УДК 37.011:37.047

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ: ПРОБЛЕМЫ, УГРОЗЫ, ПУТИ РЕШЕНИЯ

Абрамова С.В., Бояров Е.Н., Храпаль Л.Р., Рубцова С.Ю.

ФГБОУ ВО «Сахалинский государственный университет», Южно-Сахалинск, e-mail: e.boyarov@mail.ru

В данной работе сделана попытка охватить круг проблем информационной безопасности в образовательной среде. На теоретическом уровне обоснована проблема профессиональной подготовки педагогов к безопасной деятельности (ИБ) в информационной образовательной среде. Получили освещение технический и технологический аспекты информатизации образования, связанные с обеспечением информационной безопасности образовательной среды вуза. Определены объекты воздействия, представляющие собой элементы информационной инфраструктуры вуза, которые требуют обеспечения информационной безопасности. В ходе распределенного экспериментального исследования установлены ранговые показатели по уровням угроз информационной безопасности, которые отождествляют мнение преподавателей вузов с вероятными угрозами информационной безопасности. На этом основании нами сделан вывод об идентичности обобщенного понимания угроз информационной безопасности у преподавателей вузов, принявших участие в экспериментальном исследовании. Также определено, насколько индивидуальный профиль, отражающий обобщенный уровень знаний в области обеспечения информационной безопасности «эталонного преподавателя», имеющего профессиональные знания в области ИБ, коррелирует с обобщенным реальным профилем преподавателей, не имеющих такой подготовки. Сделан вывод, что мнения преподавателей не согласуются между собой. В заключение обоснована необходимость организации работы по профессиональной подготовке всех педагогов и показана важность постоянного совершенствования преподавателями своих знаний новых реальных и потенциальных угроз ИБ и методов защиты информационной образовательной среды от них.

Ключевые слова: профессиональная подготовка, информационные угрозы, информационная образовательная среда.

INFORMATION SECURITY OF MODERN PROFESSIONAL EDUCATION: PROBLEMS, THREATS, WAYS OF SOLUTION

Abramova S.V., Boyarov E.N., Khrapal L.R., Rubtsova S.Y.

FGBOU VO «Sakhalin state university», Yuzhno-Sakhalinsk, e-mail: e.boyarov@mail.ru

In this paper an attempt is made to capture the range of problems of information security in an educational environment. At the theoretical level, the problem of professional training of teachers for safe activities in the information educational environment is justified. Technical and technological aspects of digitalization of education related to ensuring information security of the educational environment of the University were highlighted. The objects of influence that are elements of the University's information infrastructure that require information security are identified. In the course of a distributed experimental study, rank indicators were established for the levels of information security threats, which identify the opinion of University teachers with likely threats to information security. On this basis, we conclude that the generalized understanding of information security threats among University teachers who participated in the experimental study is identical. Also defined as an individual profile that reflects the generalized level of knowledge in the field of information security «reference teacher» having professional knowledge in the field of information security correlated with the generalized real profile of teachers who lacked such training. It is concluded that the opinions of teachers do not agree with each other. In conclusion, the necessity of organizing professional training for all teachers is justified and the importance of continuous improvement of teachers' knowledge of new real and potential threats to information security and methods of protecting the information educational environment from them is shown.

Keywords: professional training, information threats, information educational environment.

Как показывает практика организации современного образовательного процесса в эпоху его информатизации, проблема информационной безопасности (ИБ) любой образовательной организации, обучающихся в ней предстает одной из самых актуальных. Ее

актуальность во многом определяется современной тенденцией перевода образовательного процесса частично, а иногда и полностью, в дистанционный формат. Кроме того, это становится особо актуально в условиях перманентной негативной социально-эпидемиологической ситуации, вызываемой новыми пандемическими ограничениями. При этом наиболее активное и компетентное в информационно-коммуникационном отношении население (учащиеся среднего и старшего школьного звена, студенты вузов, молодые специалисты, переведенные на дистанционный режим работы), получая практически круглосуточный доступ к глобальной информационной сети из дома, имеет все потенциальные возможности для проведения самостоятельно или в рамках распределенных сообществ информационных акций, оказывающих негативное воздействие на информационную инфраструктуру в общем, и, в частности, на информационные образовательные среды образовательных организаций.

Соответственно, закономерным становится рост количества информационных угроз из Интернета, и, следовательно, необходимо менять методы и средства обеспечения информационной безопасности образовательного процесса.

Проблемам обеспечения ИБ информационных образовательных сред посвящены исследования вопросов риск-менеджмента [1-3], онлайн-рисков [4, 5], вопросов безопасности персональных данных [6], общих вопросов информационной безопасности вузов [7, 8], политики информационной безопасности в вузе [9].

Однако следует констатировать, что в значительном количестве трудов не получают должного рассмотрения вопросы, связанные с исследованием уровня осведомленности педагогов о сути проблемного поля информационной безопасности образовательной среды и вероятных угроз для информационной инфраструктуры образовательной организации. Необходимость изучения проблемы создания современной безопасной информационной образовательной среды вуза и профессиональной подготовки педагогов к безопасному взаимодействию с информационной инфраструктурой определила актуальность и проблемоориентированность нашего исследования.

В качестве цели исследования мы определили необходимость изучения уровня осведомленности педагогов вуза в вопросах обеспечения информационной безопасности образовательной среды и ее информационной инфраструктуры. Данная цель интерполируется по тренду всеобщего вовлечения профессорско-преподавательского, учебно-методического и вспомогательного состава вуза в работу по созданию, наполнению и сопровождению информационной образовательной среды и обеспечению ее безопасного во всех планах функционирования. Этому, на наш взгляд, будет способствовать профессиональная подготовка педагогов к безопасному взаимодействию с информационной

инфраструктурой вуза.

Материалы и методы исследования

В период с марта по июль 2020 г. научным коллективом СахГУ (г. Южно-Сахалинск) и РГПУ им. А.И. Герцена (г. Санкт-Петербург) было проведено исследование, которое в сложившихся пандемических условиях образовательного процесса с ограничением прямой контактной работы и расширением онлайн- и офлайн-взаимодействия средствами информационной образовательной среды вуза позволило выявить состояние проблемы осведомленности педагогов в вопросах информационной безопасности образовательной среды, а также наметить приоритетные направления решения данной проблемы.

Также в ходе исследования нами осуществлялись анализ имеющихся в информационной образовательной среде СахГУ и доступных для педагогов цифровых технологий, применяемых для осуществления современного смешанного образовательного процесса и взаимодействия с его удаленными участниками; наблюдение за структурными и качественными изменениями образовательного процесса в СахГУ; беседы с субъектами информационной образовательной среды СахГУ о проблемных вопросах информационной безопасности. На этом основании ними был сделан обобщающий вывод о необходимости проведения исследования для ответа на следующие проблемные вопросы. 1. Имеют ли преподаватели представление о существующих угрозах для информационных образовательных сред? 2. Обладают ли преподаватели необходимыми знаниями в вопросах обеспечения информационной безопасности образовательной среды? 3. Какой информационный контент требуется преподавателям для повышения уровня их профессиональных знаний в области информационной безопасности при работе с современными образовательными средами? Постановка этих вопросов рассматривается авторами статьи как исходные методические предпосылки для исследования.

Результаты исследования и их обсуждение

Теоретическое обоснование проблемы профессиональной подготовки педагогов к безопасной деятельности в информационной образовательной среде сводится нами к тезису о том, что в современном образовательном процессе информационная инфраструктура становится один из главных его элементов [10, 11]. Соответственно, рассмотрим основные предпосылки, определяющие необходимость повышения уровня профессиональной грамотности в области информационной безопасности современного педагога в вузе.

Во-первых, учебные аудитории оснащены компьютерной техникой, и ее качественное бесперебойное функционирование существенно определяет средства эффективной реализации образовательного процесса, направленного на получение качественных знаний и способствующего формированию профессиональных компетенций

обучающихся. Сюда можно отнести постоянно повышающиеся требования к техническому оснащению оборудования, обусловленные, в том числе, и ростом требований к программному обеспечению образовательной направленности, связанным с повышением роли мультимедийного и VR контента. Это так называемый ***технический*** аспект.

Во-вторых, представители современного цифрового общества знания – все категории обучающихся – сейчас, как никогда, имеют потенциальную возможность использовать средства доставки знаний независимо от своего местоположения и времени суток. Почему потенциальную? Ответ очевиден – современные средства доставки информации представляют собой перманентную информационную среду, часто изобилующую необъективной, недостоверной, а иногда негативной и даже вредной информацией. В бытовом понимании это так называемые фейк ньюс – «фейки», которыми подменяются факты. И найти в таком информационном потоке полезную информацию для преобразования ее в знание – довольно сложный интеллектуальный процесс. Поэтому средства доставки информации устанавливают определенные технологии получения данной информации. И это так называемый ***технологический*** аспект.

В-третьих, само качество образовательного контента должно соответствовать установленным требованиям – он должен быть актуальным, объективным, достоверным, доступным для всех категорий обучающихся, в том числе и с особыми образовательными потребностями ввиду ограниченных возможностей здоровья, а также доступным для получения по режиму функционирования образовательной среды.

В **техническом** плане информационная образовательная среда вуза представляет собой совокупность рабочих станций персонала, различных сетевых устройств полного цикла работы с информацией (в том числе сбора, обработки, хранения и отображения), сетевых ресурсов для осуществления образовательной деятельности, сопутствующих и обеспечивающих устройств функционирования среды в целом (таких как источники бесперебойного питания, системы резервирования данных, аппаратные сетевые и межсетевые экраны и др.).

В **технологическом** плане информационная образовательная среда вуза представляет собой совокупность, *во-первых*, массивов образовательной информации, обеспечивающей образовательный процесс; *во-вторых*, массивов нормативно-правовой документации (такой как стандарты, учебные планы, рабочие программы дисциплин, ФОСы и иное, а также различные инструкции, приказы, нормативные акты); *в-третьих*, значительного массива персональных данных субъектов образовательного процесса, необходимых для работы кадрового и финансового аппарата (это личные дела, паспортные данные для договорной работы, данные о сетевых партнерах), а также сведений для работы всей инфраструктуры

образовательной среды – учетных данных для авторизации пользователей среды; *в-четвертых*, объектов интеллектуальной собственности (полнотекстовых баз выпускных работ, издаваемых вузом учебно-методических материалов, научных трудов, проектно-исследовательских наработок); и*, наконец, в-пятых*, приобретенных университетом программного обеспечения и лицензий, кража которых может повлечь за собой наступление уголовной или административной ответственности.

Соответственно, широкое и разнообразное наполнение информационной образовательной среды (ИОС) неминуемо обусловливает появление реальных и потенциальных угроз для нее.

Отметим, что к **объектам воздействия** могут быть отнесены следующие:

- бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные;
- серверы баз данных;
- консоль управления учетными записями;
- www/ftp серверы;
- ЛВС и серверы исследовательских проектов.

Совокупность рассмотренных предпосылок составляет контентный массив, определивший содержание базовых знаний в области информационной безопасности (ИБ) для педагогов вуза, на основе которого и путем применения методов.

На основе теоретического анализа и результатов проведенного эксперимента было определено, что современный образовательный процесс с активным включением в него информационных технологий вызывает у преподавателей ряд трудностей, связанных с проблемным полем ИБ, к числу которых были отнесены незнание наиболее вероятных информационных угроз и неумение их определить при работе с цифровыми образовательными технологиями; недостаточное понимание важности обеспечения ИБ информационной образовательной среды; низкая мотивация к изучению проблемных вопросов и современного состояния ИБ в образовании; нехватка молодых и умеющих работать в современной информационной образовательной среде педагогических кадров; отсутствие экспресс-курсов корпоративного повышения квалификации педагогических работников в вопросах ИБ.

В проведенном исследовании приняли участие 21 преподаватель Института естественных наук и техносферной безопасности СахГУ и 27 преподавателей факультета безопасности жизнедеятельности РГПУ им. А.И. Герцена. В первой части исследования для реализации цели эксперимента им было предложено оценить по 10-балльной шкале, какие виды угроз возможны при реализации образовательного процесса средствами

информационной образовательной среды и в ее инфраструктуре. Данные, полученные по 10-балльной шкале, были усреднены и проранжированы. В таблице 1 представлены ранговые показатели полученных ответов. При проведении эксперимента проверялось, совпадают ли ранговые последовательности видов угроз ИБ. Были сформулированы следующие гипотезы.

H_0 – корреляция между упорядоченными перечнями видов угроз ИБ в выборке СахГУ и выборке РГПУ им. А.И. Герцена не достигает уровня статистической значимости.

H_1 – корреляция между упорядоченными перечнями видов угроз ИБ в выборке СахГУ и выборке РГПУ им. А.И. Герцена статистически значима.

В таблице 1 представлены расчеты, необходимые для вычисления рангового коэффициента корреляции Спирмена при сопоставлении упорядоченных перечней видов угроз информационной безопасности в выборках СахГУ и РГПУ им. А.И. Герцена.

Таблица 1

Ранговые показатели по уровням угроз информационной безопасности

№	Угрозы информационной безопасности	Ранг в выборке СахГУ	Ранг в выборке РГПУ им. А.И. Герцена	d
1	Отсутствие или недостаточное обеспечение лицензированным программным продуктом	1	1	0
2	Отсутствие или потеря актуальности антивирусной защиты	2	2	0
3	Снижение достоверности образовательного контента	12	12	0
4	Хакерские атаки	3	4	-1
5	Некомпетентные действия персонала	5	5	0
6	Кража персональных данных	8	13	-5
7	Кража объектов интеллектуальной собственности	10	10	0
8	Несанкционированная модификация контента	14	6	8
9	Несанкционированное подключение пользовательских сетевых устройств	13	16	-3
10	Несоблюдение политики информационной безопасности	7	7	0
11	Несвоевременный аудит информационной безопасности	11	11	0
12	Применение в образовательном процессе нелицензированных оборудования и программных продуктов	4	3	1
13	Незнание требований законодательства в области информационной безопасности	6	9	-3
14	Несанкционированный доступ к персональным данным	15	8	7
15	Аппаратные сбои объектов вычислительной техники	9	14	-5
16	Утрата (потеря) носителей информации	16	15	1

Для определения эмпирического значения коэффициента корреляции Спирмена $r_{sэмп}$ используем формулу:

$$r_{s\ эмп} = 1 - \frac{6 \cdot \Sigma(a^2)}{n(n^2-1)} = 0{,}729 \qquad (1)$$

Критические значения r_s определены с использованием таблицы критических значений выборочного коэффициента корреляции рангов. Учитывая, что в исследовании было 16 измерений (n=16), имеем:

$$r_{s\ кр} = \begin{cases} 0{,}50 (\rho \leq 0.05) \\ 0{,}64\ (\rho \leq 0.01) \end{cases}$$

$$r_{s\ эмп} < r_{s\ кр}$$

На основании этого принимается гипотеза H_1.

Таким образом, корреляция между упорядоченными перечнями видов угроз ИБ в выборке СахГУ и РГПУ им. А.И. Герцена достигает уровня статистической значимости и является положительной. Следовательно, обобщенное понимание угроз информационной безопасности у преподавателей СахГУ и РГПУ им. А.И. Герцена как при 5%-ном, так и при 1%-ном уровне значимости одинаково.

Во второй части исследования преподавателям предлагалось ответить на вопрос: «Какие методы обеспечения информационной безопасности в образовательной среде, на ваш взгляд, наиболее эффективны?» В таблице 2 представлены средние значения, полученные для каждого выявляемого метода в выборке преподавателей без специфических знаний в области обеспечения информационной безопасности образовательной среды (не проходивших когда-либо профессиональное обучение, подготовку или переподготовку по данным вопросам) («реальный ряд»), и индивидуальные значения одного из преподавателей с продвинутым уровнем знаний в области ИБ, имеющего профессиональную подготовку в области ИБ («эталонный преподаватель»). Нами была поставлена задача определить, насколько индивидуальный профиль «эталонного преподавателя» коррелирует с обобщенным реальным профилем преподавателей, не имеющих такую подготовку.

Таблица 2

Усредненные оценки «реального ряда» (n=48) и индивидуальные показатели «эталонного преподавателя»

№	Методы обеспечения информационной безопасности	Усредненные реальные оценки преподавателей	Индивидуальные показатели эталонного преподавателя
1	Краткосрочное профессиональное обучение по вопросам ИБ	7,20	10
2	Постоянный аудит ИБ	7,59	9

3	Разграничение прав доступа к информационным ресурсам	8,18	8
4	Использование лицензированного программного продукта	8,54	8
5	Резервирование электропитания	6,29	5
6	Использование средств антивирусной защиты	7,51	8
7	Применение современных технологий обеспечения информационной безопасности	9,20	9
8	Организация защищенного доступа к образовательным материалам и системам из любой точки мира	6,18	6
9	Защита информации ограниченного доступа (персональных данных, коммерческой тайны и т.п.)	8,68	8
10	Защита интеллектуальной собственности	7,68	8
11	Выполнение требований законодательства в области информационной безопасности (защита персональных данных, защита прав на интеллектуальную собственность, защита от негативной информации)	8,60	8
12	Соблюдение политики информационной безопасности в вузе	8,83	7
13	Обновление технологического фонда (устаревшего оборудования)	8,17	5
14	Соблюдение морально-этических норм	8,23	5
15	Разумное ограничение посещений агрессивных информационных пространств	7,41	6
16	Использование паролирования доступа к данным	8,80	7
17	Применение контентной фильтрации	7,20	8

Оценка преподавателей осуществлялась нами по 10-балльной шкале, далее значения ранжировались. При этом единицей измерения был принят 1 ранг, а максимальное значение составляло 17 рангов.

Для того чтобы увидеть, на каком месте по значимости для респондентов находится тот или иной метод, большему значению был определен меньший ранг. Результаты ранжирования представлены в таблице 3, в которой также выполнен расчет для определения коэффициента корреляции Спирмена между «эталонным» и «реальным» профилями наиболее значимых методов обеспечения ИБ образовательной среды.

Таблица 3

Определение коэффициента корреляции Спирмена между «эталонным» и «реальным» профилями наиболее значимых методов обеспечения информационной безопасности образовательной среды

№	Методы обеспечения информационной безопасности	Ранг метода в «эталонном» профиле	Ранг метода в «реальном» профиле	d

1	Краткосрочное профессиональное обучение по вопросам ИБ	3,5	17	–13,5
2	Постоянный аудит ИБ	7	15,5	–8,5
3	Разграничение прав доступа к информационным ресурсам	10	11	–1
4	Использование лицензированного программного продукта	12	11	1
5	Резервирования электропитания	2	2	0
6	Использование средств антивирусной защиты	6	11	–5
7	Применение современных технологий обеспечения информационной безопасности	17	15,5	1,5
8	Организация защищенного доступа к образовательным материалам и системам из любой точки мира	1	4,5	-3,5
9	Защита информации ограниченного доступа (персональных данных, коммерческой тайны и т.п.)	14	11	3
10	Защита интеллектуальной собственности	8	11	-3
11	Выполнение требований законодательства в области информационной безопасности (защита персональных данных, защита прав на интеллектуальную собственность, защита от негативной информации)	13	11	2
12	Соблюдение политики информационной безопасности в вузе	16	6,5	9,5
13	Обновление технологического фонда (устаревшего оборудования)	9	2	7
14	Соблюдение морально-этических норм	11	2	9
15	Разумное ограничение посещений агрессивных информационных пространств	5	4,5	0,5
16	Использование паролирования доступа к данным	15	6,5	8,5
17	Применение контентной фильтрации	3,5	11	-7,5
18	Краткосрочное профессиональное обучение по вопросам ИБ	3,5	17	-13,5

Нами были сформулированы следующие гипотезы.

H_0 – корреляция между индивидуальным профилем «эталонного преподавателя» и «реальным профилем» незначительна.

H_1 – корреляция между индивидуальным профилем «эталонного преподавателя» и «реальным профилем» статистически значима.

В сопоставленных ранговых рядах имеются группы одинаковых рангов. Поэтому перед вычислением коэффициента ранговой корреляции были внесены поправки на одинаковые ранги T_a и T_b:

$$T_a = \frac{\sum(a^3 - a)}{12} = 0{,}5$$

$$T_b = \frac{\sum(b^3 - b)}{12} = 31{,}5,$$

где a – число одинаковых рангов в ранговом ряду «Эталонный профиль»;

b – число одинаковых рангов в ранговом ряду «Реальный профиль».

Для вычисления эмпирического значения r_s использована формула:

$$r_s = 1 - 6\,\frac{\sum d^2 + T_a + T_b}{n(n^2 - 1)} = 0{,}176$$

Критические значения r_s определяются с использованием таблицы критических значений выборочного коэффициента корреляции рангов.

Для n=18

$$r_{s\,\text{кр}} = \begin{cases} 0.48 \ (\rho \le 0.05) \\ 0.62 \ (\rho \le 0.01) \end{cases}$$

$$r_{s\,\text{эмп}} < r_{s\,\text{кр}}$$

По результатам расчетов гипотеза H_1 отвергается. Корреляция между индивидуальным профилем «эталонного преподавателя» и «реальным профилем» преподавателей статистически незначима $(\rho \le 0.05)$ и является положительной. Мнения преподавателей не согласуются между собой, что подтверждает в целом бессистемность таких знаний. При этом примечательно, что в ответе о важности дополнительного обучения по вопросам информационной безопасности образовательной среды мнения всех преподавателей схожи, что говорит о необходимости организации работы по профессиональной подготовке всех педагогов и важности постоянного совершенствования своих знаний новых реальных и потенциальных угроз ИБ и методов защиты от них информационной образовательной среды.

Заключение

Современное состояние цифровизации образовательного процесса способствует появлению новых информационных угроз и опасностей. Часто преподаватели в силу недостаточной осведомленности о таких угрозах и мерах по обеспечению безопасности себя и обучающихся от информационных угроз в образовательной среде не готовы к активным и продуктивным действиям по обеспечению собственной и коллективной информационной

безопасности. В результате проведенного исследования показано, что большинству преподавателей не хватает базовых профессиональных знаний в области информационной безопасности в современных быстро меняющихся условиях цифрового образовательного процесса. Это свидетельствует о необходимости разработки вузовской целевой образовательной программы, направленной на профессиональную подготовку педагогов к работе с информационной образовательной средой, в том числе и в аспекте обеспечения ее информационной безопасности.

Список литературы

1. Ruzic-Dimitrijevic L., Dakic J. The risk management in higher education institutions. Online Journal of Applied Knowledge Management A Publication of the International Institute for Applied Knowledge Management. 2014. vol. 2. no. 1. P. 137-149.
2. Huber M. Colonised by risk - the emergence of academic risks in British higher education. Cambridge: Cambridge University Press, 2010. P. 114-136.
3. Nikolic B., Ruzic-Dimitrijevic L. Information system and risk reassessment. Issues in Informing Science and Information Technology. 2010. vol. 6. P. 191-207.
4. Солдатова Г.У., Шляпников В.Н., Журина М.А. Эволюция онлайн-рисков: итоги пятилетней работы линии помощи «Дети онлайн» // Консультативная психология и психотерапия. 2015. Т. 23. № 3. С. 50–66.
5. Livingstone S., Haddon L., Görzig A. Children, Risk and Safety Online: Research and policy challenges in comparative perspective. Bristol: The Policy Press. 2012. vol. 29. issue 1. P. 83-84.
6. Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. Практическая психология безопасности: управление персональными данными в интернете. Федеральный институт развития образования Москва, 2016. 204 с.
7. Волков А.В. Обеспечение ИБ в вузах // Информационная безопасность. 2006. № 3, 4. [Электронный ресурс]. URL: http://www.itsec.ru/articles2/bepub/insec–3+4–2006 (дата обращения: 10.11.2020).
8. Проталинский О.М. Ажмухамедов А.М. Информационная безопасность ВУЗа // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. 2009. № 1. С. 18-23.
9. Труфанов А.И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. 2004. Вып. 9. [Электронный ресурс]. URL: http://library.istu.edu/civ/default.htm (дата обращения: 10.11.2020).

10. Полезный и безопасный интернет. Правила безопасного использования интернета для детей младшего школьного возраста: практическое пособие / Под ред. Г.У. Солдатовой; 3-е изд., перераб. и доп. М.: Федеральный институт развития образования, 2017. 64 с.
11. Stankevich P.V., Abramova S.V., Boyarov E.N. Bachelor In Education (Life Safety) Competency Assessment / 18th PCSF 2018 - Professional Culture of the Specialist of the Future. The European Proceedings of Social & Behavioural Sciences EpSBS. (30 December 2018). 2018. no. 75. P. 689-700. DOI: 10.15405/epsbs.2018.12.02.75.