4. Статистически значимой зависимости показателей НПУ у пожарных и горноспасателей от стажа работы не обнаружено.

5. Чем выше НПУ у пожарного, тем позитивнее оценивается она экспертами по показателям здоровья ($r = 0,32$; $p < 0,05$) и по перспективе профессионального роста ($r = 0,23$; $p < 0,05$).

**Литература**

1. Александровский Ю.А. Состояния психической дезадаптации и их компенсация. – М. : Наука, 1976. – 272 с.

2. Булка А.П. Система организации психологических мероприятий в вооруженных силах Российской Федерации : автореф. дис. ... д-ра мед. наук. – СПб., 2011. – 325 с.

3. Лебедев В.И. Личность в экстремальных условиях. – М. : Политиздат, 1989. – 304 с.

4. Марищук В.Л., Евдокимов В.И. Поведение и саморегуляция человека в условиях стресса. – СПб.: Сентябрь, 2001. – 259 с.

5. Оценка психической адаптации военнослужащих-женщин к особым условиям деятельности / В.В. Юсупов, Р.Х. Кузина, В.И. Евдокимов [и др.] // Вестн. психотерапии. – 2007. – № 23. – С. 143–147.

6. Павлов И.П. Экспериментальная патология высшей нервной деятельности. – М. : Наука, 1988. – 244 с.

7. Прикладная социальная психология / под ред. А.Н. Сухова, А.А. Деркача – М. : Ин-т практ. психологии ; Воронеж : МОДЭК, 1998. – 688 с.

8. Шевченко Т.И. Особенности эмоциональных состояний сотрудников государственной противопожарной службы МЧС России : автореф. дис. ... канд. психол. наук. – СПб., 2007. – 143 с.

УДК 159.9 : 614.8

**Т.В. Тулупьева, А.Л. Тулупьев, А.А. Азаров**

# ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОНТЕКСТЕ СОЦИОИНЖЕНЕРНЫХ АТАК*

Санкт-Петербургский институт информатики и автоматизации РАН;
Санкт-Петербургский государственный университет

Комплексные корпоративные информационные системы в настоящее время получают все большее распространение в современном мире. Разработка, поддержка и защита подобных систем занимают значительное количество времени и ресурсов, кроме того, только высококвалифицированные специалисты могут заниматься подобными системами. Информация, хранимая в таких информационных системах, имеет огромную ценность для компаний – владельцев систем, поэтому значительные усилия затрачиваются на построение системы защиты таких систем от различных угроз безопасности. Целью данной статьи является комбинация нечеткого и вероятностного подхода к оценке защищенности пользователя по отношению к атакующим действиям злоумышленника, причем рассматриваются действия достаточно элементарного характера («одноходовки»), нацеленные на «элементарные» уязвимости пользователя, воздействие на которые приводит непосредственно к какому-то действию пользователя.

Ключевые слова: социоинженерная атака, информационная система, пользователь, профиль уязвимостей, информационная безопасность.

В современном мире остро встает вопрос безопасности информации и хранения данных. В связи с этим все большую актуальность получают системы обеспечения безопасности таких данных и информации, которые чаще всего являются конфиденциальными. В организациях создаются отделы обеспечения информационной безопасности. И руководители после создания такого отдела вправе рассчитывать на сохранность конфиденциальной информации. Специалисты отдела информационной безопасности внедряют и поддерживают функционирование различных систем защиты, политики безопасности организации, принимают определенные организационные меры и декларируют высокую степень защищенности информационной системы организации. Однако утечки конфиденциальной информации все же могут случиться (и случаются). При этом сотрудники отдела информационной безопасности могут не наблюдать никаких попыток технического взлома системы, поскольку могло не быть вообще никаких программно-технических атак. В подобных случаях с заметной степенью уверенности можно предположить, что утечка конфиденциальной информации связана не с техническим состоянием компьютерной сети, не с провалом системы мер безопасности, обеспечивающих

* Исследования частично поддержаны грантами РФФИ 10-01-00640, 12-01-00945, СПбГУ 6.38.72.2011.

защиту от программно-технических атак, а с более уязвимым элементом – пользователем. Пользователи информационных систем могут быть подвержены социоинженерным (социотехническим) атакующим воздействиям злоумышленника, попасть под его влияние и выдать ему искомую конфиденциальную информацию [1].

Любой сотрудник компании (как санкционированный пользователь информационной системы, так и несанкционированный), имеющий доступ к конфиденциальной информации или к устройствам, на которых эта информация хранится, может нарушить ее безопасность (в частности, конфиденциальность, целостность или доступность) преднамеренно или случайно. Именно поэтому требуется как изучать, выявлять и предотвращать социоинженерные атаки, направленные на пользователя, так и выявлять особенности самих пользователей, создающие благоприятный контекст для развития и успешной реализации социоинженерных атак. Иначе говоря, для выработки эффективных методик предотвращения социоинженерных атак необходимо выявить причину успешности осуществления этих атак, т. е., в частности, понять, чем они обусловлены или какой психологический контекст способствует их успеху. В настоящей статье предлагается описание частичного профиля уязвимостей, построенного на основании выявленных зависимостей между уязвимостями пользователя и психологическими особенностями личности. За исключением единичных случаев употребления «профессионализмов» материал излагается преимущественно на языке, доступном широкому кругу специалистов, поскольку данное исследование носит ярко выраженный междисциплинарный и прикладной характер.

В силу относительной новизны данной тематики необходимо дать ряд ключевых определений. Пользователь – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею [7].

Уязвимость – характеристика или свойство системы, в нашем случае – человека, использование которой злоумышленником может привести к нарушению безопасности информации.

Социоинженерная атака – совокупность действий злоумышленника, направленные на другое лицо (или группу лиц) с целью достижения желаемого результата, в частности, нарушения безопасности информации (организации доступа к информации, передача ее другому лицу и т. п.).

Атакующее действие – действие, которое совершает злоумышленник в рамках социоинженерной атаки.

Злоумышленники, обладающие навыками социоинженеров, с легкостью могут повлиять на неподготовленного сотрудника, имеющего доступ к компьютеру, подключенному к корпоративной сети, с целью получения именно той информации, которая им нужна. Для предотвращения этого необходимо научиться прогнозировать степени выраженности уязвимостей пользователей информационных систем, знать степень их подверженности технологиям социального манипулирования [5, 6, 9]. Если разработать методики выявления уязвимостей пользователя, то появится возможность строить модели социоинженерных атакующих воздействий на пользователя и ответные реакции пользователя на такие воздействия. Кроме того, появляются способы строить вероятностные оценки как успешности социоинженерных атакующих воздействий на пользователя, исходя из степени выраженности его уязвимостей, так и агрегированные показатели достижимости определенных критичных документов, в случае анализа возможных сценариев реализации социоинженерных атакующих воздействий на множество пользователей информационных систем. Непрерывный мониторинг ситуации, обеспечение степени защищенности персонала на необходимом уровне позволяют снизить вероятность успешных реализаций социоинженерных атакующих воздействий, а значит, уменьшить риски компании утратить конфиденциальную информацию.

Мы предполагаем, что в построение профиля уязвимостей пользователя существенный вклад может сделать его психологический профиль, отражающий уровень выраженности психологических особенностей. Вместе с тем, нельзя упускать из виду, что психологический профиль пользователя является важной, но не единственной информационной составляющей в построении профиля уязвимостей пользователя. Одной из перспективных составляющих в построении профиля уязвимостей пользователя представляется использование общего уровня подверженности манипулятивному воздействию на пользователя [10]. Данный показатель может влиять на подверженности пользователя к социоинженерным атакующим воздействиям, которые используют именно такие характеристики пользователя, как доверчивость, лень, любезность и даже энтузиазм сотрудников организации. Ряд других потенциальных составляющих требуют отдельных исследований, которые не входят в список задач настоящей работы.

На уровень выраженности уязвимостей пользователя влияет два крупных класса особенностей [4]: личностные качества; социальные и личные факторы, влияющие на уязвимость человека.

Принципиальным отличием между особенностями 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. Эти качества можно выявить в процессе психологической диагностики, например, при приеме на работу; они являются, условно говоря, «фоновыми» для данного пользователя. Уязвимости, обусловленные личностными качествами или ассоциированные с ними, скорее всего, носят статичный характер.

Особенности же II класса являются временными, динамичными, обусловленными контекстом, т. е. они не так сильно зависят от воспитания и социализации человека. Выявить их при приеме на работу не всегда предоставляется возможным – они могут не существовать или не быть актуальными (либо обостренными) на момент трудоустройства. Наличие особенностей II класса стоит принимать во внимание при организации рабочей деятельности сотрудника и их необходимо учитывать при анализе степени защищенности персонала от социоинженерных атак.

Чтобы на основании имеющихся психологических особенностей сделать предположение об уязвимостях пользователя, необходимо разработать процедуру, которая позволит переводить оценки степени выраженности психологических особенностей пользователя в оценки степени проявления его уязвимостей. С этой целью было проведено исследование, основной задачей которого был поиск взаимосвязи между психологическими особенностями, угрозообразующими действиями пользователя и выявлением степени проявления некоторых «элементарных» уязвимостей пользователя.

Исследование носило пилотный характер, применялись достаточно «грубые» методы анализа зависимостей, поэтому следует отметить, что возможно возникновение погрешностей при интерпретации результатов [4]. В исследовании принимали участие студенты двух вузов Санкт-Петербурга. Всего отвечали на вопросы анкеты 84 человека. Возраст респондентов составлял 17–24 года. Подавляющее большинство студентов учатся по гуманитарным специальностям. Респондентам предлагалось ответить на 43 вопроса специально разработанной анкеты для получения информации о действиях, которые могут привести к утечке информации и/или предоставить злоумышленнику доступ к содержимому компьютера. При составлении анкеты были рассмотрены 4 вида угрозообразующих действий пользователя, которые могут привести к нарушению конфиденциальности информации: использование одних и тех же идентификационных данных на разных ресурсах, разглашение своих идентификационных данных, чтение спама, подкупаемость. В соответствии с этими видами деятельности составлялись блоки вопросов.

Респондентам также были предложены психологические методики, которые определяли ряд личностных характеристик, особенности памяти, психологической защиты, склонность к риску и потребность в новых ощущениях [2, 3].

Результаты, полученные при первичном анализе данных, показали, что значительная часть респондентов, оказавшихся в выборке, демонстрируют поведение, которое создает контекст для успешного осуществления социоинженерной атаки.

В ходе исследования было выявлено, что пользуются сервисом запоминания логина и пароля, предоставляемым браузером, 38 % респондентов, снимают пароль и код логина же при окончании работы с информационным ресурсом лишь 49 %, т. е. чуть больше половины респондентов не снимают индивидуальный пароль для работы в сети, а следовательно, подвергают опасности сохранность своих идентификационных данных, так как у злоумышленника появляется возможность прямого доступа к тому информационному ресурсу, с которым работал не пользователь, который при разъединении с ресурсом не снял пароль. Например, где-нибудь в компьютерном центре посетитель завершил Интернет-сессию, но не завершил работы в почтовых агентах и социальных сетях – его могли незаметно, но целенаправленно отвлечь. После него компьютером без труда может воспользоваться злоумышленник, который может не только зайти на страничку социальной сети пользователя, но и извлечь логин и пароль, которые могут оказаться идентификационными данными для доступа к другим, более «серьезным» ресурсам. Тем не менее, около 73 % 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 дан-

ные, как минимум, двум людям. Не умаляя общности, можно судить о том, что такой показатель является существенной преградой для профилактики защиты от социоинженерных атак, так как в число этих самых доверенных лиц может быть включен и злоумышленник: примеры таких ситуаций описаны в [6]. Было выявлено, что 14 сайтов – среднее число сайтов, на которых зарегистрированы опрашиваемые. Среди всех опрашиваемых практически не нашлось никого, у кого ни разу не взламывали электронную почту, что также говорит в пользу того, что пользователи используют легко подбираемые логины и пароли. 41 % респондентов готовы передавать тайную информацию за определенное материальное вознаграждение, а значит, данные сотрудники могут обеспечить формирование реальной угрозы для своей компании, позитивно ответили на действия рекомпенсационного характера со стороны злоумышленника. И, подводя итоги по средним значениям, осталось отметить, что респонденты будут со значительной вероятностью принимать участие в социальных акциях из серии «Расскажи про это своим друзьям и получи бесплатную толстовку» (12 % случаев согласно результатам опроса), отсылать полученные «письма счастья» (7 %) и, наконец, переходить по ссылкам, которые браузер объявляет небезопасными (21 %) [4].

85 % респондентов хоть раз сообщали свои идентификационные данные (логин и пароль) другому человеку. Чаще всего свои идентификационные данные респонденты хранят в собственной памяти – 87 %, 12 % – в файлах домашнего компьютера, столько же респондентов хранят эти данные «на бумаге», 2 % – в файлах рабочего компьютера, 4 % – на стикере, 5 % – в мобильном телефоне. Вопреки складывающемуся при первом взгляде на результаты анализа впечатлению, то, что респонденты преимущественно (87 %) предпочитают хранить свои идентификационные данные в собственной памяти, явно говорит не в пользу уникальности и сложности таких данных. Ввиду данного факта, вероятность подбора логина и пароля злоумышленником становится исключительно велика. 61 % респондентов допускают, чтобы их идентификационные данные знали их близкие, а также 85 % готовы дать 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, т. е. подавляющее большинство респондентов готовы сообщить свои идентификационные данные, а также могут сообщить какую-то другую информацию, которая считается персональной или секретной, если они решат, что доверяют потенциальному адресату, получателю таких данных. Следовательно, для получения доступа к идентификационным данным пользователя злоумышленнику достаточно заполучить его доверие, а иногда и просто оказаться в нужное время в нужном месте и «помочь» своему так называемому «другу». Больше половины респондентов (64%) довольно беспечно относятся к своим идентификационным данным и будут 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, соответственно 63 и 74 %. При этом используют одну и ту же комбинацию логинов и паролей 85 % человек [4].

Большинство результатов показали, что респонденты легко могут сообщить свои идентификационные данные близким родственникам и знакомым, что говорит о том, что опрашиваемые могут стать жертвой злоумышленника, который является для них тем самым «близким знакомым». Как правило, большинство пользователей, хранящих пароли в собственной памяти, легко вспоминают комбинацию логин-пароль, так как в большинстве случаев используются или одинаковые, или идентичные пары. Все это говорит о том, что пароли респондентов злоумышленнику будет довольно легко подобрать или даже выяснить лично. Подводя итог, можно утверждать, что у респондентов в большинстве своем довольно сильно прослеживается возможная уязвимость к социоинженерным атакам «элементарного» характера («одноходовкам») [4].

В результате факторного анализа были выявлены 5 латентных факторов, каждый из которых тесно ассоциирован с одной из «элементарных» уязвимостей и может служить количественной оценкой степени их выраженности (в скобках указаны психологические особенности, с которыми они оказались связаны) [8]:

1) информационная неосмотрительность (низкая потребность в поиске новых ощущений, высокая общая самооценка, низкая самооценка внешности);

2) слабый пароль (психологическая защита по типу регрессия, подозрительность, самооценка уверенности в себе, недостаточный уровень слуховой памяти, выраженность меланхолических черт);

4) техническая халатность и установка на получение личной выгоды (уровень притязаний по

практическим умениям, пониженный уровень притязаний по уверенности в себе, повышенная самооценка своего авторитета, пониженная самооценка умственных способностей, несклонность к мстительности, дипломатичность, несклонность к риску, психологическая защита по типу отрицания, подозрительность);

5) техническая неопытность (психологическая защита по типу вытеснение и рационализация, сдержанность, пониженная чувствительность, консерватизм, склонность к компромиссам, психологический возраст);

6) техническая безграмотность (психологическая защита по типу замещение, интеллект, эмоциональная нестабильность, расслабленность, высокая общая интернальность, низкая интернальность в области неудач и достижений, высокая интернальность в области межличностных отношений).

В зависимости от того, какую из этих уязвимостей пользователя злоумышленник намерен использовать в социоинженерной атаке, можно выделить различные варианты атакующих воздействий и ответные (точнее, результирующие) действия пользователя на них.

Было рассмотрено несколько возможных, но не исчерпывающих вариантов атакующих воздействий и ответов на них. Все они представлены в таблице.

Рассмотрим подробнее некоторые из этих ситуаций. Если злоумышленник решил направить свое атакующее воздействие на уязвимость «Техническая неосмотрительность», то он может воспользоваться одним из видов вышеописанных воздействий. Так как пользователь является активным участником виртуальной среды, у него высокая широта социальных связей. Как правило, такие люди зарегистрированы в различных социальных сетях, ведут свои блоги или пишут в twitter. Если злоумышленник примет данный факт во внимание, он может, например, в той же социальной сети выслать пользователю приглашение зарегистрироваться на каком-то похожем сайте (социальная сеть, живой журнал и т. д.). Естественно, такой сайт будет подставным, и так как у пользователя в той или иной степени проявляется уязвимость «информационная неосмотрительность», он, соответственно, с той или иной степенью может зарегистрироваться на подставном сайте, используя старые идентификационные данные, которые без труда узнает злоумышленник, или же последний сможет отправить пользователю письмо на электронную почту с каким-то интересным для данного пользователя приложением (например, программа для просмотра переписки своих друзей с третьими лицами). Пользователь, ввиду степени проявления своей уязвимости,

Атакующие воздействия и ответы пользователя на них [4]

| Уязвимость | Атакующее воздействие | Действие пользователя |
|---|---|---|
| Техническая неосмотрительность | Предложение зарегистрироваться на каком-то Интернет-ресурсе (потенциально привлекательном для пользователя) | Пользователь регистрируется, вводя старые идентификационные данные |
| | Отправка письма с потенциально «полезным» для пользователя приложением | Пользователь читает письмо и устанавливает присланное приложение |
| | Виртуальное знакомство с пользователем в сети | Под действием обаяния злоумышленника пользователь выдает свои идентификационные данные |
| Слабый пароль | Взломать | - |
| | Подсмотреть | - |
| Техническая халатность и установка на получение личной выгоды | Подкуп | Передача злоумышленнику идентификационных данных за услугу |
| | Предложение зарегистрироваться на каком-то привлекательном сайте | Пользователь регистрируется, вводя старые идентификационные данные |
| Техническая неопытность | Предложение зарегистрироваться на каком-то Интернет-ресурсе (потенциально привлекательном для пользователя) | Пользователь регистрируется, вводя старые идентификационные данные |
| | Отправка письма с потенциально «полезным» для пользователя приложением | Пользователь читает письмо и устанавливает присланное приложение |
| | Виртуальное знакомство с пользователем в сети | Под действием обаяния злоумышленника пользователь выдает свои идентификационные данные |
| Техническая безграмотность | Предложение зарегистрироваться на каком-то Интернет-ресурсе (потенциально привлекательном для пользователя) | Пользователь регистрируется, вводя старые идентификационные данные |
| | Отправка письма с потенциально «полезным» для пользователя приложением | Пользователь читает письмо и устанавливает присланное приложение |
| | Предложение помощи в решении компьютерных дел | Принять помощь |

установит данное приложение с той или иной вероятностью. И наконец, опять же ввиду того, что пользователь является очень активным виртуальным собеседником, злоумышленник может с ним познакомиться в виртуальной среде и тем или иным способом, используя свое обаяние или другие качества, с той или иной вероятностью выяснить идентификационные данные пользователя.

Когда злоумышленник направляет свое атакующее воздействие на уязвимость «Слабый пароль», он не взаимодействует непосредственно с самим пользователем, т. е. пользователь на исход социоинженерной атаки никаким образом повлиять не сможет. Более того, он даже не узнает, что она состоялась, и его идентификационными данными обладает другой человек. В данном случае, если злоумышленник взламывает пароль пользователя, то вероятность получения этого пароля будет зависеть только от его сложности и места, где он находится. Если же злоумышленник использует атакующее воздействие «подсмотр пароля», то тут пользователь также может не понять, что произошло, и успешный исход социоинженерной атаки зависит от сложности пароля и поведения злоумышленника.

«Техническая халатность и установка на получение личной выгоды» – уязвимость, сочетающая в себе две отличительные характеристики пользователя. С одной стороны, он небрежно относится к своим идентификационным данным, с другой – нацелен на получение личной выгоды. Злоумышленник может принять каждую из этих сторон (или одновременно обе) во внимание и выполнить вышеперечисленные атакующие воздействия. Если злоумышленник решил воздействовать на стремление пользователя получить личную выгоду, то он может либо подкупить его деньгами, либо получить идентификационные данные, оказав пользователю какую-либо услугу.

Часто одной из проблем современных сотрудников фирмы является их компьютерная безграмотность. За решение той или иной компьютерной проблемы (завис компьютер, не печатает принтер и др.) на работе они обращаются за помощью к системному администратору. Но как быть пользователю, если последнего нет на месте или, например, пользователь работает дома в удаленном режиме? Злоумышленник может воспользоваться такой ситуацией и предложить пользователю свою помощь, а так как у пользователя присутствует уязвимость «Техническая безграмотность», он с той или иной вероятностей предоставит доступ к своему компьютеру, причем сам при этом может даже удалиться, например, на кухню заваривать чай для хорошего «помощника» [4].

При вычислении вероятности успешности социоинженерных атакующих воздействий злоумышленника на пользователей информационных систем перспективным представляется учёт такой особенности, как подверженность пользователя манипулятивному воздействию. Эта особенность может усиливать проявление уязвимостей пользователя (т. е. повышать вероятность угрозообразующего поведения пользователя в ответ на социоинженерное атакующее действие), связанные с принуждением пользователя сделать те или иные деструктивные действия в информационной системе.

## Заключение

В данной статье приведены основные результаты исследования, направленного на выявление взаимосвязей между психологическими особенностями пользователя и «элементарными» уязвимостями. Результаты данного исследования могут быть интересны сотрудникам отделов по работе с персоналом, поскольку дают основу для балансирования требований к потенциальному сотруднику в процессе подбора кадров, приема на работу и совершенствования процедур сопровождения сотрудников организации. Полученные данные также могут оказаться полезными для построения обоснованной стратегии защиты корпоративной конфиденциальной информации, а также для обучения персонала техникам и приемам противодействия социоинженерным атакам злоумышленника.

### Литература

1. Вероятностно-реляционный подход к представлению модели комплекса «Информационная система – персонал – критичные документы» / А.А. Азаров, Т.В. Тулупьева, А.А. Фильченков, А.Л. Тулупьев // Тр. СПИИРАН. – 2012. – Вып. 1(20). – С. 57–71.

2. Грановская Р.М. Элементы практической психологии. – СПб. : Речь, 2003. – 560 с.

3. Грановская Р.М., Никольская И.М. Защита личности: психологические механизмы. – СПб., 1999. – 507 с.

4. Классификация психологических особенностей, составляющих основу уязвимостей пользователя при угрозе социоинженерных атак / О.Ю. Ванюшичева, Т.В. Тулупьева, А.Е. Пащенко, А.Л. Тулупьев // Тр. СПИИРАН. – 2011. – Вып. 2(17). – С. 70–99.

5. Кузнецов М., Симдянов И., Социальная инженерия и социальные хакеры. – СПб. : БХВ-Петербург, 2007. – 368 с.

6. Митник К. Д., Саймон В. Л. Искусство обмана. – М. : АйТи, 2004. – 360 с.

7. Об информации, информатизации и защите информации : [федер. закон : в ред. от 10.01.2003 г. №15-ФЗ]. – М. : Ось-89, 2005. – 32 с.

8. Психологические особенности персонала, предрасполагающие к успешной реализации социоинженерных атак / А.Л. Тулупьев, Т.В. Тулупьева, О.Ю. Григорьева, А.А. Азаров // Науч. тр. Сев.-Зап. ин-та управления РАНХиГС. – 2012. – Т. 3, вып. 3(7). – С. 256–266.

9. Филиппов Г.Г. Опыт классификации технологий социального манипулирования / Управленческое консультирование // Актуал. пробл. гос. и муницип. упр. – 2011. – № 1. – С. 112–122.

10. Шейнов В.П. Скрытое управление человеком (психологи манипулирования). – М. : АСТ ; Минск : Харвест, 2001. – 848 с.

УДК 316.354 : 355.441.1 (470.23-25)

**Р.М. Грановская**

## СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ПРИЧИНЫ СТОЙКОСТИ ЖИТЕЛЕЙ БЛОКАДНОГО ЛЕНИНГРАДА (1941–1944 гг.)

Всероссийский центр экстренной и радиационной медицины им. А.М. Никифорова, Санкт-Петербург

Представлены личные воспоминания подростка-девочки о днях блокады в осажденном немецкими фашистами Ленинграде (1941–1944 гг.), ныне доктора психологических наук профессора. Анализируются социально-психологические причины стойкости жителей блокадного Ленинграда.

Ключевые слова: Великая Отечественная война 1941–1945 гг., блокада Ленинграда, установки, моральные ценности.

Подростком я перенесла блокаду, но только теперь, после 55 лет психологического стажа начала понимать всю грандиозность подвига жителей Ленинграда. Действительно в истории человечества – это не первая блокада, но не было совокупности обстоятельств, так сильно напрягавших психику жителей [1]. Эта совокупность включала:

– большую продолжительность блокады – около 900 дней;

– жестокий голод;

– исключительно суровые зимы;

– отсутствие дров для печей;

– постоянные обстрелы и бомбардировки

– полную неопределенность времени окончания блокады, т. е. сколько еще надо выдержать.

Такой перечень трудностей и породил у немцев уверенность, что жители не выдержат и сдадутся. Любой нейропсихолог знает, что это – непосильная нагрузка для человека. Действительно много жителей нашего города не вынесли ее и скончались. Однако город не только выстоял, он работал на поддержку фронта и проявлял небывалую выдержку. В чем причина такого поведения граждан? Они отстаивали не только свою жизнь, но и свою мечту о светлом будущем, где люди будут равны и свободны. Как теперь известно психологам, нет силы более мощной, чем идеалы, мобилизующие все силы личности. Таких идеалов немного – это вера в Бога, любовь к человеку и одержимость творческой задачей. Поэтому теперь я вспоминаю поведение ленинградцев в блокаду с великой гордостью. Я думаю, что когда человек живет во имя своего идеала, он может вынести практически любую нагрузку! Теперь несколько личных эпизодов.

Как-то вечером мы с мужем смотрели телевизионную передачу про защиту Ленинграда во время блокады. В передаче принимали участие несколько военных журналистов и одна дама. Военные журналисты обращали внимание на отдельные участки обороны и на то, с каким трудом доставлялось оружие в осажденный Ленинград. Они гордились защитниками и не скрывали этого. Вдруг в беседу вступила дама. Оказалось, что она из какого-то литературного журнала. Со всем пылом она стала доказывать, что весь героизм ленинградцев был напрасной тратой сил и здоровья. Что незачем было сопротивляться и умирать от голода, а надо было сразу сдать город, и тогда в нем сохранились бы все архитектурные ценности и красоты.

Мы были потрясены. Нам казалось, что на наши головы вылили ведро помоев. Во-первых – что-то я не помню, чтобы фашисты бережно сохраняли города, даже в тех редких случаях, когда им не оказывали сопротивления, а во-вторых, наши люди не представляли себе жизнь под фашистским господством.

К моменту начала войны мне было всего 12 лет, но и теперь, по прошествии многих лет (сейчас мне 83 года), я отчетливо помню тот всеобщий