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

ПСИХОЛОГИЧЕСКАЯ ЗАЩИТА КАК ФАКТОР УЯЗВИМОСТИ ПОЛЬЗОВАТЕЛЯ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК

Тулупьева Т.В., Тулупьев А.Л., Азаров А.А. Пащенко А.Е. **Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак.**
Аннотация. С точки зрения анализа защищенности от социоинженерных атак, в статье предложено рассматривать комплекс «информационная система – персонал» как сложную реляционную систему, состоящую из критичных документов, хостов, пользователей, злоумышленника, причем каждый элемент системы может быть снабжен набором атрибутов, характеризующих его свойства и связи с другими элементами. В рамках предложенной реляционной модели особую роль играет профиль уязвимостей пользователя; в этом контексте были проанализированы связи между проявлениями психологической защиты пользователя и его склонностью к совершению в условиях социоинженерной атаки небезопасных действий.
Ключевые слова: информационная система, персонал, социоинженерная атака, визуальный редактор, злоумышленник, реляционные модели.

Tulupyeva T.V., Tulupyev A.L., Azarov A.A., Paschenko A.E. **Psychological defense as a factor of user's vulnerability in a socio-engineering attacks context.**
Abstract. The prototype of the program complex, used for demonstration of basic possibility for estimation the protection of personnel of information system from socioengineering attacks on the base of generalized approach, focused on analysis of trees of attacks, is described. The representation of information system and its personnel in the specified program complex is based on hierarchy of information models, which consist of information model of the user, information model of the users group, information model of control area, information model of hardware and software complex, information model of critical information objects (system of documents), information model of information system itself and links between corresponding objects. The list of technologies, used during the development of this product, the reasons for using this technologies and brief substantiation of some technical solutions are worked out. The example of proceeding of program complex prototype during editing the information about socioengineering attack, as well as during the imitation of socioengineering attack on the recompensation type on the personnel of this system is considered.
Keywords: information system, personnel, socio-engineering attack, visual editor, malefactor, relational models.

1. Введение. В статье [2] были рассмотрены основные классы и подклассы психологических особенностей, лежащих в основе уязвимостей пользователя. В разработанной ранее классификации нами было выделено 29 психологических особенностей, которые разбиты на классы и подклассы.

Основные классы уязвимостей, выявленные ранее:

1. Психологические качества, влияющие на уязвимость человека;
2. Социальные и личные факторы, влияющие на уязвимость человека.

Психологические качества являются «фоновыми» уязвимостями (или образуют основу для проявления таких уязвимостей) для человека и относительно легко выявляются при помощи тестов, анкет, опросов. В этом классе в свою очередь было выделено 3 подкласса:

1.1. Потребности человека;

1.2. Черты характера человека;

1.3. Психологическая защита.

Однако для прикладных исследований недостаточно знать степень проявления той или иной психологической особенности. Для полного построения информационной модели «автоматизированная информационная система –персонал» нам необходимо сопоставлять степень выраженности и вероятность успешности осуществления социоинженерной атаки. Для этого целесообразно все данные тестов, анкет, опросов и иных методик выявления выраженности уязвимостей пользователя переводить в количественные показатели. Мы не ставим своей целью в данной статье определять пороговые значения уязвимостей для осуществления той или иной успешной социоинженерной атаки, а лишь предполагаем их вероятность. Для получения точных данных следует проводить соответствующие исследования и выявление конкретных значений экспертным и экспериментальным путем.

Целью этой статьи является рассмотрение роли психологической защиты в профиле уязвимостей пользователя, а также описание (на уровне идеи) подхода к применению реляционных и вероятностно-реляционных представлений соответствующих данных и знаний в моделях «автоматизированная информационная система – персонал».

2. Психологическая защита. Как определяет это понятие словарь, «*психологическая защита* — специальная регулятивная система стабилизации личности, направленная на устранение или сведения до минимума чувства тревоги, связанного с осознанием конфликта» [12].

В течение всей жизни у человека формируется Картина мира, которая основывается на собственном опыте. Эта модель является представлением человека о мире и себе. Как правило, психика конкретного человека выделяет из общего потока информации ту часть, которая отвечает определенным требованиям, и таким образом формируется субъективная картина мира. Поступление новых сведений приводит к дополнению или преобразованию модели мира, в том случае если новый опыт совместим с уже существующим в модели мира на данный момент. Пока поступающая извне информация не расходится со сложившимся у человека представлением об окружающем мире, о себе, человек не испытывает дискомфорта [9]. 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. С.Р. Мадди [36], сравнивая различные теории психологической защиты, отмечал, что большинство связывает психологическую защиту с чувством тревоги, которая могла бы возникнуть из-за боязни наказания, чувства вины или понижения самооценки. Ф.В. Бассин предлагает рассматривать психологическую защиту как «специфическое преобразование системы установок» [1]. Эта система включает отношения субъекта к самому себе и к окружающему миру и выражается в форме оценок, намерений, влечений, истолкований. Это преобразование возникает как реакция на психическую травму и нейтрализует тягостные эмоциональные переживания [13, 14]. В результате восприятие окружающего изменяется, и значимость психической травмы снижается.

Таким образом, если пользователь находится в ситуации нарушения каких-либо правил, то это должно привести к изменению самооценки и представления о себе. Но если в данной ситуации активизируются механизмы психологической защиты, то пользователь может не осознать последствия своего поступка, оправдать себя каким-либо образом, частично модифицировать информацию, отрицать факты, которые другим кажутся совершенно очевидными или забыть «неудобную» информацию.

Плутчик считает [41], что в течение жизни индивид сталкивается с большим числом ситуаций, которые вызывают определенные эмоциональные состояния такие, как гнев, страх, уныние и т.д. Довольно часто выражение эмоционального состояния создает дальнейший конфликт и дополнительную опасность. Результатом является то, что человек развивает защитные стратегии, которые представляют косвенные пути разрешения эмоциональных конфликтов. Однако специфические защитные стратегии развиваются в зависимости от специфических эмоций, вовлеченных в конфликт. Более того, защитные стратегии проявляются и закрепляются в определенных жизненных ситуациях, и в течение жизни у человека формируется защитный стиль, который заключается в предпочтении одних видов защиты другим. Таким образом, индивид с сильными характеристиками личности имеет тенденцию выбирать определенные защитные механизмы. Некоторые авторы указывают на связь видов защиты и личностных характеристик, которая представлена в табл. 1 [8, 41].

Таблица 1. Взаимосвязи личностных черт, эмоций и механизмов защиты

эмоция	черта личности	защитный процесс
страх	застенчивость	вытеснение
уверенность в себе	самонадеянность	отрицание
удивление	наивность	регрессия
гнев	агрессивность	замещение
уныние	депрессивность	компенсация
восторг	жизнерадостность	реактивное образование
отвращение	подозрительность	проекция
удовлетворение	контролирование	рационализация

Далее рассмотрим различные виды психологической защиты и укажем, каким образом они могут проявляться в контексте уязвимости пользователя.

3. Защитные механизмы.

3.1. Компенсация. Компенсация представляет собой интенсивные попытки исправить или как-то восполнить собственную реальную или воображаемую физическую или психическую неполноценность [9]. С помощью компенсации человек стремится восполнить слабости и неудачи в одной области достижениями в другой [4]. Пользователи с высокой компенсацией должны вызывать повышенное внимание сотрудников службы безопасности. У таких людей может возникнуть стремление при каких-то неудачах повысить свою значимость пусть даже в собственных глазах путем передачи кому-то информации. Это может дать им ощущение контроля над ситуацией, зависимости от них других людей, которые их обижали. Так пользователь, которого не повысили по службе, не признали его достижений, не отпустили во внеочередной отпуск, не дали отгул, объяснив это тем, что он недостаточно поработал, может захотеть показать свою важность и совершить действия, которые выгодны злоумышленнику. Более того, компетентный злоумышленник может подтолкнуть пользователя к мысли, что его недооценивают. И в этом случае снова запустится механизм проекции.

Особенно тревожащими в этом отношении являются пользователи с высокой компенсацией, которые не имеют достаточного авторитета и сильно страдают в коллективе от насмешек и прозвищ. К сожалению, такие ситуации характерны не только для подростковых групп, но встречаются и в трудовых коллективах. Такие люди становятся наиболее уязвимыми к действиям злоумышленника.

3.2. Отрицание. Отрицание — недостаточное осознание определенных событий, переживаний и ощущений, которые причинили бы

человеку боль при их признании [41]. Отрицание представляет собой барьер, расположенный на входе. При отрицании избегаются темы, ситуации, книги, кинофильмы, подозреваемые в провоцировании у себя нежелательных эмоций. В отличие от других защитных барьеров, отрицание осуществляет селекцию сведений, а не их трансформацию из неприемлемых в приемлемые [4]. Этот способ защиты вступает в действие при конфликтах любого рода, не требует предварительного научения, характеризуется заметным искажением восприятия действительности, часто принимающим форму ухода от нее в «болезнь».

Высокое отрицание может привести к тому, что человек не воспринимает информацию, отличную от его мнения. Такие люди могут достаточно скептически и пренебрежительно относиться к требованиям по технике безопасности, к предостережениям по поводу открытия неизвестных файлов, к различного рода инструкциям. Инструкции не являются для них чем-то важным и значимым, поскольку, «это все перестраховка, и ничего страшного произойти не может». Такие люди просто оставляют возможность для технического получения информации. Они могут сообщать пароль от своего компьютера, устанавливать вредоносные программы. В [3]приводится пример отрицания, которое влечет за собой недооценку последствий. В частности, один из экспертов говорит: «Большинство специалистов по информационным технологиям, которых я знаю, даже еще начинающие ребята, сразу же при вступлении в должность первым делом устанавливают программу скрытого управления (rootkit) в корпоративную систему. Это рефлекс. Ребята не хотят никому навредить и не строят вредоносных планов, им просто нужен надежный доступ к системе, чтобы можно было спокойно работать из дома или колледжа». Таких людей нужно инструктировать особым образом, добиваясь осознания важности предоставляемых инструкций.

3.3. Замещение. Замещение — смена направления негативных чувств с реального объекта на более безопасный [7]. Замещение — психологическая защита, осуществляющая перенос реакции с недоступного объекта на доступный или замену действия неприемлемого на приемлемое [4]. Замещение выступает как разрядка эмоций на объекты, животных или людей, воспринимаемых индивидом как менее опасные, чем те, которые действительно вызывают эти эмоции. Стандартным замещением грубой силы, нацеленной на наказание или оскорбление, служит брань или словесные оскорбления. Замещение исходной деятельности может реализоваться не только переходом на другой объект или к другому действию, но и переводом в другой

план — из реального мира в мир утешительных фантазий [5]. Замещение разряжает напряжение, но не приводит к желаемой цели.

Высокое замещение может толкать пользователя отомстить начальнику или сотруднику, который его каким-то образом обидел. Такой сотрудник намеренно может передать сведения злоумышленнику или по-другому навредить. Для предотвращения этой ситуации нужно контролировать эмоциональное состояние сотрудника, выводить его из эмоционального напряжения и убирать чувство обиды.

Пример замещения описан в [3]. «Компания выяснила, что сотрудник достаточно хорошо разбирается в дизайне и программировании, и попросила его разработать корпоративный веб-сайт. Несколько месяцев спустя этому служащему был объявлен выговор за систематические прогулы, а президент компании сообщил ему, что руководство планирует отстранить его от работы. В тот же день обиженный сотрудник удаленно вошел в корпоративную сеть, стер некоторые данные, поменял текст и картинки на веб-сайте компании. Когда саботажника задержали правоохранительные органы, он объяснил свое поведение тем, что разозлился на работодателя, поскольку его отстранили.»

3.4. Проекция. Проекция — неосознаваемое отвержение собственных эмоционально неприемлемых установок или желаний и приписывание их другим людям [10]. Это вид психологической защиты, который подразумевает выделение в другом лице или объекте качеств, желаний, которые сам субъект не признает или отвергает в самом себе. При проекции информация трансформируется таким способом, что человек считает, что не он сам враждебно настроен, агрессивен, жаден, а другое лицо по отношению к нему [6]. Проекция — это неосознаваемое отвержение собственных эмоционально неприемлемых мыслей, установок или желаний и приписывание другим людям, животному или объекту качеств, чувств и намерений, которые исходят от самого приписывающего. «Никогда нельзя верить никому» — (я и сам могу иной раз обмануть кого-нибудь). Пусковым механизмом проекции может являться низкая самооценка, тогда человек недоволен собой, вследствие конфликта между реальным и желаемым «Я», и это ведет к отрицательному восприятию окружающих. Поэтому низкая самооценка повышает вероятность возникновения проекции. Механизм проекции лежит в основе перекладывания ответственности за поступки на других людей или на обстоятельства.

Сотрудник с высокой проекцией может считать, что это из-за действий администрации он не добивается успехов на работе, а все со-

трудники так и ждут, когда он совершит какой-нибудь промах. Или может считать, что любой сотрудник готов «продать» информацию, только не всем такая возможность предоставляется. Такие мысли помогают ему не чувствовать вину и угрызения совести за совершенные действия.

3.5. Рационализация. Механизм рационализации проявляется в псевдообъяснении человеком собственных неприемлемых желаний, убеждений и поступков с целью самооправдания [7]. Рационализация — психологическая защита, связанная с осознанием и использованием в мышлении только определенной части информации, которая помогает описать собственное поведение как хорошо контролируемое [6]. При этом травмирующая, неприемлемая часть ситуации удаляется из сознания и после трансформации осознается в преобразованном виде. Защита осуществляется с помощью построения убедительных доводов для оправдания своих социально-неприемлемых желаний и действий. Рационализация — это нахождение ложных приемлемых причин или оснований для неприемлемых мыслей или действий.

Существуют наиболее яркие феномены рационализации, которые получили названия «кислый виноград» и «сладкий лимон» [4]. Первый известен по басне Эзопа о лисе, которая не могла добраться до виноградной кисти и потому решила, что ягоды еще не созрели. Этот механизм понижает привлекательность, значимость недоступного объекта.

Рационализация может помочь сотруднику оправдать свои действия. Пользователь может объяснить, в первую очередь, себе, что ничего страшного он не совершил, что, на самом деле, это была не такая уж важная информация, что злоумышленники ее и так бы получили, а он, зато, за это имеет какие-то выгоды.

4. Изучение механизмов психологической защиты. На основании вышесказанного можно сделать вывод, что диагностика механизмов психологической защиты поможет выявить уязвимые места пользователя, предсказать его возможные стратегии поведения.

Несмотря на то, что о психологической защите говорят достаточно давно (впервые термин «защита» появился в 1894 году в работе Фрейда З. «Защитные нейропсихозы»), признавая ее роль в модификации поведения, проблема диагностики защитных механизмов из-за их бессознательной природы существовала достаточно долго.

В 30-е годы XX века интерес к психологической защите усилился, и была проведена серия исследований, направленных на изучение защитных механизмом. Большая часть этих лабораторных исследований фокусировалась либо на защите по типу вытеснение, либо на защите

по типу проекция. Большинство исследований, направленных на изучение вытеснения можно разделить на два типа: (а) эксперименты, связанные с запоминанием (научением) и памятью, и (б) изучение перцептивной защиты [20].

Подобные исследования были достаточно активны с 30-х по 60-е годы XX века, но их результаты были подвергнуты критике. Один из активных критиков, D. S. Holmes [27, 28, 30], заключил, что большинство результатов исследований на память, первоначально приписываемых вытеснению, лучше могут быть объяснены различиями в процессах внимания. Были предъявлены претензии к методологии организации исследований по перцептивной защите. Трудности, которые испытуемые имели при восприятии слов-табу, также могли бы быть объяснены такими факторами, как длина слова, различная степень привычности слов и социальная неприемлемость [32]. В результате возникло мнение, что вытеснение, как защитный процесс, которые происходит без осознания, не существует. Такая критика имела негативное воздействие на исследования психологической защиты, в результате к концу 1970-х лабораторные исследования вытеснения практически исчезли [31, 37].

При изучении проекции парадигмы были изначально двух типов: приписывание личностных характеристик неясным стимулам и парадигма Я–Другие (приписывание черт самому человеку и другим). Holmes [26, 29] пришел к выводу, что в такого рода экспериментах не было доказательств неосознанной проекции. Cramer в своей работе подчеркивает [19], что Holmes не говорил, что явления проекции не существует. Скорее, он полагал, что этот процесс более осторожно категоризован как атрибуция. Исследования этого процесса, без учета его значения как защитного механизма, были взяты социальными психологами и включены в теорию атрибуции. [34, 35].

Таким образом, к концу 1970-х, вытеснение было объяснено процессами внимания и ответным подавлением, в то время как проекция была объяснена атрибуцией. По крайней мере, так как это исследовалось в лаборатории, эти процессы не выглядели вовлеченными в бессознательное функционирование и таким образом, по определению, не являлись защитными механизмами [19].

Однако, несмотря на такого рода критику, в клинической психологии и психологии личности продолжали использовать концепцию защиты. Одной из задач было найти адекватное измерение защиты. Хотя несколько измерений защиты в виде опросника было разработано [17, 24, 33], каждое из этих измерений имело психометрические недо-

статки [21]. Наиболее широко используемой из оценочных процедур был Defense mechanisms Inventory (Список защитных механизмов), разработанный Gleser и Ihilevich [23]. Однако, свидетельства надежности и валидности этой методики были недостоверны [18]. Недавно, Bond разработал другой самооценочный опросник Defense Style Questionaire (опросник защитного стиля) [16]. Одним из широко применяемых в России методов для определения уровня выраженности защитных механизмов является Life Style Index (Индекс жизненного стиля), разработанный Plutchik R., Kellerman H., Conte H.R. [41].

В течение нескольких лет новые идеи о защитных механизмах начали развиваться. Современные психологические теории расширили роль защиты и включили в нее поддержание самооценки и защиту самоорганизации [38,22]. В соответствии с этим изменением в теории появились новые подходы к оценке защитных механизмов. Исследователи, недовольные логическим несоответствием, заключающимся в необходимости получения самоотчета испытуемых об операциях, которые, по определению, бессознательны, развили несколько новых подходов [19]. Эти методы наблюдения — включая оценку использования защиты в клинических интервью [39, 43], кодирование повествовательного материала [18] и Q-сортировка [20, 25,42] — гарантируют свободное выражения мыслительного содержания и стиля и в тоже самое время снабжают наблюдателя систематическим планом для оценки присутствия защитных механизмов. Особенности правил кодирования делают возможным определить как надежность, так и валидность измерений. Достоинства и недостатки и самоотчета, и методов наблюдения были обсуждены Davidson'ом и MacGregor'ом [21] и Perry и Ianni[40].

Для количественной оценки выраженности видов психологической защиты существовали методики, чаще на основе MMPI, которые измеряли только несколько видов защиты (отрицание, рационализация и проекция) [31]. Более интенсивно психологическая защита стала изучаться после разработки опросника Келлермана-Плутчика для определения интенсивности выраженности защитных механизмов [11]. В настоящий момент эта методика является наиболее оптимальным инструментарием для выявления защитного профиля пользователя в контексте социоинженерных атак.

5. Приложение реляционного подхода к моделированию комплексов «информационная система–персонал». Н.В. Хованов, обобщая и адаптируя в [15] результаты и положения ряда общетеоретических, частных и учебных публикаций, предложил моделировать

комплекс «товар – посредник – потребитель» на основе реляционного подхода. Под товаром понимается некоторое экономическое благо, циркулирующее на рынке. Для простоты мы рассматриваем модель с одним посредником, однако их может быть больше (пи этом они в модели выстроятся последовательно в цепь). Распространение предлагаемой модели на случай с бóльшим числом посредников будет очевидным.

Согласно [15], товар характеризуется вектором $v = (c, u, p)$, где c — градация производственной ценности товара, u — градация потребительской ценности и, наконец, p — градация меновой ценности. Заметим, что обозначения обладают выверенной мнемоникой: cost, utility, price — стоимость, полезность, цена. Каждый компонент (атрибут) вектора v измеряется в определенной шкале (C, U, Pсоответственно), которая полагается конечной и дискретной.

В детерминированном случае возможность перехода товара от производителя к посреднику характеризуется отношением $R_1(c, p)$ — подмножеством декартова произведения $C \times P$, возможность перехода товара от посредника к потребителю — отношением $R_2(p, u)$ (подмножество декартова произведения $P \times U$), и, наконец, существенным ограничением на обмен является отношение $R_3(\mathrm{c}, u)$ —подмножество декартова произведения$C \times U$. Распространение модели на случай нескольких посредников может быть реализовано введением нескольких отношений $R_{2i}(p_i, u_i)$, где i индексирует множество посредников, для первого посредника $P_i = P$, для последнего посредника $U_i = U$, а в отношениях между посредниками $P_{i+1} = U_i$; соотвественно задаются и декартовы произведения доменов.

В стохастическом случае каждой паре значений в отношении сопоставляется вероятность «реализации» отношения, то есть того, что обмен произойдет (или, более точно, что при указанном сочетании значений отношение не воспрепятствует проведению обмена.)

На основе отношений R_1, R_2, R_3 строится отношение $R_1(c, u, p)$, которое и характеризует возможность того, что товар при заданных сочетаниях градаций перейдет от производителя покупателю. В стохастическом случае при некоторых предположениях вычисляется вероятность такого перехода.

Указанный подход можно адаптировать к представлению отношений в комплексе «информационная система – персонал». С точки зрения анализа защищенности от социоинженерных атак, в указанном комплексе можно выделить следующие компоненты: I — критичная информация, более точно — система документов, каждый из которых,

с одной стороны, характеризуется показателем или показателями критичности, а с другой стороны, атрибутами, характеризующим его доступность с такого-то хоста с правами такого-то пользователя; H — хосты, которые характеризуются своими связями с другими хостами, рядом атрибутов, описывающих текущую конфигурацию программно-технического обеспечения (по этим атрибутам определяется успешность реализации атакующих действий программно-технического характера), а также рядом атрибутов, описывающих права пользователей на данном хосте;U — пользователи, которые характеризуются своими отношениями к группам пользователей, в отношении которых установлены определенные политики безопасности, допуском в определенные зоны, а также профилем уязвимости (который формируется, в том числе, на основе сведений о *психологической защите*), причем профиль уязвимости определяет вероятность успеха социоинженерных атакующих действий, и связями с другими пользователями; H — злоумышленник или группа злоумышленников, которые характеризуются своими связями с пользователем, первоначальной возможностью доступа к хостам, а также ресурсами, которые они могут расходовать для осуществления СИ-атаки.

Отношения между элементами указанных компонент допускают формализацию тем же путем, как это было выполнено в [15], но семантика таких отношений будет иной, отражающей особенности предметной области. Например, с помощью отношения$R_1(i,h)$ — подмножества декартова произведения $I \times H$ — можно представить сведения о возможности доступа с хоста h к критичному документу i. Далее, с помощью отношения $R_2(i,u)$ — подмножества декартова произведения $I \times U$ — можно представить допуск пользователя u к документу i. Наконец, с помощью отношения $R_3(h,u)$ — подмножества декартова произведения $H \times U$ — можно представить допуск пользователя u к хосту h.

Уже спецификация только этих трех отношений, критичности документов и вероятности того, что подвергшийся социоинженерной атаке санкционированный пользователь предпримет нарушающие конфиденциальность информации действия, при некоторых предположениях позволит распространить оценку критичности на хосты и на пользователей. Разумеется, указанная выше вероятность, как правило, не задается изначально, а оценивается на основе отношений между пользователями, между пользователями и злоумышленниками и других отношений и связях в комплексе «информационная система – персонал».

Стоит особо подчеркнуть, что на данном этапе исследований особенно важным и открытым вопросом является формализация профиля уязвимостей пользователя в рамках предложенного подхода. Результаты (см. табл. 2) исследования отношений степени проявления видов психологической защиты пользователя и его склонности к небезопасным действиям позволяют предположить, что такие отношения могут быть формализованы в рамках представленного выше реляционного подхода.

Таблица 2. Примеры возможных действий по нанесению вреда и профилактических мер по некоторым видам защиты.

Защитный механизм	Возможные действия по нанесению вреда	Профилактические меры
Компенсация	Сознательная передача информации	Особое внимание к сотрудникам с высокой компенсацией, которых чем-то обделили
Отрицание	Сообщение пароля от своего компьютера, установка вредоносных или несанкционированных программ	Соответствующий инструктаж, контроль
Замещение	Намеренная передача информации или нарушение целостности данных	Контроль эмоционального состояния сотрудника, выведение его из состояния эмоционального напряжения
Проекция	Перекладывание ответственности на других за совершение какого-либо действия.	Особое внимание и тренинговая работа с сотрудниками, имеющими низкую самооценку
Рационализация	Оправдание себя за совершенные действия.	Разъяснение санкций
Защитный механизм	Возможные действия по нанесению вреда	Профилактические меры

5. Заключение. В рамках исследования подходов к формированию понятия «профиль уязвимостей пользователя» и к выработке инструментария по выявлению наличия таких уязвимостей рассмотрена связь различных видов психологической защиты и склонности пользователя совершать несанкционированные действия.

Кроме того, предложено моделировать отношения между элементами комплекса «информационная система – персонал» и между указанными элементами и злоумышленником в рамках реляционного (и вероятностно-реляционного) подхода.

Связь между степенями проявления психологической защиты и склонностью пользователя, подвергшегося социоинженерной атаке, к небезопасным действиям допускает удобное представление в виде реляционных моделей, описанных выше.

Литература

1. *Бассин Ф.В., Бурлакова М.К., Волков В.Н.* Проблема психологической защиты // Психологический журнал. 1988. Т. 9, № 3.С. 78–86.
2. *Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.* Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социо-инженерных атак // Труды СПИИРАН. 2011. Вып. 17. С. 70–99.
3. *Доля А.* Саботаж в корпоративной среде // Экспресс Электроника. 2006. URL: http://citforum.ru/security/articles/sabotage/ (доступ 25.05.2011).
4. *Грановская Р.М.* Элементы практической психологии. Л.: ЛГУ, 1988. 564 с.
5. *Грановская Р.М.* Актуальность исследования психологической защиты // Вестник Балтийской академии. 1988. Вып. 18.С. 47–51.
6. *Грановская Р.М., Никольская И.М.* Защита личности: психологические механизмы. СПб.: Знание, 1999. 352 с.
7. *Карвасарский Б.Д.* (общ.ред.) Психотерапевтическая энциклопедия. СПб: Питер Ком, 1998. 752 с.
8. *Коржова Е.Ю.* Жизненные ситуации и стратегии поведения // Психологические проблемы самореализации личности / Под ред. Крылова А.А., Коростылевой Л.А. СПб.: СПбГУ, 1997. С. 75–88.
9. *Коул М.* Культурно-историческая психология: наука будущего. М.: «Когито-Центр», «ИП РАН», 1997. 432 с.
10. *Михайлов А.Н., Роттенберг В.С.* Особенности психологической защиты в норме и при соматических заболеваниях // Вопросы психологии. 1990. № 5.С. 106–111.
11. Психологическая диагностика индекса жизненного стиля. (Пособие для врачей и психологов.) / Под ред. Вассермана Л.И. СПб., 1998. 48 с.
12. Психология. Словарь/ Под ред. Петровского А.В., Ярошевского М.Г. М.: Политиздат, 1990. 494 с.
13. Руководство по психотерапии / Под ред. Рожнова В.Е. Ташкент: Медицина, 1979. 620 с.
14. *Стоиков И.Д.* Анализ защитных проявлений личности: Дис. на соиск. учен.степ. канд. психол. наук: 19.00.01. М., 1986. 160 с.
15. *Хованов Н.В.* Общая модель измерения ценности экономических благ // Применение математики в экономике. Вып. 18 / Под. ред. Воронцовского А.В. СПб.: ООО «ИПК «КОСТА», 2009. С. 108–134.

16. *Andrews G., Pollock C., Stewart G.* The determination of defense style by questionnaire // Archives of General Psychiatry. 1989. № 46.P. 455–460.
17. *Byrne D.* The Repression-Sensitization Scale: Rationale, reliability, and validity // Journal of Personality. 1961. № 29.P. 334–349.
18. *Cramer P.* The development of defense mechanisms: Theory, research and assessment. New York: Springer-Verlag, 1991. 240 p.
19. *Cramer P.* Defense mechanisms in psychology today: Further processes for adaptation // American Psychologist. 2002. № 55. P. 637–646.
20. *Davidson K., MacGregor M.W.* Reliability of an idiographic Q-sort measure of defense mechanisms // Journal of Personality Assessment. 1996. № 66. P. 624–639.
21. *Davidson K., MacGregor M.W.* A critical appraisal of self-report defense mechanisms measures // Journal of Personality. 1998. № 66. P. 965–992.
22. *Fenichel O.* The psychoanalytic theory of neurosis. New York: Norton, 1945.
23. *Gleser G.C., Ihelivich D.* An objective instrument for measuring defense mechanisms // Journal of Consulting and Clinical Psychology. 1969. № 33.P. 51–60.
24. *HaanN.* Coping and defense mechanisms related to personality inventories // Journal of Consulting Psychology. 1965. № 29.P. 373–378.
25. *Haan N.* Processes of moral development: Cognitive or social disequilibrium? // Developmental Psychology. 1985. № 21. P. 996–1006.
26. *Holmes D.S.* Dimensions of projection // Psychological Bulletin. 1968. № 69. P. 248–268.
27. *Holmes D.S.* Repression or interference? A further investigation // Journal of Personality and Social Psychology. 1972. № 22. P. 163–170.
28. *Holmes D.S.* Investigation of repression: Differential recall of material experimentally or naturally associated with ego threat // Psychological Bulletin. 1974. № 81. P. 632–653.
29. *Holmes D.S.* Projection as a defense mechanism // Psychological Bulletin. 1978. № 85. P. 677–688.
30. *Holmes D.S.* The evidence for repression: An examination of sixty years of research // Repression and dissociation / J. L. Singer (Ed.). Chicago: University of Chicago Press, 1990. P. 85–102.
31. *Holmes D.S., McCaul K.D.* Laboratory research on defense mechanisms // Advances in the investigation of psychological stress / R. W. J. Neufeld (Ed.). New York: Wiley, 1989. P. 161–192.
32. *Howes D.H., Solomon R.L.* A note on McGinnies' "Emotionality and perceptual defense" // Psychological Review. 1950. № 57.P. 229–234.
33. *Joffe P., Naditch M.P.* Paper and pencil measures of coping and defense processes // Coping and defending / N. Haan (Ed.). New York: Academic Press, 1977. P. 280–297.
34. *Jones E.E., Davis K.E.* From acts to dispositions: The attribution process in person perception // Advances in experimental social psychology. Vol. 2 / L. Berkowitz (Ed.). New York: Academic Press, 1965. P. 220–266.

35. *Kelly H.H.* (1967). Attribution theory in social psychology // Nebraska symposium on motivation.Vol. 15 / D. Levine (Ed.). Lincoln: University of Nebraska Press, 1967. P. 192–238.
36. *Maddi S.R.* Personality theories, comparative analysis. Homewood, Illinois. Irvin-Dorsey limited, Nobleton, Ontario:The Dorsey Press, 1986. 520 p.
37. *Paulhus D.L., Fridhandler B., Hayes S.* Psychological defense: Contemporary theory and research //Handbook of personality / R. Hogan, J. Johnson, S. Briggs (Eds.). New York: Academic Press, 1997. P. 544–580.
38. *Perry J.C., Cooper S.H.* An empirical study of defense mechanisms: I. Clinical interview and life vignette ratings // Archives of General Psychiatry. 1989. № 46. P. 444–452.
39. *Perry J.C., Cooper S.H.* What do cross-sectional measures of defense mechanisms predict? // Ego mechanisms of defense: A guide for clinicians and researchers / G. E. Vaillant (Ed.). Washington, DC: American Psychiatric Press, 1992. P. 195–216.
40. *Perry J.C., Ianni F.F.* Observer-rated measures of defense mechanisms // Journal of Personality. 1998. № 66. P. 993–1024.
41. *Plutchik R., Kellerman H., Conte H.R.* A structural theory of ego defenses and emotions. // Emotions in personality and psychopathology / Izard C.E. (ed.). N.Y., 1979. P. 229–257.
42. *Roston D., Lee K.A., Vaillant G.E.* A Q-sort approach to identifying defenses // Ego mechanisms of defense: A .guide for clinicians and researchers /G. E. Vaillant (Ed.). Washington, DC: American Psychiatric Press, 1992.P. 217–236.
43. *Vaillant G.E.* Theoretical hierarhy of adaptive ego mechanisms // Archives of General Psychiatry. 1971.Vol. 24. P. 107–118.

Тулупьева Татьяна Валентиновна — к.психол.н., доцент; старший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики (ТиМПИ) Учреждения Российской академии наук С.-Петербургский институт информатики и автоматизации РАН (СПИИРАН), доцент кафедры информатики математико-механического факультета С.-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 проведения 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, г. 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, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Тулупьев Александр Львович — д.ф.-м.н., 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 — 250. ALT@iias.spb.su, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, г. 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, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Азаров Артур Александрович — младший научный сотрудник научно-исследовательской группы междисциплинарных проблем информатики Учреждения Российской академии наук С.-Петербургский институт информатики и автоматизации РАН (СПИИРАН). 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, г. Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Azarov Artur Alexandrovich — — 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: the analyzing protection of information systems concerning socioengineering's attacks. The number of publications — 2.artur-azarov@yandex.ru, 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.

Пащенко Антон Евгеньевич — младший научный сотрудник научно-исследовательской группы междисциплинарных проблем информатики Учреждения Российской академии наук С.-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, г. 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.

Поддержка исследований. Поддержано грантами: Грант РФФИ на 2010–2012 гг., проект № 10-01-00640-а «Интеллектуальные модели и методы анализа защищенности информационных систем от социо-инженерных атак (деревья атак)», Грант СПбГУ на 2011–2013 гг. Проект № 6.38.72.2011 «Моделирование комплексов «информационная система—персонал» для агрегированной оценки их готовности к отражению социоинженерных атак», Грант Правительства Санкт-Петербурга для победителей конкурса грантов Санкт-Петербурга для студентов, аспирантов, молодых ученых, молодых кандидатов наук 2011 г.

РЕФЕРАТ

Тулупьева Т.В., Тулупьев А.Л., Азаров А.А., Пащенко А.Е. **Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак.**

Психологические качества являются «фоновыми» уязвимостями (или образуют основу для проявления таких уязвимостей) для человека и относительно легко выявляются при помощи тестов, анкет, опросов. Среди указанных качеств выделяются 3 подкласса: потребности человека, черты характера человека, психологическая защита.

Для прикладных исследований недостаточно знать степень проявления той или иной психологической особенности. Для полного построения информационной модели «автоматизированная информационная система – персонал» необходимо сопоставлять степень выраженности психологической особенности и вероятность успешности осуществления социоинженерной атаки (точнее, атакующего действия). Для этого целесообразно все данные тестов, анкет, опросов и иных методик выявления выраженности уязвимостей пользователя переводить в количественные показатели. Для получения количественных данных с нужной точностью следует проводить соответствующие исследования и выявление конкретных значений экспертным и экспериментальным путем.

Целью этой статьи является рассмотрение роли психологической защиты в профиле уязвимостей пользователя, а также описание (на уровне идеи) подхода к применению реляционных и вероятностно-реляционных представлений соответствующих данных и знаний в моделях «автоматизированная информационная система – персонал».

В рамках исследования подходов к формированию понятия «профиль уязвимостей пользователя» и к выработке инструментария по выявлению наличия таких уязвимостей рассмотрена связь различных видов психологической защиты и склонности пользователя совершать несанкционированные действия.

Кроме того, предложено моделировать отношения между элементами комплекса «информационная система – персонал» и между указанными элементами и злоумышленником в рамках реляционного (и вероятностно-реляционного) подхода.

Связь между степенями проявления психологической защиты и склонностью пользователя, подвергшегося социоинженерной атаке, к небезопасным действиям допускает удобное представление в виде реляционных моделей, описанных в статье.

SUMMARY

Tulupyeva T.V., Tulupyev A.L., Azarov A.A., Paschenko A.E. **Psychological defense as a factor of user's vulnerability in a socio-engineering attacks context.**

Psychological traits can be considered as a background for user's vulnerabilities or as the base for such vulnerabilities. The traits can be relatively easy detected with psychological tests, questionnaires, and interviews. These traits fall into three subclasses: human needs, human character traits, and psychological defense.

In case of applied research, it is not enough just to know how strong one or another psychological trait manifests itself. For the complete specification of the "automated information system – personnel" complex, we have to associate an estimate of probability for a socio-engineering attack success to the degree showing how strong a psychological trait manifests itself. To be more precise, we can speak about the success of an attack (elementary) act. To make the association, we should collect all the available results of psychological tests, questionnaires, and interviews and convert them into a set of quantitative parameters. To make the parameter values precise enough, we should perform the related studies as well as rely upon experts' opinions.

The paper goal is to consider the impact of psychological defense onto the user's vulnerabilities profile as well as to describe (as an idea) an approach to application of relational and probabilistic relational representations of uncertain data and knowledge in the models of "automated information system – personnel" complex components.

To consider possible ways to make a formal definition of "user's vulnerabilities profile" and to elaborate a set of instruments to detect the components of this profile, we analyze the interconnections between various types of psychological defense and user's inclinations to perform illegal, forbidden or threatening activities without proper authorization.

We offer to model the interconnections between "automated information system – personnel" complex components, user's vulnerabilities profile, and malefactor(s) with the help of relational or probabilistic relational approach.