TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 9, 2020

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

Mitigating hiring risks through pre-employment background screening: Methodology based on the personnel security approach

Julia Rushchenko

Ph.D. in Criminology, Associate Professor, University of West London, United Kingdom Ph.D. in Criminology, Associate Professor, University of West London, United Kingdom
Julia.rushchenko@uwl.ac.uk

Ihor Rushchenko

Dr.Sc., Professor, National Technical University «Kharkiv Polytechnic Institute», Ukraine
Ihor.Rushchenko@khpi.edu.ua

Olena Plakhova

Ph.D., Associate professor, V. N. Karazin Kharkiv National University, Ukraine
Lena_plakhova@ukr.net

Abstract. In the wake of the corporate scandals linked to negligent hiring, many organisations worldwide have prioritised background investigations to avoid harm or legal liability and ensure safety of their assets, employees and clients. Negligent hiring takes place when an employer fails to verify that a prospective employee may pose a threat to their company. The article discusses the process of pre-employment screenings aimed at mitigating the risk of corporate fraud, unethical behaviour and organisational deviance. The goal of the article is to analyse a methodological basis for pre-employment background checks carried out by the in-house recruitment experts or third party employee screening companies. A large number of the existing studies have examined the theory and policies of pre-employment screenings, have scrutinised functionality and efficiency of background investigations and have addressed the methods used as part of this process. However, prior research has not identified a comprehensive and integrated technique of carrying out a pre-employment background check. To fill this gap, the paper suggests a vacancy-specific background screening of potential candidates according to the previously defined security criteria formulated in the article. The objective of the abovementioned approach is to generate an effective mechanism of identifying the so-called "risky hires" before the onboarding stage of recruitment. It is argued that both risk evaluation and pre-employment assessments of candidates should be viewed as a standard business practice integrated into a comprehensive hiring corporate policy.

Keywords. pre-employment screening, personnel security, risk management, corporate fraud prevention, employee background investigations

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

Introduction

In the early 20th century, Henry Ford, an industrialist who revolutionized the assembly line production for the automobile industry and a pioneer of "welfare capitalism", advocated for occupational staffing processes aimed at the principles of efficiency and support encouraging the "open hiring" model. Each candidate was given an opportunity to join the factories of his company, and their career advancement depended on the contribution and performance at the workplace rather than their past histories (Ford, 2016). In the context of the mass production the recruitment managers were mostly concerned about employee turnover instead of focusing on conscientiousness, work ethic and trustworthiness. However, in the wake of the corporate scandals linked to fraud and unethical activity over the past few decades, the idea about hiring new staff members has been changing. Nowadays employers differ in the extent they rely on the cognitive and behavioral assessments but the vast majority of today's top executives and managers believes that a basic pre-employment background screening is a fundamental part of the hiring process.

In keeping with the risk management approach, pre-employment screening is comprised of a range of mechanisms devised to identify a potential employee able to inflict a significant damage on the company's reputation, circumvent the systems for their own benefit or engage in a data breach resulting in information disclosure or data leakage. Negligent hiring triggers financial consequences too. It is estimated that companies lose an average of 5% of revenue annually to occupational fraud (Coenen, 2008), and severe employee misconduct can damage the brand. According to the recent studies, in Ukraine internal fraud results in the loss of 5 to 12% of profit, and corporate fraud was named as the third most significant threat to the Ukrainian companies in 2019 (Roik, 2019). Therefore, the need to reduce the costs of misconduct and unethical behavior has resulted in distinguishing the goals of personnel security from the general agenda of the human resource services.

1. Theoretical and methodological underpinnings

1.1. Literature review

The issue of personnel security is closely linked to the corporate fraud problem which has been covered in the academic literature from the financial, organisational and behavioural perspectives (Levi, 2008; Albrecht & Albrecht, 2004; Benson et al., 2009; Coleman, 2001; Lou and Wang, 2009; Shover and Hochstetler, 2002). Corporate fraud can be manifested in multiple forms. KPMG Forensic (2014) identifies the following categories of corporate fraud and misconduct: fraudulent financial reporting, misappropriation of assets, and other illegal or unethical acts (bribery, corruption or market rigging). Besides financial losses, a deliberate attempt to misuse the established systems, policies and regulations for a personal gain leads to a wide range of issues that impact businesses worldwide, including reputation risks, a decrease of public trust, internal conflicts, corruption, sanctions, and litigation. Executives and management are increasingly aware about the necessity to ensure that certain controls and programs such as pre-screening and aptitude tests are in place to address the risks of fraud and prevent an undesired behaviour.

Personnel security as an independent research area has been developing over the past two decades in several areas. First, academic literature has explored the nature and outcomes of the pre-hire screening assessments focusing on the processes and their functionality (Chiang and Berkoff, 2017; Williams, 2005; Weber and Feintzeg, 2014; Jattuso and Sinar, 2003). Second, a large number of existing studies has focused on the risk management approach analysing policies and controls implemented to reduce and mitigate the risk of fraud and misconduct

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

(Buckhoff, 2002; Holton, 2009; Meiners, 2005). Third, there was an attempt to identify and address the issue of toxic employees and risks associated with employing them (Templer, 2018; Jonason et al., 2012; Cavaiola and Lavender, 2000; Koeke, 2000; Furnham and Taylor, 2004; Roy and Lubit, 2004; Tsygichko et al., 2016). Fourth, a considerable amount of research has been directed at understanding the general theory of personnel security (Huang and Capelli, 2006; Zatonatskiy, 20119; Rushchenko, 2007; Zhivko, 2012; Zubko and Laptieva, 2018; Sidak and Migus, 2012; Chumarin, 2003). Finally, textbooks and training manuals have been created to provide methodological support for personnel security courses at universities (Solomanidina and Solomanidin, 2017).

1.2. Social engineering and the screening algorithm

Our review of existing sources regarding personnel security reveals a methodological gap linked to the absence of a single methodology that would combine different approaches, methods, techniques into a clear algorithm of the recruitment managers' activity at the stage of the candidate selection. Although private companies worldwide have been developing a wide range of corporate practices aimed at establishing anti-fraud policies, detecting where and how they occur and taking corrective measures to remedy the harm (KPMG, 2014), most of the corporate white papers and policy documents do not suggest any comprehensive and integrated techniques on how to detect fraudulent behavior prior to employment.

The aim of the article is to formulate a methodological basis for the pre-employment screening tool that can later be used by the internal staffing experts or outsourcing services to improve its recruitment processes and practices. One of the goals of a pre-employment screening is to identify and filter potentially dangerous and toxic individuals whose presence at workplace could be detrimental to the organization. The methodology of the pre-employment screening test is based on the theory of social technologies, or the social engineering approach (Podshivalkina, 1997) common for occupational psychology, including employee behavior and information security culture. Its application has been linked to the need of standardizing complex social process and optimizing and rationalizing relevant activities.

1.3. Conceptualising pre-employment screening techniques

The next section will discuss the basic principles and concepts that enable us to conceptualize the task of building a pre-employment screening technique. The following principles will be helpful as a methodological basis for the latter, and incorporating them before the onboarding process can contribute to mitigating risks related to new hires.

Integration of technology into the overall personnel selection process in such a way that the step-by-step design does not result in artificial obstacles for the organization and does not unnecessarily increase the operational costs of staffing. Candidate loyalty testing can be performed by the same HR managers responsible for the overall process of selecting candidates for the organization provided that the screening process itself is data-driven and that there are certain processes and protocols aimed at detection and prevention for managers.

Financial justification. Since devising pre-employment screening techniques requires extra costs, it is important for on organization to justify these expenses. The general idea is that the cost of running and maintaining a pre-screening technology is a valuable investment in the security of the organization and protection of its assets. As part of the financial justification process, one should consider potential costs linked to non-compliance, data breaches and unethical behavior.

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

Differentiation is the application of different screening algorithms to different professional positions. This stage makes the process of screening more affordable and ensures its justification as a necessary measure. It also tests against a certain range of criteria.
Consistency is the ability to apply the vetting tools to all employees before being hired by the company, including when internal staffing is being used by the HR services.
Transparency revolves around an ability to implement innovative scientific achievements in the field of occupational psychology and risk management.
Besides discussing methodological principles, it is essential to include the definitions of main concepts that underpin the process of pre-employment screenings. Furthermore, the sections below will focus on introducing the idea of risk profiling and will address the steps of the screening algorithm.

2. Findings

2.1. Main terms and concepts

The following terms are important to define while generating a technique of the pre-employment screening:
Personnel security as a term is used to define a number of activities: 1) as one of the indicators of the effectiveness of the organizational security linked to trustworthy and compliant staff; 2) as a "system of policies and procedures used to mitigate the risk of workers exploiting their legitimate access to an organization's assets for unauthorized purpose" (Centre for Protection of National Infrastructure, 2000); 3) as a research area aimed at devising methods and techniques to prevent and detect occupational fraud.
Candidates are individuals who have responded to an organization's request as part of a recruitment campaign and with whom company's or a third party's recruitment managers are required to work during the selection process. Screening candidates according to the criteria of the personnel security principles is a process that consists of: a) identifying certain personality traits that can be flagged as possible threats to the organizational behavior; b) taking managerial decisions about the outcomes of the recruitment process.
Personnel security subsystem is a set of elements, activities, procedures, methods and technologies that are collectively used to address the issue of personnel security of a company. It plays a key role in the functioning of other security subsystems, including economic, physical, information and psychological security aspects.
Personnel threats and risks are a set of potential situations when the employees', consultants', or contractors' actions (or a lack of actions) generate extraordinary scenarios and contribute to the adverse consequences regarding a company's revenues or its reputation.
"Risky" candidates are individuals who pose a threat to the organization in terms of perpetrating any crimes or engaging in unethical behavior, and the internal staffing or the employee-screening outsourcing systems are meant to identify these individuals before they are hired by a company. The focus of the screening is meant to be on the "risky hires" who are part of the society's social fabric and whose behavior is reflected in the statistics. The latter category is represented by the addicts (including substance dependency and gambling), individuals with various types of personality disorders, and candidates with a clear evidence of criminogenic behavior.
Personnel security criteria are the person specifications used to evaluate a candidate's profile while determining their corporate security risks. They are based on a set of psychological and behavioral indicators that can be considered as "red flags" and should be tested as part of the pre-employment applicant screening process.

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

Typology of personnel security criteria is a typology that ensures "risky hires" are categorized according to their behavior patterns. Typologies may be based on cognitive, behavioral, physical and societal factors. Each type in turn is divided into several types depending on the nature of the deviation. In general, the typological scheme is a fluid set of tools developed depending on the nature of the organization and activities. However, there should also be the so-called minimum security criteria that are the minimum requirements included in the screening system.

Personnel safety profile is a job specification document that consists of a possible security-related impact of a certain individual on the whole organization or its employees, vendors, contractors or consultants. It should be considered as part of the pre-employment screening as different job groupings pose dissimilar risk patterns and requite different screens. In other words, screening should be vacancy-specific.

"Risky" individuals are applicants prone to employee misconduct and to circumvent business processes, rules and procedures. In doing so, they threaten the well-being of an organization and might trigger severe financial implications. A wide range of employees could engage in organizational deviance throughout their service. However, only a certain category of "risky hires" systematically engages in workplace deviance, and they are the most dangerous for an organization and its members.

The concept of personnel security is based on the idea that organizational deviance is conditioned by certain factors. The theories of deviant behavior revolve around an assumption that its causes are either rooted in the psychological or societal factors. In the table 1, we attempt to systematize the aspects or scenarios that contribute to the diachronic structure of deviant behavior. We also suggest a range of possible criteria for the personnel security staffing systems to be used at the pre-employment screening stage.

Table 1. Structure of organisational deviance.

Physiological factors	A failure to satisfy a job specification regarding physical abilities (e.g. a requirement to lift or carry items) Age limitations Illnesses not compatible with a role Physiological addictions
Psychological factors	Psychological addictions
Societal factors	Criminal connections Current job assignments for a competitor
Types of organizational deviance	Violent and aggressive behavior (mobbing, bullying, sexual harassment) Intentional conflicts and destructive behavior Fraud Corruption Criminal behavior (lying, stealing) Voluntary absenteeism Addictions Sabotage Espionage Suicidal ideation (for jobs where other employees' or customers' safety will be at risk)

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

3. Risk profiling

Besides factors conducive to organizational deviance, it is important to emphasize the significance of risk profiling as it determines the success or failure of the entire algorithm. While in the personnel security literature this stage is not specifically addressed, we believe that it should determine the strategy and tactics of the applicant screening process. We suggest that the recruitment managers should consider the following aspects while generating the applicant screening systems: 1) the corporate security concept; 2) the personnel security concept; 3) risk profiling. The latter is meant to ensure a more consistent, logical, justified, and integrated approach, and eventually will make the whole process more robust and comprehensive.

Risk evaluation is an analytical assessment of the potential for risk in a certain profession, and it should consist of several key elements: 1) a description of threats and risks; 2) a link between a vacancy and a company's security subsystem; 3) a process of determining the extent of potential adverse consequences; 4) a process of aligning a job specification with a certain category of risk; 5) a definition of the personnel security criteria.

The first step is a detailed examination of the threats and risks that are potentially associated with the activities of individuals who are to perform a particular professional role. The description of a possible scenario is derived from risk-based forecasting and security breaches that have already occurred prior to the assessment, including examples of damage worldwide. Forecasting effective incident risk scenarios should be completed taken into consideration the following aspects: 1) financial losses; 2) damage or loss of property and goods; 3) reputation damage; 4) information leakage; 5) destruction of property and goods because of arson; 6) intentional accidents at workplace; 7) intentional injury and death; 8) behavior that affects employee morale and overall work environment; 9) espionage; 10) bankruptcy.

The second step is to link threats and risks to a specific security subsystem of an organization mentioned above. For example, a chief accountant who oversees financial reports can significantly affect the economic security of an organization; a refueller can cause any detrimental consequences for the fire safe subsystem; a storekeeper who oversees loss prevention can affect the physical security subsystem, and a system administrator can lead to the issues with the information security subsystem. Occupational fraud is often triggered by the breaches of a certain security subsystem, and a loyal or a dishonest employee can either weaken or strengthen a specific security subsystem by preventing a malicious behavior of other individuals at workplace.

The third step is to determine the extent of a potential detrimental effect that an employee's unlawful or unethical actions in a particular position may carry. Negative impact can be measured using the terms such as "relatively low", "local", "high", and "very high". The latter case refers to an extraordinary scenario when an employee's malicious or negligent activities could lead to a company's physical destruction or bankruptcy. For example, in 1995 one of the oldest London-based investment banks Barings ended its two-hundred-year-old history as a result of fraud carried out by the branch manager Nick Leeson (Rodrigues, 2015). Further to one of the biggest financial scandals in history, Barings suffered losses of $ 1.3 billion and eventually became part of the Dutch bank ING that paid for it £1.00 in 1995 (Ibid).

The fourth step is to formalize the work done to study the potential for danger by aligning each professional position with a certain risk category. We argue that the number of steps should not exceed five categories of risk but it depends on specific circumstances. Following this logic, the top category combines executive and managerial roles that can be a key to organizational security, including cyber security (the C-suite, senior accountant positions, system administrator, and other). The bottom category is comprised of vacancies that carry a minimum degree of risks, including interns, junior staff, employees with no access to information,

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

valuables, cash, and sophisticated equipment. The abovementioned typology ensures standardization of the screening algorithms and could be considered a benchmark for the recruitment managers.

The fifth step consists in determining the personnel security criteria and defining critical values within the selected category. This process is based on the identification of structural elements of organizational deviation (table 1). For example, gaming addiction could be considered as one of the examples of an addictive behavior. It is essential that individuals entrusted with access to cash and financial transactions are not affected by the gaming or gambling addictions. At the same time, this criterion is not that significant for other professional roles, and may not be applied at all. Therefore, as part of the algorithm two aspects have to be identified: the personality and biography aspects required for a background screening check and minimum requirements for a certain job from a security perspective. This approach will result in the formulation of "red flags" used in the screening process. It is crucial to tailor the security considerations to a certain job specification as any background investigations have to be vacancy-specific, and excessively rigid requirements for wrong positions can be ineffective. For example, alcohol addiction could only lead to adverse consequences if individuals operate machinery or tasked with performing surgeries.

The most striking examples of the deficient pre-screening systems are well-documented cases of pilots who have deliberately crashed airlines with passengers. Although pilot suicides are rare, the Aviation Safety Network identifies at least eight situations since 1976 where pilots intentionally crashed planes with unsuspected passengers on board (The Aviation Safety Network, 2013). The most recent case took place in March 2015 with the Germanwings flight. Although his intentions are not clear, it is believed that co-pilot Andreas Lubitz locked the pilot out of the cabin and crashed the airplane in the French Alps killing all 149 people on board (Plumer, 2015). The newly revealed information suggests that Lubitz was suffering from depression and other health concerns and was taking antidepressants (Sims, 2016). He was also scared of being dismissed from his job and was hiding his health history (Ibid). This is one of the examples of a situation when adequate screening technique regarding suicidal ideation was not applied.

4. Steps of the screening process

The next step of creating an algorithm is defining screening techniques linked to the personnel security criteria. Although a number of screening criteria are currently used by either in-house or outsourced recruitment professionals, it is important to understand that all criteria have to flexible enough to be adapted to different vacancies and a certain organizational context. One of the suggested recommendations is to work with candidates' personal documents in the format of cross-analysis of documents. It consists of the following steps: the candidate's biography is analyzed chronologically without any gaps; second, each stage is examined by cross-checking dates and records using all available sources; finally, some gaps will have to be discussed with the candidate specifically. Further to these steps, a decision is made regarding the tactics of working with a candidate.

The background checks are part and parcel of most investigative agencies' services, and they are intended to gather as much information as possible about a certain candidate using open sources, specialized databases and private information. There is a wide range of private sources used in this process, including ex-partners and friends, insights provided by the colleagues, and offender databases used for a criminal due diligence check. Pre-employment screening is meant to be supplemented by this data, including information regarding addictions such as drug abuse. Besides the abovementioned steps, the final evaluation is derived from an in-person interview

Technium Social Sciences Journal
Vol. 9, 577-587, July 2020
ISSN: 2668-7798
www.techniumscience.com

with the recruitment managers that is meant to make a certain judgement regarding a candidate's aptitudes and personality traits.

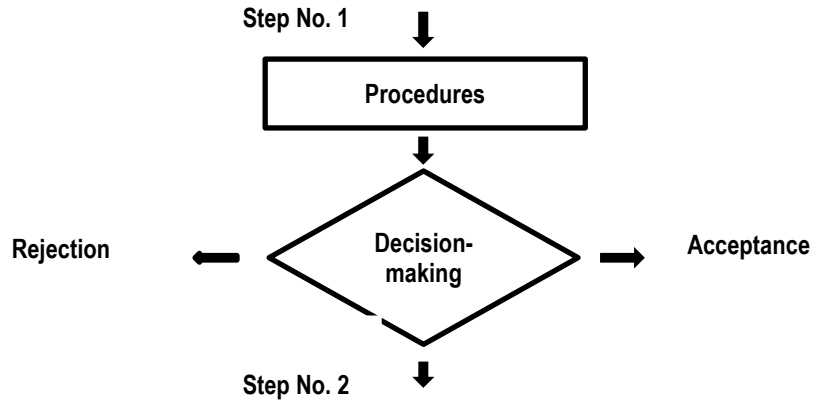
Table 2. Pre-employment screening map

Vacancy _____

Risk category	Main threats	Personnel security criteria	Marginal meanings	Quantity and content of algorithm steps	Screening methods step by step

The abovementioned table helps generating a screening algorithm that consists of a set of clusters, as per picture 1.

Figure 1. Screening algorithm



The procedural segment refers to measures taken to test a candidate's personality traits and biography as per the selected personnel security criteria. It contains techniques and other important aspects such as resources and organizational aspects. The decision-making cluster is composed of the outcomes of the screening processes applied to decide about a candidate's suitability. If necessary, next steps are applied. The algorithm clusters could be either face-to-face or remote depending on the situational context. While it is important this algorithm is applied to all candidates, it might take longer to evaluate an individual's suitability for the managerial and executive positions.

Conclusion

Making uninformed decisions regarding hiring can be quite costly as "risky hires" may affect shareholders, customers, partners, and business interests. Negligent hiring can lead to a wide range of damage, including reputation risks and financial losses. Furthermore, establishing a rigorous and efficient screening process fulfils a company's legal obligations in some jurisdictions. This article suggests a methodology of screening based on the theory of social technologies (or the principle of social engineering). We argue that it is important to follow a consistent pre-employment screening model tailored to specific job groupings as part of the recruitment process. A vacancy-specific model based on the personnel security methodology should be viewed as a standard business practice. It is essential that both risk evaluation and pre-employment assessment of candidates, including background checks, are considered as part and parcel of a systematic and integrated hiring corporate policy aimed at mitigating risks.

References

[1] Albrecht, W.S. and Albrecht, C.O. (2004) Fraud Examination and Prevention. Mason: South-Western Educational.
[2] Benson, M.L., Madensen, T.D. and Eck, J.E. (2009) White-collar crime from an opportunity perspective. In: S.S. Simpson and D. Weisburd (eds.) The Criminology of White-collar Crime. New York: Springer Science+Business Media, pp. 175–193.
[3] Buckhoff. T. (2002). Preventing employee fraud by minimising opportunity. The CPA Journal. Vol. 72, Issue 5. Retrieved from: https://search.proquest.com/openview/aac81b0e171f255d11aab5f5828c02e6/1?pq-origsite=gscholar&cbl=41798
[4] Cavaiola, A. A & Lavender, N. J. (2000). Toxic Coworkers: How to Deal with Dysfunctional People on the Job. Oakland, CA, New Harbinger Publications, Inc.
[5] Centre for the Protection of National Infrastructure (n.d.). Personnel and people security. Retrieved from: https://www.cpni.gov.uk/personnel-and-people-security
[6] Chiang, J. & Berkoff, R. (2017). How are pre-hire assessments contributing to unbiased and more targeted, successful hires? Cornell University. Retrieved from http://digitalcommons.ilr.cornell.edu/student/149
[7] Chumarin, I. (2003). What is personnel security? Personnel of a company. No 2, pp. 34-41. [in Russian] Retrieved from http://www.kapr.ru/articles/2003/2/519.html
[8] Coleman, J.W. (1989) The Criminal Elite: The Sociology of White-collar Crime, 2nd edn. New York: St. Martin.
[9] Coleman, J.W. (2001) The causes of white-collar crime and the validity of explanation in the social sciences. In: S.-A. Lindgren (ed.) White-collar Crime Research: Old Views and Future Potentials. Stockholm: National Council for Crime Prevention, pp. 55–68.
[10] Dukhnovsky, S. (2019). Personnel security of an organisation: Textbook and guidance for bachelor degree. Moscow: Urayt. [in Russian]
[11] Dvorshchenko, V. (2008). A test to diagnose personality disorders. Saint Petersburg: Rech. [in Russian]. Retrieved from: https://www.studmed.ru/dvorschenko-vp-diagnosticheskiy-test-lichnostnyh-rasstroystv_19f0a8d91eb.html
[12] Ford H. (2016). My life and work. Kyiv: Nash Format. [in Ukrainian].
[13] Furnham, A. & Taylor, J. (2004). The Dark Side of Behaviour at Work. Understanding and avoiding employees leaving, thieving and deceiving. Palgrave McMillan.
[14] Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. Decision Support Systems, Issue 4, March. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0167923608002078
[15] Huang, F. & Capelli, P. (2006). Employee Screening: Theory and Practice. National Bureau of Economic Research. Retrieved from: https://www.nber.org/papers/w12071.pdf
[16] Jonason, P., Slomski, S., Partyka, J. (2012). The dark triad at work: How toxic employees get their way. Personality and Individual Differences. Vol. 52, Issue 3. https://www.sciencedirect.com/science/article/abs/pii/S0191886911005150
[17] Koeke, J. (2000). The Market for Corporate Control in Germany: Causes and Consequences in Ultimate Share Ownership. Mannheim: Centre for Economic Research (ZEW), 39.
[18] KPMG Forensic (2014). Fraud Risk Management. Retrieved from: https://assets.kpmg/content/dam/kpmg/pdf/2014/05/fraud-risk-management-strategy-prevention-detection-response-O-201405.pdf

[19] Levi, M. (2008) The Phantom Capitalists: The Organization and Control of Long-firm Fraud, 2nd edn. Aldershot: Ashgate.
[20] Lou, Y.I. and Wang, M.L. (2009) Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting. Journal of Business & Economics Research 7 (2): 61–78.
[21] Meiners, C. (2005). Employee fraud: Detecting and eliminating the unintentional perk. Risk Management. Vol. 52, Issue 4. Retrieved from: https://go.gale.com/ps/anonymous?id=GALE%7CA131609254&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=00355593&p=AONE&sw=w
[22] New Zealand Goverment. (n.d). Protecting our people, information and assets. Retrieved from: https://protectivesecurity.govt.nz/assets/About-PSR-documents/2df0872393/PSR-Introductory-brochure.pdf
[23] Plumer, B. (2015). The disturbing history of pilots who deliberately crash their own plane. Vox. Retrieved from: https://www.vox.com/2015/3/26/8294971/pilot-suicide-crash
[24] Podshivalkina, V. (1997). Social technologies: Methodology and practice problems". Kishinev: Central Typography. [In Russian].
[25] Rodrigues, J. (2015). Barings collapse at 20: How rogue trader Nick Leeson broke the bank. The Guardian. Retrieved from: https://www.theguardian.com/business/from-the-archive-blog/2015/feb/24/nick-leeson-barings-bank-1995-20-archive
[26] Roik, E. (2019). Company Fraud: How to Protect your business. Lawyer & Law, 09. [in Russian]. Retrieved from: https://www.asterslaw.com/ru/press_center/publications/corporate_fraud_how_owners_can_protect_their_business/
[27] Roy, H. & Lubit (2004). Coping with Toxic Managers, Subordinates… and Other Difficult People. Prentice Hall.
[28] Rushchenko, I. (2007). Three Measurements of Skilled Safety. Methodology, Theory and Practice of a Sociological Analysis of the Modern Society, pp. 438-444. Kharkiv, V.N. Karazin Kharkiv National University Publishing House. [in Ukrainian] Retrieved from: http://ir.duan.edu.ua/bitstream/123456789/112/1/Прошин_с_181_184.PDF
[29] Shover, N. and Hochstetler, A. (2006) Choosing White-collar Crime. Cambridge, UK: Cambridge University Press.
[30] Sidak, V., Migus, I. (2012). Personnel security of the agricultural sector: Management of insiders. Cherkasy: Maklaut. [in Ukrainian]. Retrieved from: https://www.academia.edu/35292880/Кадрова_безпека.pdf
[31] Sims, A. (2016). Germwanwings crash: Co-pilot Andreas Lubitz's final email reveals his "depression" and "fear of going blind". The Independent. Retrieved from: https://www.independent.co.uk/news/world/europe/germanwings-crash-co-pilot-andreas-lubitzs-final-email-reveals-depression-and-fear-of-going-blind-a6915736.html
[32] Solomanidin, T. and Solomanidin, V. (2017). Personnel security of a company: Textbook. Moscow: Infra-M. [in Russian]. Retrieved from: https://znanium.com/catalog/product/753429
[33] Templer, K. (2018). Dark personality, job performance ratings, and the role of political skill: An indication of why toxic people may get ahead at work. Personality and Indvidual Differences, Vol. 124. Retrieved from:https://www.sciencedirect.com/science/article/abs/pii/S0191886917306876
[34] The Aviation Safety Network (2015). List of aircraft accidents caused by pilot suicides. Retrieved from: http://news.aviation-safety.net/2013/12/22/list-of-aircraft-accidents-

caused-by-pilot-suicide/

[35] Tsygichko, V.N., Smolyan, G.L. & Solntzseva, G.N. (2016). The Human Factor as a Threat to the Security of Critical Facilitiesm. Sciences of Europe. 1 (1), 60-65, [in Russian]. Retrieved from https://istina.msu.ru/journals/20130889/

[36] Weber, L. & Feintzig, R. (2014). Why companies are taking longer to hire? The Wall Street Journal. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2389.00236

[37] Williams, N. (2005). Pre-hire pregnancy screening in Mexico's maquilladoras: Is it discrimination? 12 Duke J. Gender L. & Pol'y 131. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/djglp12&div=9&id=&page

[38] Zatonatskiy, D. (2019). Innovation Methods and Models of Personnel Security Management: Opportunities and Imperatives of Use at Ukrainian Enterprises. Marketing and Management of Innovations, 1, 294-301. Retrieved from http://doi.org/10.21272/mmi.2019.1-24

[39] Zhivko, Z. (2012). Economic security of a company: Content and mechanism of implementation and management. Lviv: Liga Press. [in Ukrainian] Retrieved from http://dspace.lvduvs.edu.ua/bitstream/1234567890/433/1/Живко%20економ%20безпека%20моногpаф.pdf

[40] Zubko, T. & Laptieva, V. (2018). Indicators of personnel security of an enterprise. Messenger of KNTEU, 4, pp. 57-56. [in Ukrainian] Retrieved from http://visnik.knteu.kiev.ua/files/2018/04/7.pdf