НАУЧНЫЙ ДАЙДЖЕСТ ТГУ:

Обзор российских и зарубежных ресурсов

Тема выпуска:

«Суверенные технологии: защита критической информационной инфраструктуры»

2023 №4 (35)

Погружение в проблему

Что требует защиты и регулирования ключевыми игроками мирового киберпространства?

Павел Карасев, Дмитрий Стефанович Кибербезопасность критически важной инфраструктуры: новые вызовы // Россия в глобальной политике, 2022

Защита от кибервоздействий стала в XXI веке одной из важнейших задач национальной безопасности. Прежде всего, подлежат защите субъекты критической информационной инфраструктуры (КИИ), к которым относятся федеральные и региональные органы исполнительной власти, государственные фонды, корпорации и компании, стратегические предприятия, стратегические акционерные общества и системообразующие организации российской экономики (в их числе предприятия оборонной и атомной промышленности, энергетики, транспорта, кредитно-финансовой сферы и другие). Развитые страны активно работают над созданием доктринальных, нормативно-правовых, организационных и технических основ защиты КИИ. Научные сотрудники Центра информационной безопасности ИМЭМО РАН сравнивают подходы США, ЕС, КНР и России к регулированию вопросов кибербезопасности, обозначают перспективы и риски.

Почему нельзя укреплять свою безопасность за счет безопасности других?

Международная информационная безопасность: в поисках консолидированных подходов: интервью с Андреем Владимировичем Крутских // Вестник Российского университета дружбы народов, 2022

По словам Андрея Крутских, спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Россия всегда выступала за развитие всеобъемлющего сотрудничества в этой сфере с учетом интересов всех государств, стремилась к созданию международных площадок равноправного и прозрачного общения. И хотя текущая обстановка на глобальной арене не располагает к оптимистичным прогнозам, безопасность в киберсфере требует международных договоренностей. В интервью рассказывается о шагах, предпринятых дипломатами и учеными РФ на этом пути.

Можно ли строить цифровой суверенитет в партнерстве?

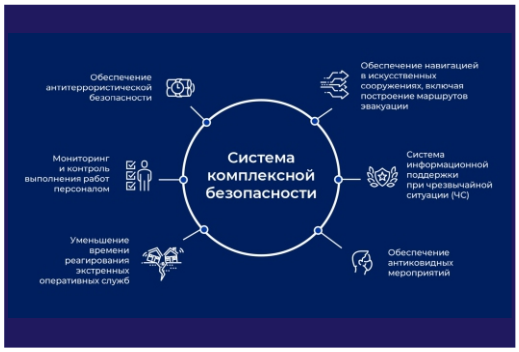
Эпоха российской ориентации на Запад в сфере программного обеспечения завершилась // Сайт Ассоциации компаний-разработчиков программного обеспечения России «РУССОФТ», 2023

Использование организациями, относящимися к субъектам КИИ, отечественного программного обеспечения (ПО) — приоритетная задача цифровой трансформации России. Данные «РУССОФТ» показывают рост внутреннего рынка и экспортных поставок в «дружественные страны» отечественного ПО. При этом аналитики отмечают, что продвижение российских ИТ-продуктов, услуг и платформ не может рассматриваться лишь с точки зрения получения компаниями доходов, а государством — налогов. Цифровая трансформация «дружественных стран» — это ключ к долгосрочной взаимозависимости, обеспечивающей геополитическое партнерство. Поскольку при обеспечении цифрового суверенитета в странах Ближнего Востока, Африки, Латинской Америки и Азии возникают примерно те же проблемы, что и в России, некоторые сложные задачи можно решать совместно с государствами, которые стремятся к технологической независимости тот стран Запада.

Томский государственный университет: курс на суверенные технологии в безопасности

В августе 2023 года подведомственное Минтрансу России Федеральное государственное унитарное предприятие «ЗащитаИнфоТранс» и Национальный исследовательский Томский государственный университет подписали соглашение о сотрудничестве в области образования и науки. ФГУП «ЗащитаИнфоТранс» является центром компетенций в области цифровизации на транспорте, включая информационную и транспортную безопасность. *Подробнее здесь.*

Прототип системы комплексной безопасности, реагирующей на ЧС в автоматическом режиме, был протестирован в Томском госуниверситете в феврале этого года. В ней интегрированы разные подсистемы — от «умной» навигации до видеонаблюдения и «тревожных кнопок». Система индорнавигации, разработанная учеными ТГУ совместно с АО «ГЛОНАСС», ООО «Хайтэк» и ООО «ПКС», станет первым в России подобным продуктом для образовательных учреждений. *Подробнее здесь.*



Томский государственный университет и Институт точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук создадут первый вузовский Центр компетенций в области кибербезопасности. Проект станет частью научно-технической политики Томской области по развитию суверенных технологий. *Подробнее здесь.*

В сентябре в ТГУ состоялся международный научно-практический форум «Политика устойчивости, многовекторности и технологический суверенитет в современных условиях», приуроченный к 145-летию университета. Форум собрал экспертов из Индии, Индонезии, Лаоса, Китая, Пакистана, Таджикистана, Узбекистана, Казахстана и других государств. Центральные темы обсуждения — сотрудничество со странами Азиатско-Тихоокеанского региона, продвижение российского образования, проведение совместных исследований, создание новых технологий для обеспечения государственного суверенитета. *Подробнее здесь.*

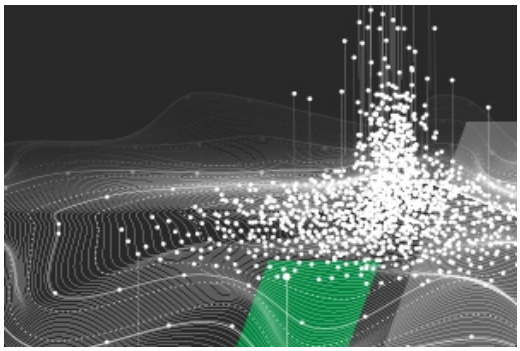
Мониторинг / аналитика / статистика

Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы

В связи с развитием цифровых технологий и необходимостью обеспечения кибербезопасности, а также текущей геополитической обстановкой, повлекшей массовый уход западных производителей с отечественного рынка, в России уже сформировался отечественный рынок решений, включающий в себя реализацию средств защиты информации и услуг в области обеспечения информационной безопасности, что подтвердило исследование ЦСР 2022 года. Фонд представляет обновленные данные о рынке, а также прогноз его развития до 2027 года.

Стратегии кибербезопасности государств Европейского Союза

Экспертно-аналитический центр группы компаний InfoWatch представляет отчет по результатам исследования стратегий кибербезопасности ряда государств Европейского Союза. По ходу исследования проводятся сравнения с ранее рассмотренными стратегиями кибербезопасности Великобритании и США. Также уделено внимание политике государств в отношении наступательных операций в киберпространстве, если таковые упоминаются в их стратегиях.



Safeguarding Critical Information Infrastructure: Risk & Opportunities

Белая книга международной телекоммуникационной компании, штаб-квартира которой расположена в Сингапуре, обозначает тему защиты критической инфраструктуры от злонамеренных кибератак как ключевую проблему для национальной безопасности любого государства. В руководстве делается акцент на внедрении межсекторальных подходов к повышению уровня кибербезопасности, а также на важности диалога и сотрудничества между правительством, частными компаниями, научными кругами, оборонными ведомствами и международными организациями для выработки единой и эффективной стратегии безопасности.

Научные СМИ и тематические порталы

2035 NEWS: Национальная технологическая инициатива

Портал для представителей бизнеса и экспертных сообществ, объединившихся для развития в России перспективных технологических рынков и отраслей, в том числе, информационной безопасности. На сайте публикуются новости, обзоры, аналитика и прогнозы, а также информация о мерах поддержки государством отечественных высокотехнологичных решений.

CISOCLUB

Информационный портал и профессиональное сообщество специалистов, заинтересованных в совершенствовании системы информационной безопасности России. Редакция портала ежедневно публикует наиболее интересные новости, статьи, обзоры, исследования, интервью, вакансии, а также рассказывает о предстоящих мероприятиях по информационной безопасности.

Anti-Malware.ru

Первый в России независимый информационно-аналитический центр, посвященный информационной безопасности и выбору средств корпоративной безопасности. Редакция ставит задачу в равной мере освещать все представленные на российском рынке продукты и услуги в области информационной безопасности, проводить и публиковать непредвзятые тесты, сравнения и обзоры различных решений и методов защиты от всех видов современных IT-угроз.

CIPedia©

Междисциплинарный онлайн-глоссарий по темам защиты критической инфраструктуры (CIP, Critical Infrastructure Protection) и устойчивости критической инфраструктуры (CIR, Critical Infrastructure Resiliency) создан в 2014 году при поддержке Европейского Союза. Сегодня функционирует как Wiki-сервис, контент которого формируется добровольцами международного IT-сообщества.

Актуальные научные публикации

Andrea Pinto, Luis-Carlos Herrera, Yezid Donoso & Jairo A. Gutierrez Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure // Sensors, 2023
DOI: 10.3390/s23052415

Поскольку кибератаки стали более изощренными, системы обнаружения вторжений (IDSS) используют методы машинного обучения (ML), которые могут справляться с более широкими видами угроз. Тем не менее, обнаружение атак «нулевого дня» и нехватка технологических ресурсов для внедрения ряда решений в реальном мире вызывают озабоченность операторов критической инфраструктуры (CI). Цель обзорной статьи — представить подборку эффективных современных IDSS, которые использовали алгоритмы ML для защиты CI. Также в ней представлены наиболее актуальные исследования по этой теме за последние пять лет.

Menelaos N. Katsantonis, Athanassios Manikas, Ioannis Mavridis, et al. Cyber range design framework for cyber security education and training // International Journal of Information Security, 2023
DOI: 10.1007/s10207-023-00680-4

Для эффективной подготовки персонала по кибербезопасности, работающего на объектах критически важной инфраструктуры, используется такой инструмент обучения как эволюция кибердиапазонов (CRS). Авторы статьи провели анализ текущей ситуации в этой области и предложили структуру проектирования Cyber Range (CRDF), которая устраняет слабые стороны существующих подходов к CRS и минимизируют затраты на их подготовку и эксплуатацию с целью обучения специалистов.

Halima Ibrahim Kure, Shareeful Islam & Haralambos Mouratidis An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing and Applications, 2022
DOI: 10.1007/s00521-022-06959-2

Кибератаки на объекты CI превратились из технических в социотехнические, и защита от них требует контекстной информации (о свойствах аналитики угроз, развивающихся тенденциях атак и пр.). В исследовании предлагается новая интегрированная структура управления рисками кибербезопасности: систематическая идентификация критически важных активов осуществляется посредством механизма поддержки принятия решений, построенного на теории нечетких множеств, путем прогнозирования типов рисков с помощью методов ML и оценки эффективности существующих средств контроля. Авторы статьи демонстрируют работу модели на реальном примере CI: она показала свою эффективность в прогнозировании различных типов рисков, включая отказ в обслуживании, кибершпионаж и вредоносное ПО.

Актуальные научные публикации

Prasetyo Adi, Dana Sensuse Review of Security Principles and Security Functions in Critical Information Infrastructure Protection // International Journal of Safety and Security Engineering, 2022
DOI: 10.18280/ijsse.120406

Существует множество работ по защите критической информационной инфраструктуры (CIP), часть которых посвящена угрозам и уязвимостям, а часть описывает принципы безопасности. Однако остается неясным, какие угрозы и уязвимости учитываются в том или ином принципе безопасности. Данное исследование представляет собой обзор моделей CIP с использованием платформы Kitchenham framework. На основе 31 научной публикации и 5 стандартов CIP было установлено, что существует 13 угроз и 16 уязвимостей, которые были классифицированы по трем принципам безопасности. В результате измерения функций безопасности в CIP обнаружено, что только 25% моделей обеспечивают все функции безопасности.

Yuxuan (Cicilia) Zhang, Richard Frank, Noelle Warkentin & Naomi Zakimi Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure // Journal of Cybersecurity, 2022
DOI: 10.1093/cybsec/tyac003

На различных этапах кибератаки инструменты разведки с открытым исходным кодом (OSINT) могут собирать данные с общедоступных платформ и, тем самым, помогать хакерам выявлять уязвимости, разрабатывать вредоносные программы и стратегии атак против целевых секторов CI. Контент-анализ 4000 сайтов на четырех веб-платформах с открытым исходным кодом (Google, YouTube, Reddit и Shodan) показал, что 250 из них предоставляли злоумышленникам информацию, связанную со взломом и / или кибербезопасностью объектов CI. Определены три основных типа данных, которые хакеры могут получить с помощью инструментов OSINT: данные косвенной разведки, коды для проверки концепции и образовательные материалы.

Вклад российских ученых

Daria Gaskova, Elena Galperova & Aleksei Massel Decision Support in the Analysis of Cyber Situational Awareness of Energy Facilities // **The Proceedings of 15th International Conference "Intelligent Systems" (INTELS'22), 2023**
DOI: 10.3390/engproc2023033031

Киберситуационная осведомленность в энергетическом секторе стала интересом современных исследователей ввиду цифрового преобразования энергетики и критической значимости энергетических объектов для экономики стран. Авторы статьи описывают основные концепции осведомленности о киберситуации, некоторые модели представления знаний и ряд показателей безопасности в энергетике. Далее рассматривается использование фреймовых, производственных и сетевых моделей представления знаний при анализе киберситуационной осведомленности энергетических объектов и программных компонентов, реализующих эти модели.

Andrei Dakhnovich, Dmitrii Moskvin & Dmitrii Zegzhda A Necessary Condition for Industrial Internet of Things Sustainability // **Mobile Internet Security. MobiSec 2021. Communications in Computer and Information Science, 2022**

В статье кибербезопасность промышленного IoT сравнивается с промышленными системами управления на базе SCADA, которые используют 5-уровневую модель Purdue Enterprise Reference Architecture для сегментации сети. В системе управления на базе SCADA каждая «вещь» защищена физически, что называется безопасностью, в то время как в системах на базе IoT должны быть обеспечены как безопасность, так и защищенность, что называется кибербезопасностью. Затем авторы предоставляют типичную архитектуру IoT, в которой связь между узлами IoT осуществляется через среду с нулевым уровнем доверия, подобную интернету. Эта архитектура нуждается в новых подходах для обеспечения безопасности коммуникаций. Цель статьи показать, что системы анонимности и теория анонимности могли бы помочь в решении этой проблемы кибербезопасности.

Yong Chen, Yang Lu, Larisa Bulysheva & Mikhail Kataev Applications of Blockchain in Industry 4.0: a Review // **Information Systems Frontiers, 2022**
DOI: 10.1007/s10796-022-10248-7

Интернет вещей (IoT) сегодня широко используется в различных областях промышленности. Однако облачное хранение данных, вычисления и коммуникация в IoT вызывают множество проблем, таких как задержка передачи, единая точка отказа и раскрытие конфиденциальности. Более того, централизованный контроль доступа в IoT ограничивает его доступность и масштабируемость. Блокчейн — это децентрализованная, защищенная от несанкционированного доступа, надежная, прозрачная и неизменяемая база данных, доступная только для добавления. Авторы обзорной статьи описывают, как интеграция технологий блокчейна и IoT привела к созданию надежных распределенных приложений и цифровой трансформации всех сфер индустрии 4.0.

Вклад российских ученых

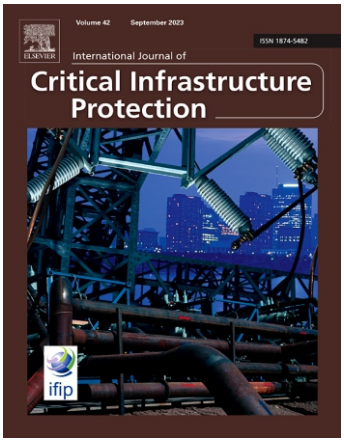
Елена Зиновьева Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии // Полис. Политические исследования, 2022
DOI: 10.17976/jpps/2022.02.02

Информационная глобализация на уровне данных сосуществует с усилением цифровых границ и практикой укрепления цифрового суверенитета. Критическая география изучает цифровые границы как материальные объекты и как социальные конструкты, дискурсивные практики, которые отражают характер властных отношений на международной арене и являются источником власти для тех, кто их создает и контролирует. В статье выделено два уровня цифровых границ — дискурсивный и онтологический. На дискурсивном уровне они отражают секьюритизацию информационной сферы, которая выражается в публичных заявлениях и законодательных актах государства, а на онтологическом — в контроле над инфраструктурой с целью защиты от угроз информационной безопасности.

Мирзет Рамич, Данил Пискунов Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // Вестник Российского университета дружбы народов. Международные отношения, 2022
DOI: 10.22363/2313-0660-2022-22-2-238-255

Конфликты, возникающие в информационно-сетевом пространстве, требуют согласования норм и выработки инструментов правового регулирования. Авторы статьи рассматривают процесс конструирования таких норм с точки зрения теории «сетевого общества» М. Кастельса (управление обществом стало осуществляться за счет инструментов контроля над информацией и формирования фреймов) и теории секьюритизации (информационное пространство стало полноценным политическим пространством, где критично наличие «цифрового суверенитета» и информационной безопасности). С этих позиций «rule maker» способны влиять на глобальные цепочки производства высокотехнологичных товаров, проводить наступательные и оборонительные кибероперации, формировать международно-правовые режимы. Остальные акторы выступают объектом конкуренции таких держав в информационном пространстве.

Международные научные журналы

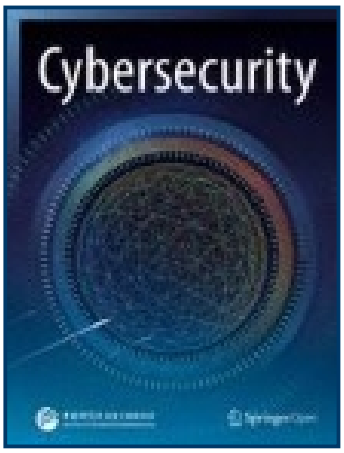


International Journal of Critical Infrastructure Protection

Международный журнал по защите критической инфраструктуры публикует часть статей в открытом доступе. Проблемы информационной безопасности рассматриваются во взаимозависимости между секторами инфраструктуры. Приветствуются статьи, в которых наука, технология, законодательство и политика переплетаются для выработки сложных, но практичных решений по обеспечению безопасности активов в различных секторах критической инфраструктуры.

Journal of Cybersecurity

Научный высокорейтинговый журнал принимает к публикации оригинальные междисциплинарные исследования в области кибербезопасности. Редакция настаивает на недостаточности подходов, основанных лишь на компьютерных науках, поскольку для понимания различных аспектов кибербезопасности необходимы научные материалы из ряда дисциплин. Журнал поддерживает открытый доступ и стремится стать площадкой для формирования международного междисциплинарного сообщества исследователей проблем кибербезопасности.

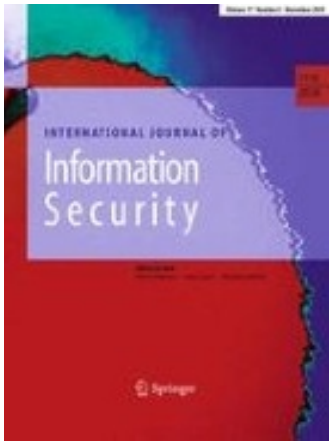


Cybersecurity

Международный журнал открытого доступа освещает все существенные аспекты кибербезопасности. Особое внимание уделяется результатам последних исследований и внедрению технологий безопасности в реальном мире. Среди прочих направлений журнал публикует статьи и обзоры в области анализа вредоносных программ, безопасности сети и критической инфраструктуры.

International Journal of Information Security

Англоязычный научный журнал предлагает оперативную публикацию работ по широкому спектру направлений информационной безопасности. Среди них: обнаружение вторжений, безопасность баз данных, инфраструктуры безопасности, сетевая безопасность, защита контента, конфиденциальность, контроль доступа, аутентификация, идентификация, прикладная криптография и др.
Часть публикаций размещаются в журнале в открытом доступе.



Книги и монографии

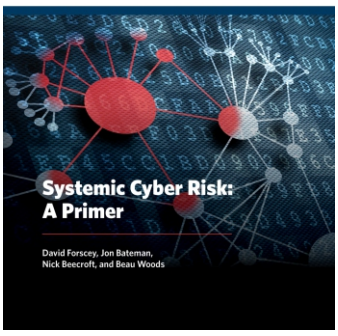
What Is Cybersecurity For?
Tim Stevens

Кибербезопасность является одной из ключевых практических и политических задач нашего времени. Однако общественное понимание этой проблемы все еще находится в зачаточном состоянии: изображения в СМИ хакеров в толстовках, не передают ее сложности или значения для современной жизни. Автор книги устраняет этот пробел, показывая, что политическое измерение так же важно, как и технологическое.

Искусственный интеллект управления информационной безопасностью объектов критической информационной инфраструктуры
Владимир Фисун

В монографии с позиции системного анализа предложен подход к ситуационному управлению процессами информационной безопасности (ИБ) объектов КИИ. Методологическая основа — интеллектуализация процессов управления, начиная от формирования политики ИБ объекта КИИ, и, заканчивая обнаружением и предупреждением компьютерных атак (КА). Интеллектуализация осуществляется с помощью нейросетей, нечеткой логики, генетического алгоритма, базы знаний, экспертной системы поддержки и принятия решений. Эти процедуры искусственного интеллекта (ИИ) контролируются должностными лицами в рамках концепции Государственной системы обнаружения и предупреждения КА (ГосСОПКА).

Systemic Cyber Risk: A Primer
David Forscey, Jon Bateman, Nick Beecroft & Beau Woods



Системный киберриск — возможность того, что единичный сбой где-то в киберпространстве может вызвать расширяющуюся «рябь» с катастрофическими последствиями. Однако это понятие до сих пор остается расплывчатым, а инструменты и методологии для поиска и измерения источников системного киберриска остаются весьма ограниченными. Киберпространство невероятно сложное. Трудно собрать полезные данные о стольких взаимозависимостях, а модели все еще слишком грубы, чтобы делать уверенные выводы на основе имеющихся данных. Авторы издания обобщили существующие исследования с целью создания общей основы для понимания и решения проблем системного киберриска.

Анонсы мероприятий

1

Eurasia Data Center & Cloud Forum

3 – 4 октября 2023 г.

Сайт: dcforum.uz

2

Форум Global Information Security Days (GIS Days 2023)

4 – 6 октября 2023 г.

Сайт: gisdays.ru

3

III Международный форум кибербезопасности государства «ЦИФРОТЕХ»

16 – 20 октября 2023 г.

Сайт: ctexpo.ru

4

Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность» («КИБ-2023»)

18 – 19 октября 2023 г.

Сайт: kib.mephi.ru

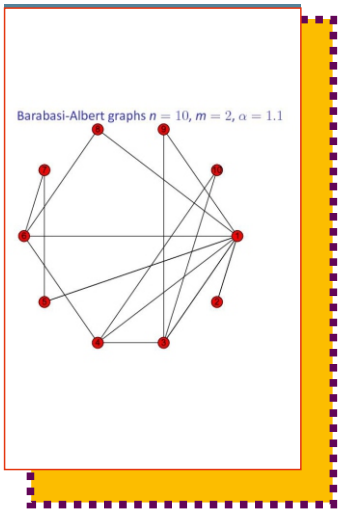
5

SOC-ФОРУМ 2023: Практика противодействия кибератакам и построения центров мониторинга ИБ

14 – 15 ноября 2023 г.

Сайт: forumsoc.ru

Карл фон Клаузевиц
О войне. Избранное.
АСТ, 2017, 320 с.
(впервые опубликована в 1832 г.)



Reka Albert,
Albert-Laszlo Barabasi
Statistical mechanics of complex networks.
Reviews of Modern Physics: journal, 2002, Vol. 74, P. 47–97.

Василий Леонтьев
Межотраслевая экономика.
Изд. дом «Экономика», 1997, 477 с.

Дополнительные ссылки

Погружение в проблему

Positive Research: сборник исследований по практической безопасности // Сайт компании Positive Technologies, 2023

Алексей Комаров Запрет иностранного в КИИ // Zlonov.ru, сайт Алексея Комарова, 2023

Егор Богомолов CyberEd: Наступательная кибербезопасность — скорее творческая, а не детерминированная область // CyberMedia, 2023

Елена Зиновьева, Бай Яцзе Практика цифрового суверенитета в России и КНР // Сайт Российского совета по международным делам, 2023

Кирилл Круглов, Вячеслав Копейцев, Артем Снегирев Техники, тактики и процедуры атак на промышленные компании // SECURELIST by Kaspersky, 2023

Регулирование ИИ в мире и в России: топ событий 2022 года // Tadviser. Государство. Бизнес, Технологии, 2023

Критическая информационная инфраструктура России // Tadviser. Государство. Бизнес. Технологии, 2023

Материалы докладов (презентации) исследователей международных конференций этичных хакеров BlackHat USA и BlackHatAsia // Телеграм-канал «Библиотека хакера», 2023

Наталья Касперская О цифровом суверенитете // InfoWatch, 2023

Научные СМИ и тематические порталы

ComNews.ru

CONNECT. Мир информационных технологий

Cybercrime Magazine

Журнал «Стратегия»

Журнал RuБЕЖ

Центр ГосСОПКА

Дополнительные ссылки

Актуальные научные публикации

Hugo Riggs, Shahid Tufail, Itmiaz Parvez, et al. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure // Sensors, 2023

Roberto Setola New threats and research problems for critical infrastructure // International Journal of Critical Infrastructure Protection, 2023

Casper Almén, Nicholas Hagström, Jyri Rajamäki ECHO Early Warning System as a Preventive Tool against Cybercrime in the Energy Sector // Information & Security: An International Journal, 2022

Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman & Ali Chehab Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations // International Journal of Information Security, 2022

Xiang Liu, Ahmad Sayed Fayaz, Anser Muhammad Khalid, et al. Cyber security threats: A never-ending challenge for e-commerce // Frontiers in Psychology, 2022

Anupam Chander, Haochen Sun Sovereignty 2.0 // Georgetown Law Faculty Publications and Other Works, 2021

Dimitra Markopoulou, Vagelis Papakonstantinou The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular // Computer Law & Security Review, 2021

Norma Möllers Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State // Science, Technology & HumanValues, 2021

Rogier Creemers China's conception of cyber sovereignty: rhetoric and realization // Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics Lanham: Rowman & Littlefield, 2020

Todor Tagarev, George Sharkov & Andon Lazarov Cyber Protection of Critical Infrastructures, Novel Big Data and Artificial Intelligence Solutions // Information & Security: An International Journal, 2020

Дополнительные ссылки

Вклад российских ученых

Владислав Денисов, Сергей Петренко, Александр Костюков Технология анализа программного кода критических приложений цифровой экономики России // Защита информации. Инсайд, 2023

Григорий Гавдан, Александр Вавичкин, Виталий Иваненко, Юлия Кулешова, Элина Рыбалко Устойчивость технологических процессов в аспекте безопасности критической информационной инфраструктуры // Безопасность информационных технологий (IT Security), 2023

Виктор Гаврилов, Александр Зацаринный Проблемы и угрозы некоторых новых цифровых технологий // Системы и средства информатики, 2022

Владимир Фисун Экспертная система поддержки и принятия решений по управлению информационной безопасностью объектов критической информационно инфраструктуры // GLOBUS: Технические науки, 2022

Наталья Иванова Развитие цифровых технологий и новые задачи государственной антимонопольной политики // Полис. Политические исследования, 2022

Aleksandr Ometov, Krustof Zeman, Pavel Masek, Lukas Balazevic & Mikhail Komarov A Comprehensive and Reproducible Comparison of Cryptographic Primitives Execution on Android Devices // IEEE Access, 2021

Международные научные журналы

Digital Government: Research and Practice

EURASIP Journal on Information Security

IET Information Security

Information and Computer Security

Information Security Journal

Intelligence and National Security

Journal of Information Security and Applications

Дополнительные ссылки

Книги и монографии

Anupam Chander and Haochen Sun Data Sovereignty: From the Digital Silk Road to the Return of the State, 2023

Ahmed A. Elngar, Nalesan Thillaiarasu, Mohamed Elhoseny, Kulandairaj Martin Sagayam Cyber Security and Operations Management for Industry 4.0, 2022

Melissa Lukings, Arash Habibi Lashkari Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective, 2022

Cecilia Rikap, Bengt-Ake Lundvall The Digital Innovation Race: Conceptualizing the Emerging New World Order, 2021

Gregory J. Falco, Eric Rosenbach Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity, 2021

Hui Li & Xin Yang Co-governed Sovereignty Network: Legal Basis and Its Prototype & Applications with MIN Architecture, 2021

Maribel Guerrero, David Urbano Technology Transfer and Entrepreneurial Innovations: Policies Across Continents, 2021

Анонсы мероприятий

Сентябрь' 2023: V отраслевой чемпионат в сфере цифровых технологий DigitalSkills

Сентябрь' 2023: Двенадцатый форум по цифровизации оборонно-промышленного комплекса — «ИТОПК-2023»

Сентябрь' 2023: «Информационная безопасность 2023», конференция CNews

Февраль' 2024: 3rd IEEE International Conference on AI in Cybersecurity 2024

Февраль' 2024: International Conference on Information Systems Security and Privacy

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;

— популяризация науки и научной деятельности.

Таким образом, дайджест представляет собой подборку наиболее актуальных научных и научно-популярных источников за последние 3 года с их краткими аннотациями. 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
- Мониторинг / аналитика / статистика
- Научные СМИ и тематические порталы
- Актуальные научные публикации
- Вклад российских ученых
- Международные научные журналы
- Книги и монографии
- Анонсы мероприятий
- «Золотой архив»

Дайджест подготовлен лабораторией сравнительных исследований качества жизни ТГУ
(руководитель — проф. Э. В. Галажинский),
кафедрой социальных коммуникаций ФП ТГУ
и лабораторией гуманитарных новомедийных технологий
ФП ТГУ при содействии Научной библиотеки ТГУ.

Руководитель проекта и научный редактор:
И. П. Кужелева-Саган

Менеджер проекта:
Д. И. Спичева

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

Иллюстрация для обложки: revibeenergy.com

Архив научных дайджестов НИ ТГУ