УДК 614.8+002.6:004.89

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

КОЛИЧЕСТВЕННЫЕ ИЗМЕРЕНИЯ ПОВЕДЕНЧЕСКИХ ПРОЯВЛЕНИЙ УЯЗВИМОСТЕЙ ПОЛЬЗОВАТЕЛЯ, АССОЦИИРОВАННЫХ С СОЦИОИНЖЕНЕРНЫМИ АТАКАМИ

Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А. **Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками.**

Аннотация. В статье рассматриваются результаты социологического исследования, проведенного сотрудниками лаборатории СПИИРАН с целью выявления взаимосвязи между психологическими особенностями, уязвимостями и возможными действиями пользователя информационной системы в рамках понятия социоинженерных атак. Данное исследование служит основой для построения профиля уязвимостей пользователя информационной системы и является промежуточным экспериментальным этапом между переходом от профиля психологических особенностей пользователя к профилю уязвимостей пользователя. На основании проделанной работы предлагаются дальнейшие направления этапов исследования.

Ключевые слова: социоинженерные атаки, уязвимости пользователя, действия пользователя, социологическое исследование

Vanushicheva O. Yu., Tulupyeva T.V., Pashchenko A.E., Tulupyev A.L., Azarov A.A. **Quantitative measurements of behavioral displays of user's vulnerabilities associated with socio-engineering attacks.**

Abstract. Article is devoted to the results of sociological research, held by the SPIIRAN laboratory's employees. This research was devoted to the revealing interrelations between psychological features, vulnerabilities and possible actions of information system's users, who are under the threat of socio-engineering attacks. Structuring the user's vulnerability profile is based on this research. Moreover, this research is experimental intermediate level between user's psychological features profile and user's vulnerability profile. Further direction of research phases are based on the current paper.

Keywords: socioengineering attack, features of the person, requirements of the person, informative model of the user, user’s actions, user’s vulnerabilities, sociological survey.

1. **Введение.** Одной из важнейших проблем любой современной компании является обеспечение безопасности своей секретной информации [2,5]. Поэтому большинство из них закупают дорогие современные информационные системы безопасности. Однако, как показывает практика, такие средства не гарантируют стопроцентной защиты, а все потому, что самым слабым звеном в цепочке обеспечения информационной безопасности фирмы является сотрудник [3]. Так как сотрудник может быть подвергнут социоинженерной атаке, стоит задаться вопросом: «А при каких условиях возможно осуществление успешной со-

циоинженерной атаки?». Ранее нами было определено понятие уязвимостей пользователя, степень выраженности которых и определяет возможность осуществления социоинженерной атаки [6]. Необходимо напомнить еще и о таком понятии, как действие пользователя — реакция на совершение социоинженерной атаки. Ранее нами были рассмотрены осознанные и неосознанные действия пользователя [1]. Однако любое из них может привести к успешному исходу социоинженерной атаки [7, 6]. Для того, чтобы построить профиль уязвимостей пользователя, нам необходимо знать взаимосвязь между уязвимостями и психологическими особенностями пользователя [4]. Для выявления этой взаимосвязи и было проведено социологическое исследование, речь о котором пойдет ниже.

2. Социологическое исследование: постановка проблемы и цели. О классификации психологических особенностей было рассказано ранее [1]. Однако для построения профиля уязвимостей мало знать психологические особенности пользователя, необходимо придумать алгоритм, при помощи которого можно будет переводить психологические особенности пользователя в уязвимости. С этой целью было проведено социологическое исследование, основной задачей которого был поиск взаимосвязи между психологическими особенностями, действиями пользователя и определением уязвимостей пользователя. Исследование носило пилотный характер, и следует отметить, что возможно возникновение погрешностей при интерпретации результатов.

В исследовании принимали участие студенты двух вузов Санкт-Петербурга. Всего отвечало на вопросы анкеты 84 человека. Возраст респондентов составлял 17–24 года. Подавляющее большинство студентов учится на гуманитарных специальностях. Респондентам предлагалось ответить на 43 вопроса анкеты. Полученные данные обрабатывались на программе SPSS.

3. Интерпретация результатов исследования. При составлении анкеты были рассмотрены 4 вида действий пользователя: использование одних и тех же идентификационных данных на разных ресурсах, разглашение своих идентификационных данных, чтение спама, участие в рекомпенсационных действиях. В соответствии с этими видами деятельности составлялись блоки вопросов. Так, для выявления использования одних и тех же идентификационных данных на разных ресурсах были придуманы следующие вопросы:

2. Используете ли Вы преимущественно один и тот же логин?
а) да
б) нет
3. Используете ли вы преимущественно одинаковые пароли?
а) да

б) нет

Для действия разглашения своих идентификационных данных:

1. Случалось ли Вам хоть раз сообщать кому-либо свои идентификационные данные?

а) да

б) нет

2. Где Вы преимущественно храните свои идентификационные данные?

а) в собственной памяти

б) в файлах домашнего компьютера

в) в файлах рабочего/учебного компьютера

г) на бумаге

д) на стикере

е) в мобильном телефоне

ж) другое

Выше приведены только некоторые вопросы из анкеты. В основном они принадлежат к бинарным и метрическим шкалам, однако есть и открытые вопросы.

2.1. Первичная статистика. Результаты, полученные при первичном анализе данных, показали, что респонденты демонстрируют поведение, при котором возможно осуществление успешной социоинженерной атаки.

Средний возраст респондентов составил 19 лет.

В ходе исследования было выявлено, что пользуются сервисом запоминания логина и пароля, предоставляемым браузером 37,62% респондентов, разлогиниваются же при окончании работы с информационным ресурсом лишь 49,4%. Около 72,55% респондентов принимают меры по сохранению безопасности своих идентификационных данных (имеются в виду такие меры безопасности, как, например, использование функции «Чужой компьютер» при входе на электронную почту, социальные сети). В среднем респонденты готовы доверить свои идентификационные данные как минимум 2 людям. Не умаляя общности, можно судить о том, что такой показатель является существенной преградой для профилактики защиты от социоинженерных атак. 14 сайтов – среднее количество сайтов, на которых зарегистрированы опрашиваемые. 68,32% такова вероятность вспомнить забытый пароль респондентом. Среди всех опрашиваемых практически не нашлось людей, у которых ни разу не взламывали электронную почту, среднее число взломов равно 1. В анкете был вопрос относительно того, стоит ли материально поощрять тех, кто готов помочь комиссии по ЕГЭ бороться с утечкой ответов на экзамене. Тем, кто ответил по-

ложительно на данный вопрос, предлагалось назвать справедливое на их взгляд вознаграждение. В среднем оно составило 5000 р. Этот вопрос очень показательный, он отражает, что 40,5% респондентов, готовы продавать информацию. И, подводя итоги по средним значениям, осталось отметить, что респонденты будут принимают участие в социальных акциях из серии «Расскажи про это своим друзьям и получи бесплатную толстовку» в 11,82% процентах случаев, отсылать полученные «письма счастья» в 7,15% процентах случаев, и наконец, переходить по ссылкам, которые браузер объявляет небезопасными в 20,86% процентах случаев.

Что касается частоты первичных данных, то тут также наблюдались интересные результаты. Так, например, хоть раз сообщали свои идентификационные данные 84,5% респондентов. Чаще всего свои идентификационные данные респонденты хранят в собственной памяти — 86,9%, 11,9% — в файлах домашнего компьютера и столько же респондентов хранит на бумаге, 2,4% — в файлах рабочего компьютера, 3,6% — на стикере, 4,8% — в мобильном телефоне. 60,7% респондентов допускают, что их идентификационные данные знают их близкие, а также 84,5% дадут свои идентификационные данные от электронной почты другу, если им нужно будет срочно получить оттуда информацию, но у них при этом не будет возможности сделать это лично. То есть, подавляющее большинство респондентов готово сообщить свои персональные данные, а также может сообщить какую-то другую информацию, которая считается персональной или секретной, если они решат, что доверяют этому человеку. Больше половины респондентов (64,3%) довольно беспечно относится к своим идентификационным данным и будет их вводить, даже если их может увидеть кто-то чужой. Показательно, что на вопросы «используете ли Вы преимущественно одинаковые пароли» и «используете ли Вы один и тот же логин» больше половины респондентов ответило утвердительно, 62,7% и 74,1% соответственно. При этом используют одну и ту же комбинацию логинов и паролей 84,5% человек. Вспомнят свой забытый пароль путем перебора 78,6% респондентов. Большинство респондентов (83,3%) считает, что в первую очередь спам – реклама товаров и услуг, но при этом больше половины (59%) считает это попыткой взлома системы. При этом подавляющее большинство респондентов 67% сообщат в деканат о том, что их соратник списывал на экзамене, если от этого будет зависеть, возьмут ли их на единственное бюджетное место или нет.

Выше была показана часть полученных данных по первичной статистике. Какие-то из них оказались ожидаемыми, какие-то удивили.

Большинство результатов показало, что респонденты легко могут сообщить свои идентификационные данные близким родственникам и знакомым, что говорит о том, что опрашиваемые могут оказаться жертвой злоумышленника, который может стать для них тем самым «близким знакомым». Хранение пароля в памяти также указывает на весьма большую вероятность забывания пароля, однако респонденты легко вспоминают свои идентификационные данные и преимущественно используют одну и ту же комбинацию логинов и паролей. Все это говорит о том, что пароли респондентов злоумышленнику будет довольно легко подобрать или даже выяснить лично. Подводя итог, можно утверждать, что у студентов в большинстве своем довольно сильно прослеживается возможная уязвимость к социоинженерным атакам.

2.2. Различия между подвыборками. Для выяснения различия между подвыборками был проведен тест Манна–Уитни. При проведении данного теста было получено, что те, кто хоть раз сообщал свои идентификационные данные, больше участвовали в акциях социальной сети. Если говорить про связь психологической защиты с совершаемыми действиями, то здесь были получены следующие результаты:

1) Регрессия, Замещение и Компенсация у тех, кого хоть раз взламывали, выше;
2) Регрессия и рационализация у тех, кто допускает, чтобы их идентификационные данные знали близкие, выше, чем у тех, кто этого не допускает;
3) Замещение выше у тех, кто преимущественно использует один и тот же логин;
4) Регрессия выше у тех, кто хоть раз вводил свои идентификационные данные на других ресурсах с целью совершения каких-либо действий (скачивания музыки, видео и т.д.);
5) Высокая компенсация у тех, кто считает, что комиссия по ЕГЭ должна материально поощрять тех, кто помогает ей бороться с утечкой ответов на экзаменационные тесты.
6) Отрицание и замещение гораздо выше у тех, кто считает, что рекламный спам может быть опасным;
7) Рационализация у тех, кто поделится за определенные услуги со своим одногруппником результатами теста, существенно выше, чем у тех, кто сделает это безвозмездно. Общий уровень у тех, кто поделится с одногруппниками результатами теста за определенные услуги, существенно выше, чем у тех, кто поделится безвозмездно;

8) Высокое отрицание наблюдается у тех, кто пользуется браузером Mozilla Firefox.

Что касается остальных результатов по Манна–Уитни, то здесь тоже были получены весьма интересные результаты. Так, например, те, кто просматривает приложения в письмах неизвестных результатов, больше склонны участвовать в социальных акциях. Те, кто хранят свои идентификационные данные в собственной памяти, больше пользуются сервисом запоминания логина и пароля, предоставляемым браузером. А те, кто пользуются таким браузером, как Internet Explorer, в больших процентах случаев пересылают «письма счастья», чем те, кто не пользуется.

Мы не будем приводить ожидаемые результаты, так как их присутствие говорит только о том, что в целом исследование составлено, проведено и обработано корректно. Под ожидаемыми результатами мы понимаем такие, как, например, тот факт, что, если пользователь готов предоставить свои идентификационные данные одногруппнику для входа в сеть, то он готов доверить их и большему количеству знакомых.

2.2. Корреляционный анализ. Это проверка гипотез о связях между переменными с использованием коэффициентов корреляции, - мера прямой и обратной пропорциональности между двумя переменными [7]. Мы рассматривали данные по корреляционному анализу с использованием коэффициентов корреляции Пирсона и Спирмана.

Сначала также рассмотрим данные по психологической защите.

1) Чем старше человек, тем ниже у него потребность в поиске новых ощущений;
2) Чем выше отрицание, тем ниже потребность в поиске новых ощущений;
3) Чем выше рационализация, тем выше вытеснение;
4) Чем выше регрессия, тем выше замещение;
5) Чем выше регрессия, тем выше проекция;
6) Чем выше регрессия, тем выше общий уровень;
7) Чем выше компенсация, тем выше общий уровень;
8) Чем выше компенсация, тем на меньшем количестве сайтов человек зарегистрирован;
9) Чем выше гиперкомпесация, тем выше проекция;
10) Чем выше гиперкомпенсация, тем выше общий уровень;
11) Чем выше гиперкомпенсация, тем ниже потребность в новых ощущениях;
12) Чем выше гиперкомпенсация, тем в больших процентах случаев пользователь пересылает письма счастья;

13) Чем выше гиперкомпенсация, тем в меньших процентах случаев пользователь перейдет по небезопасным ссылкам;
14) Чем выше проекция, тем выше общий уровень;
15) Чем выше рационализация, тем ниже потребность в поиске новых ощущений;
16) Чем выше общий уровень, тем меньше потребность в поиске новых ощущений;
17) Чем больше вытеснение, тем больше респонденты предпринимают меры по сохранению безопасности идентификационных данных;
18) Чем больше замещение, тем больше проекция;
19) Чем больше замещение, тем больше общий уровень;
20) Чем больше общий уровень, тем больше склонность к риску;
21) Чем больше склонность к риску, тем в меньших процентах случаев будут участвовать в социальных акциях.

Если рассматривать не только психологическую защиту, то здесь результаты также разделись на ожидаемые и неожиданные, начнем с последних. Чем в больших процентах случаев респондент разлогинивается, тем большему количеству знакомых он готов предоставить свои идентификационные данные. Чем чаще респондент посылает письма счастья и чем чаще он переходит по небезопасным ссылкам, тем на большем количестве сайтов зарегистрирован. Чем в больших процентах случаев респондент будет участвовать в социальных акциях, тем в больших процентах случаев он пересылает письма счастья.

2.3. Дисперсионный анализ ANOVA. Это метод сравнения нескольких (более двух) выборок по признаку, измеренному в метрической шкале[7]. Существует несколько видов дисперсионного анализа: однофакторный, многофакторный, с повторяемыми изменениями и многомерный. При интерпретации наших результатов исследования, мы пользовались однофакторным анализом или One-way ANOVA. Как уже было замечено выше, дисперсионный анализ подходит для тех вопросов, в которых больше двух вариантов ответа. Однако часто возникает ситуация, когда при ответе на вопрос, состоящий, к примеру, из 4 ответов, респонденты выбирают только преимущественно 2 варианта ответа, игнорируя остальные. Такая ситуация говорит, в первую очередь, о погрешности составления вопроса, раз некоторые ответы на него оказались лишними, и о том, что в данном случае анализ ANOVA не удастся провести, вместо него надо делать тест Манна–Уитни. В нашем исследовании удалось провести анализ Anova только по двум вопросам. Выглядят они так:

21. *Представьте ситуацию. Вам необходимо быстро скачать книгу(музыку, видео и другое), однако, чтобы это сделать, необходимо зарегистрироваться. Что вы будете делать:*

а) не буду скачивать

б) зарегистрируюсь, используя новые идентификационные данные

в) зарегистрируюсь, используя старые идентификационные данные

г) попрошу знакомого скачать для меня

д) другое

31. Представьте ситуацию. В вашей группе появилось одно бюджетное место, на которое претендуете Вы и ваш одногруппник, решение о переводе будет принято по результатам контрольной работы. При этом Вы узнаете, что ваш одногруппник списал эту контрольную работу. Сообщите ли Вы об этом в деканат, если в этом случае Вы гарантированно попадете на это бюджетное место?

а)да

б) скорее да

в) скорее нет

г) нет

Разберем сначала результаты по 21 вопросу. Респонденты, у которых высокое вытеснение, зарегистрируются, используя старые идентификационные данные. Самая высокая регрессия у тех, кто выбрал ответ «другое», самая маленькая у тех, кто попросит знакомого скачать за него. Самая высокая проекция у тех респондентов, кто зарегистрируется, используя старые идентификационные данные, самая низка у тех, кто выбрал ответ «другое». Самый высокий общий уровень у тех, кто зарегистрируется, используя старые идентификационные данные, самый низкий — «другое». В больших процентах случаев сервисом запоминания логина и пароля будут пользоваться те респонденты, кто зарегистрируется, используя старые идентификационные данные, в меньших процентах случаев — те, кто попросит знакомого и зарегистрируется, используя новые идентификационные данные. В больших процентах случаев мерами по сохранению безопасности своих идентификационных данных воспользуются те, кто зарегистрируется, используя новые идентификационные данные. В меньших — те, кто не будет скачивать. Тот, кто попросит знакомого скачать за него, в больших процентах случаев будет участвовать в социальных акциях.

Теперь рассмотрим результаты по 31 вопросу. Наблюдается разница между теми, кто ответил «скорее нет» (самое низкое отрицание), и теми, кто ответил «нет» (самое высокое отрицание). Вытеснение у тех, кто ответил «скорее да» выше, чем у тех, кто ответил «нет». Замещение у тех, кто ответил «скорее нет», гораздо выше, чем у тех, кто

ответил «нет». Те, кто ответил «скорее да», с большей вероятностью вспомнят свой пароль от сетевого ресурса, чем те, кто ответил «нет». Те, кто ответил «скорее да», с гораздо большей вероятностью будут участвовать в социальных акциях, чем те, кто ответил «нет».

2.4. Переход от психологических особенностей пользователя к уязвимостям. Еще на начальных этапах исследования нами была выдвинута проблема перехода от профиля психологических особенностей пользователя к профилю уязвимостей. Наше исследование не имело своей целью непременно решить эту задачу, но наметить дальнейшие пути действия было необходимо. После получения первичной статистики и результатов вышеописанных тестов и анализов было выдвинуто предположение, что уязвимости пользователя являются латентными переменными, и обнаружить их наличие нам поможет факторный анализ.

Основная идея факторного анализа была сформулирована еще Ф. Гальтоном, основоположником измерений индивидуальных различий. Она сводится к тому, что если несколько признаков, измеренных на группе индивидов, изменяются согласованно, то можно предположить существование одной общей причины этой совместной изменчивости — фактора как скрытой, непосредственно недоступной измерению переменной [7]. Факторный анализ очень сложно проводить. Как правило, сначала проводят анализ главных компонент для того, чтобы выявить предполагаемое количество факторов, затем переходят непосредственно к самому факторному анализу, выбирая один из методов оценки.

При проведении факторного анализа на программе SPSS часто возникают ошибки, происходит это из-за того, что большинство бинарных переменных не является непрерывным. В нашем случае произошло именно так. Факторный анализ на урезанном количестве переменных не показал существенных результатов. Поэтому на момент выхода в печать данной статьи один из сотрудников нашей лаборатории начал переводить бинарные переменные в непрерывные метрические при помощи метода экспертных оценок, задавая им различные веса.

4.Заключение. В данной статье приводятся результаты экспериментального социологического исследования, проведенного для выявления взаимосвязи между психологическими особенностями пользователя, а именно факторами психологической защиты, действиями пользователя и его уязвимостями. При интерпретации исследования было обнаружено множество интересных результатов. Погрешность при составлении исследования и при интерпретации его результатов также

присутствовала, но большое количество полученных ожидаемых результатов данного социологического исследования делает его значимым. В конечном итоге был предложен вариант выявления уязвимостей пользователя как латентных переменных при помощи факторного анализа. В настоящее время ведутся дальнейшие исследования по построению алгоритма перехода от профиля психологических особенностей пользователя к профилю уязвимостей. Помимо этого продолжается работа над интерпретацией результатов исследования, их корректировка при обнаружения погрешностей и ошибок.

Литература

1. *Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л.* Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социоинженерных атак // Тр. СПИИРАН. 2011. Вып. 2(17). С. 70–99.
2. *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 социоинженерных атак /./ Тр. СПИИРАН. 2010. Вып. 4(15). С. 231–245.
3. *Тулупьева Т.В., Тулупьев А.Л., Пащенко А.Е., Азаров А.А. и др.* Социально-психологические факторы, влияющие на степень уязвимости пользователей информационных систем, с точки зрения социоинженерных атак // Тр. СПИИРАН. 2010. Вып. 1(12). С. 200–214.
4. *Фролова А.Н., Пащенко А.Е., Тулупьева Т.В., Тулупьев А.Л.* Анализ уровня защищенности информационных систем в контексте социоинженерных атак: постановка проблемы // Труды СПИИРАН. 2008. Вып. 7. С. 170–176.
5. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационные модели компонент комплекса «Информационная система – персонал», находящегося под угрозой социоинженерных атак // Труды СПИИРАН. 2010. Вып. 3(14). С. 50–57.
6. *Тулупьев А.Л., Пащенко А.Е., Азаров А.А.* Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. Вып. 2(13). С. 143–155.
7. *Наследов А.Д.* Математические методы психологического исследования. СПб.: Речь, 2004. 392 с.

Ванюшичева Оксана Юрьевна — студентка 5 курса математико-механического факультета Санкт-Петербургского Государственного университета. Область научных интересов: социоинженерия, 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 Faculty of Saint-Petersburg State University. Research interests: socioingeeneria, mathematical statistics, application of mathematics and computer science in 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 автоматиза-

ции 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
Труды СПИИРАН. 2010. Вып. 1(12). ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2010. Issue 1(12). ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.rthe 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.

Азаров Артур Александрович — аспирант математико-механического факультета Санкт-Петербургского государственного университета. Область научных интересов: автоматизация анализа защищенности информационных систем с учетом социоинженерных атак. Число научных публикаций — 17. artur-azarov@yandex.ru, www.tulupyev.spb.ru; СПИИРАН, 14-я линия В.О., д. 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-3337, факс +7(812)328-4450.

Azarov Artur Alexandrovich — PhD student of Saint-Petersburg State University of the Mathematics and Mechanics Faculty. Research interests: the analyzing protection of informative systems concerning socioengineering's attacks. The number of publications — 17. artur-azarov@yandex.ru, www.tulupyev.spb.ru; SPIIRAS, 39, 14th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812)328-3337, fax +7(812)328-4450.

Поддержка 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)), грантом СПбГУ шифр 6.38.72.2011 (Моделирование комплексов «информационная система — персонал» для агрегированной оценки их готовности к отражению социоинженерных атак) и грантом Правительства Санкт-Петербурга для победителей конкурса грантов Санкт-Петербурга для студентов, аспирантов, молодых ученых, молодых кандидатов наук 2011 г.

Рекомендовано ТиМПИ СПИИРАН, зав. лаб. д-р физ.-мат. наук, доцент А.Л. Тулупьев.
Статья поступила в редакцию 20.11.2011.

РЕФЕРАТ

Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А. **Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками.**

В данной статье рассматриваются результаты социологического исследования, проведенного сотрудниками лаборатории СПИИРАН, возглавляемой заведующим лабораторией д-р физ.-мат. наук, доцентом Тулупьевым А.Л.. Исследование имело цель выявить взаимосвязи между психологическими особенностями пользователя, а именно факторами психологической защиты, действиями пользователя и его уязвимостями. Основная задача исследования сводилась к поиску путей перехода от профиля психологических особенностей пользователя к профилю уязвимостей. В статье приводится интерпретация результатов исследования и определяются дальнейшие направления анализа, в частности, проведение факторного анализа для выявления латентных переменных, которые и будут являться уязвимостями пользователя в контексте рассматриваемых действий пользователя, провоцирующих совершение по отношению к нему социоинженерных атак.

Собранные первичные данные социологического исследования обрабатывались на программе SPSS. Помимо получения первичной статистики были также проведены тест Манна–Уитни, корреляционный анализ, дисперсионный анализ и факторный анализ. В статье сообщается о результатах этих тестов. Обнаруженные погрешности при интерпретации результатов тестирования в данный момент обрабатываются и корректируются. Основываясь на подтвержденных ожидаемых результатах исследования можно сказать, что в целом исследование значимо и корректно.

В статье также указываются дальнейшие направления исследования, в частности перевод бинарных переменных, искажающих факторный анализ, в непрерывные при помощи задания им весов. Веса для бинарных переменных задаются методом экспертных оценок. После перевода будет снова проведен факторный анализ, результатом которого будут новые переменные уязвимости, которые можно будет сопоставлять с рассматриваемыми в статье действиями пользователя. После этого продолжится работа над алгоритмом перехода от профиля психологических особенностей пользователя к профилю уязвимостей.

SUMMARY

Vanushicheva O. Yu., Tulupyeva T.V., Pashchenko A.E., Tulupyev A.L., Azarov A.A. **Quantitative measurements of behavioral displays of user's vulnerabilities associated with socio-engineering attacks.**

The paper is devoted to the results of sociological research held by the SPIIRAN laboratory's employees under the guidance of the head of the laboratory Dr. Sci. in Math A.L. Tylypiev. This research was devoted to the revealing interrelations between psychological features, vulnerabilities and possible actions of information system's users who are under the threat of socioengineering attacks. The main task of this research was the finding the way for changing user's psychological features profile to the user's vulnerabilities profile. The research results' interpretation and further development of this research are founded in this article. This development includes carrying out the factorial analysis for revealing of latent variables which will be the user's vulnerabilities in the context of considered user's actions on fulfillment in relation to socio-engineering attacks.

The primary data of sociological research collected was processed on SPSS program. Besides the acquiring of primary statistics, the test of Mann-Uitni, the Correlation analysis, the dispersive analysis and the factorial analysis also have been carried out. The results of these tests are mentioned in this paper. The found out errors at interpretation of results of testing, are processed and corrected at present. Basing on the confirmed expected results of the research we can postulate that as a whole the research is significant and correct.

Further directions of research are mentioned in this paper. They are, for example, the transferring of the binary variables in continuous, as they deform the factorial analysis in continuous. Weight for binary variables are set by a method of expert estimations. After transfer factorial analysis will be carried out once more. The result of this research will present new variables-vulnerability which can be compared with actions of the users considered in the paper. After that the analysis of algorithm of transition from a user's psychological features profile to user's vulnerabilities profile will proceed.