УДК 614.8+002.6:004.89

О.Ю. Ванюшичева, Т.В. Тулупьева, А.Е. Пащенко,
А.Л. Тулупьев

КЛАССИФИКАЦИЯ ПСИХОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ, СОСТАВЛЯЮЩИХ ОСНОВУ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ ПРИ УГРОЗЕ СОЦИО-ИНЖЕНЕРНЫХ АТАК

Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л. **Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социо-инженерных атак.**

Аннотация. Статья посвящена теоретическому рассмотрению психологических особенностей, составляющих основу уязвимостей пользователя, находящегося под угрозой социо-инженерной атаки. Для удобства последующего изучения социо-инженерных атак и их профилактики у пользователей представлена подробная классификация психологических особенностей по различным параметрам, таким как характер протекания, характер вызываемого действия пользователя и др. При построении классификации было выделено 2 основных класса: психологические качества и социальные и личные факторы, влияющие на уязвимость человека. Также представлено дальнейшее дробление этих классов на подклассы, выявлены взаимосвязи между уязвимостями и представлены соответствующие блок-схемы и таблицы, отражающие эти характеристики. На основании проделанной работы делается вывод о дальнейшем направлении исследования.

Ключевые слова: социо-инженерные атаки, уязвимости пользователя, действия пользователя, классы уязвимостей.

Vanushicheva O. Yu., Tulupyeva T.V., Pashchenko A.E., Tulupyev A.L. **Classification of the Psychological Traits Underlying User's Vulnerabilities to Socio-engeneering Attacks.**

Abstract. The paper is devoted to the theoretical consideration of psychological traits underlying user's vulnerability under the threat of socio-engineering attack, their properties and features. For the convenience of the subsequent studying of socio-engineering attacks and their prevention a detailed classification of psychological traits on various parameters is presented, including the way of proceeding, character of caused action of the user, etc. While constructing classification 2 main classes have been allocated: psychological characteristics and social and personal factors influencing the vulnerability of a person. Also, the further subdivision of these classes to subclasses is presented, vulnerabilities' interrelations have been determined and corresponding block diagrams and tables reflecting these characteristics are presented. What is more, indicators and scales of the users' vulnerabilities have been presented, their core parameters were revealed and summarized in the users' vulnerabilities complete list. The conclusion about the further direction of research based on the fulfilled work has been made in the end of the article.

Keywords: socio-engineering attack, features of the person, requirements of the person, informative model of the user, user actions, user's vulnerabilities.

1. Введение. Современные системы безопасности, несмотря на декларируемые эффективность, надежность и сложность структуры, не полностью решают вопрос обеспечения информационной безопасности фирмы: концентрируясь на программно-технической составляющей автоматизированных информационных систем, они упускают из виду человеческий фактор. В действительности же сотрудник нередко оказывается самым уязвимым элементом в системе безопасности фирмы, в том числе и в системе ее информационной безопасности. Именно поэтому требуется изучать, выявлять и предотвращать социо-инженерные атаки, направленные на пользователя. Для предупреждения атак на сотрудника необходимо выявить причину возможности осуществления этих атак, то есть понять, чем они обусловлены. В настоящей статье систематизируются для дальнейшей формализации психологические особенности пользователя, позволяющие злоумышленнику осуществить успешную социо-инженерную атаку. Материал излагается на языке, доступном широкому кругу специалистов, поскольку данное исследование носит ярко выраженный междисциплинарный и прикладной характер. Систематизация психологических особенностей, лежащих в основе уязвимостей пользователя, сопровождается примерами социо-инженерных атак, заимствованными из ряда источников [13]. Основные определения, которыми мы оперируем, приведены в [14].

Прежде чем переходить непосредственно к самим психологическим особенностям, лежащим в основе уязвимости пользователя, и их описанию, обозначим информационную модель пользователя, в рамках которой мы рассматриваем классификацию уязвимостей, социо-инженерные атаки и понятия с ними связанные.

Для автоматизированного анализа степени защищенности персонала информационной системы от социо-инженерных атак требуется построить ряд информационных моделей объектов [5–7, 15] из рассматриваемой совокупности, в том числе, информационную модель пользователя. В [5] предложена одна из возможных моделей пользователя, в атрибуты которой входят уязвимости пользователя. Таким образом, неизбежным этапом моделирования и анализа социо-инженерных атак является построение профиля уязвимостей пользователя. Авторы предполагают, что в построении профиля уязвимостей пользователя существенную роль играет его психологический профиль, отражающий уровень выраженности психологических особенностей. Достижение заявленной цели данной статьи позволит создать основу для формализации перехода от психологического профиля к

профилю уязвимостей пользователя. Вместе с тем, нельзя упускать из виду, что психологический профиль пользователя является важной, но не единственной информационной составляющей в построении профиля уязвимостей пользователя. Ряд других информационных составляющих требует отдельных исследований, которые не входят в список задач настоящей работы.

На уровень выраженности уязвимостей пользователя влияет два крупных класса особенностей:

- личностные качества,
- социальные и личные факторы, влияющие на уязвимость человека.

Классы уязвимостей в свою очередь делятся на подклассы, которые также могут делиться на более мелкие составляющие. В каждом из этих двух классов были рассмотрены схожие между собой по какимлибо свойствам уязвимости и выявлены как внутренние, так и внешние связи между классами и подклассами.

Принципиальным отличием между уязвимостями этих двух классов является природа их формирования у пользователя. Так личностные качества формируются у человека с момента его рождения, и для их модификации нужно приложить значительные усилия; как правило, личностные качества малоизменчивы во взрослом возрасте. Эти качества можно выявить в процессе психологической диагностики, например, при приеме на работу; они являются, условно говоря, «фоновыми» для данного пользователя.

Уязвимости же второго класса являются временными, обусловленными контекстом, то есть они не так сильно зависят от воспитания и социализации человека. Выявить их при приеме на работу не всегда представляется возможным (они могут не существовать или не быть актуальными на момент поступления на работу), но, тем не менее, большинство уязвимостей этого класса носит ярко выраженный внешний характер (могут сопровождаться внешними проявлениями, сказывающимися в общении или в процессе иной деятельности). Наличие уязвимостей второго класса стоит учитывать при организации рабочей деятельности сотрудника и необходимо учитывать при анализе степени защищенности персонала от социо-инженерных атак.

Также можно отметить еще одно отличие уязвимостей заявленных классов. Уязвимости первого класса носят долговременный характер, как было уже замечено выше, они являются фоновыми и незначительно изменяются в течение жизни пользователя. Уязвимости второго класса зачастую носят кратковременный характер.

Как было отмечено выше, в дальнейших исследованиях предстоит обобщить полученные в результате исследования сведения об уязвимостях пользователя и, на основании имеющихся данных по психологическим особенностям, составить ряд шкал и показателей для количественной оценки уязвимости, что позволит облегчить учет и контроль степени выраженности тех или иных уязвимостей у пользователя и, соответственно, принятие в зависимости от этого определенных мер по защите информации. Последующим шагом исследований является составление интегрального показателя (или интегральных показателей) степени уязвимости пользователя на основе профиля его уязвимостей. Данный показатель призван объединить в себе степень выраженности той или иной уязвимости у пользователя и вероятность успешной социо-инженерной атаки на этого пользователя с учетом данной уязвимости и в заданном контексте. Будучи формализованным, этот показатель будет являться основным, на который надо будет ориентироваться при учете возможностей социо-инженерных атак и их профилактики, что и является конечной целью описанного комплекса исследований.

2. Личностные качества. Данные качества являются наиболее устойчивыми, по сравнению с другими факторами. В психологии достаточно много внимания уделялось диагностике различных личностных качеств [9]. Существует множество моделей и теорий личности, на основе которых сформированы способы диагностики, учета и коррекции личностных особенностей, например, [10].

Учитывая многообразие теорий личности, в классе личностных особенностей можно выделать различные подклассы. В данной статье мы будем рассматривать только потребности, черты характера и особенности психологической защиты, как наиболее показательные особенности, лежащие в основе успешности социо-инженерных атак. Объединяет эти подклассы то, что они формируются у пользователя под воздействием воспитания и социализации. Особенности этих подклассов в принципе могут изменяться в течение жизни индивида, но в большинстве случаев остаются такими, какими были сформированы к периоду взрослости.

Рассмотрим подробнее каждый из подклассов.

2.1. Потребности человека. Согласно установившемуся в [16, 17] мнению в основе любого намеренного действия индивида лежит мотив, порождаемый потребностью. Существует много потребностно-мотивационных теорий, некоторые из них были проанализированы с точки зрения влияния на уязвимость в [7]. Как отмечалось, в настоя-

щей работе мы ограничимся рассмотрением только некоторых, наиболее показательных, потребностей с описанием ассоциированных с ними возможных социо-инженерных атак. Разумеется, формирование полного систематизированного списка потребностей выходит за рамки настоящей работы и является самостоятельным предметом исследований.

2.1.1. Потребность в материальном благополучии. Стремление людей к материальному благополучию широко распространено. Материальное благополучие предполагает удовлетворение в достаточной или избыточной степени первичных (потребности в еде, воде и т.д.) и вторичных потребностей (потребности в досуге, безопасности и т.д.). Если сотрудник недоволен своей зарплатой, премией и иными материальными вознаграждениями за труд, то он становится уязвимым для социо-инженерной атаки. Такого сотрудника легче, чем других, подкупить, а если у него к тому же ярко выражены такие черты характера, как безалаберность, низкий самоконтроль, мстительность и др. (см. ниже), то его степень уязвимости становится еще больше. Если рассматривать вероятность успешной реализации социо-инженерной атаки, то уровень указанной вероятности становится весьма высоким.

Примерный сценарий социо-инженерной атаки, ассоциированной с данной психологической особенностью, может выглядеть так. Злоумышленник по каким-то своим каналам выявляет сотрудника, неудовлетворенного своим финансовым вознаграждением на фирме. Далее он входит к нему в доверие и пытается подкупить. Если потребность в финансовом благополучии высока, то вероятность проведения успешной социо-инженерной атаки повышается. Сотрудник соглашается на противоправные действия, и либо сам предоставляет злоумышленнику информацию (или разрушает ее целостность), либо открывает/обеспечивает выход на других сотрудников, либо предоставляет доступ к информационной системе и информации, хранящейся в системе, непосредственно злоумышленнику, а тот уже сам завершает атаку.

2.1.2. Потребность в безопасности. Если человеку кто-то или что-то угрожает, то в зависимости от степени выраженности данной потребности от него можно ожидать большую уязвимость к социо-инженерным атакам. Как правило, запугать можно любого человека, вопрос только, как и каким образом. Последнее остается в компетенции злоумышленника, и мы заранее не можем предугадать, как именно он будет действовать, т.е. запугивать. Однако, вполне можно предположить, что радикальные меры запугивания (угроза здоровью, жизни,

похищение близких) будут применяться в исключительных и редких случаях. Достаточно распространены угрозы в отношении тщательно оберегаемого имиджа или доброго имени. Атака на пользователя с указанными уязвимостями будет тщательно спланирована. Однако трудность в реализации запугивания уменьшает вероятность успешности данной социо-инженерной атаки.

Если рассматривать данную потребность с точки зрения совершения действия при ассоциированной с ней уязвимости пользователя, то оно (действие) будет намеренным. Вероятность успешной реализации такой атаки будет низким, так как на ее проведение потребуется много ресурсов, а риски окажутся слишком высокими.

Можно предположить, что подвергается такой атаке высшее руководство, топ-менеджмент, то есть, все те сотрудники, у которых есть прямой доступ к необходимой информации.

Сценарий атаки может выглядеть так. Злоумышленник собирает информацию о сотруднике. Далее возможны варианты различных угроз: от запугивания до похищения. Сотрудник соглашается на условия пользователя и предоставляет тому нужную информацию или доступ к ней.

Не стоит упускать из рассмотрения возможность того, что потребность в безопасности у сотрудника настолько гипертрофирована, что он опасается элементарных угроз и все готов сделать во избежание их исполнения. При возникновении подобной фобии инструментарий для работы с потребностями не пригоден; психические расстройства, пограничные состояния, отклонения формируют отдельный класс сведений, которые должны учитываться при построении профиля уязвимости пользователя; однако, этот класс не входит в предмет рассмотрения настоящей статьи.

2.1.3. Потребность в достижениях. Данная потребность по сути является стремлением оправдать свои же собственные ожидания, самому себе доказать что-либо, например, в карьерном плане. Например, многие люди стремятся к самореализации, успешной карьере [10]. Часто это свойство тесно переплетается с потребностью в финансовом благополучии, но не обязательно. Как правило, наиболее выражена данная потребность у карьеристов, соответственно именно они становятся наиболее уязвимыми для социо-инженерных атак, в случае, когда потребность в достижениях не удовлетворяется. Дополнительными факторами, увеличивающими вероятность успешной социо-инженерной атаки, являются такие черты сотрудника, как мстительность (например, когда сотрудник мстит руководству за то, что по-

следнее не назначило его на определенную должность), излишняя самоуверенность и переоценивание собственной значимости. Таким образом, можно сделать вывод, что в случае социо-инженерной атаки, основанной на данной потребности, сотрудник совершает намеренные действия по нарушению информационной безопасности. В общем, уровень реализации успешной социо-инженерной атаки для данной уязвимости будет высоким.

Примером реализации социо-инженерной атаки, направленной на данную уязвимость сотрудника, может выступать предоставление злоумышленником каких-то компенсирующих функций пользователю в обмен на доступ к информации или саму информацию. К таким функциям может относиться, например, обещания карьерного роста в обмен на содействие в получении информации.

2.1.4. Потребность в одобрении. Данная потребность отличается от потребности в достижениях тем, что направлена не столько на удовлетворение собственных амбиций, сколько на соответствие ожиданиям третьих лиц. Сюда же мы можем косвенно отнести потребность в уважении, признании, престиже. Стремление оправдать ожидания других людей делает сотрудника уязвимым для злоумышленника. Однако, если оценивать данную потребность с точки зрения уровня реализации успешной социо-инженерной атаки, то ее уровень будет низким. Довольно сложно провести успешную социо-инженерную атаку ориентируясь лишь на эту потребность, скорее имеет смысл рассматривать ее в совокупности с остальными. Вероятность успешной социо-инженерной атаки повышается в том случае, если злоумышленник выступает в роли лица, одобрение которого пользователь хочет получить. Действия сотрудника здесь могут быть как намеренными, так и ненамеренными. Примером ненамеренного действия может быть, например, такая ситуация. Молодой человек влюблен в девушку и не знает, что она является злоумышленником. Чтобы заслужить ее одобрение, он совершает ненамеренные или намеренные действия (например, проверяет USB-диск на вирусы на рабочем компьютере, потому что, якобы, домашнему девушка не доверят, а потом возвращает девушке или намеренно делится какой-то рабочей информацией), не подозревая к чему это может привести. Вероятность совершения сотрудником намеренного действия в контексте атаки только на данную потребность минимальна.

2.1.5. Потребность во власти. Сюда же входит потребность занимать лидирующее положение, потребность в доминировании над остальными. У большинства людей эта потребность сопряжена с по-

требностью в финансовом благополучии, потребностью в достижениях и потребностью в одобрении. Надо заметить близкую взаимосвязь потребности во власти и потребности в достижениях. Можно сказать, что вторая является частью первой. Однако сама по себе потребность во власти носит более высокий уровень реализации социо-инженерной атаки, при этом сотрудник практически всегда совершает намеренные действия по нарушению информационной безопасности.

Сам по себе сотрудник с большим стремлением к власти не заинтересован в том, чтобы фирма, в которой он работает, несла убытки, если он планирует занимать в ней ключевые должности. Тем не менее такой сотрудник, возможно, согласится на противоправные действия в двух случаях:

1) если злоумышленник предложит ему лучшее место в другой фирме;

2) если его действия продвинут его по службе, и при этом фирма, в которой он трудится, не понесет серьезных убытков и об этом не станет известно.

Второй вариант все же менее вероятен, хотя бы потому, что любые успешные действия злоумышленника ведут к ухудшению благосостояния фирмы, а сотрудник, рассчитывающий на продвижение по службе, совсем в этом не заинтересован.

Данную потребность в наибольшей степени испытывает топ-менеджмент, так как бывает обделен желаемыми должностями и часто не привязан к фирме. Рассмотрим это на примере социо-инженерной атаки. Злоумышленник выявляет менеджера, обделенного желаемой должностью. Вступает с ним в контакт и предлагает более высокое место в другой фирме (часто в своей) в обмен на информацию. Менеджер соглашается, предоставляет злоумышленнику доступ или саму информацию, и после проведения успешной социо-инженерной атаки и злоумышленник, и сотрудник уходят в свою фирму, которая с полученной информацией становится более конкурентноспособной, а в некоторых случаях даже ведущей в отрасли.

Таким образом, уровень реализации успешной социо-инженерной атаки средний, а в сочетании с другими уязвимостями сотрудника становится еще выше.

2.1.6. Потребность в справедливости. Существуют работники, которые считают, что высшее руководство относится к ним предвзято, пренебрегает ими, в общем, относится несправедливо. Основываются они на сравнении соотношений затрат и вознаграждений (поощрений), которые имеют они сами и другие сотрудники. Ярко выраженные

формы этой потребности могут варьировать от высказывания осторожного недовольства до намеренных действий по нарушению безопасности информации предприятия. Сотрудник с доминирующей потребностью в справедливости, при наличии других уязвимостей, таких как вспыльчивость, мстительность, низкий уровень интеллектуального развития становится жертвой социо-инженерной атаки. Но в целом уровень реализации успешной социо-инженерной атаки остается низким, и осуществление успешной атаки во многом зависит от выраженности других уязвимостей. Действия сотрудников могут быть как намеренными, так и ненамеренными.

Примером атаки может послужить пример из пункта 2.1.5., в том случае, если сотрудник считает несправедливым притеснение себя по должности.

2.1.7.Потребность в причастности. Для любого человека, как существа социального, характерно отождествление себя с какой-то группой людей. Для того, чтобы быть «своим», необходимо перенимать отличительные признаки группы, идентифицироваться с ней. Поэтому люди стремятся к статусности, быть не хуже остальных. Потребность в причастности является дополняющей к таким уязвимостям, как потребность в финансовом благополучии, одобрении и власти. Сотрудник стремится носить определенную одежду, иметь машину, отдыхать в соответствующих странах. Стремление в причастности толкает его на противоправные действия как намеренные, так и ненамеренные. Примерами реализации социо-инженерной атаки в данном случае могут выступать примеры из пунктов 2.1.1., 2.1.4., 2.1.5. Однако для самой по себе отдельно взятой потребности в причастности уровень реализации успешной социо-инженерной атаки низкий.

Подводя итог, можно сказать, что потребности становятся основой формирования уязвимостей: они сильно мотивируют сотрудника на те или иные противоправные действия, как намеренные, так и ненамеренные. Большинство потребностей, взятые сами по себе, не составляют значительной угрозы для информационной безопасности, однако их совокупное проявление у человека надо контролировать. Обобщенные результаты подкласса потребностей человека представлены в таблице ниже.

Таблица 1. Потребности человека и нацеленные на них социо-инженерные атаки

№	Название потребности	Характер совершаемого действия	Вероятность успешной реализации социо-инженерной атаки
1	Потребность в финансовом благополучии	Намеренное	Высокая
2	Потребность в безопасности	Намеренное	Низкая
3	Потребность в достижениях	Намеренное	Высокая
4	Потребность в одобрении	Намеренное/Ненамеренное	Низкая
5	Потребность во власти	Намеренное	Высокая
6	Потребность в справедливости	Намеренное/Ненамеренное	Низкая
7	Потребность в причастности	Намеренное/Ненамеренное	Низкая

2.2. Черты характера человека, делающие его уязвимым к социо-инженерным атакам. Под действием воспитания и становления у человека в течение жизни выделяются и проявляются определенные черты характера, и не всегда они являются безобидными с точки зрения успешности реализации социо-инженерной атаки, то есть, могут составить основу формирования уязвимостей пользователя по отношению к социо-инженерным атакам.

2.2.1. Доверчивость и наивность. Жертвами социо-инженерных атак могут стать доверчивые и наивные люди. Такие люди склонны совершать ненамеренные действия для реализации успешных социо-инженерных атак. Сотрудник может быть исключительным специалистом в своей области и при этом быть очень наивным и доверчивым человеком. Начальство и коллектив, как правило, знают о такой особенности этих людей, но как уже было сказано выше, не придают ей значения, если сотрудник — великолепный специалист. Надо всегда помнить о том, что такие сотрудники легко становятся жертвами социо-инженерных атак благодаря своей доверчивости и ограничивать их доступ к важной информации либо вести работу по нейтрализации возможных социо-инженерных атак. В целом, если говорить об уровне реализации успешной социо-инженерной атаки в таких случаях, то он является высоким.

Примеров реализации социо-инженерных атак здесь множество [11], все они нацелены на усыпление бдительности сотрудников, ма-

нипулирование их доверчивостью. Скажем, злоумышленнику необходимо достать секретную информацию с ноутбука пользователя. Злоумышленник завоевывает доверие последнего и просит его одолжить компьютер и через него получает необходимую информацию.

2.2.2. Боязливость (трусость). Эта черта характера обусловлена потребностью в безопасности, но по своему существу гораздо опаснее. Трусливых людей легче всего запугивать и шантажировать, как правило, такие люди не дорожат корпоративными ценностями, а в сочетании с доверчивость и наивностью и вовсе становятся нешуточной угрозой для безопасности информации. Уровень реализации успешной социальной атаки у данной уязвимости средний. Сотрудники с проявлением данной уязвимости склонны совершать намеренные действия по нарушению безопасности информации фирмы.

Вариант развития сцены социо-инженерной атаки. Допустим, сотрудник очень боится ограбления на улице. Злоумышленник, выявив такую уязвимость у пользователя, может запугать его и начать шантажировать. Пользователь из-за страха подвергнуться ограблению предоставляет злоумышленнику доступ к информации или ее саму.

2.2.3. Слабоволие. В какой-то степени это свойство перекликается с предыдущим. Разница лишь в том, что на пользователя можно повлиять пользуясь не его трусостью, а слабохарактерностью, невозможностью отказать — неумением говорить «нет». Причем на работе данная черта характера может не бросаться в глаза, а наоборот приниматься в плюс сотрудника, так как слабовольные люди реже других сопротивляются выполнению дополнительных обязанностей, демонстрируют конформистское поведение, что очень ценится руководством. Как правило, такие сотрудники совершают ненамеренные действия под влиянием злоумышленников. Последним необходимо заручиться доверием слабовольного сотрудника и постараться завуалировать процесс атаки. Уровень реализации успешной социо-инженерной атаки средний.

Рассмотрим такой пример. Сотрудник (системный администратор) является очень мягким и податливым человеком, который редко может кому-либо в чем-либо отказать. Другой сотрудник (водитель) просит системного администратора предоставить ему доступ в интернет через его [водителя] собственный ноутбук. Администратор выполняет просьбу, водитель заходит в интернет через свой компьютер и подвергается внешней сетевой атаке, так как его компьютер плохо защищен, после чего через корпоративную сеть распространяет вирус.

2.2.4. Излишняя самоуверенность и склонность к переоцениванию собственной значимости. Излишняя самоуверенность, а порой даже наглость толкает пользователей на намеренные и ненамеренные действия по нарушению информационной безопасности. Когда человек считает себя лучше других – это уже проблема для трудового коллектива, но когда такой человек оказывается под угрозой социо-инженерной атаки, вероятность утечки секретной информации сильно увеличивается. Сотрудники с данной уязвимостью совершают как намеренные, так и ненамеренные действия. Излишняя самоуверенность толкает их на глупые поступки и делает объектом манипулирования в руках злоумышленника. Если же рассматривать эту уязвимость как дополнение к потребностям в достижении, во власти, в финансовом благополучии, то вероятность проведения успешной социо-инженерной атаки увеличивается. И все же отдельно взятая данная уязвимость имеет средний уровень вероятности успешной реализации атаки.

В качестве примера могут подойти сцены, рассмотренные в предыдущих пунктах 2.1.6., 2.1.5.

2.2.5. Невнимательность. Часто ненамеренные действия по нарушению безопасности информации сотрудники совершают из-за своей невнимательности или забывчивости. Бороться с этим можно ужесточением санкций за несоблюдение правил безопасности компании и ограничением доступа к важной информации. Как показывает практика, именно эта уязвимость пользователя в большинстве случаев является причиной успешных социо-инженерных атак. В силу своей невнимательности сотрудник становится доступной целью для злоумышленника. Известны случаи [11], когда таким пользователям подкладывали USB-диски («флешки») с вирусом, которые потом благодаря невнимательности сотрудников попадали в информационную систему. Поэтому вероятность успешной реализации социо-инженерной атаки с использованием данной уязвимости является высоким.

2.2.6. Любопытство. Классический пример любопытства, которое ведет к успешным социо-инженерным атакам, это просмотр спама на электронной почте, «битых» ссылок, скачивание программ с вирусами. Бороться с этой проблемой нужно так же, как и в предыдущем случае. Очень коварная, с точки зрения обеспечения информационной безопасности, черта человека, и вероятность успешной реализации социо-инженерной атаки является высокой. Очевидно, что в данном случае пользователь совершает ненамеренные действия по нарушению безопасности информации.

2.2.7. Безалаберность. Недостаточно ответственное отношение к своей работе априори является недопустимым качеством сотрудника, к тому же оно предоставляет широкий простор для реализации социо-инженерной атаки. Эта уязвимость тесно перекликается с невнимательностью и ведет к ненамеренным действиям сотрудника по нарушению информационной безопасности. Уровень реализации успешной социо-инженерной атаки средний. Примером сцены данной социо-инженерной атаки может быть пример, разобранный в пункте 2.2.5.

2.2.8. Мстительность. Обиженный на свое высшее руководство сотрудник часто способен на любые поступки, чтобы свою обиду компенсировать. Например, в компании освободилась одна из вышестоящих должностей. Сотрудник N считал себя самым достойным на нее кандидатом. Однако начальство распорядилось по-другому. Разобиженный и разозленный сотрудник легко становится жертвой социо-инженерной атаки и в порыве мести готов предоставить доступ и любые сведения злоумышленнику, чем последний и воспользуется. Уровень сложности реализации успешной социо-инженерной атаки в данном случае является высоким, а действия, совершаемые сотрудником, — намеренными. К тому же в дополнение к другим уязвимостям эта черта характера представляет серьезную угрозу безопасности информации компании.

2.2.9. Вспыльчивость. Эта черта характера сама по себе не является положительной в контексте трудовых отношений. Однако если рассуждать с точки зрения защищенности информации или благосостояния фирмы от легко вспыльчивого сотрудника, то уязвимость, ассоциированная с данной чертой, достигает критической точки. Злоумышленнику порой достаточно просто довести до такого состояния сотрудника, а дальнейшие его действия могут быть непредсказуемыми: от испорченного программного обеспечения в приступе гнева до импульсивной выдачи секретной информации. Впрочем, всего этого может и не случиться, ведь действия вспыльчивого сотрудника очень сложно предугадать, так как мы рассматриваем здесь вспыльчивость как основу уязвимости пользователя к ненамеренным действиям, иначе это свойство несет ту же нагрузку, что и мстительность (разозлился на начальство, вспылил – предоставил злоумышленнику всю информации, либо нанес ущерб фирме). Если оценивать данную уязвимость с точки зрения атаки для злоумышленника, то ее уровень можно отнести к низкому. Для более детального анализа нужно проводить дополнительное исследование на сочетаемость данной уязвимости с остальными и соответственно на усиление ее другими уязвимостями.

Обобщенные данные о подклассе черт характера, делающих его уязвимым к социо-инженерным атакам, представлены в таблице ниже.

Таблица 2. Черты характера человека и нацеленные на них социо-инженерные атаки

№	Название потребности	Характер совершаемого действия	Вероятность успешной реализации социо-инженерной атаки	Соответствующий механизм психологической защиты
1	Наивность и доверчивость	Ненамеренное	Высокий	не зависит от вида психологической защиты
2	Боязливость (трусость)	Намеренное	Средний	компенсация
3	Слабоволие	Ненамеренное	Средний	не зависит от вида психологической защиты
4	Безалаберность	Ненамеренное	Средний	Компенсация замещение рационализация отрицание
5	Любопытство	Ненамеренное	Высокий	не зависит от вида психологической защиты
6	Мстительность	Намеренное	Высокий	Компенсация замещение проекция
7	Вспыльчивость	Ненамеренное	Низкий	Компенсация замещение
8	Невнимательность	Ненамеренное	Высокий	Регрессия рационализация отрицание
9	Излишняя самоуверенность и склонность к переоцениваю собственной значимости	Намеренное/ Ненамеренное	Средний	не зависит от вида психологической защиты

Черты характера сотрудника являются довольно весомым фактором, влияющим на профиль уязвимостей сотрудника. По существу они являются достаточно устойчивыми, фоновыми психологическими качествами и выявляются, например, при анкетировании и тестировании сотрудника. Природу проявления именно таких свойств характера объясняет психологическая защита человека, речь о которой пойдет ниже.

2.3.Психологическая защита человека и ее влияние на степень уязвимости при социо-инженерных атаках. Одним из факторов, влияющих на уязвимость пользователя при социо-инженерных атаках, является система психологической защиты, сформированная у данного пользователя. Механизмы психологической защиты помогают человеку устранить или свести до минимума чувство тревоги, негативные переживания, связанные с нарушениями норм и правил, которые он совершает, находясь под воздействием социо-инженерной атаки. Существует множество классификаций психологической защиты [12]. Количество выделяемых видов защиты колеблется от 10 до 23. Однако имеется ряд механизмов, существование которых признается многими авторами. Это отрицание, проекция, компенсация, рационализация, замещение и некоторые другие [2].

2.3.1 Регрессия. Возвращение к онтогенетически более ранним, инфантильным личностным реакциям [3]. Этот вид защиты проявляется в демонстрации беспомощности, зависимости, «детскости» поведения с целью уменьшения тревоги и ухода от требований реальной действительности [12]. Сотрудник с высокой регрессией может несерьезно относиться к требованиям информационной безопасности. Эта уязвимость порождает склонность к безалаберности, невнимательности и даже слабоволию. Поэтому сотрудник с повышенной регрессией склонен поступать так, как описано в пунктах 2.2.3., 2.2.5., 2.2.7. А именно совершать ненамеренные действия по нарушению информационной безопасности: читать на электронной почте письма в спаме, переходить по вредноносным ссылкам и т.д. Уровень реализации успешной социо-инженерной атаки в этом случае будет высоким. Пользователь склонен совершать противоправные действия «по глупости», чем успешно может пользоваться злоумышленник.

2.3.2. Компенсация. Представляет собой интенсивные попытки исправить или как-то восполнить собственную реальную либо воображаемую физическую или психическую неполноценность [9]. При помощи этого механизма защиты субъект заменяет нестерпимое для него чувство иным, возникающим в результате не имеющего отноше-

ния к данной ситуации поступка.[2] Данная уязвимость может выражаться в следующих чертах характера человека: мстительность, вспыльчивость, трусость. Соответственно мотивы поведения сотрудника при данной уязвимости совпадают с теми, которые представлены в пунктах 2.2.2., 2.2.7., 2.2.8. То есть пользователь склонен совершать как намеренные, так и ненамеренные действия по нарушению информационной безопасности. Уровень реализации успешной социо-инженерной атаки средний.

Пример социо-инженерной атаки: допустим, сотрудника притесняет на работе начальник, если у первого высокая компенсация, то от него можно ожидать возможности в отместку предоставить третьему лицу секретную информацию или доступ к ней, если злоумышленник знает об этой особенности пользователя, то он ею воспользуется.

2.3.3. Замещение. Смена направления негативных чувств с реального объекта на более безопасный [4]. Эта психологическая защита осуществляет перенос реакции с недоступного объекта на доступный или замену действия неприемлемого на приемлемое [5]. Человек с повышенным замещением склонен срывать свою злость на других. Причем как на живых, так и неодушевленных предметах. Сотрудник с превалированием этого свойства вспыльчив, раздражителен, часто несамокритичен и мстителен. Соответственно для повышенного замещения как уязвимости характерно все то, что содержится в пунктах 2.2.8, 2.2.9. Уровень реализации успешной социо-инженерной атаки средний, а пользователь склонен совершать как намеренные, так и ненамеренные действия по нарушению информационной безопасности. Примеры социо-инженерных атак можно посмотреть в пунктах 2.2.8, 2.2.9

2.3.4. Проекция. Неосознаваемое отвержение собственных эмоционально неприемлемых установок или желаний и приписывание их другим объектам (людям или животным) [6]. Этот вид психологической защиты 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, будто не он сам враждебно настроен, агрессивен, жаден, а другое лицо по отношению к нему [4]. Типичный пример высокой проекции, это когда сотрудник склонен считать, что не он плохо выполнил работу, а начальник к нему придирается. Данный механизм психологической защиты влечет за собой такие уязвимости, как мстительность, излишняя самоуверенность и склонность к переоценке собственной значимости. Люди с повышенной проекций любят возмущаться любой (с их точки зрения) несправедливостью, совер-

шенной по отношению к ним. Отсюда вытекает потребность в справедливости, желание расквитаться с обидчиком. Бывает, что такие люди оказываются с еще и низким уровнем интеллектуального развития, излишне объяснять, чем это грозит с точки зрения защиты информации. Механизм проекции лежит в основе перекладывания ответственности, поиска виноватого в сложившейся ситуации. Человек с высокой проекцией легко найдет оправдание своим поступкам.

Уровень реализации успешной социо-инженерной атаки высокий, и чаще всего сотрудники склоны совершать намеренные действия по нарушению информационной безопасности.

Самый классический пример сцены социо-инженерной атаки– рекомпенсационный, то есть подкуп сотрудника злоумышленником. Или злоумышленник может объяснить сотруднику, что все его неприятности на работе исключительно связаны с тем, что начальник отдела к нему придирается. И для того, чтобы уволили начальника отдела, можно совершить определенные действия.

2.3.5. Рационализация. Проявляется в псевдообъяснении человеком собственных неприемлемых желаний, убеждений и поступков с целью самооправдания [4]. Эта психологическая защита связана с осознанием и использованием в мышлении только определенной части информации, которая помогает описать собственное поведение как хорошо контролируемое [7]. Повышенная рационализация ведет к отсутствию контроля за своими противоправными действиями, оправдание их. По-другому можно сказать, что человек с завышенной рационализацией бывает несамокритичным и даже халатным по отношению к своей работе, то есть у него ярко выражены такие черты характера, как безалаберность, невнимательность, излишняя самоуверенность и склонность к переоценке собственной значимости. Уровень реализации успешной социо-инженерной атаки в данном случае будет средним, а пользователь склонен совершать как намеренные, так и ненамеренные действия по нарушению информационной безопасности.

Примеры социо-инженерных атак варьируют в зависимости от таких действий пользователя, как использование одного и того же пароля на разных, в том числе и небезопасных ресурсах, просмотр спама на электронной почте, до сознательных рекомпенсационных действий.

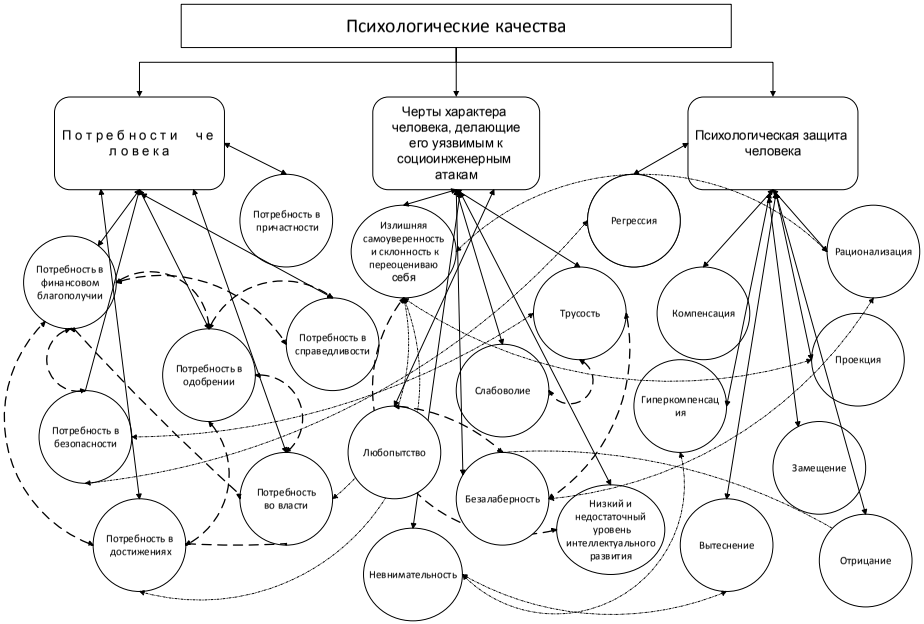
2.3.6. Отрицание. Недостаточное осознание определенных событий, переживаний и ощущений, которые причинили бы человеку боль при их признании [6]. Человек с высоким отрицанием не склонен переживать из-за каких бы то ни было проблем. С одной стороны это хорошо, так как его личные жизненные проблемы не будут толкать его

на необдуманные эмоциональные поступки. С другой стороны, человек, не склонный переживать из-за чего бы то ни было, вряд ли будет серьезно воспринимать и корпоративные проблемы, меры информационной безопасности. А отсутствие серьезности восприятия влечет за собой пренебрежение к работе, халатность. Сотрудник становится легкой мишенью для злоумышленника. Например, пренебрежение требованием не использовать свой рабочий пароль на других сетевых ресурсах. Злоумышленник может украсть пароль с такого ресурса и воспользоваться им для взлома системы. Уровень реализации успешной социо-инженерной атаки в данном случае будет средним, а пользователь склонен совершать ненамеренные действия по нарушению информационной безопасности.

Ниже приведенная таблица обобщает сведения о подклассе «Психологическая защита человека и ее влияние на степень уязвимости при социо-инженерных атаках».

Таблица 3. Психологическая защита человека и ее влияние на степень уязвимости при социо-инженерных атаках.

Механизм психологической защиты	Характер совершаемого действия	Уровень реализации успешной атаки	Соответствующая черта характера
1. Регрессия	Ненамеренное	Высокий	Слабоволие безалаберность невнимательность
2. Компенсация	Намеренное/ненамеренное	Средний	Трусость безалаберность мстительность
3. Замещение	Намеренное/Ненамеренное	Средний	Мстительность вспыльчивость
4. Проекция	Намеренное	Высокий	Мстительность, излишняя самоуверенность и склонность к переоценке собственной значимости
5. Рационализация	Намеренное/Ненамеренное	Средний	Безалаберность невнимательность излишняя самоуверенность и склонность к переоценке собственной значимости
6. Отрицание	Ненамеренное	Средний	Безалаберность невнимательность



- взаимосвязи между уязвимостями одного подкласса
- взаимосвязи между уязвимостями разных подклассов

Рис.1 Психологические качества пользователя и их составляющие

Труды СПИИРАН. 2011. Вып. 2(17). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2011. Issue 2(17). ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

3. Социальные и личные факторы, влияющие на уязвимость человека. Непосредственно связаны с психикой человека, но при этом в отличие от каких-то свойств нервной системы и черт характера, возникают в течение жизни человека под действием случая, то есть, в частности, обусловлены сложившимся в определенный момент времени контекстом, который потом может измениться. Уязвимости этого типа наиболее легко распознаваемы, т.к. имеют явно выраженный эмоциональный и физический контекст. Уязвимости данного блока объединяет еще и то, что они имеют в долгосрочной перспективе непродолжительный характер. Так, любые сложные жизненные потрясения и проблемы со временем можно разрешить или забыть.

В этом классе уязвимостей можно выделить серьезные жизненные потрясения, психологические расстройства и отклонения, физические проблемы и болезни.

3.1.Серьезные жизненные потрясения. Например, болезнь или потеря близкого человека [1], внезапные значительные материальные проблемы и др. Здесь в свою очередь можно выделить следующие подклассы.

3.1.1. Серьезные потрясения душевного характера (проблемы и потрясения, не имеющие материального контекста). Эта уязвимость ведет к неустойчивому морально-эмоциональному состоянию, которое делает пользователя легкой добычей для злоумышленника. Последний может либо довести пользователя до такого состояния, либо воспользоваться им в своих целях. Например, у сотрудника умер кто-то из близких людей. В таком состоянии, человек часто не до конца или совсем не контролирует свои действия, а значит, у него обостряются невнимательность, безалаберность, вспыльчивость со всеми вытекающими отсюда последствиями. Часто такие потрясения идут рука об руку с материальными трудностями, что опять же в свою очень увеличивает степень уязвимости сотрудника. В целом уровень реализации успешной социо-инженерной атаки можно назвать высоким. Правда есть еще одна особенность у уязвимостей данного класса: они легко обнаруживаются со стороны работодателя и коллектива, а следовательно — допускают своевременную нейтрализацию.

В качестве примера сцены атаки рассмотрим следующий. У пользователя умирает близкий человек, и он впадает в депрессию, у него резко ухудшается самоконтроль и внимательность. Злоумышленник, пользуясь угнетенным и подавленным состоянием сотрудника, входит к нему в доверие и заставляет совершить последнего ненамеренное действие по нарушению безопасности информации фирмы (подкидывает программу с вирусом, получает доступ к компьютеру и др.). Оче-

видно, что в контексте обострения данной уязвимости пользователя, тот склонен совершать ненамеренные действия по нарушению безопасности информации, но если данная уязвимость пересекается с материальными проблемами (смотреть ниже), то пользователь вполне способен совершить и намеренное действие.

3.1.2. Серьезные потрясения материального характера (проблемы и потрясения, имеющие материальный контекст). Нетрудно заметить близкую взаимосвязь этой уязвимости с предыдущей. Так потрясения душевного характера могут вызвать серьезные материальные потребности (например, болезнь близкого человека может вызвать финансовые проблемы, связанные с покупкой лекарств) и наоборот. Поэтому при учете степени проявления этих уязвимостей у того или иного пользователя имеет смысл рассматривать их совокупность, т.е. если, например, значительна степень серьезных потрясений душевного характера, то можно ожидать проявления высокой степени серьезных потрясений материального характера. Материальные проблемы влекут за собой один из самых распространенных видов социо-инженерных атак – рекомпенсационный. Злоумышленник может подкупить сотрудника, а тот соответственно в обмен на деньги или иные материальные ценности предоставить ему доступ к информации. Уровень реализации успешной социо-инженерной атаки у данной уязвимости, пожалуй, самый высокий из всех, так как в современном мире люди могут пойти на рискованные поступки, если у них серьезные материальные трудности, а если при этом выражены другие уязвимости и проблемы, например, тяжелая болезнь близкого человека, то у сотрудника просто не остается выбора. В данном случае можно говорить только о намеренных действиях по нарушению информационной безопасности у сотрудника.

3.2.Физические проблемы и болезни. Сами по себе проблемы физического характера и болезни не влияют на уязвимость пользователя. Зато очень существенно обостряют другие классы и подклассы уязвимостей, таких как: потребность в финансовом благополучии, потребность в безопасности и др. Болезни в общем и целом ухудшают умственное восприятие человека, притупляют внимание, и пользователь становится легкой мишенью для социо-инженерной атаки. Уровень реализации успешной социо-инженерной атаки в данном случае будет средним. А сотрудник способен совершать как намеренные, так и ненамеренные действия по нарушению информационной безопасности.

Представим такую ситуацию. Сотрудник сломал ногу и не может выйти из дома, а на работе нужно сдать проект. Злоумышленник может войти в доверие к сотруднику и под предлогом помощи, например,

передачи информации с проектом на цифровом носителе, внедрить в информационную сеть фирмы вирус или вредноносное программное обеспечение.

Таким образом, можно подытожить, что класс социальных и личных факторов, влияющих на уязвимость человека, отличается от класса личностных качеств следующими свойствами:

1) не является фоновым для пользователя, и уязвимости данного класса возникают вследствие стечения жизненных обстоятельств и по воле случая;

2) как правило, уязвимости данного класса имеют более объективные внешние проявления, чем уязвимости класса Личностные качества;

3) уязвимости данного класса характерны для всех сотрудников, и их действия более легко предугадываемы, чем действия сотрудника с доминированием уязвимостей первого класса.

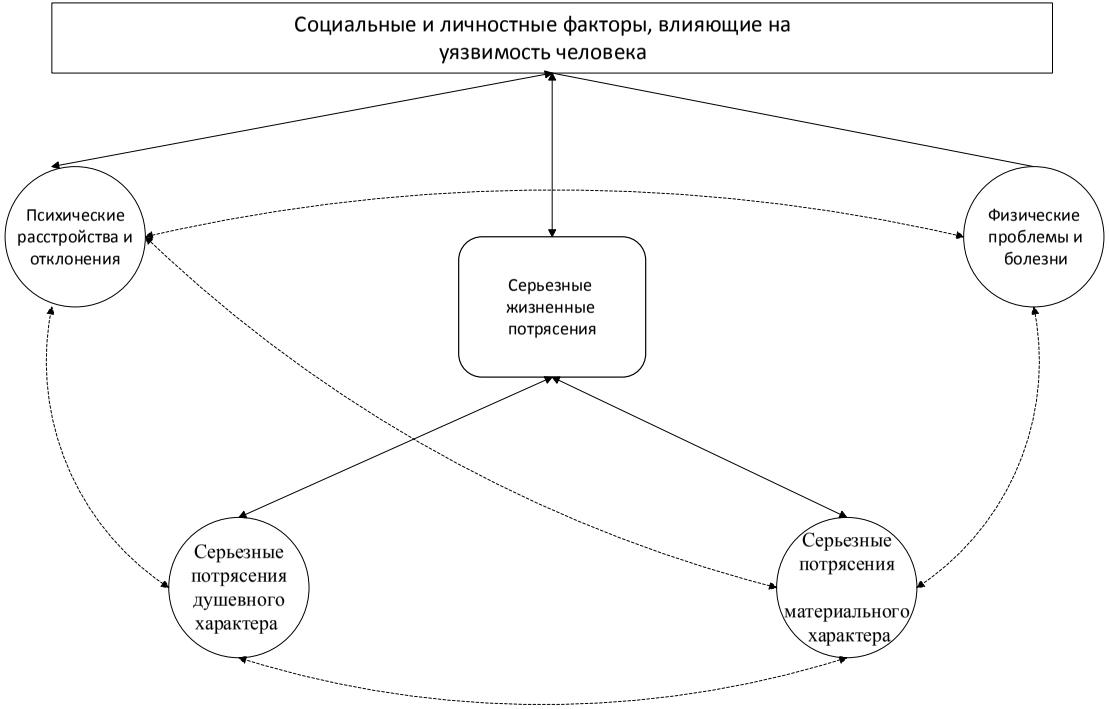


Рис.2 Социальные и личностные факторы, влияющие на уязвимость человека к социо-инженерным атакам

Труды СПИИРАН. 2011. Вып. 2(17). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2011. Issue 2(17). ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Таблица 4. Психологическая защита человека и ее влияние на степень уязвимости к социо-инженерным атакам

ОБЪЕДИНЁННАЯ ТАБЛИЦА УЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ, ПОДВЕРГАЮЩЕГОСЯ СОЦИО-ИНЖЕНЕРНОЙ АТАКЕ							
УЯЗВИМОСТЬ				Характер протекания		Характер совершаемого действия	
				Кратковременный	Долговременный	Намеренное	Ненамеренное
ПСИХОЛОГИЧЕСКИЕ КАЧЕСТВА	Потребности человека	№	Название				
		1	Потребность в финансовом благополучии	-	+	+	_
		2	Потребность в безопасности	_	+	+	_
		3	Потребность в достижениях	+	+	+	-
		4	Потребность в одобрении	+	+	+	+
		5	Потребность во власти	_	+	+	_
		6	Потребность в справедливости	_	+	+	+
		7	Потребность в причастности	-	-	+	+
	Черты характера человека, делающие его уязвимым к социо-инженерным атакам	8	Наивность и доверчивость	-	+	_	+
		9	Боязливость (трусость)	-	+	+	+
		10	Слабоволие	-	+	+	+
		11	Безалаберность	-	+	+	_
		12	Любопытство	-	+	+	_
		13	Мстительность	-	+	+	_
		14	Вспыльчивость	-	+	_	+
		15	Отсутствие самоконтроля	-	+	_	+
		16	Невнимательность	-	+	+	_
		17	Излишняя	-	+	+	_

			самоуверенность и склонность к переоценке собственной значимости				
	Психологическая защита человека	18	Регрессия	-	+	+	+
		19	Компенсация	-	+	+	+
		20	Гиперкомпенсация	-	+	+	+
		21	Вытеснение	-	+	+	+
		22	Замещение	-	+	+	+
		23	Проекция	-	+	+	+
		24	Рационализация	-	+	+	+
		25	Отрицание	-	+	+	+
Социальные и личностные факторы, влияющие на уязвимость человека	Серьезные жизненные потрясения	26	Серьезные потрясения душевного характера	+	–	+	+
		27	Серьезные потрясения материального характера	+	–	+	+
		28	Физические проблемы и болезни	+	–	+	+

4.Заключение. В статье рассмотрены 2 класса уязвимостей пользователя: личностные качества и социальные и личные факторы, влияющие на уязвимость человека. В каждом из этих классов были выявлены свои подклассы уязвимостей, рассмотрены их свойства, взаимосвязь друг с другом. В рассмотренных таблицах были представлены обобщенные результаты исследования по уязвимостям пользователя, их классификация, свойства и уровни безопасности. Также были приведены возможные варианты сцен социо-инженерных атак для каждой из уязвимостей или групп уязвимостей.

Дальнейшим направлениям исследований предстоит выяснить, какими способами (тесты, анкеты, опросы, интервью) можно выявить степень проявления у пользователя тех или иных уязвимостей, интегрировать все полученные результаты в показатели, которые потом, в свою очередь, будут использованы при построении информационной модели пользователя и внедрении ее в программный продукт. Кроме того, полученная систематизация психологических особенностей открывает возможность для их дальнейшей формализации с целью построения информационной модели психологического профиля пользователя; а, как уже отмечалось, психологический профиль пользователя оказывает существенное влияние на формирование профиля уязвимости пользователя по отношению к социо-инженерным атакам.

Литература

1. *Грановская Р.М.* Элементы практической психологии. СПб.: Речь. 2003
2. *Грановская Р.М., Никольская И.М.* Защита личности: психологические механизмы. СПб., 1999.
3. *Михайлов А.Н., Роттенберг В.С.* Особенности психологической защиты в норме и при соматических заболеваниях // Вопросы психологии. 1990. № 5. С. 106–111.
4. Психотерапевтическая энциклопедия / Под ред. Б.Д. Карвасарского. СПб., 1998.
5. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационная модель пользователя, находящегося под угрозой социо-инженерной атаки // Тр. СПИИРАН. 2010. Вып. 1(13). С. 143–155.
6. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А., Тулупьева Т.В.,* Визуальный инструментарий для построения информационных моделей комплекса «Информационная система-персонал», использующихся в имитации социо-инженерных атак // Труды СПИИРАН. 2010. Вып. 3(15). С. 231–245.
7. *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 // Труды СПИИРАН. 2010. Вып. 12. С. 200–214.
8. *Тулупьева Т.В.* Психологическая защита и особенности личности в период ранней юности. СПб.: Изд-во С.-Петерб. ун-та, 2000. 92 с.
9. Практическая психодиагностика. Методики и Тесты. Учебное пособие / Под ред. *Райгородского Д.Я.* Самара: БАХРАХ-М, 2000. 670 с.
10. *Хьел Л., Заглер Д.,* Теория личности. СПб.: Питер, 2006. 402 с.

11. *Mitnik K. The Art of Deception.* URL: http://bugtraq.ru/library/books/mitnick.
12. *Plutchik R., Kellerman H., Conte H.R.* A structural theory of ego defenses and emotions. // Emotions in personality and psychopathology / Izard C.E. (ed.) 1979. P. 229–257.
13. *Кузнецов М., Симдянов И.* Социальная инженерия и социальные хакеры// СПб.: БХВ-Петербург, 2007. 358 с.
14. *Фролова А.Н., Пащенко А.Е., Тулупьева Т.В., Тулупьев А.Л.* Анализ уровня защищенности информационных систем в контексте социо-инженерных атак: постановка проблемы // Труды СПИИРАН. 2008. Вып. 7. С. 170–176.
15. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационные модели компонент комплекса «Информационная система – персонал», находящегося под угрозой социо-инженерных атак // Труды СПИИРАН. 2010. Вып. 14. С. 50–59.
16. *Хекхаузен Х.* Мотивация и деятельность. СПб.: Питер; М.: Смысл, 2003. 860 с.
17. *Ильин Е.П.* Мотивация и мотивы. СПб.: Питер, 2003.

Ванюшичева Оксана Юрьевна — студентка 5 курса математико-механического факультета Санкт-Петербургского Государственного университета. Область научных интересов: социо-инженерия, математическая статистика, применение методов математики и информатики в социокультурных исследованиях и экономике. grigoreva.oy@mail.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.

Vanushicheva Oxana Yurievna – 5th course student of Mathematics and Mechanics Department at Saint-Petersburg State University. Research interests: socioingeenering, mathematical statistics, application of mathematics and computer science to sociocultural studies and economy. grigoreva.oy@mail.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.

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 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, 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.

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.

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)3284450.

Поддержка исследования. Работа выполнена при финансовой поддержке РФФИ, проект № 10-01-00640-а (Интеллектуальные модели и методы анализа защищенности информационных систем от социо-инженерных атак (деревья атак)) и грантом СПбГУ шифр 6.38.72.2011 (Моделирование комплексов «информационная система --- персонал» для агрегированной оценки их готовности к отражению социо-инженерных атак).

Рекомендовано ТиМПИ СПИИРАН, зав. лаб. д-р физ.-мат. наук, доцент А.Л. Тулупьев.
Статья поступила в редакцию 15.07.2011

РЕФЕРАТ

Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л. **Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социо-инженерных атак.**

Данная статья повествует о психологических особенностях, составляющих основу уязвимостей пользователя при угрозе социо-инженерных атак. Для удобства рассмотрения уязвимости пользователя сгруппированы в классы уязвимостей, таким образом, для последующего изучения социо-инженерных атак и их профилактики у пользователей представлена подробная классификация уязвимостей по различным параметрам, таким как характер протекания, характер вызываемого действия пользователя и др. При построении классификации было выделено два основных класса уязвимостей: психологические качества и социальные и личные факторы, влияющие на уязвимость человека. В каждом из этих классов были выявлены свои подклассы уязвимостей, рассмотрены их свойства, взаимосвязь друг с другом. Статья снабжена таблицами, блок-схемами для отображения всех заявленных характеристик и свойств уязвимостей пользователя. Для удобства сортировки уязвимостей было выделено несколько показателей и шкал, таких как характер совершаемого действия и характер протекания данной уязвимости. Для каждой уязвимости пользователя были приведены свои варианты возможных сцен социо-инженерных атак, некоторые примеры были позаимствованы из книг таких авторов, как Митчик, Кузнецов, Симдянов. Обобщенная информация по всем классам уязвимостей приведена в соответствующей таблице.

Дальнейшие направления исследований нацелены на то, чтобы выяснить, какими способами (тесты, анкеты, опросы, интервью) можно выявить степень проявления у пользователя тех или иных уязвимостей. Затем предстоит интегрировать все полученные результаты в показатели, которые потом, в свою очередь, будут использованы при построении информационной модели пользователя. Полученная систематизация психологических особенностей дает возможность их дальнейшей формализации с целью построения информационной модели психологического профиля пользователя, который в свою очередь внесет существенный вклад в формирование профиля уязвимости пользователя по отношению к социо-инженерным атакам.

SUMMARY

Vanushicheva O.Yu., Tulupyeva T.V., Pashchenko A.E., Tulupyev A.L.
Classification of the psychological features making a basis for the vulnerability of the user at the threat of socio-engeneering attacks.

In this article psychological features are presented which form the basis for the vulnerabilities of the user under the threat of socio-engineering attacks. Users' vulnerabilities are grouped into classes of vulnerability for the amenity, thus, a detailed classification of the vulnerabilities is presented for the subsequent studies of socio-engineering attacks and their preventive measures for users, such as coursing character, character of caused action of the user, etc. Two main classes of vulnerabilities were outlined during the classification construction. They are psychological qualities and social and personal factors influencing vulnerability of the person. Subclasses of vulnerabilities were revealed in these two main classes, also their properties and interrelations with each other were considered. The article is supplied with tables, block diagrams to display all declared characteristics and properties of the user's vulnerabilities. For the convenience vulnerabilities were sorted due to some indicators and scales, such as character of fulfilled action and character of course of the given vulnerability has been allocated. For each user's vulnerability the alternatives of possible scenes of socio-engineering attacks have been given, some examples were borrowed from books of such authors as Mitchik, Smiths, Simdjanov. The generalized information about every vulnerability class is fetched in the corresponding table.

The further directions of research are aimed at finding out possible ways (tests, questionnaires, polls and interviews) for determining the degree of display of user's vulnerabilities. Then it will be necessary to integrate all received results into the indicators which then will be used for construction of user's information model. The received systematization of psychological features gives the chance for their further formalization aimed at the construction of information model of the user's psychological profile; which essentially contribute to formation of a vulnerability profile of the user in relation to the socio-engineering attacks.