УДК 004.056.53 DOI: 10.18698/2541-8009-2020-04-601

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ: НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ, МЕРЫ ПРОТИВОДЕЙСТВИЯ, ПЕРСПЕКТИВЫ ИЗУЧЕНИЯ

А.В. Ванин vaninav@student.bmstu.ru
SPIN-код: 2224-2566

А.В. Марченко mart0n@mail.ru
SPIN-код: 2567-4813

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В последние 20 лет наблюдается возрастающий интерес к вопросам человека и социоорганизационным проблемам информационной безопасности. Конечные пользователи (сотрудники организации) признаются в качестве слабейшего звена по причине своей уязвимости по отношению к многочисленным угрозам безопасности. На этом фоне исследование поведения сотрудников в области информационной безопасности становится новой, перспективной и бурно развивающейся областью научного поиска. В настоящей публикации представлены основные направления исследований социоорганизационных и психологических аспектов обеспечения информационной безопасности. Рассмотрены основные угрозы целостности и конфиденциальности информации организации со стороны человеческого фактора, представлены меры противодействия им. Предложен анализ перспектив дальнейшего развития в изучении данной научной проблемы.

Ключевые слова

Человеческий фактор, информационная безопасность, культура информационной безопасности, социоорганизационные и психологические аспекты, политика безопасности, угрозы безопасности, осведомленность, холистический подход

Поступила в редакцию 25.04.2020

Введение. Традиционно информационную безопасность рассматривают преимущественно как техническую проблему, и лишь относительно недавно исследователи стали признавать, что обеспечение информационной безопасности невозможно вне рассмотрения всей палитры взаимодействия между технологическим, организационным и поведенческим аспектами [1]. На этом фоне актуальным становится изучение человеческого фактора в обеспечении информационной безопасности организации. Так, по меткому замечанию известного криптографа и специалиста в области компьютерной безопасности Брюса Шнайера: «Я говорю потенциальным клиентам, что математика непогрешима, компьютеры могут быть взломаны, как и сети, а люди ужасны своей непредсказуемостью. Я долго занимался решением проблем защиты компьютеров и сетей, но это не приблизило меня ни на дюйм к решению проблемы человека» [2, с. 149].

В этом смысле именно конечные пользователи (сотрудники организации) представляют собой центр обеспечения информационной безопасности органи-

зации [3]. Хотя установленные технические средства, содействующие компании в защите ценной информации, оказываются успешно внедренными, аналогичный уровень, основанный на защите от человеческого фактора, по-прежнему не применяется [4]. Вместе с тем знания и техники из области криминологии, социологии, поведенческой науки, психологии и человеческой коммуникации могут и должны играть здесь поддерживающую роль наравне с компьютерной наукой и информационными технологиями, чтобы гарантировать более надежную защиту целостности и конфиденциальности информации.

Основные аспекты изучения человеческого фактора в информационной безопасности организации. Можно выделить следующие направления исследований: изучение особенностей личности сотрудников в их проекции на совершение киберпреступлений [5]; использование и обновление ими антивирусных приложений [6]; готовность к резервированию данных [7] и защите корпоративной сети [8]. Исследуются поведенческие факторы, оказывающие влияние на соблюдение сотрудниками организации политик ее безопасности [9], и неподобающее использование ими информационных систем [10]. Анализируется человеческий фактор как имеющий дело с психологией человека, его внутренней мотивацией, образованием и различными социальными аспектами в своем стремлении объяснить, почему некоторые сотрудники более склонны быть «взломанными» и оказываться жертвами кражи личных и корпоративных данных [11].

Другим интересным направлением исследований становится анализ особенностей восприятия сотрудников как ключевого звена в понимании их психологических установок, намерений и последующего поведения [12]. При этом демонстрируется, что актуальное поведение сотрудников может значительно отклоняться от декларируемых ими намерений, что представляет реальную опасность для информационной безопасности организации [13]. В этом случае причиной утечки чувствительной информации могут оказаться незлонамеренные и/или случайные действия сотрудников, такие как пассивное несоблюдение ими принятых на предприятии политик безопасности, банальная лень или же отсутствие должной мотивации [14]. Прикладной задачей в этом случае становится поиск эффективных методов повышения восприимчивости сотрудников к проблемам информационной безопасности, которые поощряли бы их в принятии соответствующих техник, увеличивающих их желание соблюдать правила безопасности на предприятии [15].

Наиболее известным аспектом человеческого фактора продолжает оставаться проблема изучения инсайдерской угрозы [16]. Так, согласно широко известным статистическим данным, более 75 % случаев нарушений в работе системы безопасности организации являются результатом инсайдерской деятельности. В этом смысле величайшая угроза информационной безопасности находится не за пределами периметра безопасности (злоумышленники и применяемые ими вредоносные программы и коды), но скорее в беспечных и/или откровенно злонамеренных действиях внутренних пользователей, таких как сотрудники и/или другие доверительные участники с легким доступом к ресурсам информации предприятия [17]. Другое направление исследований обращается к угрозам извне. В частности, отмечается, что технологии безопасности могут быть без

труда преодолены при атаке неподготовленного и наивного пользователя с использованием техник социальной инженерии [18].

Исследователи обращаются также к теориям и объяснительным принципам из множества научных областей (см. таблицу).

Сводная таблица теорий, адаптированных в исследованиях поведения сотрудников в области информационной безопасности

Теоретическое основание	Описываемые индивидуальные когнитивные процессы в их влиянии на информационную безопасность	Ссылки на релевантные исследования
Теория социального научения (Social Learning Theory)	Личная уверенность в навыках безопасности (самоэффективность) может быть усилена за счет ситуационной поддержки	Bandura (1977); Warkentin с коллегами (2011)
Теория социальных связей и родства (Social Bonding Theory)	Восприятие личностью связи с коллегами мотивирует соблюдение правил информационной безопасности	Hirschi (1964); Ifinedo (2014)
Теория организационной несправедливости (Organizational Injustice)	Личное убеждение касательно несправедливости в организации при переживании неуверенности в стиле управления ведет к нарушению дисциплины и безопасности	Posey et al. (2011)
Теория климата информационной безопасности (Information Security Climate)	Представления личности, полученные в результате наблюдения особенностей среды безопасности (например, действия коллег и начальства по отношению к поддержанию самодисциплины), мотивируют соблюдение требований безопасности	Chan et al. (2005); Goo et al. (2014); Jaafar, Ajis (2013)
Общая теория деформации (General Strains Theory)	Рабочий стресс и восприятие организационной несправедливости мотивируют сотрудников на нарушения по отношению к соблюдению мер безопасности	Agnew (2001); Dang (2014)
Теория запланированного поведения (Theory of Planned Behavior)	Люди обрабатывают информацию и оценивают свою эффективность по отношению к контролю над своим поведением, что (де)мотивирует их в конечном итоге к принятию правил безопасности	Ajzen (2011)
Теория мотивации защиты (Protection Motivation Theory)	Люди оценивают угрозы и контрмеры, что мотивирует их к своевременному принятию (или непринятию) средств противодействия угрозам информационной безопасности организации	Dang-Pham, Pittayachawan (2015)
Общая теория сдерживания (General Deterrence Theory)	Люди имеют представления о политиках безопасности и мерах наказания, что лишает их намерения нарушать правила безопасности	D'Arcy, Hovav (2008); D'Arcy, Hovav, Galletta (2009); Straub (1990)

Так, Детмар Штрауб [19], исследуя степень, с которой суровость и неотвратимость наказания может влиять на преступления в области высоких технологий, обращается к криминологии и постулатам *теории общего сдерживания* (Theory of General Deterrence). Применимой оказывается и *теория компенсации рисков* (Risk Compensation Theory), согласно которой предполагается, что люди склонны совершать менее предусмотрительные действия, когда чувствуют себя более защищенными. Так, демонстрируется, что восприятие сотрудником большей защищенности (например, при наличии установленной на его рабочий компьютер антивирусной программы) ведет к его меньшему намерению соблюдать правила и процедуры, предписанные политикой информационной безопасности организации (не посещать сомнительные интернет-ресурсы, не проходить по ссылкам в электронных письмах, полученных от неизвестных отправителей, и т. п.) [20].

Меррилл Варкентин с коллегами [21], используя *теорию социального научения* (Social Learning Theory) Альберта Бандуры, утверждают, что самоэффективность сотрудников в реализации задач безопасности может быть улучшена при наличии ситуационной поддержки (доступности помощи коллег и наличия сопутствующих материалов), коммуникационного воздействия (наличия релевантных инструкций и обратной связи), вербального убеждения, опосредованного опытом, приобретенным посредством наблюдения за работой коллег. Наконец, обращаясь к общей теории деформации (General Strains Theory), исследователи демонстрируют, что рабочий стресс и восприятие несправедливости в организации функционирования предприятия и в решениях его руководства мотивируют сотрудника на нарушения дисциплины и правил безопасности [22].

Основные меры противодействия угрозам информационной безопасности организации со стороны человеческого фактора. Меры противодействия, предлагаемые исследователями, в общем случае включают три основных слоя:

1) технологии и техники;

2) политики и практики;

3) образование и обучение.

При этом могут быть задействованы следующие четыре превентивные меры:

1) пенетрационные тесты с использованием технологий и техник все той же социальной инженерии (в данном аспекте носящей несколько более позитивно-окрашенное название — *этичный взлом* (Ethical Hacking)) для выявления брешей и проблем в уровне осведомленности отдельных сотрудников организации;

2) психологические оценочные тесты для мониторинга сотрудников организации с целью определения наличия или отсутствия у них предпосылок к осуществлению инсайдерской деятельности;

3) скрининг безопасности, включающий в себя проверку бэкграунда и биографических данных сотрудников, их мотивацию, и др.;

4) правовые и организационные методы, включающие установление как политик и руководств, так и санкций за их несоблюдение.

Рекомендуемые интервенции для решения проблемы разрыва между знанием и поведением сотрудников в сфере информационной безопасности, в свою очередь, включают:

1) наказания [23];

2) инструкции по ситуационной этике [24];

3) повышение уровня осведомленности [5].

Целесообразно также усиление процедур безопасности, адресованных ситуационным факторам, таким как сокращение трудовой нагрузки, чтобы сотрудники имели необходимые им временные и энергетические ресурсы для внедрения предписанных процедур повышения качества политик безопасности; усиление степени внутренней согласованности между целями безопасности организации и ее практиками [25].

Особую значимость приобретает комплексное обучение и информирование сотрудников организации, материализующихся в учебных курсах, практических семинарах, презентациях, посвященных безопасности посещения интернет-ресурсов и использования корпоративных электронных почтовых ящиков, при содействии мотивирующих постеров, предметов канцелярии, ролевых игр и т. п. [26].

В общем случае комбинация процедурного и технического контроля служит императивом в управлении информационной безопасностью организации. Обмен информацией между сотрудниками, посредничество (различные тренинговые методы) и кооперация — вот три основные составляющие увеличения уровня осведомленности, позитивно влияющие на установки, намерения и конечное поведение сотрудников в области информационной безопасности организации [27].

Перспективы дальнейших исследований человеческого фактора в информационной безопасности организации. Актуальность и значимость изучения социоорганизационных и психологических аспектов обеспечения информационной безопасности будет сохраняться и даже усиливаться вопреки все более успешному внедрению технологий, ужесточению законодательства, совершенствованию внутренних трудовых актов и политик безопасности на предприятиях. Создание субкультуры информационной безопасности в будущем может явиться ключом к управлению человеческим фактором, при этом соблюдение сотрудниками всех предписанных правил по-прежнему будет вызывать озабоченность руководителей организаций. Типичные способы контроля, используемые для стимулирования безопасного поведения сотрудников, неизменно будут включать программы развития осведомленности, разработку ясных и согласованных политик информационной безопасности, применение различных методов сдерживания.

Для решения проблем информационной безопасности организации от науки и практики потребуется принятие целостного (холистического) подхода [28], включающего помимо прочего анализ установок, убеждений, субъективных норм, поведенческих паттернов сотрудников. Подобный подход будет призван анализировать взаимосвязи между людьми, технологиями и рабочей средой, привлекая для этого релевантные знания из области психологии, социологии, менеджмента и множества других наук социогуманитарного склада.

Выводы. Безопасное управление информационными системами продолжает сохранять решающее значение для финансового и репутационного благополучия предприятия. И хотя большинство организаций давно и успешно используют релевантные задаче технологии, проблема обеспечения информационной безопасности стоит все столь же остро по причине влияния человеческого фактора. Как следствие, область изучения поведенческих аспектов будет оставаться актуальной и все так же привлекать повышенный интерес к изучению и имплементации методов эффективного управления информационной безопасностью организации.

Литература

[1] Furnell S., Clarke N. Power to the people? The evolving recognition of human aspects of security. *Comput. Secur.*, 2012, vol. 31, no. 8, pp. 983–988. DOI: https://doi.org/10.1016/j.cose.2012.08.004

[2] Schneier B. Secrets and lies: digital security in a networked world. Wiley, 2015.

[3] Padayachee K. Taxonomy of compliant information security behavior. *Comput. Secur.*„ 2012, vol. 31, no. 5, pp. 673–680. DOI: https://doi.org/10.1016/j.cose.2012.04.004

[4] Gudaitis T.M. The missing link in information security: three dimensional profiling. *Cyberpsychol. Behav. Soc. Netw.*, 1998, vol. 1, no. 4, pp. 321–340. DOI: https://doi.org/10.1089/cpb.1998.1.321

[5] Straub D.W., Nance W.D. Discovering and disciplining computer abuse in organizations: a field study. *Manag. Inf. Syst. Q.*, 1990, vol. 14, no. 1, pp. 45–60. DOI: https://doi.org/10.2307/249307

[6] Lee Y., Larsen K.R.T. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inf. Syst.,* 2009, vol. 18, no. 2, pp. 177–187. DOI: https://doi.org/10.1057/ejis.2009.11

[7] Crossler R.E. Protection motivation theory: understanding determinants to backing up personal data. *43rd Hawaii Int. Conf. Syst. Sci*., 2010. DOI: https://doi.org/10.1109/HICSS.2010.311

[8] Woon I., Tan G.-W., Low R. A protection motivation theory approach to home wireless security. *ICIS*, 2005. *aisel.aisnet.org: веб-сайт*. URL: https://aisel.aisnet.org/cgi/ viewcontent.cgi?article=1237&context=icis2005 (дата обращения: 15.01.2020).

[9] Bulgurcu B., Cavusoglu H., Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Manag. Inf. Syst. Q.*, 2010, vol. 34, no. 3, pp. 523–548. DOI: https://doi.org/10.2307/25750690

[10] D'Arcy J., Hovav A., Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf. Syst. Res.*, 2009, vol. 20, no. 1, pp. 79–98. DOI: https://doi.org/10.1287/isre.1070.0160

[11] Kabay M. Social Psychology holds lessons for security experts. *The Risks Digest*, 1993, vol. 15, no. 16, p. 33.

[12] Crossler R.E., Johnston A.C., Lowry P.B., et al. Future directions for behavioral information security research. *Comput. Secur.*, 2013, vol. 32, pp. 90–101. DOI: https://doi.org/10.1016/j.cose.2012.09.010

[13] Guo K., Yuan Y., Archer N., et al. Understanding nonmalicious security violations in the workplace: a composite behavior model. *J. Inf. Technol. Manag.*, 2011, vol. 28, no. 2, pp. 203–236. DOI: https://doi.org/10.2753/MIS0742-1222280208

[14] Rhee H.-S., Kim C., Ryu Y.U. Self-efficacy in information security: its influence on end users' information security practice behavior. *Comput. Secur.*, 2009, vol. 28, no. 8, pp. 816–826. DOI: https://doi.org/10.1016/j.cose.2009.05.008

[15] Huang D.-L., Rau P.-L.P., Salvendy G., et al. Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int. J. Hum. Comput. Stud.*, 2011, vol. 69, no. 12, pp. 870–883. DOI: https://doi.org/10.1016/j.ijhcs.2011.07.007

[16] Schultz E.E. A framework for understanding and predicting insider attacks. *Comput. Secur.*, 2002, vol. 21, no. 6, pp. 526–531. DOI: https://doi.org/10.1016/S0167-4048(02)01009-X

[17] Posey C., Bennett R.J., Roberts T.L. Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. *Comput. Secur.*, 2011, vol. 30, no. 6-7, pp. 486–497. DOI: https://doi.org/10.1016/j.cose.2011.05.002

[18] Lineberry S. The human element: the weakest link in information security. *JOFA*, 2007, vol. 204, no. 5, p. 44.

[19] Straub D.W. Effective IS security: an empirical study. *Inf. Syst. Res.*, 1990, vol. 1, no. 3, pp. 255–276. DOI: https://doi.org/10.1287/isre.1.3.255

[20] Zhang J., Reithel B.J., Li H. Impact of perceived technical protection on security behaviors. *Inform. Manag. Comp. Sec.*, 2009, vol. 17, no. 4, pp. 330–340. DOI: https://doi.org/10.1108/09685220910993980

[21] Warkentin M., Johnston A.C., Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *Eur. J. Inf. Syst.*, 2011, vol. 20, no. 3, pp. 267–284. DOI: https://doi.org/10.1057/ejis.2010.72

[22] Dang D. Predicting insider's malicious security behaviours: a General Strain Theory-based conceptual model. *Conf-IRM*, 2014, p. 1–11.

[23] Straub D.W., Welke R.J. Coping with systems risk: security planning models for management decision making. *Manag. Inf. Syst. Q.*, 1998, vol. 22, no. 4, pp. 441–469. DOI: https://doi.org/10.2307/249551

[24] Kurland N.B. Ethical intentions and the theories of reasoned action and planned behavior. *J. Appl. Soc. Psychol.*, 1995, vol. 25, no. 4, pp. 297–313. DOI: https://doi.org/10.1111/j.1559-1816.1995.tb02393.x

[25] Debar H., Viinikka J. Security information management as an outsourced service. *Inform. Manag. Comp. Sec.*, 2006, vol. 14, no. 5, pp. 417–435.

[26] Albrechtsen E., Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Comput. Secur.*, 2010, vol. 29, no. 4, pp. 432–445. DOI: https://doi.org/10.1016/j.cose.2009.12.005

[27] Feledi D., Fenz S., Lechner L. Toward web-based information security knowledge sharing. *Inform. Sec. Tech. Rep.*, 2013, vol. 17, no. 4, pp. 199–209. DOI: https://doi.org/10.1016/j.istr.2013.03.004

[28] Soomro Z.A., Shah M.H., Ahmed J. Information security management needs more holistic approach. *Int. J. Inf. Manage.*, 2016, vol. 36, no. 2, pp. 215–225. DOI: https://doi.org/10.1016/ j.ijinfomgt.2015.11.009

Ванин Александр Владимирович — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Марченко Антон Васильевич — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Ванин А.В., Марченко А.В. Человеческий фактор в информационной безопасности организации: направления исследований, меры противодействия, перспективы изучения. *Политехнический молодежный журнал*, 2020, № 04(45). http://dx.doi.org/ 10.18698/2541-8009-2020-04-601

THE HUMAN FACTOR IN THE INFORMATION SECURITY OF AN ORGANIZATION: AREAS OF RESEARCH, COUNTERMEASURES, PROSPECTS FOR STUDY

A.V. Vanin vaninav@student.bmstu.ru
SPIN-code: 2224-2566

A.V. Marchenko mart0n@mail.ru
SPIN-code: 2567-4813

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Over the past 20 years, there has been an increasing interest in human issues and the socio-organizational problems of information security. End users (organization employees) are recognized as the weakest link because of their vulnerability to numerous security threats. Against this background, the study of employee behavior in the field of information security is becoming a new, promising and rapidly developing area of scientific research. This publication presents the main directions of research on the socio-organizational and psychological aspects of ensuring information security. The paper considers the main threats to the integrity and confidentiality of the organization's information on the part of the human factor, presents countermeasures. An analysis of the prospects for further development in the study of this scientific problem is proposed.

Keywords

Human factor, information security, information security culture, socio-organizational and psychological aspects, security policy, security threats, awareness, holistic approach

Received 25.04.2020

References

[1] Furnell S., Clarke N. Power to the people? The evolving recognition of human aspects of security. *Comput. Secur.*, 2012, vol. 31, no. 8, pp. 983–988. DOI: https://doi.org/10.1016/j.cose.2012.08.004

[2] Schneier B. Secrets and lies: digital security in a networked world. Wiley, 2015.

[3] Padayachee K. Taxonomy of compliant information security behavior. *Comput. Secur.*,, 2012, vol. 31, no. 5, pp. 673–680. DOI: https://doi.org/10.1016/j.cose.2012.04.004

[4] Gudaitis T.M. The missing link in information security: three dimensional profiling. *Cyberpsychol. Behav. Soc. Netw.*, 1998, vol. 1, no. 4, pp. 321–340. DOI: https://doi.org/10.1089/cpb.1998.1.321

[5] Straub D.W., Nance W.D. Discovering and disciplining computer abuse in organizations: a field study. *Manag. Inf. Syst. Q.*, 1990, vol. 14, no. 1, pp. 45–60. DOI: https://doi.org/10.2307/249307

[6] Lee Y., Larsen K.R.T. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inf. Syst.,* 2009, vol. 18, no. 2, pp. 177–187. DOI: https://doi.org/10.1057/ejis.2009.11

[7] Crossler R.E. Protection motivation theory: understanding determinants to backing up personal data. *43rd Hawaii Int. Conf. Syst. Sci.*, 2010. DOI: https://doi.org/10.1109/HICSS.2010.311

[8] Woon I., Tan G.-W., Low R. A protection motivation theory approach to home wireless security. *ICIS*, 2005. *aisel.aisnet.org: website*. URL: https://aisel.aisnet.org/cgi/ viewcontent.cgi?article=1237&context=icis2005 (дата обращения: 15.01.2020).

[9] Bulgurcu B., Cavusoglu H., Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Manag. Inf. Syst. Q.*, 2010, vol. 34, no. 3, pp. 523–548. DOI: https://doi.org/10.2307/25750690

[10] D'Arcy J., Hovav A., Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf. Syst. Res.*, 2009, vol. 20, no. 1, pp. 79–98. DOI: https://doi.org/10.1287/isre.1070.0160

[11] Kabay M. Social Psychology holds lessons for security experts. *The Risks Digest*, 1993, vol. 15, no. 16, p. 33.

[12] Crossler R.E., Johnston A.C., Lowry P.B., et al. Future directions for behavioral information security research. *Comput. Secur.*, 2013, vol. 32, pp. 90–101. DOI: https://doi.org/10.1016/j.cose.2012.09.010

[13] Guo K., Yuan Y., Archer N., et al. Understanding nonmalicious security violations in the workplace: a composite behavior model. *J. Inf. Technol. Manag.*, 2011, vol. 28, no. 2, pp. 203–236. DOI: https://doi.org/10.2753/MIS0742-1222280208

[14] Rhee H.-S., Kim C., Ryu Y.U. Self-efficacy in information security: its influence on end users' information security practice behavior. *Comput. Secur.*, 2009, vol. 28, no. 8, pp. 816–826. DOI: https://doi.org/10.1016/j.cose.2009.05.008

[15] Huang D.-L., Rau P.-L.P., Salvendy G., et al. Factors affecting perception of information security and their impacts on IT adoption and security practices. *Int. J. Hum. Comput. Stud.*, 2011, vol. 69, no. 12, pp. 870–883. DOI: https://doi.org/10.1016/j.ijhcs.2011.07.007

[16] Schultz E.E. A framework for understanding and predicting insider attacks. *Comput. Secur.*, 2002, vol. 21, no. 6, pp. 526–531. DOI: https://doi.org/10.1016/S0167-4048(02)01009-X

[17] Posey C., Bennett R.J., Roberts T.L. Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. *Comput. Secur.*, 2011, vol. 30, no. 6-7, pp. 486–497. DOI: https://doi.org/10.1016/ j.cose.2011.05.002

[18] Lineberry S. The human element: the weakest link in information security. *JOFA*, 2007, vol. 204, no. 5, p. 44.

[19] Straub D.W. Effective IS security: an empirical study. *Inf. Syst. Res.*, 1990, vol. 1, no. 3, pp. 255–276. DOI: https://doi.org/10.1287/isre.1.3.255

[20] Zhang J., Reithel B.J., Li H. Impact of perceived technical protection on security behaviors. *Inform. Manag. Comp. Sec.*, 2009, vol. 17, no. 4, pp. 330–340. DOI: https://doi.org/10.1108/09685220910993980

[21] Warkentin M., Johnston A.C., Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *Eur. J. Inf. Syst.*, 2011, vol. 20, no. 3, pp. 267–284. DOI: https://doi.org/10.1057/ejis.2010.72

[22] Dang D. Predicting insider's malicious security behaviours: a General Strain Theory-based conceptual model. *Conf-IRM*, 2014, p. 1–11.

[23] Straub D.W., Welke R.J. Coping with systems risk: security planning models for management decision making. *Manag. Inf. Syst. Q.*, 1998, vol. 22, no. 4, pp. 441–469. DOI: https://doi.org/10.2307/249551

[24] Kurland N.B. Ethical intentions and the theories of reasoned action and planned behavior. *J. Appl. Soc. Psychol.*, 1995, vol. 25, no. 4, pp. 297–313. DOI: https://doi.org/10.1111/j.1559-1816.1995.tb02393.x

[25] Debar H., Viinikka J. Security information management as an outsourced service. *Inform. Manag. Comp. Sec.*, 2006, vol. 14, no. 5, pp. 417–435.

[26] Albrechtsen E., Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Comput. Secur.*, 2010, vol. 29, no. 4, pp. 432–445. DOI: https://doi.org/10.1016/j.cose.2009.12.005

[27] Feledi D., Fenz S., Lechner L. Toward web-based information security knowledge sharing. *Inform. Sec. Tech. Rep.*, 2013, vol. 17, no. 4, pp. 199–209. DOI: https://doi.org/10.1016/j.istr.2013.03.004

[28] Soomro Z.A., Shah M.H., Ahmed J. Information security management needs more holistic approach. *Int. J. Inf. Manage.*, 2016, vol. 36, no. 2, pp. 215–225. DOI: https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Vanin A.V. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Marchenko A.V. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Tsirlov V.L., Cand. Sc. (Eng.), Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Vanin A.V., Marchenko A.V. The human factor in the information security of an organization: areas of research, countermeasures, prospects for study. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2020, no. 04(45). http://dx.doi.org/ 10.18698/2541-8009-2020-04-601.html (in Russ.).