious that interaction of these attributes is the subject for analyzing of the protection of informative system from socioengineering attacks. What is more, it is important to introduce new informative models. In this case, problems, which were highlighted in this article may lead for additional research.