Flow in Computer Hacking: A Model

Alexander E. Voiskounsky[1] and Olga V. Smyslova[2]

[1] Alexander E. Voiskounsky, Psychology Department, Moscow
Lomonosov State University 8/5 Mokhovaya str., Moscow, 103009, Russia
vae-msu@mail.ru
[2] Olga V. Smyslova
olga@korobka.net

Abstract. In this study hackers' motivation is investigated, using the flow paradigm. It was hypothesized that flow increases with the increase of hackers' competence in the IT use. An on-line research was administered within the Russian-speaking community (N=457). The hypothesis was not confirmed: the relationship between hackers' experience and flow is more complicated than the straightforward correlation. Periods of flow experience are changed by periods of flow crisis and then - of flow renovation. A model of hackers' motivational development was presented. Possible measures for preventing the criminal hacking were suggested.

1 Introduction

Computer hacking is widespread and impacts the results of work done by many people throughout the world. This impact is mostly negative. According to the CERT statistics, the number of reported incidents was about 82,000 in 2002 (http://www.cert.org/stats/cert_stats.html#incidents). It is widely believed that many takedowns are not reported (or unnoticed), and thus the harm is even greater.

On the daily basis IT specialists, usually grouped in institutions, advisories and associations, develop and update computer security methods. Technical tools are combined with juridical means, i.e. prosecution of hackers whose responsibility is proved. Nevertheless, these activities are far from perfect: security tools are not unbreakable, and any data put on the web is unsafe. Thus, technical and juridical methods of preventing computer crime are not satisfactory.

To our view, alternative ways might be promising. They include specialized education based on psychological research. We believe that adequate educational programs might result in reducing the recruitment of new hackers, if not diminishing destructive takedowns. If one knows reasons, causes and motivations that drive both qualified hackers and possibly less qualified amateur hackers (usually teenagers), then one might influence the development of their motivational patterns and the basis of their reasons.

To the best of the authors' knowledge hackers have never been thoroughly investigated by psychologists. An exception is the Turkle's study made two decades

C.-W. Chung et al. (Eds.): HSI 2003, LNCS 2713, pp. 176-186, 2003.

ago [1]. Thus, little is known about the modern generation of hackers. Besides, a bunch of myths about hackers and their motivation is widespread, since media and some social science researchers portray hackers as criminals (hackers are confused to "crackers").

According to some researchers [2, 3, 4], computer intruders include: professional criminals who use the Internet as a tool, white collar criminals, disgruntled employees, and teenager hackers. Obviously, there are no exact borders between them. Another classification is suggested by Rodgers [5]. The subgroups of hackers are classified dependent on their expertise, areas of interests (software, hardware, etc.) and behavior patterns. Subgroups vary from novices to professionals. Rodgers distinguishes seven groups of hackers: Tool Kit/newbies, Cyber-punks, Internals, Coders, Old guard hackers, Professional criminals, and Cyber-terrorists.

Tool kit/newbies, or wannabees are newcomers to hacking who rely on previously prepared ready-to-use pieces of software (tool kits), and on web instructions "how-to". Hackers of this group often cannot prognosticate the effects of their actions. The same kind of mistake can be done by everybody, including very skilled experts. A good example is the story of Robert Morris. Back in 1988, Morris wrote an experimental self-replicating program called a *worm* and injected it into the Internet. The program started replicating and infecting other machines at a much faster rate than he had anticipated [6].

Cyber-punks write pieces of software, but their competence is rather limited; they also engage in malicious acts, such as defacing web pages or stealing credit card numbers. Internals are ex-employees whose attacks are based on precise competence in principles of computer security practiced at their former organizations. As Mark Ward writes, almost half of the most serious security incidents the businesses suffered from in 2001 were caused by company employees [7]. Coders are highly skilled; they write new takedown programs, and everybody might use them. The old guard hackers are the most qualified and try to follow the ideology of the first-generation-hackers and are interested in the intellectual/cognitive side of hacking. The other two groups of hackers fully correspond to their indications.

The classifications give no reply to the question – why hackers/crackers/coders, etc. commit technology-mediated crimes? Thus, the key question is the motivation of hackers.

Hackers' Motivation Research

Back in 1960-s hackers enjoyed the reputation of smart and competent enthusiasts, and their dominant motivation was reportedly cognition. Many people believe that the best software products ever created were composed by hackers. Hackers' Hall of Fame includes such names as D. Ritchie and K. Thompson – the C inventors, D. Engelbart, responsible for hypertext, cross-file editing, and the mouse, S. Wozniak and S. Jobs, the creators of Apple, (Hackers' Hall of Fame, http://tlc.discovery.com/convergence /hackers/bio/bio.html), etc. Many of them would report that computers brought to their life inherent aesthetics. Outside the hackers' community many competent programmers would often express the same views.

The evolution of hackers is often analyzed in terms of succeeding generations. Usually, the following generations are distinguished: the first generation of pioneers who were involved in the development of the earliest software products and techniques of programming, the second generation of those who developed first PCs and brought computers to masses, and the third generation who invented computer games and made them available to public [8]. Taylor added the fourth generation of hackers "who illicitly access other people's computers" [9, p. 23].

When interviewed, hackers often report a variety of possible motives. D. Shelby, a former virus writer, notes: "My reasons are quite simple: boredom and a wish to see what can and cannot be done to and with an operating system" [10]. The other motives described in his publication, are "just having fun", "seeking fame and fortune", "pushing the envelope", and "causing the most harm".

P.Taylor, a sociologist from the Salford University, studied hackers and mentioned such motives as "boredom", "a desire to test the limits of the computer system", and "curiosity" [9], which is relatively close to statements described above. Psychologists from the University of California, San Diego, surveyed students about their motivations of committing cybercrime. In this study [11], over 30% of the students reported they engaged in illicit activities in order to learn more about technology, 22% - because it was exciting and challenging. And less than 10 percent of the students participated in computer piracy "in order to cause trouble for another person". Self-reports of hackers – subscribers to the www.kuro5hine.org webpage and online forum (http://www.kuro5hin.org/story/2002/5/28/155048/029) – might be classified as either getting new experience or as a sort of socializing. Some hackers would report that the feeling they adore most of all is that while hacking they experience full involvement in the task and think of no rewards[6, 12].

As one might see, most often hackers report high level of what might be called cognitive motivation (get rid of boredom, learn more, test the limits and extremes, state a challenge, curiosity, etc.). Other motives include full involvement, purposeful harm/troubles and socialization. The first two classes of motives correspond to intrinsic motives, the latter two – to extrinsic ones. Intrinsic motivation is the tendency to engage tasks for their own sake; one finds these tasks interesting or challenging. On the contrary, extrinsic motives, such as rewards are often task-unrelated.

A lot of work done in organizational science has always been dealing with the impact of extrinsic motives on work effectiveness. Intrinsic motivation has long been underestimated. Only recently, it was realized that extrinsic stimuli and rewards are not the only motives that direct human behavior effectively. Even "anthropological evidence shows that there are cultures in which material goals do not have importance we attribute to them" [13, p.3]. Thus, we are not going to investigate the role of extrinsic stimuli in hackers' behaviors. This role is strong enough. But the point of this paper is the intrinsic motivation of hacking.

Of the two motives mentioned earlier, cognition does certainly motivates hackers. Interesting, the seemingly highly-competent hackers name this motive more often than inexperienced newcomers to hacking. (It is hard to check, since hackers' qualification is always debatable, but the authors believe this is true; the belief is based on interviews held with hackers). The other motive which is often reported seems to be more universal, i.e. experience-independent. The rest of the paper is devoted to this sort of motivation.

Flow Motivation

The task involvement is an important hint of the hackers' supposed motivation. Based on self-reports, we assume that a special sort of intrinsic motivation is characteristic for hackers – at least for many of them.

The most elaborated concept of intrinsic motivation of this sort is the flow theory/paradigm [13]. Flow means that an action freely follows the previous action, and the process is in a way unconscious; flow is accompanied by positive emotions and is self-rewarding. A person "experiences it as a unified flowing from one moment to the next, in which he is in control of his actions, and in which there is a little distinction between self and environment, between stimulus and response, between past, present, and future" [14, p. 34]. The main antecedent of flow is *precise matching of skills and task challenges*. Moreover, both skills and challenges should not be too low, otherwise this way of matching leads not to flow experience but to a sort of apathy. Flow is placed at the cutting edge of person's skills, and it is a moving target: increase of skills depends on an increase of challenges to save the precise matching, and to select an ambitious challenge means that one needs to update skills urgently.

The originator of this theory Mihaly Csikszentmihalyi reports that the concept of flow proved to be useful to interpret motivations of teachers and students, of people engaged in sports and of artists, etc. Nevertheless, it is shown that flow might accompany almost every behavior. Investigation of flow in activities associated with computer and the Internet use started in 1990s [15,16,17]. Internet users are shown to experience flow [15,18]. Since hackers are known to be heavily using computers and the Internet, Beveren hypothetically supposed that hackers might experience flow. He introduced a model of hacker's development, based on Rodger's taxonomy of hackers. This model has not been proved empirically [19].

Hypothesis

Hoffman and Novak report that experienced users are characterized by high levels of flow, compared to inexperienced ones [15]. Since flow is believed to be important for hackers and to motivate them, we *hypothesize* that the more qualified and competent hackers experience flow more often than the less qualified hackers.

Research on hackers' motivation was planned and administered within the Russian-speaking community of hackers; we believe this does not diminish the universality of the results. We take as granted that hacking is an universal activity with few (if any) ethnic/geopolitical differences.

Methodology

Hackers tend to stay anonymous, they only rarely accept face-to-face contacts with experimenters/interviewers. At the same time, they might accept computer-mediated contacts via the Internet. Thus, the online methodology [20] gives a perspective for carrying on research within this community. This methodology puts certain restrictions on the choice of research instruments. First, researchers should not use the instruments (tests, questionnaires, etc.) which are familiar to the audience. Second, one should take into account insecurity and expensiveness of the long-time access to the Internet – due to these reasons, filling out online survey is recommended to take short time.

To measure flow, we used the questionnaire worked out and used by Hoffman & Novak [15]. The questionnaire was translated into Russian, shortened, and adapted. Four-point Likert-type scales ranging from "strongly disagree" to "strongly agree" were used for responses. The sum of the scores was defined as the level of flow .

The task of measuring hackers' competence is really difficult. Hackers have differing views on this specific sort of expertise. Different views and criteria might be suggested. But what is important, hackers certainly differ in their knowledge of the IT basics. So, to avoid an uncertain task of estimating the subjects' competence in hacking we inquired about their competence in computer use and IT-related experience. Namely, we request information about their duration of computers & IT use (in years), and the variety of known software products and programming languages (in the number of pieces). Thus, competence was taken as a compound two-block measure of experience in the IT use.

Procedure

The subjects were self-reported, self-selected hackers. The questionnaire was administered as a web fillout form, and subjects were solicited using online sources. The announcements and invitations to participate in the experiment were placed on the web-sites and web-pages containing special information for hackers.

The results were handled using the statistical package Statistica.

Results

Subjects' Demography and Computer Use Experience

457 subjects took part in the research. The average age was 23.5 years; 73.8% subjects were between 17 and 30 years old. Thus, the subjects were young, but mostly older than adolescents.

The Comparison of the Groups of Hackers

As it was supposed in the hypothesis, we checked the relationship between the flow variable and the variables indicating duration of computer use and the variety of known software products. No significant correlation was found between these variables (see Table 1).

Table 1. Correlations between flow and computer use variables

Variables	Spearman R	p-level
Flow experience vs. the duration of computer use	0.12	0.001
Flow experience vs. the variety of known software products	0.19	0.001

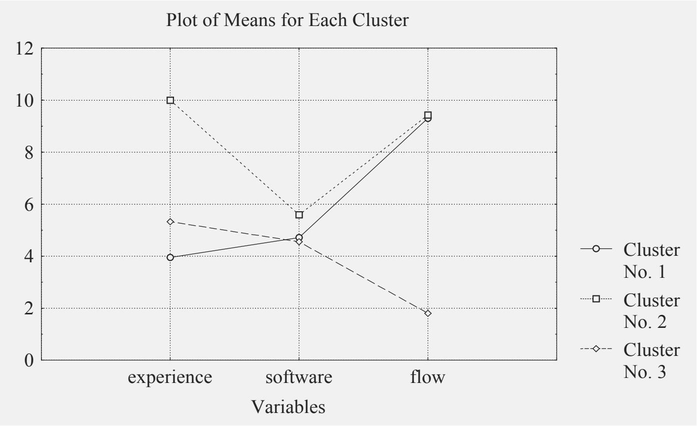

Fig. 1. Means for Clusters of Subjects

Table 2. Means for the Three Clusters

	Cluster 1 (181 Ss)	Cluster 2 (109 Ss)	Cluster 3 (167 Ss)
Experience in computer use (years)	4.0	10.0	5.3
Variety of known software products (pieces)	4.7	5.6	4.6
Flow (scores)	9.3	9.4	1.8

These correlations indicate either that the hackers with different levels of computer use competence (measured by both the duration of computer use and the variety of known software products) experience flow at a random level or that certain groups within the hackers' community experience flow differently according to their competence level or to some other characteristics. To test the latter assumption a cluster analysis of data was used.

A cluster analysis using the K-means algorithm was performed to select groups with high/low level of flow and high/low computer use experience. The data presented at the Figure 1 make it evident that the optimal classification divides our subjects into three clusters.

For the ease of analysis, the exact data – including the number of subjects in each cluster group – are presented at the Table 2.

In the group 1 the least competent Ss (i.e., small number of known products and low duration of the use of computers & IT) experience high level of flow. In the group 2 the highly competent Ss (i.e., the highest variety of known software products, and the highest duration of computers & IT experience) report high level of flow. In the group 3 the averagely competent Ss experience an unpredictably low level of flow. Thus, the moderately qualified Ss report a gap (a sort of a crisis) in the flow experience, and the flow diagram reflects a zigzag. It is reasonable to assume that this “gap” in flow experience characterising averagely experienced hackers caused the close to zero correlation between the hackers’ competence and flow variables.

To analyze the interrelations between these variables and find out predictions of flow experience, we ran the discriminant analysis procedure with three variables: flow experience, duration of computer use and the variety of known software products. The Forward Stepwise method was used: the first variable extracted in the analysis was the flow variable, and the next was the duration of the computer & IT experience. Thus the variety of software products proves to be a relatively insignificant predictor for our grouping variable (group 1/2/3). This can easily be seen even on the Figure 1.: the difference between cluster groups 1, 2 , and 3 in the variety of known software products is rather small.

When tested the canonical discriminant function to predict the variable (group1/group2/group3), the Wilks’ Lambda was significant (p<0.0001). Results show that the classification of Ss between the groups was good enough: 95.2% of correct classifications.

To understand better which flow parameters predict the flow experience and divide hackers into cluster groups 1, 2, and 3 we tested correlations between the flow variable and its components. The most significant components of flow for the subjects were: involvement (R=0.57, p<0.001), creativity (R=0.54, p<0.001), loss of sense of time(R=0.49, p<0.001), interest (R=0.49, p<0.001). These very components of flow give the heaviest load to the total scores of flow, unlike such components (presented in the experimental survey) as Arousal/Relaxation, Control, and Play items. It sounds reasonable, since it is easier to decide whether one feels the time passing, than, for instance, to be aware of one’s sense of control. These results are consistent with recent data on hackers’ psychology [22,23].

Hypothesis-Related Conclusion

The results show that the hypothesis is wrong, since flow does not linearly increase with the increase of the hackers’ competence. The relationship between hackers’ experience and flow is more complicated than the straightforward correlation. Periods of flow experience are changed by periods of flow crisis and then by periods of flow renovation. These findings make it possible to construct and present a model of hackers’ motivational development.

The Model of Computer Hackers’ Motivation

According to the model, the hacker's development might be presented in the following way. A beginner is usually using heavily the "how-to" and FAQs; supposedly, he/she is aware mostly of extrinsic rewards. At some point of his/her professional development a beginner might find a matching combination of challenges and skills. This point is of crucial importance: experience of flow is accompanied with positive emotions, with the feelings of competence and power. Strengthened by this kind of feeling, the flow motivation might become the dominant motivation. The variety of available hacking tools, decompilers, handbooks for beginners, universal standards of programming languages makes a "step-by-step" learning truly enjoyable and flow-facilitating.

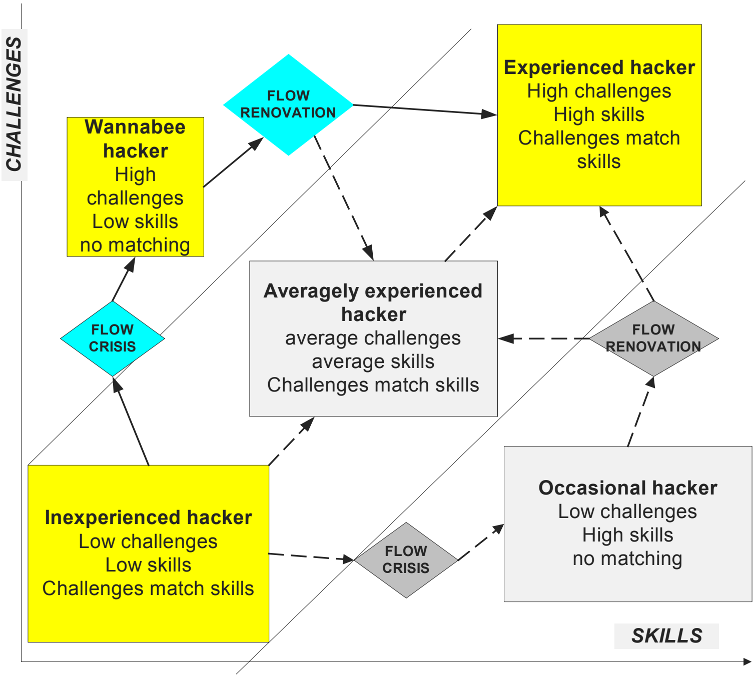

Fig. 2. Motivational model of hackers' development

While some hackers might stay at the stage of a beginner for years, others make progress in learning. The latter might take place in at least three ways. The most pleasurable and complex one is a step-by-step progress both in challenges and skills in such a way that challenges and skills keep matching at every developmental stage. This means that a hacker experiences flow all the time. The possibility to keep this delicate balance of skills and challenges seems to be beyond reach, but we can accept it as a hypothetical way of hackers' development.

The more probable ways of hackers' development mean temporary divergences between skills and challenges. For example, new skills acquired by a hacker lack the correspondence to non-updated challenges. Or else a hacker takes high challenges and finds he/she lacks non-updated skills. These two ways of a hacker's progress result in periodical losses in the flow experience.

When an inexperienced hacker gains no updated skills but increases challenges, he/she might be called a wannabee hacker. That means that the hacker looses the flow experience. Published interviews and simple observation show that a hacker might stay at the wannabee stage for years. A wannabee hacker's rewards might lie in the sphere of social prestige. To acquire the flow experience anew, a wannabee hacker might choose two ways of hacking behavior. The first is to decrease challenges and to turn into an averagely competent hacker with moderate challenges which adequately match the skills. The second is to update skills and to turn into a competent hacker whose challenges match the available skills.

When an inexperienced hacker increases skills, until his/her challenges are not updated he/she looses the fine matching of challenges and skills. The loss might be both temporary and constant. To update challenges might result in gaining the flow motive anew - at a higher level of skills/challenges matching. Quite often the challenges are not updated, and one might conclude that a hacker turns into a qualified computer user or a programmer. There are many evidences that former hackers often enough turn into computer security officers; one might assume that they loose motivation for setting high challenges in hacking (besides, they gain external motivation, e.g. salaries). There are many other options for a hacker (or a former hacker) to go on with his/her career, besides becoming a security expert. For example, he/she might turn into an occasional hacker - one who puts high challenges and realizes appropriate goals on special occasions. Among these occasions might be named a revenge to a former employer, or to an ideological/political enemy (a hactivist action), etc.

Measures which Are Supposedly Likely to Prevent Hacking

Situations when software developers' tasks don't match their high skills and they feel little or no interest in their work, is in a way dangerous. Boredom on a working place might cause programmers to perform occasional hacking. Encouraging software engineers to participate in developing different share/freeware products, might be the best solution.

Other measures should be taken to lessen the crime committed by non-professional programmers. It is widely believed that the majority of hackers are adolescents. Thus we are able to infer that they lack high stages of moral judgments, worked out by Kohlberg [21]. It is very likely that when online the adolescents' moral judgments might stay on an even lower stage than in real life. The explanation lies in the anonymity of the Internet-mediated contacts. Thus, to adapt the adolescents' system of moral judgments to the Internet anonymity is a challenge. Traditional books on cyber ethics completely miss this challenge.

The concerned educators, IT and justice experts, and parents are trying to make their best: enthusiasts work out recommendations for safe use of the Web by children and adolescents (for example, Safer Use of Services on the Internet (www.besafeonline.org/ or Cybercitizen Awareness Program www.cybercitizenpartners.org).

The world-wide community of the Internet users as well as non-users should work hard to teach new generations the essentials of the Net moral. The latter is certainly based on traditional moral and should extend the moral norms into IT-related situations.

Acknowledgements

Research was supported by the Russian Foundation for Basic Research, grant #03-06-80165.

References

[1] Turkle Sh.: The second self: Computers and the Human Spirit, Simon & Schuster (1984)

[2] Shinder, D.L., Tittel E.: Scene of the Cybercrime: Computer Forensics Handbook. Syngress Media Inc. (2002)

[3] Alves-Foss J.: Computer Crime and Security. Department of Computer Science University of Idaho. (1998) [www-document] : http://www.cs.uidaho.edu/~jimaf /cs442f99/lectures/crime-talk/

[4] Nicholson L.J., Shebar T.F., Weinberg M.R.: Computer crimes. American Criminal Law Review. (2000) [www-document] : http://www.albany.edu/acc/ courses/acc680.spring2001/curtin101.ppt

[5] Rodgers M.: A new hackers' taxonomy. Graduate Studies, Dept. of Psychology, (1999) University of Manitoba. [WWW document]: http://www.mts.net/~mkr /hacker.doc

[6] Hafner K., Markoff J.: Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon and Schuster (1992)

[7] Ward, M.: Employees seen as computer saboteurs. BBC News online (29 April, (2002) [www document]: http://news.bbc.co.uk/1/hi/sci/tech/1946368.stm)

[8] Sterling B.: The hacker crackdown: Law and Disorder on the Electronic Frontier. London: Penguin. (1992) Available at: http://www.hackzone.ru/underground /crackdown/

[9] Taylor P.: Hackers. Crime in the Digital Sublime. London: Routledge (2000)

[10] Shellby D.D.: The Viral Mind: Understanding the Motives of Malicious Coders // Security Focus Online: (2002) [www document]: http://online.securityfocus.com/infocus/1583

[11] McGuire Sh., D'Amico E., Tomlinson K., Brown S.: Teenagers self-reported motivations for participating in computer crime. In: 8th International Conference on Motivation (Workshop on Achievement and Task Motivation). Abstracts. Moscow. (2002) 72-73

[12] Voiskounsky, A.E., Babaeva, J.D., & Smyslova, O.V.: Attitudes towards computer hacking in Russia. In: D. Thomas and B. D. Loader (Eds.). Cybercrime: Law enforcement, security and surveillance in the information age. L. & N.Y.: Routledge (2000) 56–84

[13] Csikszentmihalyi, M.: Beyond boredom and anxiety: The experience of play in work and games. San Francisco: Jossey-Bass. (1975)

[14] Csikszentmihalyi, M.: Beyond Boredom and Anxiety: Experiencing Flow in Work and Play. San-Francisco: Jossey-Bass (2000)

[15] Novak T.P., Hoffman D.L.: Measuring the Flow Experience Among Web Users. (1997) [www document]: http://ecommerce.vanderbilt.edu/papers.html

[16] Repman J., Chan T. S.: Flow in Web Based Instructional Activity: An Exploratory Research Project. Texas Tech University, Georgia Southern University (1998)

[17] Trevino L. K. , Webster L. :Flow in Computer-Mediated Communication. In: Communication Research. (1992) Vol. 19(5) 539-573

[18] McKenna K., Lee S.: A Love Affair with Muds: Flow and Social Interaction in Multy-User Dungeons. (1995) [www-document] http://oak.eats.ohiou.edu/~sl302186/mud.htm

[19] Beveren J.V.: A Conceptual Model for Hacker Development and Motivations// Journal of E-Business .1.2. (2001) [www-document] http://www.ecob.iup.edu/jeb/December2001-issue/Beveren%20article2.pdf

[20] Psychological Experiments on the Internet. Ed. by M.H.Birnbaum. Academic Press (2002)

[21] Kohlberg L. The meaning and measurement of moral development. – Clark University Press (1981)

[22] Smyslova O.V. Analiz motivatsii hakerov (Hackers' motivation analysis) // Proceedings of the Conference "Social and psychological consequences of the informational technologies usage" Ed. by A.E.Voiskounsky. Moscow Public Science Foundation Publ. pp. 47-58 *(In Russian)*

[23] Voiskounsky A.E., Petrenko V.F., Smyslova O.V. Motivatsija hakerov: psikhosemanticheskoe issledovanije. (Hackers' motivation: psychosemantic research). Psykhologicheskij Zhurnal.(2003) V. 24., 1 pp. 103-118 *(in Russian)*