Весці БДПУ. Серыя 1. 2020. № 4. С. 61–65

УДК 372.862:[004.056+159.99]

ТЕХНИЧЕСКИЕ И ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ СОДЕРЖАНИЯ ПОДГОТОВКИ СПЕЦИАЛИСТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. Е. Морозов,
кандидат психологических наук, доцент, заместитель по научно-методической работе директора Института психологии Белорусского государственного педагогического университета имени Максима Танка

Поступила в редакцию 12.10.20.

UDC 372.862:[004.056+159.99]

TECHNICAL AND PSYCHOLOGICAL ASPECTS OF CONTENTS OF TRAINING OF A SPECIALIST IN THE SPHERE OF INFORMATION SECURITY

V. Morozov,
PhD in Psychology, Associate Professor, Vice-Director on Scientific and Methodical Work, Institute of Psychology, Belarusian State Pedagogical University named after Maxim Tank

Received on 12.10.20.

В статье обосновывается необходимость изменения структуры необходимых навыков для специалиста в сфере информационной безопасности (далее – ИБ). Раскрывается специфика современного состояния проблемы инсайдерской деятельности и внутреннего фрода, дается характеристика основных тенденций развития технических систем обеспечения ИБ, подразумевающих анализ поведения пользователей, обсуждается концепция платформы оркестровки безопасности, автоматизации и реагирования. Обосновывается важность всеобъемлющего учета роли человеческого фактора в обеспечении ИБ. Описываются некоторые подходы к использованию оценки поведенческих паттернов в интересах обеспечения ИБ.

Ключевые слова: информационная безопасность, поведенческий анализ, оркестровка безопасности, автоматизация и реагирование, психологические аспекты безопасности, оценка поведенческих паттернов.

The article substantiates the necessity of changing the structure of the necessary skills for a specialist in the sphere of information security (herein after IS). It reveals the specificity of the modern state of the problem of insider activity and internal fraud, gives characteristic to he main tendencies of development of technical systems of maintaining IS which presuppose the analysis of users' behavior, discusses the concept of the platform of security orchestration, automation and reaction. It substantiates the importance of comprehensive account of the role of human factor in maintaining IS. The paper describes some approaches to using the assessment of behavioral patterns in the interests of maintaining IS.

Keywords: information security, behavioral analysis, security orchestration, automation and response, psychological aspects of security, assessment of behavioral patterns.

Введение. Существующая система образования в области информационной безопасности (далее – ИБ) традиционно делает акцент на технической составляющей имеющихся в этой отрасли проблем. В процессе анализа результатов работы профильных учреждений образования Республики Беларусь и Российской Федерации, а также компаний – поставщиков решений в сфере ИБ, связанной с подготовкой специалистов и проведением исследований в области эффективного управления безопасностью сети на основе интеллектуальных подходов и приложений, был получен опыт, показывающий, что сегодня этого уже недостаточно [1]. Изменения тенденций развития всей отрасли ИБ, постоянно растущие количество и спектр угроз, их гетерогенный характер, существенное усложнение структур и подходов к реализации управления ИБ в различных условиях привели не просто к нехватке необходимых навыков у профильных специалистов, но и к необходимости существенного пересмотра их структуры. По причинам, которые будут подробно рассмотрены ниже, в содержание обучения современных ИБ-специалистов следует включить компоненты, позволяющие сформировать навыки оценки поведенческих паттернов пользователей в интересах обеспечения ИБ, а также навыки использования специализированного программного обеспечения (далее – ПО).

Краткий обзор сопутствующих работ. Аналитики одной из ведущих мировых исследовательских и консалтинговых компаний в области информационных технологий (далее – ИТ), компании Gartner, говоря о современных трендах развития средств обеспечения ИБ, подчеркивают, что технологии поведенческого анализа (UEBA/UBA) в настоящее время интенсивно развиваются, становятся все более надежными и ценными, а также более широко применяются в организациях, устремленных в будущее. Отражением указанных процессов является и то, что вендоры, ранее ориентированные на разработку UEBA/UBA-решений «в чистом виде», переходят на соседние рынки, предлагая дополнительный функционал с целью замены устаревших инструментов [2]. Возможности UEBA/UBA применяются в ряде технологий безопасности, таких как SIEM, IDPS, DCAP, CASB, IAM и EDR. Большое число новых компаний-разработчиков, например, Bay Dynamics, ClickSecurity, GuruCul, Fortscale и Securonix, стремятся использовать техники анализа больших данных, чтобы быстро оценить производительность среды передачи данных и обнаружить аномалии, указывающие на атаки. В то же время поставщики, уже давно присутствующие на рынке (например, Lancope, Solera и Splunk), расширяют свои пакеты, чтобы предоставить аналогичные возможности [3].

Таким образом, можно констатировать значительную конвергенцию указанных типов систем. Более того, о несомненном усилении взаимопроникновения различных подходов и концепций обеспечения ИБ в направлении автоматизации управления соответствующими процессами свидетельствует возникновение идеи SOAR [4; 5].

В свою очередь, чтобы расширить возможности управления безопасностью сети в рамках одной организации, углубить свои знания в области вычислительной среды, а также обеспечить в должной мере учет человеческого фактора, целесообразно объединить преимущества UEBA/UBA, SIEM и SOAR, включая их уникальный инструментарий и методики, с наработками в области прогнозирования склонности работника к совершению нарушений безопасности на основе анализа его психологических характеристик. Исследования в этой области только начались, но уже имеется определенный опыт создания соответствующих модулей заметными игроками на рынке систем ИБ [6].

Отмеченное выше значительное усложнение средств обеспечения ИБ диктует изменение подходов и к профильному образованию. О необходимости серьезной работы по лабораторной поддержке обучения сегодня говорят повсеместно. Здесь следует сослаться лишь на основоположников данной тенденции [7; 8], работы которых предоставляют полезные инструкции по проектированию лабораторий и разработке образовательного процесса на их основе. Также следует отметить публикации, демонстрирующие, каким образом можно эффективно использовать технологии виртуализации в образовательном процессе [9].

Современное состояние проблемы инсайдерской деятельности и внутреннего фрода. Проблемы, связанные с наличием в организациях инсайдерской деятельности и разного рода внутренних злоупотреблений, нельзя назвать новыми. Тем не менее в эпоху глобального распространения ИТ, характеризующейся прежде всего переходом основных активов из физической в информационную форму, любой, даже легитимный доступ к этому активу, несет в себе риск. Сегодня инсайдер все чаще оказывается не злоумышленником, осознанно преступающим черту законности, а просто человеком, не вполне понимающим, где именно эта черта проходит. В результате обозначенные выше проблемы только усугубляются. Похожая неоднозначность сохраняется и в ситуации с внутренним фродом. Перевод всех бизнес-процессов на цифровую основу, повсеместное внедрение электронного делопроизводства создает (и в ряде случае множит) возможности эксплуатировать несовершенство соответствующих систем и процедур. Оказывается, что уже не нужно обладать специальными знаниями и компетенциями, чтобы заниматься технологическим мошенничеством – организация сама предоставляет все необходимые права и возможности своим сотрудникам. Модифицированные отчеты, цифры в CRM, не соответствующие действительности, сторнированные счета, – это далеко не полный перечень того, что под силу среднестатистическому работнику. При этом ему не нужно ломать систему защиты, писать вредоносный код, внедрять backdoor, изобретательно преодолевая периметр. Ему нужно лишь осознать тот факт, что предоставленные ему права и возможности можно использовать и в своих личных целях, которые не обязательно должны совпадать с целями организации. Хрестоматийным примером такого рода является предоставление работником компании-продавца дополнительной, сравнительно небольшой скидки клиенту в обмен на «ответную любезность» с его стороны. В каждой отдельно взятой ситуации потери могут быть и невелики, однако ввиду многочисленности подобных случаев суммарные потери могут значительно превысить урон, наносимый «традиционными» хищениями, совершаемыми из-за пределов периметра. Неудивительно, что в подобной ситуации психологические факторы превращаются в столь же значимые аспекты ИБ, как и технические.

Для работника службы ИБ это означает, что помимо всего прочего он должен хорошо понимать мотивы людей, соотносить их с целями бизнеса, четко представлять «границы дозволенного» для работника в юридической, финансовой, коммуникативной сферах. Разумеется, подобные требования декларировались и раньше, но сейчас их соблюдение для многих компаний превратилось в жизненную необходимость [10]. Имеющийся опыт обучения ИБ-специалистов показывает, что наилучших результатов удается добиться путем широкого использования кейсов, включающих подробное рассмотрение существующих мошеннических схем и примеров удачного реагирования на соответствующие инциденты.

Развитие технических систем: UEBA/UBA, SIEM и SOAR. Все появившиеся в последние годы концепции обеспечения ИБ и соответствующие им типы информационных систем в гораздо большей степени учитывают роль человеческого фактора нежели это было раньше. К примеру, системы анализа поведения пользователей UEBA/UBA представляют собой решения, которые занимаются сбором и анализом всех действий пользователей с целью определения внутренних угроз, атак, финансового мошенничества и реализуют свое предназначение путем выявления фактов компрометации учетных записей, злоупотребления правами привилегированных учетных записей, предотвращения утечки конфиденциальной

информации, обнаружения подозрительного времени подключения, обнаружения попыток совместного использования учетных записей, выявления ошибок настройки прав доступа и других подобных вещей. С технической точки зрения UEBA/UBA-системы чаще всего выступают расширениями существующих SIEM-систем (например, HPE ArcSight UBA или IBM QRadar UBA), либо имеют возможность тесной интеграции с «материнской» SIEM-платформой (Splunk UBA).

Вторым вариантом, в большей степени соответствующем идеологии UBA, является интеграция функций поведенческого анализа в структуру систем обеспечения ИБ, ориентированных прежде всего на контроль пользователей и построенных вокруг DLP- и PUM-систем [2]. Несмотря на то что многие аналитики предрекают значительное сокращение в ближайшие годы ассортимента отдельных UEBA/UBA-систем (в первую очередь за счет поглощения самостоятельных вендоров более крупными компаниями), соответствующий функционал свою актуальность не потеряет.

Нетрудно заметить, что развитие многих систем ИБ идет по пути сбора все больших объемов данных о пользователях и совершенствования автоматизации этих процессов. В то же время управление ИБ не заканчивается на этапе обнаружении угроз: на угрозы нужно адекватным образом реагировать. Дальнейшее развитие концепции SIEM в направлении автоматизации различных сценариев привело к возникновению идеи SOAR (в 2017 году компания Gartner ввела термин «оркестровка безопасности, автоматизация и реагирование» для описания новой категории платформ, основанных на реагировании на инциденты, автоматизации безопасности, управлении делами и другими инструментами безопасности) [4]. В зависимости от того, что лежит в основе подобной системы, эта аббревиатура может нести различный смысл: либо «действия по обеспечению безопасности, аналитика и отчетность» – Security Operations, Analytics and Reporting (SOAR), либо «оркестровка событий безопасности и автоматическое реагирование» – Security Orchestration and Automated Response (SOAR).

Оркестровка безопасности интегрирует наиболее эффективным образом людей, процессы и технологии для укрепления безопасности организации. Это подразумевает оптимизацию процессов обеспечения ИБ, соединение разрозненных средств и технологий безопасности и поддержание правильного баланса автоматизации и вмешательства человека. Оркестровка безопасности позволяет профессионалам в области ИБ эффективно и результативно выполнять операции безопасности и реагировать на инциденты.

В отрасли принято использовать понятия «оркестровка безопасности» и «автоматизация безопасности» как синонимичные, но, строго говоря, эти термины не совпадают. Автоматизация безопасности заставляет машины целенаправленно выполнять «человеческую работу». Система обеспечения ИБ объединяет различные продукты (как защищенные, так и не связанные с безопасностью) друг с другом и автоматизирует распределение задач между продуктами с помощью рабочих процессов, а также обеспечивает контроль и взаимодействие с конечным пользователем. Таким образом, автоматизация безопасности – это часть оркестровки безопасности. Оркестровка безопасности включает в себя сочетание людей, процессов и технологий для улучшения состояния безопасности организации.

SOAR является специализированным средством для обобщения сведений об угрозах ИБ, поступающих из различных источников, и последующего анализа этих данных. К числу основных функций, реализуемых SOAR-системами относятся: оркестровка – интеграция технологий, потребных для принятия решений, относящихся к сфере ИБ и базирующихся на полученных сведениях о состоянии системы безопасности и показателях рисков; автоматизация процессов; управление инцидентами ИБ – назначение приоритетов, протоколирование действий, принятие решений в соответствии с политикой компании; управление делами – визуализация данных и формирование отчетности (несмотря на то, что это не совсем функция оркестровки и автоматизации, управление делами является важной частью процесса реагирования на инциденты и выступает еще одной функцией, которую SOAR может помочь упростить. Многие организации борются с огромным количеством разнородной информации, которая собирается во время инцидента ИБ. Электронных таблиц и общих документов просто недостаточно для управления сложным кибер-инцидентом).

Основным преимуществом SOAR является высокий уровень автоматизации процессов управления ИБ, начиная от выставления приоритетов и заканчивая реакцией на зафиксированные инциденты. По мере развития платформ SOAR пользователям требуется все меньше опыта. Поставщики внедряют в свои продукты (экспертные знания в области ИБ) в виде готовых сценариев, управляемых рабочих процессов расследования и автоматического определения приоритетов предупреждений. К примеру, оповещения о потенциально вредоносном трафике являются обычным явлением и часто находятся в очереди в течение некоторого времени, прежде чем их исследуют. Хотя большинство из них являются ложными срабатываниями или имеют низкий приоритет, любое из них может быть единственным индикатором потенциально серьезного нарушения данных. SOAR позволяет мгновенно

обрабатывать и практически сразу же реагировать на каждое из этих предупреждений, автоматизируя повседневные повторяющиеся процессы, позволяя аналитикам сосредоточиться на наиболее значимых предупреждениях.

В структуру SOAR, как правило, включают три основных модуля [5].

Первый из них – Security Incident Response – обеспечивает импорт данных из применяемых решений и упрощает идентификацию инцидентов.

Для расстановки приоритетов уязвимостей используется модуль Vulnerability Response, который помогает определять подверженность угрозам для бизнес-подсистем, имеющих критическое значение. В то же время следует иметь в виду, что SOAR не задумывалась как платформа управления уязвимостями и никогда не заменит специализированные системы управления уязвимостями. Однако некоторые аспекты процессов управления уязвимостями SOAR может упростить. На крупных предприятиях управление уязвимостями часто является задачей, выполняемой вне службы безопасности. Это может привести к потенциальному риску, так как ИБ-специалисты могут не знать о тех или иных уязвимостях, существующих в инфраструктуре. В этом случае SOAR может использоваться для обеспечения того, чтобы служба безопасности была осведомлена о любых новых уязвимостях в организации. Это позволяет ИБ-специалистам заранее исследовать уязвимый хост, когда это уместно, чтобы убедиться, что нет никаких доказательств эксплуатации уязвимости, установить любые соответствующие дополнительные меры безопасности и подвергать хост усиленному мониторингу до тех пор, пока уязвимость не будет устранена. Помимо уведомления группы безопасности SOAR-решение также может использоваться для дальнейшего обогащения информации об уязвимостях и хосте. Например, для пополнения базы данных уязвимостей путем сбора дополнительной информации об уязвимости, опроса Active Directory или CMDB для получения информации об активах или опроса SIEM или EDR о событиях безопасности. На основании информации об уязвимости, хосте или событии, случай может быть автоматически обновлен или переназначен, или хост может быть даже временно изолирован до тех пор, пока не будут выполнены соответствующие мероприятия по устранению либо смягчению угрозы [5].

Третий модуль Threat Intelligence необходим для обнаружения индикаторов возможной компрометации и отслеживания угроз на глубоких уровнях. Его преимуществом является поддержка разных стандартов, обмена сведениями о предполагаемых рисках со сторонними системами.

Несомненно, SOAR – все еще относительно новая, не вполне устоявшаяся категория в ИБ. Автоматизация и оркестровка пока еще не превратились в незаменимые инструменты, но рано или поздно это произойдет, причем с большой вероятностью нынешние подходы будут дополнены на многих платформах машинным обучением, искусственным интеллектом и другими появляющимися технологиями. Именно SOAR может стать основой для следующего поколения SOC/SIC.

Что же касается образования в области ИБ, то задача формирования у обучаемых навыков работы с описанными системами может быть решена путем внедрения развитой лабораторной поддержки учебного процесса. Поскольку в лабораторных условиях достаточно сложно воспроизвести необходимую инфраструктуру, особая роль, с нашей точки зрения, здесь должна принадлежать технологиям виртуализации. Эти технологии очень полезны, так как имеют необходимые инструменты для построения сложных виртуальных сетей на виртуальных машинах и позволяют продемонстрировать необходимые функциональные возможности соответствующих систем различного масштаба.*

* Продолжение статьи будет опубликовано в научно-методическом журнале «Весці БДПУ. Серыя 1. Педагогіка. Псіхалогія. Філалогія» № 1, 2021.

Литература

1. *Морозов, В. Е.* Внедрение в содержание обучения специалистов в области информационной безопасности вопросов практического применения DLP-систем / В. Е. Морозов, А. В. Дрозд // Научно-практический журнал «Информационное противодействие угрозам терроризма». Материалы XIX пленума учебно-методического объединения по образованию в области информационной безопасности. Опыт и передовые практики образовательных организаций по формированию и использованию в учебном процессе специализированной учебно-лабораторной базы. – 2015. – № 25, том 1. – С. 277–285.
2. Computer Business Review [Electronic resource]: Market Guide for User and Entity Behavior Analytics. – Mode of access: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2018/07/gartner-market-guide-for-ueba-2018-analyst-report.pdf. – Date of access: 10.10.2020.

References

1. *Morozov, V. E.* Vnedrenie v soderzhanie obucheniya specialistov v oblasti informacionnoj bezopasnosti voprosov prakticheskogo primeneniya DLP-sistem / V. E. Morozov, A. V. Drozd // Nauchno-prakticheskij zhurnal «Informacionnoe protivodejstvie ugrozam terrorizma». Materialy XIX plenuma uchebno-metodicheskogo ob"edineniya po obrazovaniyu v oblasti informacionnoj bezopasnosti. Opyt i peredovye praktiki obrazovatel'nyh organizacij po formirovaniyu i ispol'zovaniyu v uchebnom processe specializirovannoj uchebno-laboratornoj bazy. – 2015. – № 25, tom 1. – S. 277–285. itie individual'nogo stilya pedagogicheskoj deyatel'nosti v kontekste global'nogo obrazovaniya / V. M. Danil'chenko // Polemika. – 2011. – № 15. – S. 1–7.
2. Computer Business Review [Electronic resource]: Market Guide for User and Entity Behavior Analytics. – Mode of access: https://www.cbronline.com/wp-content/uploads/dlm_

3. *Johnson, J. T.* User behavioral analytics tools can thwart security attacks / J. T. Johnson // SearchSecurity [Electronic resource]: – Mode of access: https://searchsecurity.techtarget.com/feature/User-behavioral-analytics-tools-can-thwart-security-attacks/. – Date of access: 10.10.2020.
4. *Engelbrecht, S.* The Evolution of SOAR Platforms / S. Engelbrecht // SecurityWeek [Electronic resource]: – Mode of access: https://www.securityweek.com/evolution-soar-platforms. – Date of access: 10.10.2020.
5. *Moran, J.* 5 Common Security Orchestration, Automation and Response (SOAR) Use Cases / J. Moran // DFLabs [Electronic resource]: – Mode of access: https://www.dflabs.com/blog/5-common-security-orchestration-automation-and-response-soar-use-cases. – Date of access: 10.10.2020.
6. ProfileCenter SearchInform [Electronic resource]. – Mode of access: https://searchinform.ru/products/kib/profilecenter/. – Date of access: 10.10.2020.
7. *White, G. B.* Developing an Undergraduate Lab for Information Warfare and Computer Security / G. B. White, R. E. Sward // Proceeding of the IFIP TC11 WG11.8 First World Conference on Information Security Education, Kista, Sweden, 17–19 June 1999. – P. 163–170.
8. *Hoffman, L. J.* Information assurance laboratory innovations / L. J. Hoffman [et al.] // Proceedings of the 7th Colloquium for Information Systems Security Education. – Washington, DC, USA, 2003.
9. *Dodge, R. C.* Using Virtualization to Create and Deploy Computer Security Lab Exercises / R.C. Dodge, B. Hay, K. Nance // Proceeding of 6th World Conference on Information Security Education (WISE6). IFIP. – Vol. 278. January 2010.
10. DZone [Electronic resource]: Cybersecurity Resilience and Best Practices for Fraud Prevention. – Mode of access: https://dzone.com/articles/cybersecurity-resilience-and-best-practices-for-fr. – Date of access: 10.10.2020.
11. 2010/2011 CSI Computer Crime and Security Survey [Electronic resource]: – Mode of access: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf. – Date of access: 10.10.2020.
12. *Стрижов, Е. Ю.* Нравственно-психологические детерминанты мошенничества: дис. … д-ра психол. наук: 19.00.06 / Е. Ю. Стрижов. – М., 2011. – 400 л.
13. *Albrecht, W. S.* Fraud: Bringing Light to the Dark Side of Business / W. S. Albrecht, T. L. Williams, G. W. Wernz. – IL: Irwin, 1995. – 296 p.
14. *Пиаже, Ж.* Моральное суждение у ребенка / Ж. Пиаже. – М. : Академический Проект, 2006. – 480 с.
15. *Kohlberg, L.* Moral stages: a current formulation and a response to critics / L Kohlberg, C. Levine, Al. Hewer. – S Karger Ag, 1984. – 180 p.
16. *Tapp, J. L.* The dialectic of legal socialization in community and school / J. L. Tapp, F. J. Levine // Justice, and the Individual in Society: Psychological and Legal Issues. – New York : Holt, Rinehart. – 1977. – P. 163–182.
17. *Никитина, Н. Ш.* Методика отбора персонала на вакансию на основе нечетких показателей / Н. Ш. Никитина, Е. В. Бурмистрова // Университетское управление: практика и анализ. – 2004. – № 3(31). – С. 98–103.
18. *Войскунский, А. Е.* Информационная безопасность: психологические аспекты / А. Е. Войскунский // Национальный психологический журнал. – 2010. – № 1(3). – С. 48–53.

uploads/2018/07/gartner-market-guide-for-ueba-2018-analyst-report.pdf. – Date of access: 10.10.2020.
3. *Johnson, J. T.* User behavioral analytics tools can thwart security attacks / J. T. Johnson // SearchSecurity [Electronic resource]: – Mode of access: https://searchsecurity.techtarget.com/feature/User-behavioral-analytics-tools-can-thwart-security-attacks/. – Date of access: 10.10.2020.
4. *Engelbrecht, S.* The Evolution of SOAR Platforms / S. Engelbrecht // SecurityWeek [Electronic resource]: – Mode of access: https://www.securityweek.com/evolution-soar-platforms. – Date of access: 10.10.2020.
5. *Moran, J.* 5 Common Security Orchestration, Automation and Response (SOAR) Use Cases / J. Moran // DFLabs [Electronic resource]: – Mode of access: https://www.dflabs.com/blog/5-common-security-orchestration-automation-and-response-soar-use-cases. – Date of access: 10.10.2020.
6. ProfileCenter SearchInform [Electronic resource]. – Mode of access: https://searchinform.ru/products/kib/profilecenter/. – Date of access: 10.10.2020.
7. *White, G. B.* Developing an Undergraduate Lab for Information Warfare and Computer Security / G. B. White, R. E. Sward // Proceeding of the IFIP TC11 WG11.8 First World Conference on Information Security Education, Kista, Sweden, 17–19 June 1999. – P. 163–170.
8. *Hoffman, L. J.* Information assurance laboratory innovations / L. J. Hoffman [et al.] // Proceedings of the 7th Colloquium for Information Systems Security Education. – Washington, DC, USA, 2003.
9. *Dodge, R. C.* Using Virtualization to Create and Deploy Computer Security Lab Exercises / R.C. Dodge, B. Hay, K. Nance // Proceeding of 6th World Conference on Information Security Education (WISE6). IFIP. – Vol. 278. January 2010.
10. DZone [Electronic resource]: Cybersecurity Resilience and Best Practices for Fraud Prevention. – Mode of access: https://dzone.com/articles/cybersecurity-resilience-and-best-practices-for-fr. – Date of access: 10.10.2020.
11. 2010/2011 CSI Computer Crime and Security Survey [Electronic resource]: – Mode of access: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf. – Date of access: 10.10.2020.
12. *Strizhov, E. Yu.* Nravstvenno-psihologicheskie determinanty moshennichestva: dis. … d-ra psihol. nauk: 19.00.06 / E. Yu. Strizhov. – M., 2011. – 400 l.
13. *Albrecht, W. S.* Fraud: Bringing Light to the Dark Side of Business / W. S. Albrecht, T. L. Williams, G. W. Wernz. – IL: Irwin, 1995. – 296 p.
14. *Piazhe, Zh.* Moral'noe suzhdenie u rebenka / Zh. Piazhe. – M. : Akademicheskij Proekt, 2006. – 480 s.
15. *Kohlberg, L.* Moral stages: a current formulation and a response to critics / L Kohlberg, C. Levine, Al. Hewer. – S Karger Ag, 1984. – 180 p.
16. *Tapp, J. L.* The dialectic of legal socialization in community and school / J. L. Tapp, F. J. Levine // Justice, and the Individual in Society: Psychological and Legal Issues. – New York : Holt, Rinehart. – 1977. – P. 163–182.
17. *Nikitina, N. Sh.* Metodika otbora personala na vakansiyu na osnove nechetkih pokazatelej / N. Sh. Nikitina, E. V. Burmistrova // Universitetskoe upravlenie: praktika i analiz. – 2004. – № 3(31). – S. 98–103.
18. *Vojskunskij, A. E.* Informacionnaya bezopasnost': psihologicheskie aspekty / A. E. Vojskunskij // Nacional'nyj psihologicheskij zhurnal. – 2010. – № 1(3). – S. 48–53.