DOI 10.24411/2686-9764-2020-00022
УДК 377:378.046.4

Встроенное обучение как элемент непрерывного обучения информационной безопасности

А. В. ВИЛКОВА – заместитель начальника Научно-исследовательского института ФСИН России, доктор педагогических наук, доцент;

В. М. ЛИТВИШКОВ – старший научный сотрудник Научно-исследовательского института ФСИН России, доктор педагогических наук, профессор;

Б. А. ШВЫРЕВ – ведущий научный сотрудник Научно-исследовательского института ФСИН России, кандидат физико-математических наук

Реферат

Обучение информационной безопасности сотрудников, не имеющих базовых представлений, является трудоемким процессом. Направленные на обучение сотрудники обычно рассматривают компьютерную безопасность как чью-то проблему, не связанную с ними, абстрагированы от нее и в принципе не понимают своего влияния на компьютерную безопасность организации в целом. Повышение эффективности обучения персонала без отрыва от выполнения должностных обязанностей является актуальной современной задачей. В статье авторы приводят результаты исследования эффективности использования встроенного электронного обучения по программам повышения квалификации, реализующего непрерывное обучение.

Встроенное обучение рассматривается на примере защиты от фишинговых атак. В настоящее время фишинг стал одной из самых распространенных угроз информационной безопасности.

Авторы отмечают, что участники, просмотревшие обучающий ролик, значительно лучше распознавали фишинговые электронные письма, чем те, которые знакомились с инструкцией.

Представленные в работе результаты свидетельствуют о том, что встроенное обучение способствует получению знаний, их сохранению и передаче. Это позволяет эффективно выявлять фишинговые сообщения без неверной идентификации законных сообщений. Участники встроенного обучения научились эффективно обнаруживать электронные письма фишинг-аккаунта.

Для измерения остаточных знаний было проведено сравнение эффективности фишинг-аккаунта и законных электронных писем до обучения, сразу по его окончании и спустя неделю. Полученные результаты показывают, что участники встроенного обучения смогли сохранить полученные знания и использовать их для распознавания фишинговых и легитимных сообщений даже после недельного интервала, в то время как участники в других группах не улучшили свои результаты.

Показано, что метод встроенного обучения является важным фактором, определяющим эффективность антифишинговой подготовки.

Ключевые слова: встроенное обучение; обучение персонала без отрыва от выполнения должностных обязанностей; информационная безопасность; фишинг; антифишинговая подготовка; оценка обучения.

13.00.01 – Общая педагогика, история педагогики и образования

Integrated training as an element of extended learning of information security

A. V. VILKOVA – Deputy Head of the Research Institute of the Federal Penal Service of Russia, Dsc. in Pedagogy, Associate Professor;

V. M. LITVISHKOV – Senior Researcher of the Research Institute of the Federal Penal Service of Russia, Dsc. in Pedagogy, Professor;

B. A. SHVYREV – Leading Researcher of the Research Institute of the Federal Penal Service of Russia, PhD. in Physics and Mathematics

Abstract

Training information security for employees who do not have a basic understanding is a laborious process. Employees who are sent for training usually consider computer security as someone else's problem that is not related to them, abstracted from it and, in principle, do not understand their impact on the computer security of the organization as a whole. Improving the effectiveness of staff training on the job is an urgent modern task. In the article the authors present the results of a study on the effectiveness of using integrated training for advanced training programs that implement extended education. Integrated training is considered on the example of training in protection against phishing attacks. Phishing has now become one of the most common threats for information security.

The authors note that participants who watched the video recognized phishing emails much better than those who familiarized themselves with the instructions.

The results presented in the article indicate that the integrated learning contributes to the acquisition of knowledge, its preservation and transmission, what allows to effectively identify phishing messages without incorrect identification of legitimate messages and the participants in the integrated training have learned to efficiently detect phishing account emails.

To measure the residual knowledge a comparison was made between the effectiveness of a phishing account and legitimate emails before training, immediately after graduation and after a week. The results show that participants in the integrated training were able to save the knowledge and use it in order to recognize phishing and legitimate messages even after a weekly interval, while participants in other groups did not improve their results.

It is shown that the training method is an important factor determining the effectiveness of antiphishing training.

Key words: integrated training; staff training on the job; information security; phishing; anti-phishing training; learning assessment.

13.00.01 – General pedagogy, history of pedagogy and education

Процесс обучения сотрудников информационной безопасности при отсутствии у последних базовых представлений о ней затруднителен [1]. Неопытные, не знакомые с основными концепциями компьютерной безопасности и не имеющие мотивации сотрудники тратят время на обучение в пустую, не осваивая в итоге учебный курс и не выполняя должностные обязанности [3]. Направленные на обучение сотрудники обычно рассматривают информационную безопасность как чью-то проблему, не связанную с ними, абстрагированы от нее и не понимают своего влияния на информационную безопасность организации в целом [12]. Чтобы обучение сотрудников информационной безопасности было эффективным, занятия должны быть и понятными, и убедительными, проводиться таким образом, чтобы привлекать внимание людей, мотивировать их к самостоятельному изучению материала и появлению интереса к проблеме.

Фишинговые атаки по-прежнему остаются распространенной и актуальной угрозой информационной безопасности [2] как корпоративных сетей, так и автоматизированных систем управления технологическими процессами и в России, и в зарубежных странах [4; 5; 6; 7; 8; 9; 10; 11]. При этом типе атак используются приемы социальной инженерии – осуществляется рассылка электронных писем, содержащих ссылку на вредоносный сайт для инфицирования информационной системы или вовлечения жертвы в интерактивный обмен данными для извлечения имени и пароля от личной электронной почты, банковской карты и т. д.

По большей части информационные электронные сообщения, отправляемые сотрудникам или клиентам службами безопасности компании, неэффективны, потому что адресаты редко читают эти сообщения. Организаторы фишинговых атак используют приемы и способы создания сообщений электронной почты, которые заставляют людей открывать их, читать и переходить по указанным ссылкам.

Таким образом, актуальным является процесс обучения сотрудников без первоначальных знаний информационной безопасности и защите от фишинговой атаки, самой распространенной в настоящее время.

Один из способов сделать обучение более привлекательным и актуальным заключается в том, чтобы интегрировать обучение непосредственно в профессиональную деятельность сотрудников. Таким образом, разрабатывается встроенная система обучения, которая учит пользователей избегать фишинговых атак.

Подразделение организации, ответственное за обучение персонала, отправляет электронные письма, имитирующие вредоносные фишинговые. В указанных отправлениях доставляется встроенное обучающее сообщение, когда пользователь попадает в цепь событий фишинговой атаки и нажимает на смоделированный фишинговый URL-адрес. Обучающийся получает предупреждение и разъяснение возможных последствий, после чего знакомится с учебным материалом, представленным в виде лаконичного и привлекательного мультфильма (анимированные персонажи в краткой и доступной форме излагают учебные материалы), в котором представлено определение фишинговой атаки, указан алгоритм, следуя которому можно избежать фишинговых атак. В анимационном фильме также показано, как легко преступникам совершать представленные атаки.

Существуют три варианта обучению антифишингу: 1) электронные ресурсы с мультипликационным фильмом; 2) обучающий тест с элементами инфографики; 3) инструкция о противодействии фишингу.

Для оценки эффективности встроенного обучения в Краснодарском государственном технологическом университете была проведена статистическая серия лабораторных и реальных исследований среди первокурсников непрофильных специальностей. Высказывалась гипотеза об эффективности обучения антифишингу посредством встроенных учебных мультипликационных фильмов, в отличие от двух других способов обучения по электронной почте.

В исследованиях принимали участие 60 чел., не имеющих представления об информационной безопасности. Результаты исследования кратко представлены ниже.

Оценка способа обучения антифишингу

	Мультипликационный ролик	Обучающий тест	Уведомления о состоянии безопасности
Участники, попавшие на фишинг-аккаунт e-mail перед тренировкой	100 %	80 %	90 %
Участники, попавшие на фишинг-аккаунт e-mail после обучения	30 %	70 %	90 %
Среднее время, затраченное на чтение учебных материалов	90 с	78 с	11 с

Получение знаний рассматривалось с учетом того, нажимали ли пользователи ссылки в законных и фишинговых письмах до и после обучения. Из результатов видно, что статистически значимые различия в приобретении знаний между тремя способами обучения заметны при использовании мультипликационного ролика. Несмотря на то, что объем учебной информации, содержащейся в ролике, значительно уступает другим вариантам, ее усвоение по сравнению с другими формами подачи материала будет опережающим. Использование зрительных ассоциативных образов в 90-секундном мультипликационном ролике способствует наиболее эффективному приобретению знаний, даже с учетом наибольшего затраченного в тесте периода времени (чтение учебных материалов об осведомленности в отношении фишинговых атак в виде инструкции, составило 11 с, обучающего теста/инфографики – 78 с, комиксов – 90 с).

При использовании инструкции в качестве источника знаний об информационной безопасности 90 % участников обращались к электронной почте с фишинговым аккаунтом до начала обучения. Ранее по его окончании улучшения ситуации не отмечалось. Участники, которые видели уведомления об информационной безопасности, отметили, что их прочтение заняло слишком много времени и при этом содержание сообщений оставалось до конца не понятным.

Просмотревшие ролик значительно лучше распознавали фишинговые электронные письма, чем те участники, которые знакомились с инструкцией. Информирование в виде обучающего теста и инфографики более результативно, чем при ознакомлении с инструкцией по противодействию фишинговой атаке, но полученная разница не была значительной: до обучения члены группы в 80 % случаев переходили по фишинг-ссылкам в полученных электронных письмах, после обучения – в 70 %, однако это нельзя считать статистически значимым. В случае использования мультипликационного ролика при моделировании фишинговой атаки все участники перешли по ссылке, после просмотра контента и прохождения обучения только 30 % участников при получении повторного фишингового письма в процессе тренинга на личную электронную почту перешли по указанной в нем ссылке. Переход участников исследования по ссылке в тренировочном фишинговом письме позволил четко отследить время освоения обучающего материала и количество переходов при повторной отправке фишингового письма.

Таким образом, существующая практика отправки уведомлений об информационной безопасности по электронной почте неэффективна, поскольку сотрудники не хотят тратить время на ознакомление с ней. При определении приоритетных форм обучения большое значение имеют возрастная группа, национальная культура и менталитет. Востребованность мультипликационных материалов в данном случае имеет ярко выраженную возрастную обусловленность. Отмечается низкая эффективность текстовой информации, чуть выше эффективность материала с элементами инфографики. Стоит отметить важность визуализации подаваемой информации, по крайней мере для обучения молодежи по программам высшего образования. Популярность мультипликационного фильма определяется правильно подобранным составом популярных в молодежной среде персонажей, вызывающих симпатии целевой аудитории. Осознание участниками того, что они подверглись учебной фишинговой атаке, мотивировало их на ознакомление с учебными материалами.

Для оценки качества остаточных знаний и способности транслирования полученных знаний у лиц, прошедших встроенное электронное обучение, проводились исследования, где использовалась модель фишинговой атаки. Были определены четыре группы пользователей: 1) прошедшие встроенное обучение; 2) получившие невстроенное обучение; 3) осведомленные об угрозе; 4) не участвовавшие в образовательном процессе – контрольная группа. Участники группы встроенного обучения получили имитированное фишинговое письмо, посмотрели короткий обучающий антифишингу мультфильм, когда нажали на ссылку, содержащуюся в электронном письме. Участники невстроенного обучения получили тот же обучающий мультфильм на электронную почту, но без поддельной имитации фишинговой ссылки. Третья группа была осведомлена о существовании угрозы фишинговой атаки, для этого ее участникам на электронную почту было отправлено короткое электронное письмо от «друга», который упоминает фишинг, не предоставляя никакой информации о том, как обнаружить угрозу и защититься от нее. Участники контрольной группы также получили электронное письмо от «друга», но не прошли обучение и не были осведомлены.

Исследование проводилось в два этапа с интервалом в семь дней. На первом этапе участники увидели 36 электронных писем в папке «Входящие»: 12 электронных писем с

обучающим материалом и 24 дополнительных электронных письма. На втором этапе участники получили еще 15 писем.

Представленные в работе результаты свидетельствуют о том, что встроенное обучение способствует получению знаний, их сохранению и передаче. Это позволяет эффективно выявлять фишинговые сообщения без неверной идентификации законных сообщений, научиться участникам эффективно обнаруживать электронные письма фишинг-аккаунта. Хотя они не не продемонстрировали значительных различий в умении правильной идентификации электронных писем фишинг-аккаунта до начала тренинга, однако работали гораздо лучше по сравнению с участниками других групп сразу после обучения. Это может быть отчасти связано с тем, что участники встроенного обучения были мотивированы тратить в два раза больше времени на просмотр и чтение мультфильма, чем те, кто находился на невстроенном обучении. Участники встроенного обучения тратили в среднем 77 с на просмотр мультфильма, а участники невстроенного обучения – порядка 27 с.

Чтобы измерить остаточные знания, было проведено сравнение эффективности фишинг-аккаунта и законных электронных писем до обучения, сразу по его окончании и через неделю. В результате участники встроенного обучения смогли сохранить полученные знания и использовать их для распознавания фишинговых и легитимных сообщений даже после недельного интервала, значительно улучшили свои результаты по отношению к электронным, в то время как участники в других группах не улучшили свои результаты.

Полученные сведения подтверждают и расширяют результаты исследования, в котором говорилось, что встроенное обучение может быть эффективным методом обучения пользователей различать легитимные и фишинговые сообщения электронной почты. Тот факт, что отсутствует значительное снижение производительности после одной недели, говорит о том, что пользователи, вероятно, будут продолжать обучение в течение более длительных периодов времени. Группа, осведомленная о фишинговой угрозе, существенно не отличалась от контрольной группы. Таким образом, рассказывать пользователям о фишинге, не предоставляя им информацию о способах и методах определения фишинговых или других зловредных действий и защиты от них, не имеет смысла.

Низкие результаты, продемонстрированные группой невстроенного обучения, которые незначительно отличалась от контрольной, свидетельствуют о том, что метод обучения является важным фактором, определяющим эффективность антифишинговой подготовки.

Чтобы оценить встроенный подход к обучению на практике, было проведено экспериментальное исследование по измерению остаточных знаний через месяц после окончания обучения, участниками которого стали 153 слушателя курсов повышения квалификации по направлениям, отличным от информационной безопасности, трудоспособного возраста, представителей различных организаций и предприятий, не обладающие знаниями о фишинговой атаке как угрозе информационной безопасности. Организаторами были специально разработаны фишинговые электронные письма-стимуляторы, не несущие угрозу.

Участники эксперимента были случайным образом распределены по трем группам: контроля, одиночной тренировки и многократной тренировки. Всем участникам, независимо от условий, в течение месяца была отправлена серия из трех законных и семи смоделированных электронных писем с фишингом, в теле каждого из которых находился смоделированный фишинговый URL-адрес, симулированного фишингового веб-сайта, запрашивающего личные учетные данные, необходимые для входа на вебсайты. Участники в условиях однократного и многократного обучения, щелкнувшие по URL-адресу, в первый день увидели обучающий мультфильм вместо симулированного фишингового веб-сайта. Участники в режиме многократного обучения, щелкнувшие по URL-адресу через две недели, также увидели учебный мультфильм (второй мультфильм по содержанию был идентичен первому, но отличался другими персонажами и измененной сюжетной линией). Контрольная группа не получала антифишинговой подготовки в рамках исследования.

Разработанные семь текстовых электронных писем с фишингом тематически были связаны с изменением пароля, ограничением пропускной способности, недоставленным электронным письмом, регистрацией событий, призов и наград, скидок на товары и услуги, то есть всем, что содержится в электронных письмах, которые участники обычно получают в повседневной жизни. Все фишинговые сообщения отображали фишинговые URL-адреса в теле сообщений.

При этом в эксперименте не копировали обычную фишинговую тактику использования HTML для сокрытия фишинговых URL-адресов от пользователей.

С целью гарантировать, что совокупные коэффициенты ответов в день не будут смешаны с потенциальной разницей в естественных коэффициентах ответов для отдельных электронных писем или с взаимозависимостью уровней ответов между электронными письмами, использовались мероприятия противодействия.

Результаты показывают, что сотрудники в группах однократного и многократного обучения, попавшие на первое фишинговое сообщение, показали значительно лучшие результаты, когда получили второе фишинговое сообщение, чем те, кто находился в контрольной группе. Кроме того, не будем скрывать значительной утраты остаточных знаний через месяц. Также отметим, что существенных различий между частотой переходов по фишинговым ссылкам участников всех трех групп в первый день и количеством переходов по фишинговым ссылкам участников контрольной группы по дням исследования не было обнаружено. То обстоятельство, что пользователи, которые дважды видели обучающие курсы, с меньшей вероятностью дадут информацию поддельным фишинговым веб-сайтам, чем те, кто видел обучающий мультфильм только один раз, доказывает педагогическую основу обучения в целом.

Обучение пользователей распознаванию фишинговых писем с применением встроенных обучающих мультфильмов не повышает вероятности идентификации законных электронных писем как фишинговых. Также не обнаружены существенные различия между тремя группами в скорости ответов на законные электронные письма в первый и последний дни.

Встроенная система обучения способствует эффективному усвоению знаний пользователей на практике. Сотрудники, прошедшие ее, сохраняли полученные знания не менее месяца. Прошедшие обучение дважды значительно реже предоставляли информацию имитированным фишинговым веб-страницам по его окончании. Стоит отметить, что не выявлено влияние обучения на увеличение вероятности ложноположительных ошибок. Получен неожиданный результат: обнаружена небольшая разница в восприимчивости к фишинговым атакам по признаку пола, однако возраст является фактором предрасположенности к фишингу, поскольку участники 18–25 лет чаще попадают в фишинг, чем люди более старшего возраста.

Исследование продемонстрировало эффективность встроенного подхода к обучению с использованием обучающих моментов в сочетании с наглядными и действенными учебными материалами. Участники, которые подверглись фишинговой атаке через электронное письмо (перешли по ссылке и получили встроенное обучение), имели на 50 % меньше шансов быть ей подвергнутыми повторно, чем те, кто не прошел обучение после получения первого фишингового электронного письма.

Несмотря на то что существует множество образовательных веб-сайтов по борьбе с фишингом, большинство пользователей вряд ли посещают их добровольно. Кроме того, исследование показало, что, хотя некоторые из этих веб-сайтов способствует формированию у пользователей «подозрения» в отношении всей электронной почты, они не раскрывают методы, помогающие отличить законные электронные письма от фишинговых. Благодаря же встроенному обучающему подходу происходит усиление бдительности пользователей при сохранении желания взаимодействовать с законными сообщениями электронной почты.

Таким образом, встроенный подход к обучению позволяет осуществлять удобное и быстрое непрерывное обучение информационной безопасности, при котором каждое смоделированное фишинговое электронное письмо является обучающим элементом, а также служит для проверки того, научился ли получатель отличать легитимные сообщения от фишинговых. Предложенная система не только обучает пользователей примерно за 2 мин, но и регулярно оценивает их эффективность.

СПИСОК ЛИТЕРАТУРЫ

1. **Вилкова, А. В.** Проблемы непрерывного обучения персонала информационной безопасности / А. В. Вилкова, В. М. Литвишков, Б. А. Швырев // Мир науки, культуры, образования. – 2019. – № 4 (77). – С. 29–31.
2. Доктрина информационной безопасности Российской Федерации. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 15.01. 2020).
3. **Швырев, Б. А.** Образовательные потребности в информационной безопасности / Б. А. Швырев // Международный журнал гуманитарных и естественных наук. – 2019. – № 5-1. – С. 31–33.

4. **Швырев, Б. А.** Основные понятия национальной кибербезопасности государств, входящих в Северо-Атлантический альянс : монография / Б. А. Швырев. – Краснодар : Новация ; Москва : НИИ ФСИН России, 2018. – 114 с. – ISBN 978-5-907-133-28-0.
5. Criteria for Measurement for CAE in Cyber Operations Advanced. – URL: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/ (дата обращения: 15.01.2020).
6. Cyber Skills. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808985/Sector_Specific_Guidance__Cyber_Skills.pdf (дата обращения: 15.01.2020).
7. Learn about NSA's university-level research partnerships. – URL: https://www.nsa.gov/resources/students-educators/research-partnership/ (дата обращения: 15.01.2020).
8. NSA Partners with Schools. – URL: https://www.nsa.gov/resources/students-educators/ (дата обращения: 15.01.2020).
9. **Pedley, D.** Understanding the UK cyber security skills labour market / D. Pedley, D. McHenry, H. Motha, J. Shah. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf (дата обращения: 15.01.2020).
10. Policy paper «Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability – a call for views, Executive Summary. – URL: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary (дата обращения: 15.01.2020).
11. **Craig, R.** The history of training, in The ASTD Training and Development Handbook. – 4th edition. – New York : McGraw-Hill, 1996. – 1071 p. – ISBN-13:978-0070133594.
12. **Skudalova, O. V.** Personal factor of a social entrepreneur in the context of the inclusive economy development / O. V. Skudalova et al. // International Journal of Innovative Technology and Exploring Engineering. – 2019. – Vol. 8, no. 8. – Pp. 2996–3002.

REFERENCES

1. Vilkova A. V., Litvishkov V. M., SHvyrev B. A. Problemy nepreryvnogo obucheniya personala informacionnoj bezopasnosti [Problems of continuous training of information security personnel]. *Mir nauki, kul'tury, obrazovaniya – World of science, culture, education*, 2019, no. 4 (77), pp. 29–31. (In Russ.).
2. *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii* [Information Security Doctrine of the Russian Federation]. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (accessed 15.01.2020). (In Russ.).
3. SHvyrev B. A. Obrazovatel'nye potrebnosti v informacionnoj bezopasnosti [Educational Information Security Needs]. *Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk – International Journal of Humanities and Natural Sciences*, 2019, no. 5-1, pp. 31–33. (In Russ.).
4. SHvyrev B. A. *Osnovnye ponyatiya nacional'noj kiberbezopasnosti gosudarstv, vhodyashchih v Severo-Atlanticheskij al'yans* [Basic concepts of national cybersecurity of the states belonging to the North Atlantic Alliance]. Krasnodar, Moscow, 2018. 114 p. (In Russ.).
5. *Criteria for Measurement for CAE in Cyber Operations Advanced*. Available at: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/ (accessed 15.01.2020). (In Eng.).
6. *Cyber Skills*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808985/Sector_Specific_Guidance__Cyber_Skills.pdf (accessed 15.01.2020). (In Eng.).
7. *Learn about NSA's university-level research partnerships.* Available at: https://www.nsa.gov/resources/students-educators/research-partnership/ (accessed 15.01.2020). (In Eng.).
8. *NSA Partners with Schools.* Available at: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/ (accessed 15.01.2020). (In Eng.).
9. Pedley D., McHenry D., Motha H., Shah J. *Understanding the UK cyber security skills labour market*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf (accessed 15.01.2020). (In Eng.).
10. *Policy paper «Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability – a call for views, Executive Summary.* Available at: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views-executive-summary (accessed 15.01.2020). (In Eng.).
11. Craig, R. *The history of training, in The ASTD Training and Development Handbook*. New York, 1996. 1071 p. (In Eng.).
12. Skudalova O. V., Malanina Y. N., Tsibizova T. Y., Vilkova A. V., Litvishkov V. M., Shvyrev B. A., Poliakova I. V. Personal factor of a social entrepreneur in the context of the inclusive economy development. *International Journal of Innovative Technology and Exploring Engineering*, 2019, vol. 8, no. 8, pp. 2996–3002. (In Eng.).