Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Руослахти, Кобёрн, Трент, & Тиканмяки,
Connections QJ 20, № 2 (2021): 33-46
https://doi.org/10.11610/Connections.rus.20.2.04

Рецензированная статья

Пробелы в кибернавыках – системный обзор научной литературы

***Гарри Руослахти,*[1] *Джанель Кобёрн,*[1] *Амир Трент,*[1] *Илкка Тиканмяки*[1,2]**

[1] *Программа безопасности и учёта рисков, Университет прикладных наук Лауреа, Эспоо, Финляндия, http://www.laurea.fi/en*

[2] *Кафедра военной службы, Университет национальной обороны, Хельсинки, Финляндия, https://maanpuolustuskorkeakoulu.fi/en*

Аннотация: Этот обзор литературы является частью исследования роли электронных навыков и обучения им в современном обществе, а именно роли кибернавыков. В статье показано, как научная литература рассматривает кибернавыки и определяет электронные навыки, которые можно считать необходимыми для деятельности нынешнего общества. Во вступлении поясняется общее значение кибернавыков в нашем современном обществе. Далее описан метод анализа и кратко изложены ответы на вопросы наших исследований. Наконец, в заключении на основе результатов исследований рассматриваются достижимость, последствия, сильные и слабые стороны, а также возможные этические проблемы.

Ключевые слова: общество, кибербезопасность, киберобучение, электронное обучение, кибернавыки.

Вступление

Применение компьютеров и других цифровых технологий – повседневная реальность больше чем для половины населения планеты, особенно в современной Европе. Из примерно 7,8 млрд. обитателей планеты на март

2020 г.[1] примерно 59% пользуются Интернетом, и в 2019 г. 49% этих пользователей имели дома компьютеры.[2]

Глядя на эти цифры, логично предположить, что комплекс электронных навыков стал необходимым условием жизни в обществе. Поэтому цель этого обзора литературы – понять связь кибернавыков с электронными навыками и выявить пробелы и кибернавыки, способные заполнить эти пробелы, по данным научной литературы.

Проект ECHO[3] (Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы, European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations), начатый в 2019 г., направлен на упреждающее повышение кибербезопасности в Европейском Союзе благодаря сетевому подходу и действенному сотрудничеству разных секторов. Исследование расширяет собранный в рамках проекта массив знаний, показывая, как обучение кибернавыкам рассматривается в научной литературе, как они соотносятся с более широкими электронными навыками и как такое обучение может помочь выработать практические меры по определению и обучению специальным кибернавыкам в рамках более общих электронных навыков. Планируя это исследование, мы рассматривали электронные навыки как навыки, необходимые для работы в нынешнем цифровом мире, т.е. физической работы с компьютерами и цифровыми устройствами и эффективного использования программ, приложений и цифровой информации.

Система кибернавыков, выработанная в рамках проекта ECHO, определяет подход к описанию требований к кибернавыкам для разработки учебных программ, чтобы вооружить специалистов по кибербезопасности необходимыми знаниями для решения выявленных отраслевых, общих и межотраслевых проблем кибербезопасности.[4] Кроме того, определение конкретных навыков кибербезопасности и соответствующих программ обучения персонала всех уровней может восполнить недостаток знаний, ограничивающий реагирование на атаки. Как отмечено в исследовании ECHO, киберпрограммы и кибернавыки помогут системе здравоохранения и другим

---

1 Joseph Chamie, “World Population 2020: Overview,” *Yale Global Online*, February 11, 2020, по состоянию на 12 апреля 2020, https://yaleglobal.yale.edu/content/world-population-2020-overview.

2 Statista, “Share of Households with a Computer at Home Worldwide from 2005 to 2019,” March 2, 2020, по состоянию на 11 апреля 2020, https://www.statista.com/statistics/748551/worldwide-households-with-computer.

3 European Commission, “European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO),” Grant Agreement Number: 830943 – ECHO – H2020-SU-ICT-2018-2020/H2020-SU-ICT-2018-2 (2019).

4 European Commission, “European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO),” Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 121.

секторам сделать важный шаг к совершенно новому уровню кибербезопасности.[5]

Согласно Чейми,[6] современное общество развилось в технологический мир благодаря появлению Интернета. Интернет изменил все аспекты жизни общества, от ведения бизнеса (превратив традиционные компании в цифровые) до средств обучения (например, при помощи платформ электронного обучения) и взаимодействия между людьми (в соцсетях). С развитием инструментов информационно-коммуникационных технологий (ИКТ), например, ручных мобильных устройств, обеспечивающих постоянный и мгновенный доступ в Интернет, люди больше, чем когда-либо, связаны с ИКТ. ИКТ – неотъемлемый элемент нашей повседневной жизни. Кроме многочисленных выгод использования Интернета и других ИК технологий, к сожалению, есть и угрозы, например, от хакеров, которые пытаются воспользоваться уязвимостью этих ИКТ в преступных целях. Чтобы понять важность развития кибернавыков, в этом обзоре литературы основное внимание уделено киберобучению и развитию кибернавыков в соответствующих статьях. Цель данного исследования – расширить имеющиеся знания об обучении ИКТ. Для упорядочения, в данном исследования ставились такие вопросы:

Вопрос 1: Как научная литература описывает пробелы в кибернавыках?

Вопрос 2: Какие меры предлагаются в научной литературе для восполнения этих пробелов?

Методы

Главный метод данного исследования – системный обзор литературы. Это качественное исследование, и главная задача этого системного обзора современной литературы – выявить пробелы в знаниях о кибернавыках современного общества с целью прояснения выработки электронных навыков для дальнейших исследований.[7]

Построение качественного исследования

Согласно Китченхэму,[8] системный обзор литературы – кропотливый процесс, который может помочь представить свидетельства последствий неких событий, описанных в исследовании, которые не могут передать традиционные несистемные обзоры литературы. Системные обзоры литературы могут быть шире обычных. Для выполнения обзора литературы проводился

---

5 European Commission, “European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO),” Deliverable 2.2 ECHO Multi-sector Assessment Framework, November 13, 2019, p. 64.

6 Chamie, “World Population 2020.”

7 Barbara Kitchenham, “Procedures for Performing Systematic Reviews,” Joint Technical Report TR/SE-0401 (Keele, UK: Keele University, 2004): 1-26, https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

8 Kitchenham, “Procedures for Performing Systematic Reviews.”

научный поиск, чтобы найти ответы на вопросы исследования. Исследование проходило в четыре этапа: поиск, критерии отбора, анализ табличных данных, и написание выводов и заключения.

Поиск

Поиск статей выполнялся в марте 2020 г. Поиск производился по научным базам данных ProQuest Central и EBSCO Host. В качестве параметров поиска при логическом поиске по ключевым словам использовали словосочетания «обучение кибербезопасности» и «обучение электронным навыкам». Период для поиска охватывал литературу, вышедшую за 10 лет, в 2010-2020 гг.

Поиск в базе данных ProQuest Central выдал всего 67 рецензированных статей, а в базе данных EBSCO Host – ещё две рецензированных статьи. Окончательная выборка отбиралась для анализа, применяя критерии включения к 67 статьям из первоначального поиска по ключевым словам. К оригинальным 69 документам применялись следующие критерии включения: название или аннотация включали темы, связанные с кибер- (электронными) навыками обучения работников и кибер- (электронными) навыками обучения студентов. Применение критериев включения дало окончательную выборку в составе 21 рецензированной статьи (Таблица 1), которые были внимательно прочитаны для анализа.

Таблица 1. Этапы поиска и полученное число научных статей.

Этапы поиска	Статей в выборке
Результаты первоначального поиска в ProQuest Central и EBSCO Host	69
После применения критериев включения	21

Анализ окончательной выборки проводился путём переноса релевантных фрагментов информации в таблицу данных на основе вопросов исследования. В следующем разделе рассмотрены выводы из выборки, включавшей 21 статью.

Выводы

Внимание к кибернавыкам

Результаты показывают, что кибербезопасность представляет существенную проблему в современном обществе. С развитием новых технологий и сетевых возможностей для критической инфраструктуры и повседневной деятельности киберустройства становятся уязвимыми для кибератак, от кражи личных данных до кибершантажа, и эти атаки могут существенно влиять на финансовые, экономические и социальные системы. Большое число статей, не соответствующих критериям включения, указывает на то, что многие авторы рассматривают кибербезопасность в основном с позиций технологии или рисков.

Статьи, включённые в окончательную выборку, показывают, что большинство людей, имеющих доступ к ИКТ-устройствам, подвергаются риску. Это люди, которые слабо знакомы с кибербезопасностью или не применяют надлежащие меры кибербезопасности. Проблемы кибербезопасности различаются в зависимости от возраста. Молодёжь более подвержена кибератакам, по ряду причин: неприменение мер безопасности, излишнее доверие к защите своих персональных устройств, незнание новых технологий соцсетей, активные покупки в интернете. Разглашение личной информации в соцсетях или на сайтах, к которым имеют доступ третьи лица, тоже повышает риск для кибербезопасности.

В целом стоит отметить, что электронные навыки упоминаются намного реже, чем кибернавыки. Навыки кибербезопасности на рабочем месте и в профессиональной деятельности – главная тема обсуждения. 17 из 21 рецензированной статьи касаются навыков кибербезопасности, обучения кибербезопасности и безопасности информации (сетей). Поиск термина «электронные навыки» дал всего один результат, три другие статьи были найдены по ключевому слову «электронное обучение». Исходя из этого, один из первых выводов обзора литературы состоит в том, что научные публикации намного чаще касаются нынешних угроз кибербезопасности, недостаточности киберподготовки и квалификации для противодействия современным киберугрозам и новых методов обучения противодействию угрозам кибербезопасности.

Анализ содержания 21 статьи первоисточников об электронных и кибернавыках позволил выявить четыре крупные тематические категории.

1. Общая кибербезопасность: 8 статей касаются необходимости и практики обучения кибербезопасности, информированности и грамотности.
2. Обучение кибербезопасности: в 7 статьях речь идёт о необходимости киберобразования в числе учебных программ, рекомендуются методы обучения кибербезопасности и показаны отличия между киберобразованием и киберобучением. Среди подкатегорий обучения кибербезопасности появились кибер-полигоны и упражнения. В этих статьях описаны такие полигоны и упражнения, как механизмы обучения и то, как они работают.
3. Электронное обучение: 5 статей дают определение электронного обучения, описывают препятствия для электронного обучения, необходимость навыков ИКТ для завершения электронного обучения и эффективные и конкретные практические подходы к успешному электронному обучению.
4. Электронные навыки: только в одной статье из первоначальной выборки речь идёт о необходимости повышать навыки ИКТ в ЕС, почему эти электронные навыки нужны в повседневной работе и личной жизни, и как это влияет на экономику ЕС и всего мира.

В 8 из 21 статей упоминаются навыки, нужные для профессиональной работы или повседневной жизни, либо навыки кибербезопасности, необходимые для предотвращения успешных действий хакеров. В одной статье о специализированных электронных навыках предложены категории, в зависимости от уровня электронных навыков, нужных в повседневной работе. По Сингху,[9] это функциональные категории навыков ИКТ-практиков, ИКТ-пользователей и электронного бизнеса.

Общая кибербезопасность

В Таблице 2 ниже приводится обзор восьми статей об обучении общей кибербезопасности и их темы.

Таблица 2. Статьи об общей кибербезопасности.

Статья	Тема
Ricci et al. (2019)[10]	Результаты исследования среди взрослых и обучение кибербезопасности
Clifton (2018)[11]	Повышение информированности о кибербезопасности в хосписах
Ghafir et al. (2018)[12]	Угрозы безопасности для критической инфраструктуры: человеческий фактор
Russell and Jackson (2018)[13]	Действия в темноте: основы принятия киберрешений
Zăgan et al. (2018)[14]	Морские реалии концепции кибербезопасности

[9] Sumanjeet Singh, "Developing e-Skills for Competitiveness, Growth and Employment in the 21st Century: The European Perspective," *International Journal of Development Issues* (Emerald Group Publishing) 11, no. 1 (2012): 37-59, https://ideas.repec.org/a/eme/ijdipp/v11y2012i1p37-59.html.

[10] Joseph Ricci, Frank Breitinger, and Ibrahim Baggili, "Survey Results on Adults and Cybersecurity Education," *Education and Information Technologies* 24 (2019): 231–249, https://doi.org/10.1007/s10639-018-9765-8.

[11] Tim Clifton, "P-236: Increasing Cyber Security Awareness in the Hospice Environment," *BMJ Supportive & Palliative Care* 8, no. 2 (2018): A94, https://dx.doi.org/10.1136/bmjspcare-2018-hospiceabs.261.

[12] Ibrahim Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," *The Journal of Supercomputing* 74 (2018): 4986-5002, https://doi.org/10.1007/s11227-018-2337-2.

[13] Scott Russell and Craig Jackson, "Operating in the Dark: Cyber Decision-Making from First Principles," *Journal of Information Warfare* 17, no. 1 (2018): 1-15, https://cacr.iu.edu/files/documents/Operating_in_the_dark.pdf.

[14] Remus Zăgan, Gabriel Raicu, Radu Hanzu-Pazara, and Stănică Enache, "Realities in Maritime Domain Regarding Cyber Security Concept," *Advanced Engineering Forum* 27 (April 2018): 221-228, https://doi.org/10.4028/www.scientific.net/AEF.27.221.

Nikolova (2017)[15]	Лучшие практики развития потенциала кибербезопасности в государственном секторе Болгарии
Choi and Lee (2015)[16]	Исследование развития программ информирования о безопасности на основе системы контроля доступа RFID для предотвращения утечек внутренней информации
Rahim et al. (2015)[17]	Системное исследование подходов к оценке знаний о кибербезопасности

Согласно Рахиму и др.,[18] взрослые могут вести себя неосмотрительно в интернете, например, открывая личную почту в Wi-Fi сетях общего доступа, переходя по незнакомым ссылкам или используя один и тот же пароль для разных электронных счетов. Кроме того, пожилые люди обычно не так хорошо разбираются в кибербезопасности, как молодёжь, и более доверчивы, что можно использовать для фишинга и манипуляций, используя их незащищённость.

Обучение кибербезопасности

В Таблице 3 ниже перечислены 7 документов, попавших в окончательную выборку, и их отношение к обучению кибербезопасности.

Результаты показывают, что кибербезопасность в большинстве случаев подрывают человеческие ошибки и слабые знания и навыки кибербезопасности. Поскольку кибербезопасность становится насущной проблемой в современном обществе, затрагивая бизнес, личную жизнь и критическую инфраструктуру, растет потребность в квалифицированном, обученном кибербезопасности персонале для защиты этих систем.

[15] Irena Nikolova, “Best Practice for Cybersecurity Capacity Building in Bulgaria’s Public Sector,” *Information & Security: An International Journal* 38 (2017): 79-92, https://doi.org/10.11610/isij.3806.

[16] Kyong-Ho Choi and Donghwi Lee, “A Study on Strengthening Security Awareness Programs based on an RFID Access Control System for Inside Information Leakage Prevention,” *Multimedia Tools and Applications* 74, no. 20 (2015): 8927–8937, https://doi.org/10.1007/s11042-013-1727-y.

[17] Noor Hayani Abd Rahim et al., “A Systematic Review of Approaches to Assessing Cybersecurity Awareness,” *Kybernetes* 44, no. 4 (2015): 606-622, https://doi.org/10.1108/K-12-2014-0283.

[18] Rahim et al., “A Systematic Review of Approaches.”

Таблица 3. Статьи, касающиеся обучения кибербезопасности.

Статья	Тема
Yamin et al. (2020)[19]	Киберполигоны и испытательные стенды безопасности: сценарии, функции, инструменты и архитектура
Aaltola and Taitto (2019)[20]	Использование экспериментальных и организационных теорий обучения для улучшения показателей человека при киберобучении
Beuran et al. (2019)[21]	Обеспечение обучения кибербезопасности путём интеграции систем организации обучения: система организации киберобучения
Raineri and Fudge (2019)[22]	Изучение достаточности знаний студентов по кибербезопасности в рамках программ предпринимательства ведущих университетов
Chapman et al. (2017)[23]	Можно ли сымитировать атаку на сеть в моделируемой среде для обучения сетевой безопасности?
Adams and Makramalla (2015)[24]	Навыки обучения кибербезопасности: хакероцентричный игровой подход
Lester (2010)[25]	Практическое применение программ безопасности при обучении разработке программного обеспечения

[19] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos, "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers and Security* 88 (January 2020), 101636, https://doi.org/10.1016/j.cose.2019.101636.

[20] Kirsi Aaltola and Petteri Taitto, "Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training," *Information & Security: An International Journal* 43, no. 2 (2019): 123-133. https://doi.org/10.11610/isij.4311.

[21] Razvan Beuran et al., "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS," *Education and Information Technologies* 24 (2019): 3619-3643, https://doi.org/10.1007/s10639-019-09942-y.

[22] Ellen M. Raineri and Tamara Fudge, "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs," *Journal of Higher Education Theory and Practice* 19, no. 4 (2019): 73-92, https://doi.org/10.33423/jhetp.v19i4.2203.

[23] Samuel Chapman et al., "Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?" *Journal of Sensor and Actuator Networks* 6, no. 16 (2017), https://doi.org/10.3390/jsan6030016.

[24] Mackenzie Adams and Maged Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," *Technology Innovation Management Review* 5, no. 1 (January 2015): 5-14, http://doi.org/10.22215/timreview/861.

[25] Cynthia Y. Lester, "A Practical Application of Software Security in an Undergraduate Software Engineering Course," *International Journal of Computer Science Issues* 7, no. 3 (May 2010): 1-9.

Топхэм с коллегами [26] утверждает, что организации, готовящиеся к адекватному отражению угроз, способных нарушить их безопасность и деятельность, должны защищать все критические элементы своей инфраструктуры. Фундамент начинается с пользователей, которые, как показывают результаты, часто оказываются слабым звеном из-за необученности понятию киберугроз и отсутствия опыта снижения возможных киберугроз. Манипуляции и фишинг – самые распространённые атаки, с которыми обычно сталкиваются конечные пользователи. Без специального обучения кибербезопасности эти пользователи с трудом отличают обычный запрос от кибератаки. В результате они могут неумышленно подставить сеть своей компании под удар злоумышленников. Результатом является рекомендация вкладываться в программы информирования о кибербезопасности и киберобучения для противодействия киберугрозам. Гафир и др.[27] видят задачу внедрения обучения кибербезопасности в организациях в том, как правильно организовать обучение, которое реально научит персонал (неспециалистов в ИКТ) применять меры безопасности и развивать свои кибернавыки. Задача специалистов в ИКТ – повышать свою квалификацию для анализа и противодействия постоянно меняющимся киберугрозам.

Адамс и Макрамалла[28] отмечают, что главное препятствие, мешающее персоналу научиться применению мер безопасности и выработать навыки кибербезопасности, возникает из-за преподавания в рамках программ обучения кибербезопасности. Большинство этих программ учат безопасности традиционно, информацию бывает сложно усвоить и применить на практике. Дополнение теоретических знаний сотрудников общего профиля экспериментами и интерактивным обучением (игры, задачи, сценарии) может дать более практичную подготовку с фокусом на реальные угрозы (например, на киберполигонах). Программы обучения кибербезопасности, реализуемые собственными ИКТ-специалистами организаций, могут действенно оптимизировать развитие навыков кибербезопасности и понимание угроз у сотрудников для умелой защиты себя и своей организации от атак.

По мнению Топхэма и др.,[29] практическое обучение при помощи упражнений в сети и интерактивных киберлабораторий может помочь развить соответствующие кибернавыки студентам, изучающим кибербезопасность в ВУЗах. В результате они будут затребованы компаниями при приёме на работу в качестве компьютерно грамотных сотрудников и даже будущих кибер-специалистов, способных справиться с нынешними и будущими киберугрозами с развитием ИК технологий.

---

[26] Luke Topham et al., “Cyber Security Teaching and Learning Laboratories: A Survey,” *Information & Security: An International Journal* 35, no. 1 (2016.): 51-80, https://doi.org/10.11610/isij.3503.

[27] Ghafir et al., “Security Threats to Critical Infrastructure.”

[28] Adams and Makramalla, “Cybersecurity Skills Training.”

[29] Topham et al., “Cyber Security Teaching and Learning Laboratories.”

Электронное обучение

В Таблице 4 ниже представлен обзор пяти документов, касающихся электронного обучения. Электронное обучение считается ценным активом для инвестирования организаций с целью достижения оптимальных деловых и личных результатов во всей своей деятельности, зависящей от ИКТ. Оно предусматривает разработку программ электронного обучения, развивающих электронные навыки и дающих образование, нужное для эффективного использования современных ИКТ-устройств, сетей и систем.

Таблица 4. Статьи, касающиеся электронного обучения.

Статья	Тема
Iqbal (2016)[30]	Разработка и появление педагогической онлайн-лаборатории информационной безопасности как целостного артефакта
Topham et al. (2016)[31]	Обучение кибербезопасности и учебные лаборатории: исследование
Hagen et al. (2011)[32]	Долгосрочные результаты электронного обучения информационной безопасности для обучения в организации
Annansingh and Bright (2010)[33]	Изучение препятствий для эффективного электронного обучения: Пример DNPA
Anonymous (2010)[34]	Электронное обучение в Администрации национального парка Дартмур: Как свести к минимуму процент отсева и невосприятие будущих программ обучения

[30] Sarfraz Iqbal, "Design and Emergence of a Pedagogical Online InfoSec Laboratory as an Ensemble Artefact," *Journal of Information Systems Education* 27, no. 1 (2016.): 17-35, https://aisel.aisnet.org/jise/vol27/iss1/2.

[31] Topham et al., "Cyber Security Teaching and Learning Laboratories."

[32] Janne Hagen, Eirik Albrechtsen, and Stig Ole Johnsen, "The Long-term Effects of Information Security e-Learning on Organizational Learning," *Information Management & Computer Security* 19, no. 3 (2011): 140-154, https://doi.org/10.1108/09685221111153537.

[33] Fenio Annansingh and Ali Bright, "Exploring Barriers to Effective e-Learning: Case Study of DNPA," *Interactive Technology and Smart Education* 7, no. 1 (2010): 55-65, https://doi.org/10.1108/17415651011031653.

[34] Anonymous, "E-learning at Dartmoor National Park Authority: How to Minimize Drop-out Rates and Resistance to Future Training Programs," *Development and Learning in Organizations* 24, no. 6 (2010): 20-22, https://doi.org/10.1108/14777281011084720.

Один из самых популярных методов электронного обучения, которые упоминают Аннансингх и Брайт[35] – сетевое электронное обучение, при котором ресурсы распределяются на сетевых платформах и доступны на любом компьютере, подключённом к Интернету. Выгоды сетевого электронного обучения включают дистанционность, возможность работать на курсах в любом месте и в любое время, возможность интерактивного обучения, например, при помощи практичных приложений с ситуативными примерами, в отличие от обучения учителем посредством лекций для понимания безопасности, и возможность повторения предыдущих курсов для закрепления понимания. Наконец, знания, полученные при сетевом электронном обучении, запоминаются лучше, чем при традиционном обучении.

При всех преимуществах электронного обучения, проблемой является то, что электронное обучение требует серьёзных навыков ИКТ. Сотрудники с ограниченными навыками ИКТ могут не усвоить информацию так, как те, кто имеет опыт и навыки ИКТ. Среди препятствий отмечаются недостаток времени для электронного обучения, сопротивление изменению привычного обучения (обучение с учителем по сравнению с онлайн-обучением) и поддержание дисциплины при обучении на длительных курсах электронного обучения. Все эти причины могут привести к отсеву с увеличением продолжительности курсов. Негативный опыт курсов электронного обучения тоже может помешать успеху.

Для успешного проведения курсов электронного обучения Аннансингх и Брайт[36] рекомендуют учитывать возможности слушателя электронных курсов. Успех программ электронного обучения, с одной стороны, зависит от того, как проводится курс, а с другой – от слушателя. Слабость слушателя может помешать участию сотрудника или успеху электронного обучения. Результаты показывают, что стимулирование (например, продвижение по службе или повышение зарплаты) может сильнее побудить сотрудников заняться электронным обучением.

Электронные навыки

Как видно из Таблицы 5 ниже, в окончательную выборку попала лишь одна статья, в которой рассмотрен термин «электронные навыки».

Таблица 5. Статьи, касающиеся электронных навыков.

Статья	Тема
Singh (2012)[37]	Развитие электронных навыков для конкуренции, роста и работы в XXI веке

[35] Annansingh and Bright, “Exploring Barriers to Effective e-Learning.”

[36] Annansingh and Bright, “Exploring Barriers to Effective e-Learning.”

[37] Singh, “Developing e-Skills for Competitiveness.”

Согласно Сингху,[38] мир становится всё более ИКТ-ориентированным, и развитие общих навыков ИКТ (электронных навыков) просто необходимо. В связи с широким влиянием ИКТ на общественную и личную жизнь, электронные навыки в современном обществе важны. Инвестирование в ИКТ / электронные навыки может дать множество преимуществ, кибернавыки дают знания и возможности для защиты от киберугроз.

Заключение

В научной литературе в основном обсуждают текущие вопросы кибербезопасности: киберугрозы, киберобучение и квалификацию. Предлагается путём исследований определить, какие электронные навыки, кроме необходимых навыков кибербезопасности, нужны для успеха в современном обществе. Исследование позволило выделить четыре главные категории электронных навыков. Как видно из Таблицы 6, эти категории помогают понять роли кибер- и электронных навыков в современном обществе. Становится очевидным, что пользователи, будь то обычные граждане, работники или ИКТ/киберспециалисты, потенциально являются слабым звеном в кибервопросах. Поэтому нужны кибернавыки для защиты людей, организаций и общества от деструктивных киберинцидентов и злонамеренных кибератак.

Программы обучения кибербезопасности для всех аудиторий с разными электронными навыками и киберзнаниями могут помочь выработать культуру кибербезопасности с надлежащим поведением и установкой на защиту в Интернете. Такую платформу информирования о безопасности могут дополнять методы обучения, чётко проясняющие вопросы кибербезопасности и киберугроз для лучшего понимания кибератак. Применяя эти контрмеры кибербезопасности, люди будут легче воспринимать информацию о кибербезопасности и охотнее принимать меры безопасности в Интернете, что будет способствовать безопасному поведению в киберпространстве и окажет положительное влияние на общество.

Если пользователям сложно отличить обычный запрос от возможной кибератаки, это говорит о пробеле в обучении кибербезопасности. Поэтому инвестирование в программы обучения кибербезопасности и киберобучение противодействию киберугрозам должно быть приоритетом организаций.

Поскольку ИКТ стали важным фактором глобальной конкурентоспособности, роста и инноваций в Европе, необходимо инвестировать в обучение электронным навыкам и кибербезопасности для повышения устойчивости общественных, экономических и промышленных систем. Правительства и научные учреждения могли бы помочь различным организациям решить проблему низкой ИКТ-компетентности сотрудников, помогая организации

[38] Singh, “Developing e-Skills for Competitiveness.”

курсов обучения кибернавыкам и обучению электронным навыкам, что поможет стабильному росту и инновациям европейских экономик благодаря развитию ИКТ.

Таблица 6. Главные выводы.

Категория	Главные выводы
Общая кибербезопасность	• киберустройства уязвимы для кибератак • люди либо не знают о кибербезопасности, либо не принимают мер кибербезопасности
Обучение кибербезопасности	• конечные пользователи часто являются самым слабым звеном • рекомендуется инвестировать в программы обучения кибербезопасности и киберобучение • может быть полезным практическое обучение с помощью имитации в сети и интерактивного обучения в киберлабораториях
Электронное обучение	• электронное обучение – важный актив для инвестирования организаций • выгоды сетевого электронного обучения: удалённый доступ, работа в любом месте/в любое время, возможность интерактивного обучения
Электронные навыки	• современное обществе постепенно становится более технологичным • обучение электронным навыкам стало необходимостью • электронные навыки нужны как бизнесменам, так и обычным пользователям • выгоды развития электронных навыков велики и на личном уровне

Кроме того, чтобы внедрить эффективные программы кибербезопасности и электронных навыков, преподаватели должны устранить причины, мешающие пользователям инвестировать в эти программы. Преподаватели могут адаптировать свои педагогические методы и системы таким образом, чтобы те приносили наибольшую пользу конечным пользователям, одновременно оптимизируя совершенствование их электронных навыков. В результате учащийся получит интересный опыт этих программ и сможет использовать новые навыки для личного совершенствования, внося свой вклад в общество.

Исследование выявило общий недостаток устоявшихся терминов ИТ. Это «электронные навыки», «кибернавыки», «компьютерные навыки», «ИКТ

навыки», и все они могут иметь разные значения у разных авторов. Мы рекомендуем продолжить исследования и дать чёткое определение каждому из этих терминов.

Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Данная работа была выполнена при поддержке проекта ECHO, финансируемого по программе исследований и инноваций Европейского Союзы «Horizon 2020» согласно грантового соглашения № 830943. Финансируемые Европейской Комиссией пилотные проекты, такие, как Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы (ECHO), дают исследователям возможность проводить эксперименты и собирать эмпирические данные для изучения этих вопросов с разных точек зрения.

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторах

Д-р Гарри Руослахти – старший преподаватель программы безопасности и учёта рисков в Университете прикладных наук Лауреа. Возглавляет группу Лауреа в проекте «Европейская сеть центров кибербезопасности и хабов компетенции для инноваций и работы» (ECHO) программы «Horizon 2020». Электронная почта: harri.ruoslahti@laurea.fi

Джанель Кобёрн работала экспертом по научным исследованиям и инновациям в Университете прикладных наук Лауреа, где она принимала участие в ряде научно-исследовательских проектов, включая изучение кибернавыков в рамках проекта ECHO.

Амир Трент – студент бакалавраата по информационным технологиям для бизнеса в Университете прикладных наук Лауреа.

Илкка Тиканмяки – научный сотрудник программы безопасности и учёта рисков в Университете прикладных наук Лауреа, докторант в области оперативного искусства и тактики Университета национальной обороны Финляндии.