НАУЧНЫЙ ДАЙДЖЕСТ ТГУ:

обзор новостей и ресурсов об искусственном интеллекте

Тема выпуска:

“Технологии безопасности: искусственный интеллект на защите информации”

2022 №5 (18)

Погружение в проблему

Как искусственный интеллект усиливает кибербезопасность?

Искусственный интеллект и машинное обучение в кибербезопасности — прогноз на будущее // Сайт «Лаборатории Касперского», 2020

Несмотря на то, что на сегодняшний день кибербезопасность во многом зависит от непосредственного участия специалиста, можно значительно повысить эффективность реакции на кибератаки и противодействия киберугрозам за счет автоматизации. В статье представлен обзор проблем кибербезопасности, которые помогают преодолевать методы машинного обучения, в частности ошибки конфигурирования, усталость от оповещений об угрозах, недостаточная скорость реагирования и др.

Как искусственный интеллект и кибербезопасность определяют экономику будущего?

Artificial Intelligence in Cybersecurity Market — Global Forecast to 2026 // MarketsandMarkets, 2019

Согласно данному прогнозу, во всем мире в ближайшие несколько лет предприятия продолжат наращивать бюджеты кибербезопасности. Значительную долю этих вложений они готовы направить на развитие технологий искусственного интеллекта. Наибольший объем рынка в прогнозируемый период придется на Северную Америку. Драйверами роста рынка станут внедрение Интернета вещей и увеличение числа подключенных устройств, рост случаев киберугроз, растущая уязвимость сетей Wi-Fi к угрозам безопасности и др.

Зачем встраивать искусственный интеллект в стратегию формирования цифрового доверия?

На пути к цифровому доверию // PwC в России, 2019

Стремление компаний сформировать цифровое доверие потребителей — уверенность людей в надежности и безопасности цифровых систем — побуждает их сосредоточиться на устранении рисков, связанных с кибербезопасностью. Опрос 3000 руководителей предприятий из 81 страны мира в рамках «Глобального исследования тенденций информационной безопасности PwC» показал, как этот тренд проявляется в стратегических решениях компаний. Результаты относительно инвестиций российских компаний в технологии искусственного интеллекта демонстрируют недооценку руководителями возможностей оперативного автономного реагирования на киберинциденты извне и внутри компаний.

Усиление кибербезопасности страны — приоритет российских ВУЗов

Дмитрий Чернышенко: В новом учебном году в российских вузах появится 83 магистерские программы по искусственному интеллекту

Заместитель Председателя Правительства Дмитрий Чернышенко сообщил, что в рамках федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика» ведущие российские вузы в новом учебном году увеличат количество программ по подготовке IT-специалистов, исходя из актуальных запросов и потребностей предприятий различных отраслей экономики.

Российские вузы готовят специалистов по 63 IT-направлениям

В связи с высоким спросом на IT-специалистов в российских вузах постоянно увеличивается количество бюджетных мест по направлениям подготовки кадров для цифровой экономики. За последние три года прирост по таким образовательным программам составил почти 15 тыс. бюджетных мест. На предстоящий учебный год вузами по укрупненным группам специальностей и направлений подготовки кадров для цифровой экономики установлено 160 413 бюджетных мест, что на 532 больше по сравнению с прошлым учебным годом. Из распределенных мест 71% передан в региональные университеты.

ТГУ и МФТИ проведут апгрейд программ для подготовки IT-специалистов РФ

Министерство цифрового развития, связи и массовых коммуникаций РФ запустило проект по коренной модернизации образовательных программ в области информационных технологий. Основная цель — подготовка для страны высокопрофессиональных специалистов, способных создавать новые IT-технологии и продукты. Победителем одного из конкурсов, объявленного министерством в рамках реализации проекта, стала совместная заявка МФТИ и ТГУ. Два ведущих вуза РФ проведут апгрейд программ, которые будут реализованы в российских университетах.

Научные СМИ и тематические порталы

KASPERSKY DAILY

В блоге компании «Лаборатория Касперского» публикуются новости, обзоры, аналитика, а также практические советы в сфере кибербезопасности. По словам Евгения Касперского, само понятие «кибербезопасность», в скором времени себя изживет, а на замену ему придет концепция «кибериммунитета».

Positive Technologies

Отечественная компания на своей интернет-площадке как продвигает собственные IT-продукты, так и публикует исследования, аналитику, информацию о критических уязвимостях сайтов и приложений, а также анонсы вебинаров и других мероприятий для практиков в сфере информационной безопасности.

Информационная безопасность

На портале российского специализированного журнала, который выходит раз в месяц в электронном и печатном формате, кроме анонса очередного выпуска, можно прочесть отраслевые новости и приглашения на профессиональные конференции. На платформе социальной журналистики Medium статьи свежего выпуска журнала доступны без подписки.

Security Vision

Сайт российской компании «Интеллектуальная Безопасность» (бренд Security Vision) содержит презентации и видеодоклады руководителя и ведущих сотрудников, обзоры свежих публикаций американского методического ресурса по информационной безопасности NIST Special Publications 800 Series, а также календарь мероприятий для специалистов. Часть материалов дублируется в удобном формате подкаста Security Vision — информационная безопасность от А до Я.

Актуальные научные публикации

Yongxin Liu, JianWang, Jianqiang Li, Shuteng Niu, et al. Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey // **IEEE Internet of Things Journal**, **2022**
DOI: 10.1109/JIOT.2021.3099028

Первым шагом в обеспечении безопасности Интернета вещей (IoT) является обнаружение мошеннических и идентификация законных устройств. Традиционные подходы используют криптографические механизмы для аутентификации и проверки законных устройств, однако, в ряде случаев они не эффективны. Некриптографические подходы требуют больше усилий и еще недостаточно изучены. Авторы статьи представляют всесторонний обзор технологий машинного обучения для идентификации устройств IoT, а также обнаружения скомпрометированных или фальсифицированных устройств с точки зрения агентов пассивного наблюдения или сетевых операторов.

Mamoun Alazab, Swarna Priya Rm, Parimala M, Praveen Kumar, Reddy Maddikunta, et al. Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions // **IEEE Transactions on Industrial Informatics**, **2022**
DOI: 10.1109/TII.2021.3119038

Федеративное обучение (FL) — это недавняя разработка в области искусственного интеллекта, которая основана на концепции децентрализованных данных. Авторы статьи исследуют то, как можно использовать FL для обеспечения лучшей кибербезопасности и предотвращения различных кибератак в режиме реального времени. Они представляют обзор различных разработанных в настоящее время моделей FL для обеспечения аутентификации, конфиденциальности, управления доверием и обнаружения атак.

Yan Chen, Fatemeh Mariam Zahedi, Ahmed Abbasi, David Dobolyi Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools // **Information and Management**, **2021**
DOI: 10.1016/j.im.2020.103394

Фишинговые веб-сайты становятся серьезной угрозой кибербезопасности отдельных лиц и организаций. Инструменты обнаружения таких сайтов предназначены для защиты пользователей, однако, требуют «калибровки доверия», модель которой и предлагают авторы статьи. Эта модель, которую они тестируют с помощью контролируемого лабораторного эксперимента, эффективна для инструментов обнаружения фишинговых веб-сайтов. Результаты анализа показывают, что доверие пользователей к инструментам обнаружения можно измерить с помощью калибраторов доверия.

Актуальные научные публикации

Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, Basel Katt Weaponized AI for cyber attacks // Journal of Information Security and Applications, 2021
DOI: 10.1016/j.jisa.2020.102722

Технологии на основе искусственного интеллекта (ИИ) активно используются не только для киберзащиты, но и в наступательных целях. Исследователи изучили недавние кибератаки, в которых использовались методы ИИ, и определили стратегии, приемы и возможные сценарии, которые можно применять для контроля подобных кибератак.

Iqbal H. Sarker, Shahriar Badsha, et al. Cybersecurity data science: an overview from machine learning perspective // Journal of Big Data, 2020
DOI: 10.1186/s40537-020-00318-5

Авторы статьи подходят к кибербезопасности с позиции науки о данных, что позволяет сделать вычислительный процесс более эффективным по сравнению с традиционными процессами в области кибербезопасности. Автоматизированная и интеллектуальная система безопасности построена по принципу извлечения шаблонов инцидентов безопасности или аналитических сведений из данных о кибербезопасности, а также на создании соответствующей модели, основанной на этих данных. В этом контексте авторы описывают известные методы науки о данных и намечают направления для будущих исследований.

Вклад российских ученых

Alexander Branitskiy, Igor Kotenko, Igor Saenko Applying machine learning and parallel data processing for attack detection in IoT // IEEE Transactions on Emerging Topics in Computing, 2021
DOI: 10.1109/TETC.2020.3006351

Для сети Интернета вещей (IoT) остро стоит проблема обнаружения компьютерных атак. Для её решения авторы статьи предлагают совместить методы машинного обучения и параллельной обработки данных. Экспериментальная оценка предлагаемого подхода показывает, что точность обнаружения атак в сетях IoT приближается к 100 %, а скорость обработки набора данных увеличивается пропорционально количеству параллельных потоков.

Dmitry Zegzhda, Daria Lavrova, Evgeny Pavlenko, Anna Shtyrkina Cyber attack prevention based on evolutionary cybernetics approach // Symmetry, 2020
DOI: 10.3390/sym12111931

Авторы статьи предлагают противодействовать кибератакам путем саморегулирования структуры системы, лежащей в основе так называемого эволюционного подхода, который позволит не только повысить безопасность киберфизических систем, но и определить принципы построения систем, устойчивых к кибератакам. Применение эволюционных моделей позволяет описывать закономерности поведения систем и их технического развития.

Рим Нурмухаметов, Сергей Торин Цифровое доверие (digital trust): сущность и меры по его повышению // Известия Тульского государственного университета. Экономические и юридические науки, 2020

Авторы статьи рассматривают вопросы цифрового доверия, которое определяется как уверенность пользователей в способности электронных институтов, предприятий, организаций, технологий и процессов создать безопасный диджитал мир. Степень цифрового доверия измеряется способностью организации защищать персональные данные и конфиденциальность потребителей цифровых услуг. Составными частями цифрового доверия являются: безопасность, конфиденциальность, надежность, этика взаимоотношений. Как результат представлена структура цифрового доверия и приведены риски, которые могут негативно сказаться на нем.

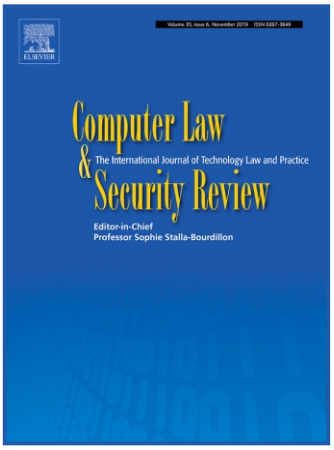
Международные научные журналы

Computers and Security

Высокорейтинговый научный журнал, признанный в качестве основного справочного источника в области IT-безопасности и экспертизы приложений. В материалах журнала сочетаются передовые исследования и надежные практические советы по управлению. Журнал предназначен для профессионалов, занимающихся компьютерной безопасностью, аудитом и целостностью данных в различных отраслях экономики.

Computer Law and Security Review

Международный журнал по проблематике технологического права публикует реферируемые научные и практические статьи по широкому кругу юридических тем, таких как интернет-право, регулирование телекоммуникаций, интеллектуальная собственность, киберпреступность, надзор и безопасность, электронная коммерция, аутсорсинг, защита данных.

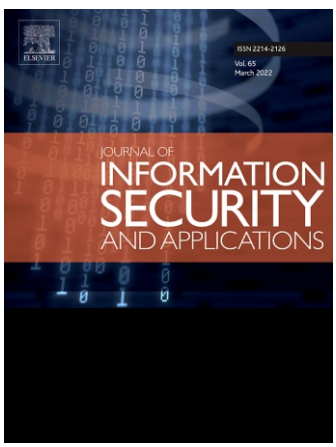


ACM Transactions on Privacy and Security

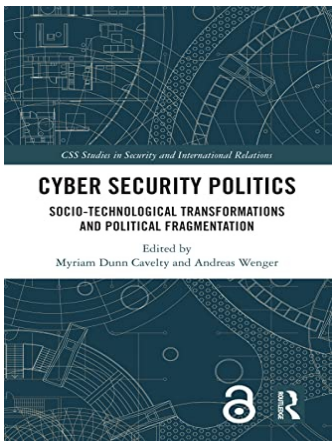
Международный научный журнал посвящен изучению, анализу и применению технологий информационной безопасности и конфиденциальности. Публикуемые теоретические работы подкреплены свидетельствами о практической значимости их результатов. В каждом выпуске журнала встречаются статьи о применении методов искусственного интеллекта в системе безопасности или конфиденциальности.

Journal of Information Security and Applications

Журнал фокусируется на перспективных научных исследованиях и лучших практиках в сфере информационной безопасности. В рамках этой тематики освещается широкий круг современных проблем и вызовов с акцентом на необходимость тесной связи между научно-исследовательским сообществом и профессионалами отрасли.



Книги и монографии



Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation

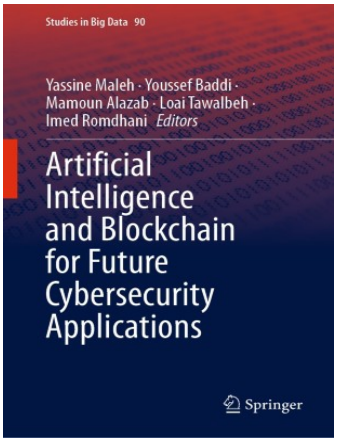
Myriam Dunn Cavelty, Andreas Wenger *(Editors)*

Современная практика использования киберпространства в конфликтных ситуациях обуславливает интерес создателей книги к вопросу достижения политического влияния государства с помощью кибероперация. Внедрение технологических инноваций влияет на государственные управленческие процессы. В этих условиях государства пытаются как-то поддерживать стабильность и сохранять стратегические отношения, хотя проблему ответственности за кибербезопасность пора рассматривать в межсекторальной и транснациональной плоскости управления.

Cyber Security: Issues and Current Trends

Nitul Dutta, Nilesh Jadav, et al.

Книгу можно воспринимать как введение в кибербезопасность. Авторы описывают различные факторы риска, говорят о важности превентивных мер, подробно раскрывают понятия конфиденциальности и анонимности в контексте кибербезопасности. Часть книги посвящена цифровой криминалистике, описанию алгоритма киберрасследований.



Artificial Intelligence and Blockchain for Future Cybersecurity Applications

Yassine Maleh, Youssef Baddi, et al. *(Editors)*

В книге представлены современные исследования в области искусственного интеллекта и блокчейна, практические результаты которых найдут применение в системах кибербезопасности в обозримом будущем. Редакторы охватили широкий спектр проблем интеллектуальных киберэкосистем. Книга может стать справочником для студентов, исследователей, инженеров и специалистов данной области.

Анонсы мероприятий

1

Международный форум по практической информационной безопасности Positive Hack Days

18 – 19 мая 2022 г.

Сайт: phdays.com

2

Конференция про искусственный интеллект и большие данные в бизнесе AI & BIG DATA

31 мая 2022 г.

Сайт: techweek.moscow

3

XXI Всероссийский форум «Информационная безопасность. Регулирование. Технологии. Практика. ИнфоБЕРЕГ»

6 – 9 сентября 2022 г.

Сайт: vipforum.ru

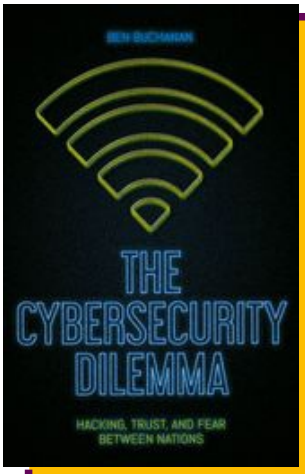
4

XIII Международный Форум «Борьба с мошенничеством в сфере высоких технологий. AntiFraud Russia»

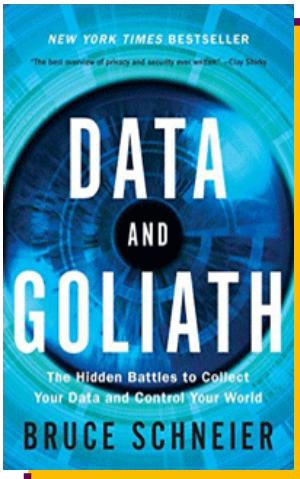
1 декабря 2022 г.

Сайт: vipforum.ru

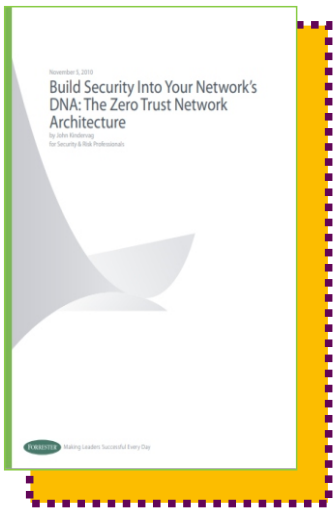
«Золотой архив»



Ben Buchanan
The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.
Oxford University Press, 2017, 304 p.



Bruce Schneier
Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.
W. W. Norton & Company, 2015, 398 p.



John Kindervag
Build Security Into Your Network's DNA: The Zero Trust Network Architecture.
Forrester Research, 2010, 25 p.

Наукометрический анализ (2018 - 2022 гг.)

Источник данных: **Scopus, 9 февраля 2022 г.**

Overall research performance *(Общая характеристика научного направления)*

2,444

Количество публикаций

716 → 70

1.12

Нормированный на отрасль уровень цитируемости

1.06 → 0.42

373

Международное сотрудничество

99 → 20

36,925

Количество просмотров

5,391

Цитируемость

Keyphrase analysis *(Облако ключевых слов)*

Top countries/regions

(Страны-лидеры по количеству публикаций в предметной области)

Countries & territories *(страны, территории)*	Scholarly Output *(количество публикаций)*	Field-Weighted Citation Impact *(нормированный на отрасль уровень цитируемости публикаций)*
China	493	0.71
United States	429	1.15
India	275	1.56
Russian Federation	122	0.91
United Kingdom	108	1.64
Australia	78	1.89
Saudi Arabia	73	1.63
Germany	68	1.38

Наукометрический анализ (2018 - 2022 гг.)

Источник данных: **Scopus, 9 февраля 2022 г.**

Top Institutions

(Университеты и научные организации, лидирующие в предметной области)

Institution *(университеты и научные организации)*	Scholarly Output *(количество публикаций)*	Field-Weighted Citation Impact *(нормированный на отрасль уровень цитируемости публикаций)*
Chinese Academy of Sciences	25	1.07
Anna University	23	0.57
Ministry of Education, China	21	1.12
National University of Defense Technology	20	0.18
CNRS	18	0.56
Beijing University of Posts and Telecommunications	16	0.70
University of Chinese Academy of Sciences	15	0.87
University of Indonesia	15	0.96
State Grid Corporation of China	14	0.19
Xi'an Jiaotong University	14	0.80

Top Authors *(Авторы, лидирующие в предметной области)*

Top Authors *(авторы, лидирующие в предметной области)*	Affiliation *(аффиляция)*	Scholarly Output *(количество публикаций)*	Field-Weighted Citation Impact *(нормированный на отрасль уровень цитируемости публикаций)*
Toapanta, Segundo, Moises Toapanta	Unknown institution	11	0.50
Ahmad, Tohar	Institut Teknologi Sepuluh Nopember	9	0.75
Singh, Madhusudan	Woosong University	9	0.00
Gallegos, Luis Enrique Mafla	Unknown institution	8	0.35
Kotenko, Igor V.	Russian Academy of Sciences	6	0.63
Ochiai, Hideya	The University of Tokyo	6	1.76
Sengupta, Shamik	University of Nevada, Reno	6	1.26
Shahriar, Hossain	Kennesaw State University	6	0.00
Tsochev, Georgi R.	Technical University of Sofia	6	1.46
Gembler, Felix W.	Rhine-Waal University of Applied Sciences	5	1.52

Наукометрический анализ (2018 - 2022 гг.)

Источник данных: ***Scopus, 9 февраля 2022 г.***

Top Scopus Sources *(Журналы-лидеры)*

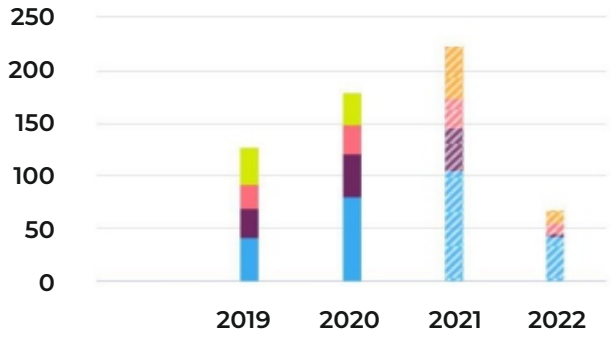
Scopus Sources *(ресурсы Scopus)*	Scholarly Output *(количество публикаций)*	Citation Count *(цитируемость)*	Field-Weighted Citation Impact *(нормированный на отрасль уровень цитируемости публикаций)*
Studies in Computational Intelligence	74	145	1.58
Journal of Intelligent and Fuzzy Systems	30	47	0.62
Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021	26	4	0.91
Neural Computing and Applications	24	127	1.16
Information Sciences	21	362	4.17
Expert Systems with Applications	20	119	1.82
Proceedings of the International Joint Conference on Neural Networks	19	80	1.69
Internet of Things	18	67	2.46
Frontiers in Artificial Intelligence and Applications	17	15	0.51

Publications by Journal quartile

(Публикации по квартилям журналов согласно CiteScore)

Share of publications per Journal quartile by CiteScore Percentile

(Публикации по квартилям журналов согласно CiteScore)



Quartiles *(цитируемость)*	Publications *(публикации)*	Publication share (%) *(доля публикаций)*
Q1 (top 25%)	270	44.9
Q2 (26% - 50%)	111	18.5
Q3 (51% - 75%)	91	15.1
Q4 (76% - 100%)	129	21.5

Дополнительные ссылки

Погружение в проблему

MEGANews. Самые важные события в мире инфосека за март // Xakep.ru, 2022

Технологии обмана. Как нейросети создают фальшивые голоса и лица // Наука и техника, 2022

Анонимизация лиц на фото, видео и веб-камере с помощью OpenCV и Python // NTA – блог компании на VC.RU, 2021

Доверие и цифровые угрозы в современном обществе // Стандарт качества, 2021

Практика противодействия кибератакам и построения центров мониторинга информационной безопасности // SOC-ФОРУМ, видеоматериалы, 2021

Оценка цифровой готовности населения России: доклад НИУ ВШЭ, 2021

A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments // Energy Reports, 2021

Big Data and Security // Third International Conference, ICBDS Proceedings, 2021

Наталья Ромашкина Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности, 2019

Научные СМИ и тематические порталы

Techopedia

Cisoclub

Neuro.net

Security

Techtarget

SecurityMedia

Дополнительные ссылки

Актуальные научные публикации

Yuying Qiu, Zhiyi Niu, Qikun Tian, Biao Song Privacy Preserving Facial Image Processing Method Using Variational Autoencoder // ICBDS 2021: Big Data and Security, 2022

Md. Farhan Haque, Ram Krishnan Toward Automated Cyber Defense with Secure Sharing of Structured Cyber Threat Intelligence // Information Systems Frontiers, 2021

Amr Tolba, Zafer Al-Makhadmeh A cybersecurity user authentication approach for securing smart grid communications // Sustainable Energy Technologies and Assessments, 2021

Parjanay Sharma, Siddhant Jain, Shashank Gupta,Vinay Chamola Role of machine learning and deep learning in securing 5G-driven industrial IoT applications // Ad Hoc Networks, 2021

Yu Zhenga, Zheng Lia, Xiaolong Xuab, Qingzhan Zhaoc Dynamic defenses in cyber security: Techniques, methods and challenges // Digital Communications and Networks, 2021

Mohamed Amine Ferrag, Othmane Friha, Leandros Maglaras, et al. Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis // IEEE Access, 2021

Subodh Mendhurwar, Rajhans Mishra Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges // Enterprise Information Systems, 2021

Naurin Farooq Khan, Naveed Ikram, Hajra Murtaza, Muhammad Aslam Asadi Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach // Kybernetes, 2021

Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash Machine learning cybersecurity adoption in small and medium enterprises in developed countries // Computers, 2021

Amir Namavar Jahromia, Sattar Hashemia, Ali Dehghantanha, et al. An improved two-hidden-layer extreme learning machine for malware hunting // Computers and Security, 2020

Дополнительные ссылки

Вклад российских ученых

Интеллектуальные системы 4-й промышленной революции // Материалы IV международного форума, Томск, 2021

Юрий Веселов, Николай Скворцов Доверие в эпоху цифровых трансформаций: опыт социологического исследования // Социологические исследования, 2021

Dmitry Zegzhda, Evgeny Pavlenko, Elena Aleksandrova Modelling artificial immunization processes to counter cyberthreats // Symmetry, 2021

Elena Popkova, Alexander Alekseev, Svetlana Lobova, Bruno S. Sergi The Theory of Innovation and Innovative Development. AI Scenarios in Russia // Technology in Society, 2020

Юрий Веселов Доверие в цифровом обществе // Вестник СПбГУ. Социология, 2020

Zarina Khisamova, Ildar Begishev, Elina Sidorenko Artificial intelligence and problems of ensuring cyber security // International Journal of Cyber Criminology, 2019

Alexander Shelupanov, Oleg Evsyutin, Anton Konev, Evgeniy Kostyuchenko, Dmitry Kruchinin & Dmitry Nikiforov Information security methods-Modern research directions // Symmetry, 2019

Международные научные журналы

Journal of Cybersecurity

International Journal of Cyber Criminology

IEEE Transactions on Dependable and Secure Computing

IEEE Security and Privacy

Eurasip Journal on Information Security

Security and Communication Networks

Дополнительные ссылки

Книги и монографии

Melissa Lukings, Arash Habibi Lashkari Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective, 2022

Thomas H. Lenhard Data Security: Technical and Organizational Protection Measures against Data Loss and Computer Crime, 2022

Stanislav Abaimov, Maurizio Martellini Machine Learning for Cyber Agents: Attack and Defencer, 2022

Xiaofeng Chen, Willy Susilo, Elisa Bertino *(Eds)* Cyber Security Meets Machine Learning, 2021

Anita Lavorgna, Thomas J. Holt Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, 2021

Sanjay Misra, Amit Kumar Tyagi *(Eds)* Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities, 2021

Sergei Petrenko Developing a Cybersecurity Immune System for Industry 4. 0, 2020

Ramjee Prasad, Vandana Rohokale Cyber Security: The Lifeline of Information and Communication Technology, 2020

Анонсы мероприятий

Сентябрь' 2022: XX Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи

Лето' 2023: Zeronights: конференция по информационной безопасности

Данный информационно-аналитический продукт создается в рамках проекта **«Научные дайджесты ТГУ: фронтирные исследования и технологии»**.

Цели проекта:

— создание информационных продуктов, необходимых для эффективной научной деятельности по самым приоритетным международным направлениям фундаментальных и прикладных исследований;

— периодический информационно-аналитический мониторинг передовых исследований и разработок новейших технологий, позволяющий ученым быстрее осваивать новые предметные поля исследований.

Таким образом, дайджест представляет собой подборку наиболее актуальных научных и научно-популярных источников с их краткими аннотациями и включает результаты наукометрического анализа «топовых» тем, статей и журналов по обозначенной проблематике. Кроме ссылок на самые высоко цитируемые публикации и недавние статьи в международных журналах 1-2 квартилей, здесь содержатся ссылки и на источники, вызвавшие наиболее острые дискуссии.

Рубрики дайджеста:

- Погружение в проблему
- Научные СМИ и тематические порталы
- Актуальные научные публикации
- Вклад российских ученых
- Международные научные журналы
- Книги и монографии
- Анонсы мероприятий
- «Золотой архив»
- Наукометрический анализ
- Дополнительные ссылки

Дайджест подготовлен лабораторией сравнительных исследований качества жизни ТГУ
(руководитель — проф. Э. В. Галажинский)
и лабораторией гуманитарных новомедийных технологий
ТГУ при содействии Научной библиотеки ТГУ
и Информационно-аналитического центра ТГУ.

Руководитель проекта:
И. П. Кужелева-Саган

Менеджер проекта:
Д. И. Спичева

Дайджест подготовили:
И. В. Гужова, Е. Н. Винокурова

Иллюстрация для обложки: shutterstock.com

Архив научных дайджестов НИ ТГУ