DOI: 10.36535/0203-6460-2021-01-1

Библиометрическое отображение исследования по подготовке пользователя для безопасного применения информационных систем*

Дамьян ФУЙС
(Damjan FUJS)
Люблянский университет,
г. Любляна, Словения

Симон ВРХОВЕЦ
(Simon VRHOVEC)
Мариборский университет,
г. Марибор, Словения

Дамьян ВАВПОТИЧ
(Damjan VAVPOTIČ)
Люблянский университет,
г. Любляна, Словения

Информационные системы повсеместно распространены в организациях всех размеров. Для их безопасного применения пользователи должны быть тщательно подготовлены соответствующим образом. В связи с распространенностью информационных систем число научных публикаций о подготовке пользователей для безопасного использования информационных систем из года в год растет. Чтобы преодолеть проблему ручного труда при обзоре такого объема знания и идти в ногу с исследовательскими тенденциями, было проведено библиометрическое отображение в виде карт исследования по подготовке пользователей для безопасного применения информационных систем. Общее число документов, равное 1955 единицам, опубликованных в период 1991-2019 гг., взято из библиографической базы данных Web of Science 21 ноября 2019 г. Авторы с топовой продуктивностью, организации, страны и области исследования были идентифицированы с помощью встроенного в Web of Science средства для анализа результатов. Кроме того, осуществлено отображение в виде карт ключевых слов (КС) на основе программного обеспечения VOSviewer. Анализ сетевой работы и входящих в нее карт КС обнаружил шесть кластеров: Здравоохранение, Принятие Технологии, Управление, Информационная Безопасность, Технические Решения и Физическая Безопасность. Результаты данного анализа предполагают для проведения в будущем привлекательные исследовательские направления, такие как подготовка в сфере информационной безопасности в здравоохранении и индивидуальная подготовка пользователя как альтернатива подходу «одна форма для всех».

* Перевод Fujs D., Vrhovec C., Vavpotič D. Bibliometric mapping of research on user training for secure use of information systems//Journal of Universal Computer Science. —2020. — Vol. 26, No. 7 —P.764 -782. — https://www.researchgate.net/profile/Damjan_Fujs/publication/344163093_Bibliometric_Mapping_of_Research_on_User_Training_for_Secure_Use_of_Information_Systems/links/5f575962458515e96d3911d3/Bibliometric-Mapping-of-Research-on-User-Training-for-Secure-Use-of-Information-Systems.pdf

ВВЕДЕНИЕ

Люди вовлечены или должны быть вовлечены в образование с раннего возраста, поскольку обучение является естественным для хода человеческого развития. Исследование образования уходит корнями к древнегреческому философу Платону, который интересовался фундаментальными вопросами образования: кто и как должен получать образование [1]? Ответ на первый вопрос кажется вполне простым – каждый должен получить какое-то образование. Это также справедливо в отношении кибербезопасности и особенно безопасности информационных систем. Пользователи информационных систем должны быть соответствующим образом подготовлены для их безопасного использования [2]. Организации стремятся научить своих сотрудников избегать киберугроз и защищать интересы организаций [3]. Однако подходы образования по схеме «одна форма подготовки для всех» не могут соответствовать всем ситуациям, а некоторые подходы будут больше, чем другие, подходить в определенных ситуациях [4]. Например, подходы могут рассматривать различия уровня знания пользователей информационных систем, относящегося к кибербезопасности [5, 6, 7]. Такие подходы способны увеличить эффективность подготовки и снизить вероятность или масштаб сопротивления относительно подготовки [8].

В последние годы было проведено много разнообразных обзоров литературы по кибербезопасности и областей исследования в сферах образования. Например, в работе [9] рассматривалось использование качественных подходов в кибербезопасности, которые включали исследование образования по безопасности и подготовке, а в работе [10] изучались компетенции информатики сферы здравоохранения, решающие для образования в информационной технологии. Однако оказывается, что здесь существует пробел в исследовании, поскольку ни один из этих обзоров литературы подробно не фокусировался на образовании в сфере кибербезопасности, а также на более детальной подготовке по безопасному использованию информационных систем. Традиционные обзоры литературы обычно используют чтение релевантных статей с добавлением к ним элемента исследовательского суждения. Эта субъективность может быть снижена анализом КС (т. е. библиометрическим отображением на картах), поскольку он опирается на автоматический качественный анализ с заранее определенным алгоритмом [11]. Недавно библиометрия стала притягательной силой для множества научных дисциплин (например, науки сферы здравоохранении [12], туризм [13] и вычислительная наука [14]).

Чтобы рассмотреть представленный научный пробел, воспользуемся библиометрией и определим направления в исследовании по подготовке пользователя к безопасному использованию информационных систем; мы составили библиометрические карты [15], которые позволяют определить научные направления и выявить наиболее заметные исследовательские вклады. Этот обзор литературы может помочь исследователям и практикам в области кибербезопасности сфокусироваться на соответствующих направлениях в исследовании относительно подготовки пользователя для безопасного применения информационных систем и найти такие, где можно продвигаться за рамки существующего положения дел. В целях достижения этого данная статья изучает следующие вопросы исследования:

Вопрос исследования 1: Кто является наиболее продуктивными авторами, каковы страны, организации и научные области, связанные с исследованием по обучению пользователей для безопасного применения информационных систем?

Вопрос исследования 2: Какие КС наиболее часто появляются в исследовании по подготовке пользователя для безопасного применения информационных систем?

Вопрос исследования 3: Какие КС появлялись раньше, а какие позже в исследовании по подготовке пользователя для безопасного использования информационных систем?

ТЕОРЕТИЧЕСКАЯ ОСНОВА

Подготовка пользователя для безопасного применения информационных систем

Информационные системы могут быть определены как сущность, состоящая из пользователей, выполняющих относящиеся к информации задачи, и разнообразных информационных технологий, использующихся для реализации этих задач [16]. Следовательно, информационные системы включают множество компонентов, таких как персональные компьютеры, социальные сети, банкоматы, смартфоны для делового и личного пользования и т.д. Уже некоторые ранние исследования в сфере информационных систем концентрировались на подготовке пользователей информационных систем (например, компьютерные инструкции) [17, 18]. Более новые исследования фокусировались на пользователях информационных систем, внедряющих меры безопасности [19, 20]. Недавно распространение исследований по образованию в сфере кибербезопасности расширилось благодаря помощи инновационных обучающих подходов, таких как правила по безопасности [21], персональная подготовка [22] и растущая реальность [23].

В течение последнего десятилетия значение обучения пользователей безопасному использованию информационных систем кажется растет [24]. Неотвечающая требованиям подготовка пользователей для безопасного использования информационных систем в организациях касается, с одной стороны, как пользователей со слабым знанием безопасного использования информационных систем, так и персонала, не имеющего навыков обучения, с другой. Кибернетическая безопасность рассматривается, как правило, в области отделений информационной технологии (IT). Персонал таких отделений обычно хорошо осведомлен о киберугрозах и контрмерах с технологической точки зрения. Однако информационно-технологический персонал часто не имеет навыков, необходимых для подготовки пользователей информационных систем, и по заведенной практике пользователи не применяют необходимые меры кибербезопасности, поскольку они считают, что кибербезопасность входит в сферу ответственности отделов IT. Даже при наличии самостоятельных отделов по информационной безопасности это представляет проблему, так как образование в сфере кибербезопасности для пользователей информационных систем часто остается без внимания из-за отсутствия персонала по кибербезопасности [25]. Эти проблемы, кажется, проявляются в большом масштабе. Например, почти половина организаций в Великобри-

тании сообщала, что их проблемы по кибербезопасности были связаны с отсутствием навыков у своих сотрудников [26]. Следовательно, решающим может быть то, что все сотрудники организации, а не только персонал, занятый информационными технологиями, должны быть в достаточной степени подготовлены для безопасного использования информационных систем. Также решающим вопросом может быть развитие организационной культуры, где кибербезопасность считается для каждого ответственностью, а не привилегией.

Библиометрия и связанные подходы

Библиометрия уходит своими корнями в статистику и библиографию и может быть описана как количественное библиографическое исследование литературы (например, ассоциации между публикациями и их ссылками) [27]. Библиометрия позволяет анализировать выбранные темы, возвращаясь на многие десятилетия назад (например, 30 лет [28] и 50 лет [29], следовательно, охватывая значительный объем данных и получая глубокое проникновение в эволюцию исследуемой темы).

Существуют две другие метрики измерения направлений публикации, имеющие отношение к терминам: наукометрия и информетрия [27]. *Наукометрия* часто используется в исследованиях, относящихся к безопасности информационных систем, применяющих качественные метрики научной деятельности (например, импакт-фактор журнала, h-индекс журнала, квартиль журнала, год публикации, ссылки), и может быть использована для определения влияния авторов [27]. Например, недавнее наукометрическое исследование обнаружило, что научные публикации с более длинными рефератами и публикации с большим числом ссылок получают высокое число ссылок в области исследования информационной безопасности [30].

Информетрия – самый широко используемый метод в вычислительной науке, поскольку он касается не только библиографической информации [27], но и включает разнообразные метрики, которые фокусируются на информационной продуктивности [31]. Информетрия затрагивает не только научные метрики, она также применима во множестве областей, где может анализироваться информация [32]. Разнообразные научные и другие БД обеспечивают информетрию. Однако есть проблемы с последовательностью метрик в разных БД. Например, Google Scholar обеспечивает иной подсчет ссылок для публикаций, чем Web of Science. Чтобы рассмотреть эту проблему имеется ряд появившихся в литературе решений, таких как использование технологии «быстрых статей» (smart papers) и блокчейна, позволяющей децентрализованную публикацию и вычисление на основе информетрии [32].

Также возникают новые подходы, такие как *взаимное посредничество публикаций (intermediacy of publications)*. Эти подходы дают возможность проводить сравнение между старыми и более поздними публикациями и могут помочь осуществить мониторинг эволюции научного знания на основе сети ссылок [33]. Поскольку научная продуктивность растет, то средства и методы, позволяющие проводить эффективный анализ массы данных, приобретут большую важность [34].

МЕТОД

Применяемая для исследования методология приведена на рис. 1 и подробно представлена в следующих подразделах.

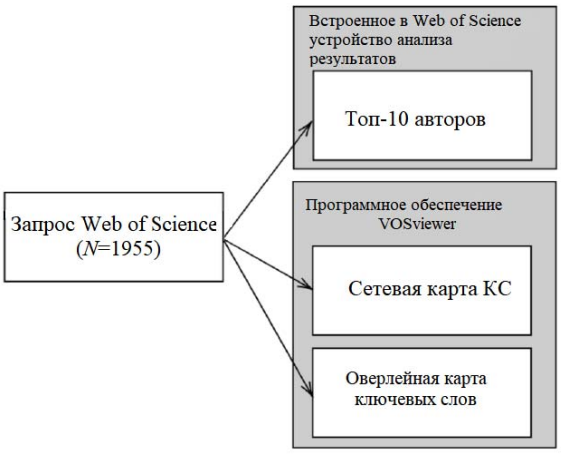

Рис. 1. Сбор данных и анализ

Сбор данных

В целях получения наиболее релевантных статей по подготовке потребителя к безопасному использованию информационных систем в анализ были включены следующие темы для просмотра в библиографических БД: информационные системы, подготовка и образование в сфере безопасности. Оба термина – education (образование) и training (подготовка) являются релевантными, так как пользователи могут либо самостоятельно обучаться, либо руководствуясь определенной подготовкой. Приведенные выше темы использовались для формирования запроса, который применялся для поиска релевантных документов в БД Web of Science (https://apps.webofknowledge.com/):

TOPIC: (*information systems* AND (*security training* OR *security education*))

Выбранные темы намеренно были очень широкими, чтобы увеличить исчерпывающую картину поисковой области. Затем результаты уточнялись по типу документов: *ARTICLE* (*СТАТЬЯ*) or *PROCEEDINGS PAPER* (*ТРУДЫ*). Это позволило осуществить поиск журнальных статей и материалов конференций, связанных с образованием в области безопасности информационных систем. Библиографические документы, общее количество равно 1955 (N=1955), были получены 21 ноября 2019 г.

Анализ данных

Первое, библиографические документы анализировались с помощью встроенного устройства Web of Science для идентификации топ-10 внесших свой вклад авторов, организаций, стран и областей исследования. Отчеты по результатам анализа включают общее число публикаций (N), долю всех публикаций, включенных в обзор, которую они представляют (%), наиболее цитируемую публикацию, не исключая самоцитирование (Ref_N), авторов самой цитируемой публикации и число ссылок для самой цитируемой публикации (TC_R). Публикации могут перекрываться между разными авторами, странами и областями исследования. Например, оба автора А и Б могут иметь одинаковое число идентифици-

рованных публикаций (например, 7 публикаций). Это означает, что они не являются соавторами любой из них и все публикации разные (т.е. 7+7=14 публикаций), они написали их совместно и все публикации перекрываются (нааример, 7 публикаций) или они написали в соавторстве несколько публикаций (например,что-то между 8 и 13 публикациями).

Второе, библиографические документы анализировались с помощью разработанного программного обеспечения VOSViewer (версия 1.6.13) [35]. Были созданы два разных библиографических наглядных представления, а именно, сетевая и оверлейная карты КС. *Сетевая карта ключевых слов* (*Network map of keywords*) отражает корреляции между КС и включает создание графов, где каждое КС визуально представлено узлом, размер которого пропорционален числу публикаций, где узлами показывают родственные КС, т.е. КС, которые обычно встречаются вместе в публикации [35]. *Оверлейная карта ключевых слов* (*Overlay map of keywords*) включает измерение времени в сетевой граф с помощью указания ранних и поздних появлений КС в публикациях. Был проведен кластерный анализ 331 (из 7310) слова, появившегося по меньшей мере 5 раз в изучаемых публикациях для обеих карт КС. Визуальное отображение тематических областей на основе совместной встречаемости КС [35] позволяет проводить как качественный, так и количественный анализ и является полезным средством, облегчающим идентификацию релевантных областей исследования, хотя для детального анализа определенной области исследования необходимо проведение систематического обзора литературы.

РЕЗУЛЬТАТЫ

Данный раздел прежде всего представляет анализ топовых авторов, организаций, стран и доминирующих научных областей в исследовании по подготовке пользователей для безопасного использования информационных систем. Далее приводятся и анализируются карты сети и перекрытия КС.

Топовые авторы

В соответствии с табл. 1 все внесшие свой вклад топовые авторы опубликовали схожее число публикаций. Тем не менее, мы можем разделить их на три группы, а именно: авторы с 7, 6 и 5 публикациями. Кроме того, разумно рассмотреть число ссылок, поскольку они могут быть наводящим на мысль показателем качества автора в дополнение к числу публикаций. Выделяются два автора с публикациями, имеющими более высокое число ссылок – Чэнь Л. – 55 ссылок [41] и Ван С.– 49 ссылок [38]. Обе статьи появились сравнительно недавно, но несмотря на это имеют высокое число ссылок, дополнительно показывающих, что обе они хорошего качества, независимо от высокой доли самоцитирований (25,4% и 26,5% соответственно).

Табл. 2 отражает топовые организации. Система Калифорнийского университета (University of California System) кажется самой продуктивной организацией, а Университетская система шт. Джорджия (University System of Georgia) – самой влиятельной среди организаций в соответствии с числом ссылок на наиболее цитируемую публикацию. Ни один из указанных в табл. 2 авторов не выглядит топовым автором, это показывает, что самые продуктивные ученые совсем необязательно выходят из самых продуктивных научных организаций.

Как видно из табл. 3, США имеют наибольшее число публикаций, за ними сравнительно близко идет Китай. К этим двум странам можно добавить Индию, которая единственная из далее приведенных стран имеет более 100 публикаций. Индия среди указанных топовых стран является страной с самой цитируемой публикацией, за ней идут США и Южная Корея.

Таблица 1

Топ-10 авторов

Автор	N	%	Ref_N	Авторы Ref_N	TC_R
Tugnait JK	7	0,35	Tugnait [36]	*Tugnait JK*	34
Kim J	7	0,35	Park [37]	Park HE, *Kim J*, Park YS	8
Wang C	6	0,30	Wang [38]	Wang HM, *Wang C* , Ng DWK	49
Li X	6	0,30	Wu [39]	Wu Y, Weng J, Tang Z, *Li X*	9
Du Q	6	0,30	Xu [40]	Xu D, Ren P, Wang Y, *Du Q*, Sun L	2
Ren P	6	0,30	[Xu [39]	Xu D, *Ren P* , Wang Y, Du Q, Sun L	2
Sun L	6	0,30	Xu [40]	Xu D, Ren P, Wang Y, Du Q, *Sun L*	2
Wang Y	6	0,30	Xu [40]	Xu D, Ren P, *Wang Y*, Du Q, Sun L	2
Chen L	5	0,25	Liu [41]	Liu X, Lu R, Ma J, *Chen L*, Qin B	55
Chen W	5	0,25	Hsu [42]	Hsu J, Liu D, Yiu YM, Zhao HT, Chen ZR, Li J, *Chen W*	21

Примечание: В квадратных скобках приводится порядковый номер автора в «Литературе».

Таблица 2

Топ-10 организаций

Организация	N	%	Ref_N	TC_R
University of California System	28	1,43	Gottlieb et al. [43]	58
Chinese Academy of Sciences	23	1,17	Peng et al. [44]	132
State University of Florida	22	1,12	Biros et al. [45]	40
University of Texas System	18	0,92	Siponen et al. [46]	129

Организация	N	%	Ref_N	TC_R
Bejing Jiaotong University	17	0,86	Zhu et al. [47]	7
Penn State University	16	0,81	D'Arcy et al. [4]	335
United States Department of Defense	16	0,81	Biros et al. [45]	40
University System of Georgia	16	0,81	Straub and Welke [48]	399
Bejing University of Posts	14	0,71	Peng et al. [44]	132
Telecommunications				
University of London	13	0,71	Perera et al.[49]	95

Таблица 3

Топ-10 стран

Страна	N	%	Ref_N	TC_R
США	486	24,84	Straub and Welke [48]	399
Китай	326	16,66	Yuan et al.[50]	171
Индия	116	5,93	Subashini and Kavitha [51]	958
Англия	88	4,49	Willison and Warkentin [52]	134
Австралия	83	4,24	Minasny et al. [53]	147
Россия	72	3,68	Klimova et al. [54]	26
Германия	67	3,42	Baumgart [55]	85
Южная Корея	63	3,22	D'Arcy et al. [56]	335
Канада	59	3,01	Stern et al. [57]	109
Испания	51	2,60	Fernaondez-Alemoan et al. [58]	190

Таблица 4

Топ-10 областей исследования

Область исследования	N	%	Ref_N	TC_R
Вычислительная наука	830	42,4	Subashini and Kavitha [52]	958
Инжиниринг	568	29,0	Ming et al. [59]	157
Образование и исследование образования	219	11,2	Einterz et al.[60]	165
Телекоммуникации	179	9,2	Yuan et al. [50]	171
Экономика бизнеса	121	6,2	Straub and Welke [48]	399
Науки здравоохранения и услуги	86	4,4	Wu et al. [61]	242
Информатика и библиотековедение	79	4,0	Straub and Welke, [48]	399
Медицинская информатика	72	3,7	Wu et al. [61]	242
Здравоохранение, окружающая среда, профессиональная защита	59	3,0	Stern et al. [57]	109
Общественные науки, другие темы	55	2,77	D'Arcy and Hovav [4]	44

Табл. 4 отражает самые доминирующие области исследования. Области вычислительной науки и инжиниринга доминируют в соответствии с числом публикаций, поскольку они охватывают более двух третьих всех публикаций.

Отображение ключевых слов и кластерный анализ

В целях более глубокого понимания и идентификации «горячих» точек исследования библиографические данные представлены визуально. Более связанные КС располагаются ближе друг к другу, что означает: между ними существуют только незначительные различия и они имеют более высокую совместную встречаемость. На рис. 2 показаны шесть идентифицированных основных кластеров*: Healthcare (Здравоохранение), Technology Adoption (Принятие Технологии), Management (Управление), Information Security (Информационная Безопасность), Technical Solutions (Технические Решения) и Physical Security (Физическая Безопасность).

Самыми известными КС в исследовании относительно подготовки пользователя для безопасного применения информационных систем являются: information security (информационная безопасность), management (управление), awareness (осознанность), machine learning (машинное обучение), intrusion detection (интрузивное детектирование), design (дизайн), network security (безопасность сети) и cyber security (кибербезопасность). Карта также предполагает наличие двух различных полюсов. Левый полюс главным образом представляет темы, относящиеся к человеку, а правый – к технологии.

* Чтобы различать названия кластеров и КС, названия кластеров будут приводиться с заглавной буквы. Для рисунков 2 и 3 это разграничение не свойственно. Рисунки приводятся так, как даны у авторов данной работы. — (*прим. ред.*)

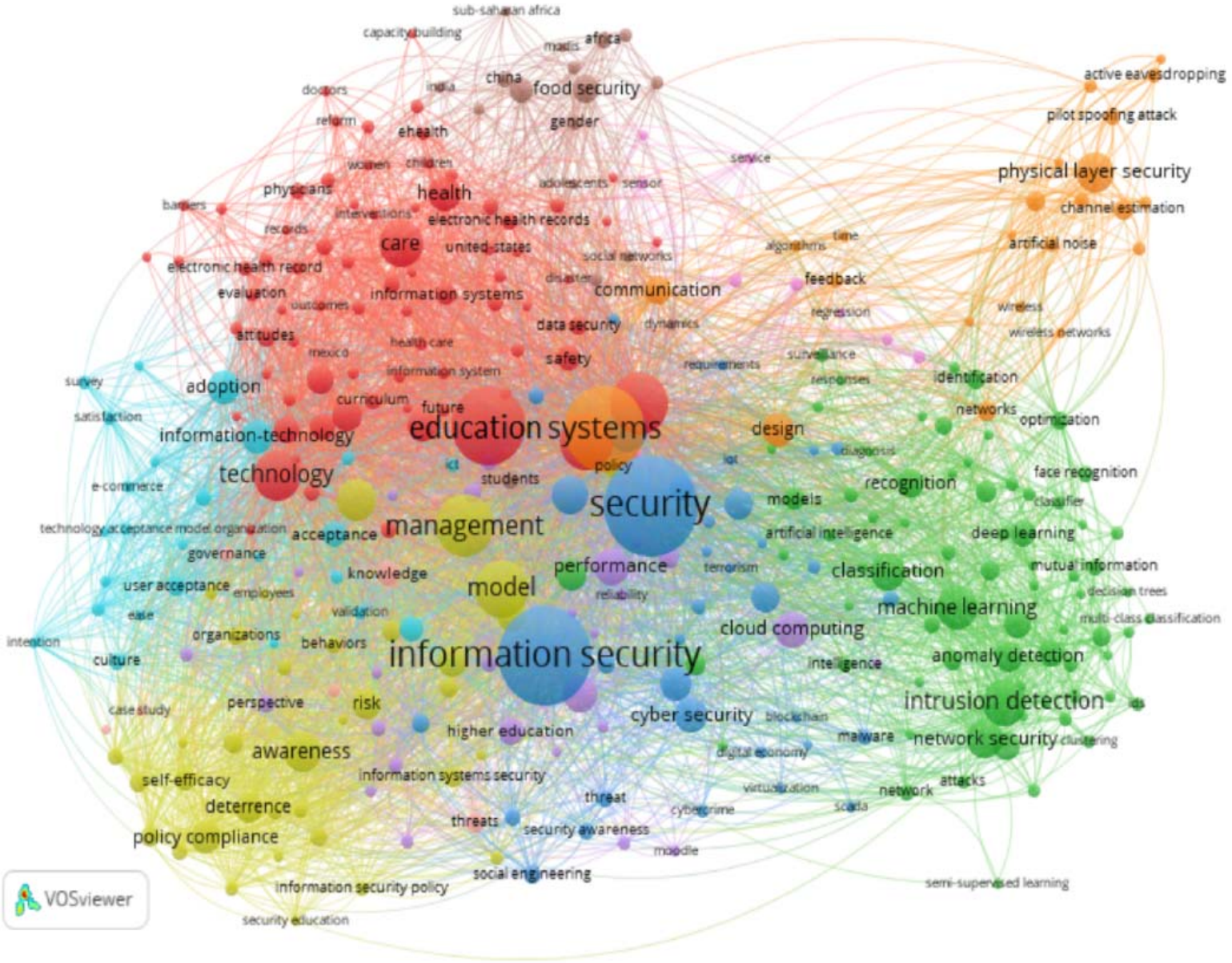

Рис. 2. Изображение сети ключевых слов с выделенными особым образом кластерами

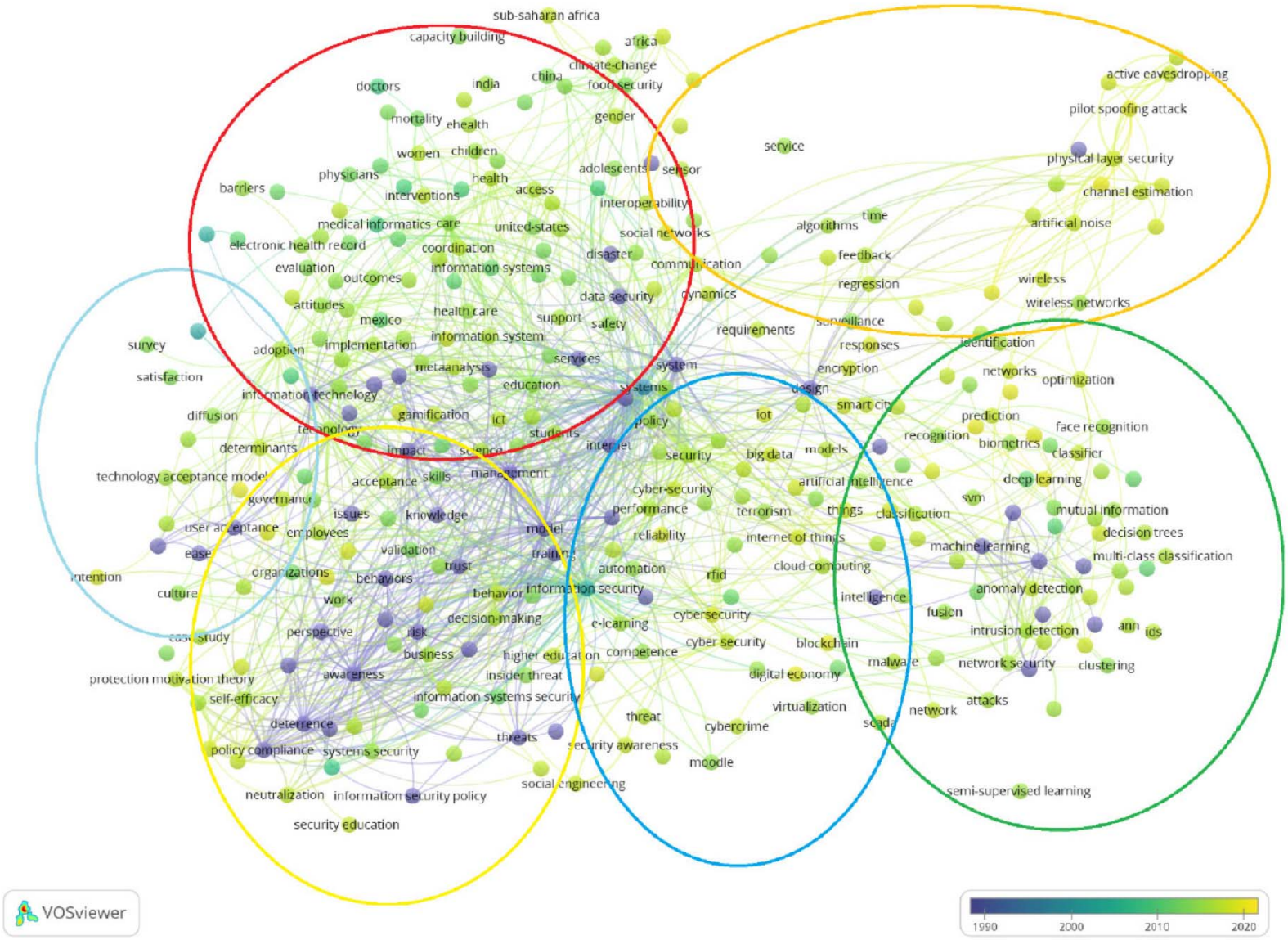

Рис. 3. Оверлейная карта ключевых слов с помеченными кластерами

Однако кажется, что некоторые темы расположены вопреки ожиданию на противоположном полюсе, например, technology (технология) располагается на левом полюсе, представляющем темы, относящиеся к человеку, возможно это из-за того, что это фраза с широким значением (например, как в Принятии Технологии) и поэтому может быть тесно связана с темами из обоих полюсов. Также интересно, что education (образование) помещено в кластер Healthcare (Здравоохранение). Это означает важность защиты чувствительных персональных данных в области здравоохранения. Следовательно, пользователи информационных систем должны быть хорошо образованы в сфере информационной безопасности и защиты данных в этом секторе.

Ключевое слово education (образование) сильно связано с information security (информационной безопасностью) в кластере Information Security (Информационная Безопасность), adoption и acceptance (принятие) – в кластере Technology Adoption (принятие технологии), a security policy compliance (согласие с политикой безопасности), management (управление) и awareness (осознанность) – в кластере Management (Управление). В кластере Technical Solutions (Технические Решения) education (образование) связано с classification (классификацией) и attacks (атаками) и с system (системой), time (временем) и с design (дизайном) – в кластере Physical Security (Физическая Безопасность). Ключевое слово security (безопасность), кажется, в преобладающей степени относится к технологическому полюсу и в меньшей степени - к социологическому. Это предполагает, что в будущем больший акцент необходимо делать на социотехнологическое исследование. Представленные в табл. 4 данные также это поддерживают, поскольку публикации в социологических науках, кажется, получают меньшее число ссылок, демонстрируя более низкую привлекательность темы.

Далее, в анализ были включены временные измерения. Рис. 3 представляет оверлейную карту КС, где отмечены шесть идентифицированных кластеров КС. Чтобы показать временное измерение этих терминов используется тоновая палитра, от более темного до светлого. Темный тон означает, что КС появилось уже в 1990-х гг., а светлый – что оно появилось только недавно. Большинство старых ключевых слов находится в кластерах Management (Управление) и Technical Solutions (Технические Решения). Узлы недавно появившихся КС, таких как security education (образование в сфере безопасности), social engineering (социальный инжиниринг), security awareness (осознанность безопасности), culture (культура), intention (намерение), identification (идентификация) и responses (реакция), находятся значительно дальше от центра, указывая, что они менее связаны.

Из обеих карт КС можно установить, что большинство КС в кластере Healthcare (Здравоохранение) появилось сравнительно недавно, что они включают КС education (образование) и что они сильно связаны с кластером Information Security (Информационная Безопасность). Это ясно указывает на важность образования по информационной безопасности в сфере здравоохранения. В основном это, возможно, произошло благодаря недавним усилиям информатизации в секторе здравоохранения, где значительная доля работников не была достаточно подготовлена в отношении сферы информационной безопасности или там просто отсутствовала мотивация придерживаться политики по информационной безопасности. Например, первая обязанность медиков – улучшение условий по сохранению здоровья своих пациентов, тогда как что-либо еще часто имеет вторичный характер, несмотря на отношение с очень чувствительными медицинскими данными. Кроме того, работники здравоохранения, как правило, менее подготовлены, чем работники других секторов с более длинной историей информатизации [62]. Также стоит отметить, что относящееся к информационной безопасности знание может в значительной степени варьироваться среди работников в одной и той же организации [63]. Важность индивидуальной подготовки пользователя дополнительно акцентируется КС в кластере Management (Управление). Ключевые слова, такие как culture (культура), behavior (поведение), awareness (осознанность) и satisfaction (удовлетворение), показывают, что принятие пользователем мер безопасности зависит не только от его знания и компетенций, но также и от других относящихся к человеку аспектов. Эти аспекты значительно влияют на то, будут ли пользователи воспринимать подготовку в качестве соответствующего и стоящего усилия [64]. Кажется, что этот вид визуализации указывает на недавно появившееся направление в исследовании. Комбинации новых терминов предполагают – индивидуальное обучение станет перспективным будущим направлением исследования. Исследователи могут идти по пути принятия подготовки пользователя для безопасного применения информационных систем на уровне знания и компетенции отдельного работника. Даже более важным может быть осуществление такой подготовки в секторах, часто имеющих дело с высокочувствительными данными, такими как здравоохранение. Этот вид исследования уже появляется (например, [6, 5, 22]), так как подходы подготовки пользователя по типу «одна форма для всех» не могут быть оптимальными [4].

Кластер Technical Solutions (Технические Решения) также является кластером с рядом последних КС, которые хорошо связаны с КС в кластере Information Security (Информационная Безопасность). Это подразумевает потенциал определенных технологий для значительного вклада в безопасное использование информационных систем. Например, deep learning (глубокое обучение), intrusion detection (интрузивное детектирование), artificial intelligence (искусственный интеллект) и КС, относящиеся к продвинутым статистическим подходам – все это облегчает и продвигает в сторону предотвращения киберугрозы, определения и получения ответа. Однако возможности для будущего исследования лежат не только в этих областях, но также и в подготовке пользователя для безопасного использования информационных систем. Общепринято, что education (образование) связано только с КС authentication (аутентификация), classification (классификация) и attacks (атаки) до тех пор, пока не появляются какие-либо заслуживающие внимания ассоциации с artificial intellingence (искусственным интеллектом, machine learning (машинным обучением) или deep learning (глубоким обучением). Это указывает на пробел исследования и возможность обратиться к нему в будущем. Однако связи между узлами могут интерпретироваться в обоих направлениях. Кроме того, это означает, что существует необходимость в исследовании того, как готовить пользователей относи-

тельно использования продвинутых технологических решений. Следовательно, важность подготовки пользователя может возрасти в связи с широким принятием больших данных, умных городов (smart cities), интернета вещей и других появляющихся продвинутых технологий. Кроме того, проникновение этих технологий в будущие информационные системы вызовет даже большую потребность в индивидуальной подготовке пользователя относительно их безопасного применения.

ОБСУЖДЕНИЕ

Теоретическое и практическое применение

В данной статье проводится изучение положения дел в исследовании по подготовке пользователей для безопасного использования информационных систем. Это комплексное исследование с рядом входящих научных областей, таких как вычислительная наука, образование, экономика, управление и т.д. В статье приводится несколько теоретических и практических выводов на основе проделанного исследования. Первое – анализ КС показывает некоторые интересные области для рассмотрения в будущем, особенно информационную безопасность в определенных контекстах, таких как здравоохранение. Кроме того, заслуживает внимания тот факт, что более высокое совпадение и корреляция КС автоматически не означает качество публикаций, т.е. количество не переходит в качество само по себе, однако это может помочь области исследования постепенно эволюционировать и в итоге дойти до полного развития [65]. Второе – даны таблицы под общим названием «топ-10». Таблицы идентифицируют участвующих (т.е. авторы, организации, страны и области) в исследовании по подготовке пользователей для безопасного использования информационных систем. Эти таблицы могут стать отправной точкой для будущих исследований, касающихся качества работ в изучаемых областях, дополняя результаты описанного в данной статье анализа. Третье – на основе КС было обнаружено, что образование или обучение может быть внедрено как на уровне человеческой деятельности [7], так и на уровне технологии (например, машинное обучение). В обоих случаях присутствует человеческий элемент – или как человек, который обучается, или как человек, который создает обучающую машину. Четвертое – результаты проведенного исследования показывают, что в будущем потребуется сделать больший акцент на индивидуальную подготовку в целях безопасного использования информационных систем.

Ограничения и будущая работа

В статье указываются некоторые ограничения, на которые читатель должен обратить внимание. Во-первых, следует отметить, что данные были взяты из библиографической БД Web of Science, включающей самые влиятельные потоки публикаций с наивысшими стандартами [13]. Поиск работ в будущем в других библиографических БД, таких как Scopus, ACM DL и IEEE Xplore, может быть выгодным, поскольку ими часто пользуются исследователи из сферы безопасности. Во-вторых, библиографическая БД Web of Science предлагает организациям разнообразные подписки. Даже если один и тот же поисковый запрос выполняется в тех же самых указателях Web of Science, поиск дает разные результаты в разных учреждениях, если их подписки различаются. Поисковый запрос был выполнен в массиве Web of Science Core Collection, который включает следующие указатели: SCI-EXPANDED (1900 г. – настоящее время), SSCI (1900 г. – настоящее время), A&HCI (1975 г. – настоящее время), CPCI-S (2011 г. – настоящее время), SPCI-SSH (2011 г. -настоящее время), BKCI-S (2011 г. – настоящее время), BKCI-SSH (2011 г. – настоящее время), ESCI (2015 г. – настоящее время), CCR-EXPANDED (2011 г. – настоящее время) и IC (2011 г. – настоящее время). Это означает, что ряд докладов конференций, опубликованных в период 1991-2010 гг. не вошел в данное исследование. В-третьих, визуальное отображение науки в виде карт не может заменить систематические обзоры литературы [66], однако оно предлагает альтернативный анализ и дает возможность посмотреть на тенденции исследований. Такие анализы динамичны, т. е. со временем они могут изменяться. Это может считаться как ограничением, так и направлением для будущих изучений в определенное время.

ЛИТЕРАТУРА

1. *Noddings N.* Philosophy of Education//Encyclopedia of the Social and Cultural Foundations of Education, pp. 1–156. — SAGE Publications, Inc., 2455 TellerRoad, Thousand Oaks California 91320 United States, 2012.

2. *Choi S., Martins J. T., Bernik I.* Information security: Listening to the perspective of organisational insiders// Journal of Information Science. — 2018. — Vol. 44, No. 6. — P. 752–767.

3. *Aldawood H., Skinner G.* Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues//Future Internet. — 2019. — Vol. 11, No. (3). — P. 73.

4. *D'Arcy J., Hovav A.* Does one size fit all? Examining the differential effects of IS security countermeasures// Journal of Business Ethics. — 2009. — Vol. 89, No. (S1). — P. 59–71.

5. *Vasileiou I., Furnell S.* Enhancing security education recognising threshold concepts and other influencing factors// ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, pp. 398–403, Funchal, Madeira, Portugal. — 2018.

6. *Friesel A., Ward A., Welzer T., Poboroniuc M., Mrozek Z.* Building a shared understanding of the skills and competences in order to respond to the current global technical challenges//2014 IEEE Global Engineering Education Conference (EDUCON), pp. 676–679, Istanbul. — IEEE, 2014.

7. *Vavpotič D., Zvanut B., Trobec I.* A comparative evaluation of e-learning and traditional pedagogical process elements// Educational Technology and Society. — 2013. — Vol. 16, No. 3. — P. 76–87.

8. *Vrhovec S. L., Hovelja T., Vavpotič D., Krisper M.* Diagnosing organizational risks in software projects: Stakeholder resistance// International Journal of Project Management. — 2015. — Vol. 33, No. 6. — P. 1262–1273.

9. *Fujs D., Mihelič A., Vrhovec S. L. R.* The power of interpretation// Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19, pp. 1–10, New York, New York, USA. — ACM Press, 2019.

10. *Kokol P., Saranto K., Blažun Vošner H.* eHealth and health informatics competences: A systemic analysis of

literature production based on bibliometrics// Kybernetes. — 2018. — Vol. 47, No. 5. — P. 1018–1030.

11. *Fergnani A.* Mapping futures studies scholarship from 1968 to present: A bibliometric review of thematic clusters, research trends, and research gaps// Futures. — 2019. — Vol. 105 (September 2018). — P. 104–123.

12. *Holman D., Lynch R., Reeves A.* How do health behaviour interventions take account of social context? A literature trend and co-citation analysis// Health: An Interdisciplinary Journal for the Social Study of Health, Illness and Medicine. — 2018. — Vol. 22, No. 4. — P. 389–410.

13. *Garrigos-Simon F., Narangajavana-Kaosiri Y., Lengua-Lengua I.* Tourism and sustainability: A bibliometric and visualization analysis// Sustainability. — 2018. — Vol. 10, No. 6. — P. 1976.

14. *Blanco-Mesa, F., Léon-Castro E., Merigó J. M.* A bibliometric analysis of aggregation operators//Applied Soft Computing. — 2019. — Vol. 81. — P. 105-488.

15. *van Eck N. J., Waltman L.* VOSviewer Manual. Technical Report September, Universiteit Leiden, CWTS Meaningful metrics. — 2019.

16. *Vavpotič D., Vasilecas O.* Selecting a methodology for business information systems development: Decision model and tool support// Computer Science and Information Systems. — 2012. — Vol. 9, No. 1. — P. 135–164.

17. *Meliopoulos A. P. S., Cokkinides G. J., Contaxis G. C.* Computer aided instruction of power system security control functions// IEEE Transactions on Power Systems. — 1987. — Vol. 2, No. 1. — P. 232–238.

18. *Chowdhury B., Clark D.* COPERITE computer-aided tool for power engineering research, instruction, training and education// IEEE Transactions on Power Systems. — 1992. — Vol. 7, No. 4. — P. 1565–1570.

19. *Sasse M. A., Brostoff S., Weirich D.* Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security// BT Technology Journal. — 2001. — Vol. 19, No. 3. — P. 122–131.

20. *Stanton J. M., Stam K. R., Mastrangelo P., Jolton J.* Analysis of end user security behaviors// Computers & Security. — 2019. — Vol. 24, No. 2. — P. 124–133.

21. *Cone B. D., Irvine C. E., Thompson M. F., Nguyen T. D.* A video game for cyber security training and awareness// Computers and Security. — 2007. — Vol. 26, No. 1. — P. 63–72.

22. *Vasileiou I., Furnell S.* Personalising Security Education: Factors Influencing Individual Awareness and AC / P. Mori P., S. Furnell, and O. Camp (ed.)// Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, pp. 315–321, Funchal - Madeira, Portugal. — Springer, 2018.

23. *Logofatu B., Visan A.* New trends in the educational area. Case study regarding the usability of google apps tools within the department for distance learning// The 11th International Scientific Conference eLearning and Software for Education, pp. 526–531, Bucharest.— 2015.

24. *Švábenský V., Vykopal J., Čeleda P.* What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE Conferences// The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). — 2020.

25. *(ISC)2.* Strategies for building and growing strong cybersecurity teams. Technical report, (ISC)2. — 2019.

26. *Furnell S., Fischer P., Finch A.* Can't get the staff? The growing need for cyber-security skills// Computer Fraud & Security. — 2017. — Vol. 2017, No.2. —P. 5–10.

27. *Hood W. W., Wilson C. S.* The literature of bibliometrics, scientometrics,and informetrics //Scientometrics. — 2001. — Vol. 52, No. 2. — P. 291–314.

28. *López-Robles J., Otegi-Olaso J., Porto Gómez, I., Cobo M.* 30 years of intelligence models in management and business: A bibliometric review// International Journal of Information Management. — 2019. — Vol. 48(January). — P. 22–38.

29. *Iqbal W., Javed R. T., Qadir J., Mian A. N., Tyson G., Hassan S. U., Crowcroft J.* Five decades of the ACM Special Interest Group on Data Communications (SIGCOMM): A bibliometric perspective// Computer Communication Review. — 2019. — Vol. 49, No. 5. — P. 29–37.

30. *Wendzel S., Lévy-Bencheton, C., Caviglione L.* Not all areas are equal: analysis of citations in information security research// Scientometrics. — 2020. — Vol. 122, No. 1. — P. 267–286.

31. *Sengupta I. N.* Bibliometrics, informetrics, scientometrics and librametrics: An overview// Libri. — 1992. — Vol. 42, No. 2. — P. 75–98.

32. *Hoffman M. R., Ibáñez, L.-D., Simperl, E.* Scholarly publishing on the blockchain – from smart papers to smart informetrics// Data Science. — 2019. — Vol. 2, No. (1-2). — P. 291–310.

33. *Šubelj L., Waltman L., Traag V., van Eck N. J.* Intermediacy of publications// Royal Society Open Science. — 2020. — Vol. 7, No. (1). — P. 190-207:1–16.

34. *Markscheffel B., Kretschmer H., Pichappan P.* Report of 14 th International Conference on Webometrics, Informetrics and Scientometrics (WIS) & 19th COLLNET Meeting 05 to 08 December 2018, University of Macau, Macau// COLLNET Journal of Scientometrics and Information Management. — 2019. — Vol. 13, No. 1. — P. 3–6.

35. *van Eck N. J., Waltman L.* Software survey: VOSviewer, a computer program for bibliometric mapping Scientometrics. — 2010. — Vol. 84, No. 2. — P. 523–538.

36. *Tugnait J. K.* Self-contamination for detection of pilot contamination attack in multiple antenna systems// IEEE Wireless Communications Letters. — 2015. — Vol. 4, No. 5. — P. 525–528.

37. *Park E. H., Kim J., Park Y. S.* The role of information security learning and individual factors in disclosing patients' health information// Computers & Security. — 2017. — Vol. 65. — P. 64–76.

38. *Wang H.-M., Wang C., Ng D. W. K.* Artificial Noise Assisted Secure Transmission Under Training and Feedback// IEEE Transactions on Signal Processing. — 2015. — Vol. 63, No. 23. — P. 6285–6298.

39. *Wu Y., Weng J., Tang Z., Li X., Deng R. H.* Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems// IEEE Transactions on Intelligent Transportation Systems. — 2017. — Vol. 18, No. 4. — P. 814–823.

40. *Xu D., Ren P., Wang Y., Du Q., Sun L.* ICASBDC: A channel estimation and identification mechanism for MISO-OFDM systems under pilot spoofing attack//2017 IEEE International Conference on Communications (ICC), pp. 1–6. — IEEE, 2017.

41. *Liu X., Lu R., Ma J., Chen L., Qin B.* Privacy-preserving patient-centric clinical decision support system on Naive Bayesian classification// IEEE Journal of

Biomedical and Health Informatics. — 2016. — Vol. 20, No. 2. — P. 655–668.

42. *Hsu J., Liu D., Yu Y. M., Zhao H. T., Chen Z. R., Li J., Chen W.* The Top Chinese Mobile Health Apps: A Systematic Investigation// Journal of Medical Internet Research. — 2016. — Vol. 18, No. 8 :e222.

43. *Gottlieb L. M., Tirozzi K. J., Manchanda R., Burns A. R., Sandel M. T.* Moving electronic medical records upstream// American Journal of Preventive Medicine. — 2015. — Vol. 48, No. 2. — P. 215–218.

44. *Peng M., Sun Y., Li X., Mao Z., Wang C.* Recent advances in Cloud radio access networks: System architectures, keytechniques, and open issues// IEEE Communications Surveys & Tutorials. — 2017. — Vol. 18, No. 3. — P. 2282–2308.

45. *Biros D. P., George J. F., Zmud R. W.* Inducing sensitivity to deception in order to improve decision making performance: A field study// MIS Quarterly. — 2002. — Vol. 26, No. 2. — P. 119.

46. *Siponen M., Adam Mahmood M., Pahnila S.* Employees' adherence to information security policies: An exploratory field study// Information & Management. — 2014. — Vol. 51, No. 2. — P. 217–224.

47. *Zhu L., Yu F. R., Tang T., Ning B.* An Integrated Train–Ground Communication System Using Wireless Network Virtualization: Security and Quality of Service Provisioning// IEEE Transactions on Vehicular Technology. — 2017. — Vol. 65, No. 12. — P. 9607–9616.

48. *Straub D. W., Welke R. J.* Coping with systems risk: Security planning models for management decision making// MIS Quarterly. — 1998. — Vol. 22, No. 4. — P. 441.

49. *Perera G., Broadbent M., Callard F., Chang C.-K., Downs J., Dutta R., Fernandes A., Hayes R. D., Henderson M., Jackson R., Jewell A., Kadra G., Little R., Pritchard M., Shetty H., Tulloch A., Stewart R.* Cohort profile of the South London and Maudsley NHS Foundation Trust Biomedical Research Centre (SLaM BRC) Case Register: Current status and recent enhancement of an Electronic Mental Health Record-derived data resource// BMJ Open. — 2016. — Vol. 6, No. 3:e008721.

50. *Yuan C., Sun X., Lv R.* Fingerprint liveness detection based on multi-scale LPQ and PCA// China Communications. — 2016. — Vol. 13, No. 7. — P. 60–65.

51. *Subashini S., Kavitha V.* A survey on security issues in service delivery models of cloud computing// Journal of Network and Computer Applications. — 2011. — Vol. 34, No. 1. — P. 1–11.

52. *Willison R., Warkentin, M.* Beyond Deterrence: An expanded view of employee computer abuse// MIS Quarterly. — 2013. — Vol. 37, No. 1. — P. 1–20.

53. *Minasny B., McBratney A. B., Malone B. P., Wheeler I.* Digital mapping of soil carbon//Advances in Agronomy. volume 118, pages 1–47. — Elsevier, 2013.

54. *Klimova A., Rondeau E., Andersson K., Porras J., Rybin A., Zaslavsky A.* An international Master's program in green ICT as a contribution to sustainable development// Journal of Cleaner Production. — 2016. — Vol. 135. — P. 223–239.

55. *Baumgart D. C.* Personal digital assistants in health care: Experienced clinicians in the palm of your hand?// The Lancet. — 2005. — Vol. 366, No. 9492. — P. 1210–1222.

56. *D'Arcy J., Hovav A., Galletta D.* User awareness of security countermeasures and its impact on Information Systems misuse: A Deterrence approach// Information Systems Research. — 2009. — Vol. 20, No. 1. — P. 79–98.

57. *Stern N. J., Hiett K. L., Alfredsson G. A., Kristinsson K. G., Reirsen J., Haedardottir H., Briem H., Gunnarsson E., Georgsson F., Lowman R., Berndtson E., Lammerding A. M., Paoli G. M., Musgrove M. T.* Campylobacter spp. in Icelandic poultry operations and human disease//Epidemiology and Infection. — 2003. — Vol. 130, No. 1. — P. 23–32.

58. *Fernández-Alemán J. L., Señor I. C., Lozoya P. á. O., Toval A.* Security and privacy in electronic health records: A systematic literature review// Journal of Biomedical Informatics. — 2013. — Vol. 46, No. 3. — P. 541–562.

59. *Ming J., Hazen T. J., Glass J. R., Reynolds D. A.* Robust speaker recognition in noisy conditions// IEEE Transactions on Audio, Speech and Language Processing. — 2017. — Vol. 15, No. 5. — P. 1711–1723.

60. *Einterz R. M., Kimaiyo S., Mengech H. N., Khwa-Otsyula B. O., Esamai F., Quigley F., Mamlin J. J.* Responding to the HIV pandemic: The power of an Academic Medical partnership// Academic Medicine. — 2007. — Vol. 82, No.8. — P. 812–818.

61. *Wu J.-H., Wang S.-C., Lin L.-M.* Mobile computing acceptance factors in the healthcare industry: A structural equation model// International Journal of Medical Informatic. — 2007. — Vol. 76, No. 1. — P. 66–77.

62. *Vrhovec S., Markelj B.* Relating mobile device use and adherence to information security policy with data breach consequences in hospitals// Journal of Universal Computer Science. — 2018. — Vol. 24, No. 5. — P. 634–645.

63. *van Niekerk J.* Establishing an information security culture in organizations: An outcomes based education approach. Dissertation, Nelson Mandela Metropolitan University. — 2005.

64. *Dincelli E., Goel S.* Research design for study of cultural and societal influence on online privacy behavior//Proceedings of 2015 IPIP 8.11/11.13 Dewald Roode Information Security Research Workshop, pp. 1–18, Newark, Delaware. — 2015.

65. *Hicks D., Wouters P., Waltman L., de Rijcke S., Rafols I.* Bibliometrics: The Leiden Manifesto for research metrics// Nature. — 2015. — Vol. 520, No. (7548). — P. 429–431.

66. *Hallinger P.* Science mapping the knowledge base on educational leadership and management in Africa, 1960–2018//School Leadership & Management. — 2019. — Vol. 39, No. 5. — P. 537–560.