Об авторе

Петренко Сергей Анатольевич — доктор технических наук, профессор, руководитель Центра информационной безопасности (ЦИБ) АНО ВО «Университет Иннополис».

Университет Иннополис

Университет Иннополис — российский вуз, опорный для Республики Татарстан в области информационных технологий и робототехники. Университет был основан 10 декабря 2012 года в форме автономной некоммерческой организации и ведет свою деятельность по уникальной для России модели, предполагающей тесное взаимодействие образования, науки и бизнеса. Миссией университета является подготовка высококвалифицированных ИТ-специалистов, а также создание и коммерциализация прорывных технологий для выведения отечественной ИТ-отрасли на качественно новый уровень.

В 2013 году университет вошел в число организаций, отобранных в рамках конкурса на создание центров прорывных исследований в области информационных технологий. В 2014 году вуз стал пилотной площадкой для тестирования современных образовательных программ в сфере информационных технологий и осуществления обучения специалистов путем их привлечения к исследованиям и разработкам.

Наряду с образовательным модулем Университет Иннополис активно занимается научно-исследовательской и внедренческой деятельностью.

Привлеченные для учебного процесса ведущие российские и зарубежные ученые из 16 стран мира имеют опыт проведения фундаментальных и прикладных научных исследований в топ-100 ведущих технических вузах мира и обладают высокими показателями цитируемости (более 115 научно-педагогических работников, максимальный индекс Хирша преподавателя — 98).

В университете функционируют три института (технологий разработки ПО, информационных систем, робототехники) и более 20 научных лабораторий

и научных центров, в том числе по направлениям сквозных технологий, с передовой исследовательской инфраструктурой, включая лабораторию анализа данных и машинного обучения в нефтегазовой отрасли, работа в которой востребована крупнейшими российскими нефтегазовыми компаниями. Перед лабораториями университета поставлена задача коммерциализации научных разработок, внедрение передовых технологий и создание передовых сервисов в области цифровой экономики. Результаты работ и разработок Университета Иннополис востребованы крупнейшими компаниями и организациями Российской Федерации и Республики Татарстан — ГК «Росатом», ГК «Роскосмос», Министерство здравоохранения Республики Татарстан, ПАО «Газпром», ПАО «КамАЗ», ПАО «Лукойл», ПАО «Роснефть», ПАО «Транснефть», ПАО «Татнефть» и др.

Научно-проектная деятельность университета направлена на решение стратегических задач сразу нескольких федеральных проектов («Кадры в цифровой экономике», «Цифровые технологии», «Информационная безопасность», «Искусственный интеллект») и преодоление технологических барьеров сквозных технологий цифровой экономики.

Проектный портфель университета включает в себя многочисленные проекты, включая технологию управления инцидентами безопасности на основе искусственного интеллекта, облачную 4D-геоинформационной платформу, геомеханическое моделирование для ПАО «Газпром» и иные проекты по направлениям сквозных цифровых технологий, например, система раннего предупреждения о компьютерном нападении на критически важную информационную инфраструктуру Республики Татарстан на основе NBIC-технологий, системы распределенных реестров (например, ПАО «Аэрофлот»), робототехника (например, ПАО «КамАЗ»), беспилотный транспорт (например, ПАО «КамАЗ», Mail.ru) и искусственный интеллект (например, ГК «Росатом»).

В 2017 году Университет Иннополис был выбран в качестве оператора по разработке и пилотной реализации на территории Республики Татарстан облачной 4D-геоинформационной платформы в целях реализации плана мероприятий «Аэронет», объединив усилия ведущих разработчиков в целях внедрения сервисов ГИС на территории Республики Татарстан. Опыт был признан удачным как руководством университета, так и руководством Республики Татарстан. В 2018 году, оценив организаторские компетенции сотрудников, было принято решение распространить опыт оператора платформы на перспективное и социально-значимое направление здравоохранения — использование технологий искусственного интеллекта для распознавания медицинских изображений.

Заказчиками разработок и консультативных услуг в 2019 году также выступали ГК «Роскосмос», ГК «Росатом», ООО «Газпром Геологоразведка», ПАО «Россети», Министерство информатизации и связи Республики Татарстан и др.

Университет сотрудничает с ведущими зарубежными вузами, входящими в топ-100 технических вузов мира (всего 41 академический партнер, включая Университет Карнеги-Меллона, Национальный университет Сингапура, Швейцарскую высшую техническую школу Цюриха, Корейский институт передовых и многие другие) и с более 75 компаниями цифровой экономики и органами власти (например, ПАО «Мегафон», ПАО «АК БАРС» Банк, ПАО «Сбербанк», АО «Сбербанк Технологии», «Лаборатория Касперского», Почта России и т. д.).

Краткая автобиография

Родился в 1968 году в городе Калининграде в семье военно-морского офицера Балтийского флота ВМФ Российской Федерации — капитана 2-го ранга и командира БЧ-5, отвечающего за устойчивость (а точнее ***остойчивость***) боевого корабля в различных условиях боевых и аварийных повреждений. В юношеские годы мне посчастливилось вместе с отцом, *Петренко Анатолием Григорьевичем*, принять участие в ряде тренировок и учений личного состава корабля с целью получения и закрепления навыков по организации борьбы за живучесть и предотвращению гибели корабля, а также приведения его в состояние, обеспечивающее ход, управляемость и использование оружия. В дальнейшем эти знания и навыки позволили под руководством профессора *Ковалева Виктора Васильевича* выбрать направления поисковых исследований и сформировать собственные научные интересы в области безопасности и устойчивости современных программотехнических систем в условиях беспрецендентного роста угроз безопасности.

В 1991 году с отличием окончил ВКА имени А. Ф. Можайского и Санкт-Петербургский государственный университет по специальности «инженер-математик» (системное программное обеспечение). Затем служил инженером в/ч 77981 на ОКИК в г. Якутске и параллельно преподавал на физико-математическом факультете (декан факультета *Максимов Василий Васильевич*) Якутского государственного университета имени М. К. Аммосова (читал дисциплины «*Экспертные системы*», «*Логическое программирование Prolog*», «*Функциональное программирование LISP*»). В 1992 году в Якутском госуниверситете подготовил свое первое учебное пособие под

названием «*Программирование экспертных систем*», 1992, ЯГУ, 240 с. Прошел обучение в очной адъюнктуре и докторантуре ВКА имени А. Ф. Можайского, в известной научной школе программотехники *Святослава Сергеевича Лаврова* (12 марта 1923, Петроград — 18 июня 2004, Санкт-Петербург) — советского и российского ученого в области прикладной математики и вычислительной техники, члена-корреспондента АН СССР (1966). В 1997 году успешно защитил кандидатскую диссертацию на тему «Метод обеспечения устойчивости функционирования АСУ военного назначения на основе теории подобия и размерностей» (по специальности 20.02.12 «Системный анализ, исследование операций, математическое моделирование»). Затем прошел путь от преподавателя до начальника (заведующего) кафедрой «Математическое обеспечение ЭВМ» ВКА имени А. Ф. Можайского (с 2004 до 2013 год.). В 2011 году первым в России защитил докторскую диссертацию по новой тогда специальности 20.02.27 «Информационное противоборство в военной сфере — технические науки» на тему «Организация самовосстанавливающихся машинных вычислений в условиях информационного противоборства». В 2013 году получил за достигнутые научные результаты ученое звание профессора по кафедре «Математическое обеспечение ЭВМ».

После увольнения в 2013 году в запас работал директором центра систем кибербезопасности АФК «Система» (АО «РТИ» и АО «НПК ВТиСС») с выполнением функций конструктора комплексных систем безопасности, ситуационных центров и систем поддержки принятия решений для органов исполнительной власти, силовых министерств и ведомств, предприятий и организаций. В том числе по линии АО «ИнфоТеКС» курировал вопросы научно-технического развития ведомственных сегментов ГосСОПКА на основе перспективных технологий сбора и обработки больших данных (Big Data) и искусственного интеллекта (AI). С 2016 года и по настоящее время работает руководителем Центра информационной безопасности (ЦИБ) АНО ВО «Университет Иннополис».

В ***область научных интересов*** автора входят, главным образом, вопросы практической кибербезопасности:

- технологии создания *киберустойчивых цифровых платформ* «облачных» (Cloud) и «туманных» (Foggy) вычислений на базе гиперконвергентной инфраструктуры (*Hyper-converged infrastructure*, *HCI*) и авторских моделей и методов подобия и размерностей;
- технологии создания безопасных и устойчивых программно-конфигурируемых сетей (*Software Defined Networks*, *SDN*), хранилищ данных (*Software-Defined Storage*, *SDS*) и сред виртуализации сетевых функций (*Network Functions Virtualization*, *NFV*);

- доверенные когнитивные (*Cogno*) суперкомпьютерные технологии высокой и сверхвысокой производительности до 10 экзафлопс (10^{18} операций в секунду с плавающей запятой);
- интеллектуальные технологии обеспечения информационной безопасности на основе больших данных и потоковой обработки данных (*BigData* + *ETL* и *Machine Learning*, *ML* и *Deep Learning*, *DL*);
- технологии *иммунной защиты киберсистем Индустрии 4.0* на основе моделей и методов биологической (*И. П. Мечников*, *Charles A. Janeway*) и кибернетической (*А. Тараканов*, *Д. Хант*, *Д. Дасгупта*, *П. Андюс*) иммунологии, в сочетании с авторскими методами подобия и размерностей;
- технологии доверенной сетки устройств (*DeviceMesh)*, безопасной системной архитектуры (*Advanced System Architecture*) и адаптивной архитектуры безопасности (Adaptive Security Architecture);
- технологии создания *безопасных систем и сетей Интернета вещей (IIoT/ IoT)* на основе *LoRa (Long Range)*, *Narrow Band IoT* консорциума *3GPP (NB-IoT)*, *XBN и NB-Fi*, *Sigfox*, *ZigBee*, *ZiNa (Zigzag Narrow-band)*, *LINC* и др.;
- гиперконвергентные технологии реагирования на инциденты компьютерной безопасности (*CERT*) на основе прорывных *NBIC*-моделей;
- технологии *динамического анализа кода программ* и *аналитической верификации* цифровых экосистем и платформ Цифровой экономики Российской Федерации на основе «паспортизации» упомянутых приложений в терминах теории подобия и размерностей;
- технологии *квантового криптоанализа* (*Q-computing*) на основе алгоритмов *Шора и Гровера*;
- технологии *гомоморфного шифрования* для защиты облачных высислений на основе криптосистем, использующих матричные полиномы (*Буртыка-Бабенко*, *Грибов-Михалев*), а также криптосистем *RSA*, *Пэйе*, *Эль-Гамаля и Крейга-Джентри* (в кольце двоичных чисел);
- технологии создания криптографических модулей (*Hardware Security Module*, *HSM*) с дополнительной функциональностью;
- технологии автоматизированного моделирования обстановки и прогнозирование поведения оппонентов (*WarGaming*);
- методики организации и проведения *национальных и международных киберучений* и др.

ОСНОВНЫЕ ПОКАЗАТЕЛИ КВАЛИФИКАЦИИ:

- Руководитель Государственной научной школы «*Информационные технологии критически важных объектов инфраструктуры Российской Федерации*». Научно-педагогический потенциал школы составляют 11 докторов технических наук и 45 кандидатов технических наук, более 100 инженеров-исследователей и программистов. Выполнено порядка 100 НИР и ОКР, в том числе выполняются научные проекты № 20-17-00005 «*Киберустойчивость Индустрии 4.0*», № 20-04-60080 «*Модели и методы обеспечения устойчивости социотехнических систем общества в условиях вирусных эпидемий типа пандемии COVID-19 на основе приобретаемого иммунитета*», № 18-47-160011 «*Разработка системы раннего предупреждения о компьютерном нападении на критическую инфраструктуру предприятий Республики Татарстан на основе создания и развития новых NBIC-технологий кибербезопасности*», которые получили поддержку Российского фонда фундаментальных исследований (РФФИ). Получено более 20 патентов на изобретения и 44 свидетельства на программы для ЭВМ, среди них: *«Платформа полностью гомоморфного шифрования для защиты облачных и туманных вычислений на основе криптосистемы, использующей матричные полиномы»*, *«Платформа гомоморфного шифрования для защиты облачных и туманных вычислений на основе криптосистемы RSA»*, *«Платформа полностью гомоморфного шифрования для защиты облачных и туманных вычислений в кольце двоичных чисел на основе криптосистемы Крейга-Джентри»*, *«Платформа гомоморфного шифрования для защиты облачных и туманных вычислений на основе криптосистемы Пэйе»*, *«Платформа гомоморфного шифрования для защиты облачных и туманных вычислений на основе криптосистемы Эль-Гамаля»*, *«Платформа аналитической верификации цифровых экосистем и приложений цифровой экономики Российской Федерации на основе инвариантов подобия и размерностей»*, *«Программа оптимизации матриц размерностей для паспортизации цифровых экосистем и платформ цифровой экономики Российской Федерации»*, *«Программа динамического контроля критериев семантической корректности типового стека протоколов TCP/IP»*, *«Программа моделирования протокола IP в терминах размерностей для динамического контроля корректности»*, *«Программа разделения связных компонент матриц размерностей цифровых экосистем и платформ для оперативности принятия решения о семантической корректности» и др.* В 2013 году научная школа «*Информационные технологии критически важных объектов инфраструктуры Российской Федерации*» была внесена в реестр ведущих научных и научно-педагогических школ г. Санкт-Петербурга (распоряжение Комитета по науке

и высшей школе от 13.12.2013 № 99 и решение Президиума Научно-технического совета при Правительстве Санкт-Петербурга (протокол № 2/13 от 09.12.2013).

- Ведущий научный сотрудник Московского физико-технического института (Физтеха), Физтех-школы радиотехники и компьютерных технологий (ФРКТ), Лаборатории космической информатики. Эксперт секции по проблемам информационной безопасности научного совета при Совете Безопасности Российской Федерации. Эксперт ряда фондов, в том числе Российского фонда фундаментальных исследований (РФФИ) и Фонда Сколково. Научный руководитель программы Университета Иннополис «*Киберустойчивость цифровой экономики Российской Федерации*». Главный редактор журнала «Инсайд. Защита информации» (журнал входит в перечень, рекомендуемый ВАК Российской Федерации).
- Конструктор более 15 национальных центров мониторинга угроз информационной безопасности и реагирования на инциденты информационной безопасности CERT (Computer Emergency Response Team) и CSIRT (Computer Security Incident Response Team). Разработчик более 40 программно-аппаратных комплексов специального назначения. В частности, разработанные опытные образцы программно-аппаратных комплексов иммунной защиты Индустрии 4.0 по своим тактико-техническим характеристикам не только не уступают, но и в ряде случаев превосходят известные зарубежные аналоги из США, Великобритании и Израиля: *Darktrace (https://www.darktrace.com)*, *Cynet (https://www.cynet.com)*, *FireEye (https://www.fireeye.com)*, *Check Point (https://www.checkpoint.com)*, *Symantec (https://www.symantec.com)*, *Sophos (www.sophos.com/)*, *Fortinet (https://www.fortinet.com)*, *Cylance (https://www.cylance.com)*, *Vectra (https://www.vectra.ai)* и др.
- Автор 17 монографий на английском, испанском и русском языках и более 350 статей по вопросам кибербезопасности (*«Труды ИСА»*, *«Труды СПИИ Российской академии наук»*, *«Вопросы кибербезопасности»*, *«Проблемы информационной безопасности»*, *«Открытые системы»*, *«Инсайд. Защита информации»*, *«Вестник связи»* и др.). В том числе монографий, подготовленных в издательствах: *Springer (Германия)*, *River Publishers (Дания)*, *«Питер»*, *«Афина» и «ДМК-Пресс» (Россия)*: «Разработка корпоративной программы непрерывности бизнеса» (2020), «Создание иммунной системы кибербезопасности» (2020), «Киберустойчивость» (2019), «Инновационные технологии кибербезопасности. Опыт Российской Федерации» (2018), *«Применение технологий Big Data для мониторинга комьютерной безопасности» (2018)*, *«Национальная система предупреждения о ком-*

пьютерном нападении» (2017), *«Методы и технологии облачной безопасности» (2014)*, *«Методы и технологии защиты информации критически важных объектов национальной инфраструктуры» (2013)*, *«Политики информационной безопасности» (2011)*, *«Управление информационными рисками» (2004)*, *«Аудит безопасности корпоративных систем Интернет/Интранет» (2002)*, *«Методы защиты информации в Интернете» (2002)* и пр. Текущий индекс Хирша автора составляет 32 (SPIN-код: 4064-9751, AuthorID: 805505 — https://elibrary.ru/author_profile.asp?id=805505).

- Удостоен почетных грамот и дипломов Правительства Российской Федерации, директора ФСБ России, министра обороны России, а также благодарственных писем ряда руководителей федеральных ведомств и глав субъектов Российской Федерации. Удостоен ряда медалей и знаков отличия Совета безопасности Российской Федерации, ФСБ России, ФСО России и Министерства обороны России. В 2014 году были присуждены национальные премии «Большой ЗУБР» и «Золотой ЗУБР» за достигнутые научные и практические результаты в области национальной информационной безопасности.

Список литературы

1. Abdelzaher T., Kott A. Resiliency and robustness of complex systems and networks. Adaptive, Dynamic and Resilient Systems, 2013. P. 67–86.
2. Abramov S. M. History of development and implementation of a series of Russian supercomputers with cluster architecture, History of domestic electronic computers, 2nd ed., Rev. and additional; color. Ill, Publishing house «Capital Encyclopedia», Moscow, Russia, 2016.
3. Bakkensen L. A., Fox-Lent C., Read L. K. and Linkov I. (2017), Validating Resilience and Vulnerability Indices in the Context of Natural Disasters. Risk Analysis, 37: 982–1004. doi:10.1111/risa.12677.
4. Barabanov A. V., Markov A. S., Tsirlov V. L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, *Journal of Theoretical and Applied Information Technology*, 2016. Vol. 88, N 1. P. 77–88.
5. Barabanov A., Markov A., Tsirlov V. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems. In Proceedings of the *12th International Siberian Conference on Control and Communications* (Moscow, Russia, May 12–14, 2016). SIBCON 2016. IEEE, 7491660, 1–4. DOI: 10.1109/SIBCON.2016.7491660.
6. Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In *Proceedings of the 8th International Conference on Security of Information and Networks* (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015. P. 30–33. DOI: 10.1145/2799979.2799980.
7. Barabanov A. V., Markov A. S., Tsirlov V. L. Statistics of Software Vulnerability Detection in Certification Testing. *Journal of Physics*: *Conference Series*. 2018. V. 1015. P. 042033.
8. Barabanov A. V., Markov A. S., Tsirlov V. L. Information Security Controls Against Cross-Site Request Forgery Attacks On Software Application of Automated Systems. *Journal of Physics*: *Conference Series*. 2018. V. 1015. P. 042034.
9. Barbier F. Five Trends for Manufacturing's Fourth Wave. 2017. Intelligence 3:1, Flex Inc. Web access: https://flex.com/intelligence/manufacturing/five-trends-manufacturing-fourth-wave.
10. Biryukov D. N., Lomako A. G. Approach to Building a Cyber Threat Prevention System. Problems of Information Security. Computer systems, Publishing house of Polytechnic University. St. Petersburg, Russia, 2013. Vol. 2. P. 13–19.
11. Biryukov D. N., Lomako A. G., Sabirov T. R. Multilevel Modeling of Pre-Emptive Behavior Scenarios. Problems of Information Security. Computer systems, Publishing house of Polytechnic University. St. Petersburg, Russia, 2014. Vol. 4. P. 41–50.

12. Biryukov D. N., Rostovtsev Y. G. Approach to constructing a consistent theory of synthesis of scenarios of anticipatory behavior in a conflict. Proc. SPIIRAS. Russia, 2015. 1(38), p. 94–111.

13. Biryukov D. N., Lomako A. G., Petrenko S. A. Generating scenarios for preventing cyber — attacks, Protecting information, Inside, 2017. N 4 (76).

14. Biryukov D. N., Petrenko A. S., Petrenko S. A. Method for synthesizing the structure of the self-healing program for computations with memory: in the collection. Distance educational technologies, Proceedings of the II All-Russian Scientific and Practical Internet Conference. Russia, 2017. P. 188–192.

15. Boccia F. (ed.), Leonardi R. (ed.). The Challenge of the Digital Economy. Springer Nature Switzerland AG. Part of Springer Nature, 2016. P. 148.

16. Bongard M. M. The Problem of Recognition, Fizmatgiz, Moscow, Russia, 1967.

17. Bostick T. P., Holzer T. H., & Sarkani S. (2017). Enabling stakeholder involvement in coastal disaster resilience planning. *Risk Analysis*, *37*(6), 1181–1200.

18. Brynjolfsson E. (2016). How IoT changes decision making, security and public policy. Blog: Research & Commentary from MIT Sloan Business & Management Experts, June 30. http://mitsloanexperts.mit.edu/how-iot-changes-decision-making-security-and-public-policy/

19. Cadwalladr C. (2016). Google, democracy and the truth about Internet search. The Guardian, Internet, The Observer, Dec. 4, https://www.theguardian.com/technology/2016/dec/04/google-democracy-truth-Internetsearch-facebook

20. Colbert E. J., Kott A., Knachel III, L., & Sullivan D. T. (2017). *Modeling Cyber Physical War Gaming* (Technical Report No. ARL-TR-8079). US Army Research Laboratory, Aberdeen Proving Ground, United States.

21. Collier Z. A., Linkov I., DiMase D., Walters S., Tehranipoor M., & Lambert J. (2014a). Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities. Computer 47:70–76.

22. Collier Z. A., Panwar M., Ganin A. A., Kott A., & Linkov I. (2016). Security metrics in industrial control systems. In *Cyber-security of SCADA and other industrial control systems* (pp. 167–185). Cham: Springer International Publishing.

23. Connelly E. B., Allen C. R., Hatfield K., Palma-Oliveira J. M., Woods D. D., & Linkov I. (2017). Features of resilience. *Environment Systems and Decisions*, *37*(1), 46–50.

24. Cyber Resilience and Response, Department of Homeland Security (DHS) 2018, https://www.dhs.gov/sites/default/files/publications/2018_AEP_Cyber_Resilience_and_Response.pdf

25. Cyber-resilience: Range of practices, Basel Committee on Banking Supervision (December 2018) , https://www.bis.org/bcbs/publ/d454.pdf

26. *Cyber-resilience*: *the key to business security*, https://www.pandasecurity.com/mediacenter/src/uploads/2018/05/Cyber-Resilience-Report-EN.pdf

27. Cyber Resilience Alliance, A Science and Innovation Audit Report sponsored by the Department for Business, Energy and Industrial Strategy, https://swlep.co.uk/docs/default-source/strategy/industrial-strategy/a-science-and-innovation-audit-for-the-cyber-resilience-alliance.pdf?sfvrsn=d1ee7f92_4

28. Cyber resilience, Specia Report (2017), https://www.acs.org.au/content/dam/acs/acs-documents/ACS%20-%20Cyber%20Resilience%20Special%20Report%20-%2021.06.pdf

29. Cyber resilience in the digital age. Implications for the GCC region, EY (2017), https://www.ey.com/Publication/vwLUAssets/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region/$File/ey-cyber-resilience-inthe-digital-age-implications-for-the-gcc-region.pdf

30. Bodeau D., Graubart R., Heinbockel W. and Laderman E. Cyber Resiliency Engineering Aid-The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, PR 15-1334, May 2015. [Online].

31. Dallas M., Ponte S., and Sturgeon T. (2017). A Typology of Power in Global Value Chains. Working Paper in Business and Politics No. 91, Copenhagen Business School. Web access: http://openarchive.cbs.dk/bitstream/handle/10398/9503/Dallas_Ponte_Sturgeon.pdf?sequence =3

32. Dalten A. (2017). IBM and Indiegogo are bringing Watson's smarts to the masses; the new partnership gives entrepreneurs unlimited access to IBM's AI. Engadget, Febrary 16, https://www.engadget.com/2017/02/16/ibm-indiegogo-watson-iot-partnership/

33. Dan Goodin. (27 January 2016). Ars Technica. Israel's Electric Authority Hit by "Severe" Hack Attack. Last accessed on 19 April 2017, http://arstechnica.com/security/2016/01/israels-electric-grid-hit-by-severe-hack-attack/.

34. Vugrin E. D. and Turgeon J. Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessment, in *Cyber Behavior*: *Concepts*, *Methodologies*, *Tools*, *and Applications*, Hershey, PA, IGI Global, 2014. P. 2033–2055.

35. Frye E. Critical Infrastructure Resilience: A Regional and National Approach (PR 14-4047), November 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/14-4047-critical-infrastructureresilience-a-regional-and-national-approach.pdf.

36. Economic Times. (2017). Layoffs scare is real, not exaggerated, finds ET's Jobs Disruption survey. Economic Times, June 1. Web access: http://economictimes.indiatimes.com/jobs/layoffsscare-is-real-not-exaggerated-finds-ets-jobs-disruption-survey/articleshow/58927915.cms

37. Epstein J. (2017). When blockchain meets big data, the payoff will be huge. VentureBeat, July 30. Web access: https://venturebeat.com/2017/07/30/when-blockchain-meets-big-data-the-payoffwill-be-huge

38. Florin M. V., & Linkov I. (eds.). (2016). *IRGC Resource Guide on Resilience*. Lausanne: EPFL International Risk Governance Council (IRGC).

39. Ganin A. A., Massaro E., Gutfraind A., Steen N., Keisler J. M., Kott A., Mangoubi R., & Linkov I. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports*, *6*, 19540.

40. Ganin A. A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D., & Linkov I. (2017a). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*.

41. Government of Singapore. (17 April 2017). Data.gov.sg. Last accessed on 17 April 2017, https://data.gov.sg/dataset/total-landarea-of-singapore.

42. Government of Singapore. (14 November 2016). National Research Foundation. "RIE2020 Plan." Last accessed on 17 April 2017, https://www.nrf.gov.sg/rie2020.

43. Government of Singapore. (4 November 2016). National Research Foundation. "Virtual Singapore." Last accessed on 17 April 2017, https://www.nrf.gov.sg/programmes/virtual-singapore.

44. Greenough J. and Camhi J. (2016). Here's why some are calling the Internet of Things the next Industrial Revolution. Business Insider, Tech Insider, Feb. 10. http://www.businessinsider.com/iot-trends-will-shape-the-way-we-interact-2016-1 34

45. Guzik V. F., Kalyaev I. A., Levin I. I. (2016). Reconfigurable computing systems; [under the Society. ed. I.A. Kalyayeva], Publishing house SFU, Rostov-on-Don, p. 472.

46. Cam H. and Mouallem P. Mission-Aware Time-Dependent Cyber Asset Criticality and Resilience, in *Proceedings of the 8th CSIIRW Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Lab, Oak Ridge, TN, 2013.

47. Willis H. H. and Loa K. Measuring the Resilience of Energy Distribution Systems, RAND Justice, Infrastructure, and Environment, PR-1293-DOE, July 2014. [Online]. Available: http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR883/RAND_RR883.pdf

48. Hagiu A., & Wright J. (2015). Multi-sided platforms. International Journal of Industrial Organization, 43, 162–174.

49. Hampson F. and Jardine E. (2016). Look Who's Watching, Centre for International Governance Innovation, Waterloo, ON Canada.

50. Hassell S., Case R., Ganga G., Martin S. R., Marra S. and Eck C. Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of Systems, and Networks Against Cyber Threats, *INCOSE Insight*, pp. 26–28, April 2015.

51. Helveston J. P., Wang Y., Karplus V. and Fuchs E. (2017). Innovating Up, Down, and Sideways: The (Unlikely) Institutional Origins of Experimentation in China's Plug-in Electric Vehicle Industry. Manuscript, February 21. Available at SSRN: https://ssrn.com/abstract=2817052 or http://dx.doi.org/10.2139/ssrn.2817052

52. Holling C. S. (1996). Engineering resilience versus ecological resilience. In P. C. Schulze (ed.), *Engineering within ecological constraints*. Washington D. C.: National Academy Press.

53. Hollnagel E., Woods D. D. & Leveson N. C. (2006). *Resilience engineering*: *Concepts and precepts*. Aldershot: Ashgate.

54. Homeland Security Presidential Directive — 7, Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003.

55. Homeland Security Presidential Directive — 20/National Security Presidential Directive — 51, National Continuity Policy, May 9, 2007.

56. Hughes. R. B. (2009) Atlantisch Perspectief, Ap: 2009 Nr. 1/4, *NATO and Cyber-Defense*: *Mission Accomplished*, *Netherlands*, *Netherlands Atlantic Committee*.

57. IBM Corporation (2018), James Boyles, «Cybersecurity and YOU!! CYBER RESILIENCE — PREPARE FOR WHEN, NOT IF», https://files.nc.gov/ncdit/documents/files/2018%20NCSAM%20Symposium%20-%20Cyber%20Resilience%20-%20IBM.pdf

58. IBM Corporation (2018), Felicity March, «Cyber Resilience», https://www-05.ibm.com/dk/think-copenhagen/assets/pdf/Studie3_Session2_Speaker4_Felicity_March_IBM.pdf

59. IBM Corporation (2018), Jean-Michel Lamby Associate Partner — IBM Security, «Cyber Resiliency. Minimizing the impact of breaches on business continuity», https://www-05.ibm.com/be/think-brussels/assets/pdf/Minimizing_the_impact_of_breaches_on_business_continuity_by_Jean_Michel_Lamby.pdf

60. IBM Corporation (2018), ARNE JACOBSEN, «IBM RESILIENT: INTELLIGENT ORCHESTRATION THE NEXT GENERATION OF INCIDENT RESPONSE», https://www-05.ibm.com/se/securitysummit/assets/pdf/IBM_Resilient-Arne_Jacobsen.pdf

61. IBM “IBM’s Smarter Cities Challenge: Boston—Report.” Last accessed on 12 April 2017, https://www.smartercitieschallenge.org/assets/cities/boston-united-states/documents/boston-united-states-full-report-2012.pdf.

62. Johnson I. (15 June 2013). The New York Times. China’s Great Uprooting: Moving 250 Million into Cities. Last accessed on 12 April 2017, http://www.nytimes.com/2013/06/16/world/asia/chinas-great-uprooting-moving-250-million-into-cities.html?pagewanted=all&_r=0.

63. IDC (June 2018), Phil Goodwin, Sean Pike, «Five Key Technologies for Enabling a Cyber-Resilience Framework», https://cdn2.hubspot.net/hubfs/4366404/QRadar/QRadar%20Content/Five%20Key%20Technologies%20for%20Enabling%20a%20Cyber%20Resilience%20Framework.pdf?t=1535932423907

64. INCOSE, “Resilience Engineering,” in *INCOSE Systems Engineering Handbook*: *A Guide for System Life Cycle Processes and Activities*, *Fourth Edition*, Hoboken, NJ, John Wiley & Sons, 2015. P. 229–231.

65. Park J., Seager T. P., Rao P. S., Convertino M. and Linkov I. Integrating risk and resilience approaches to catastrophe management in engineering systems, *Risk Analysis*. 2013. Vol. 33. N 3. P. 356–367.

66. Zalewski J., Drager S., McKeever W., Kornecki A. J. and Czejdo B., Modeling Resiliency and Its Essential Components for Cyberphysical Systems, in *Position Papers of the Federated Conference on Computer Science and Information Systems (FedCSIS)*.

67. Allen J. and Davis N. Measuring Operational Resilience Using the CERT® Resilience Management Model. September 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tn030.pdf.

68. Kahan J. H. Resilience Redux: Buzzword or Basis for Homeland Security, *Homeland Security Affairs Journal*. Vol. 11. N 2, February 2015.

69. King J. DTCC’s Bodson Discusses Cyber Resilience at World Economic Forum, Depository Trust and Clearing Corporation, 3 February 2016. [Online]. Available: http://www.dtcc.com/news/2016/february/03/dtccs-bodson-discusses-cyber-resilience.

70. Watson J.-P., Guttromson R., Silva-Monroy C., Jeffers R., Jones K., Ellison J., Rath C., Gearhart J., Jones D., Corbet T., Hanley C. and Walker L. T. Conceptual Framework for Developing Resilience Metrics for US Electricity, Oil, and Gas Sectors, SAND2014-18019, September 2015. [Online].Available: http://energy.gov/sites/prod/files/2015/09/f26/EnergyResilienceReport_%28Final%29_SAND2015-18019.pdf.

71. John R., Davis Jr. Major, (2015) Joined Warfare Center, Continued Evo-lution of Hybrid Threats, Three Sword Magazine, 28/2015, http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf [seen may 12 2016].

72. Johnson P. (2017). With The Public Clouds Of Amazon, Microsoft And Google, Big Data Is The Proverbial Big Deal. Forbes, Jun 15. Web access: https://www.forbes.com/sites/johnsonpierr/2017/06/15/with-the-public-clouds-of-amazonmicrosoft-and-google-big-data-is-the-proverbial-big-deal/#2a37a76b2ac3

73. Kaplan S., & Garrick B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27.

74. Kang C. (2017). Pittsburgh Welcomed Uber's Driverless Car Experiment. Not Anymore. New York Times. Technology, May 21. Web access: https://www.nytimes.com/2017/05/21/technology/pittsburgh-ubers-driverless-carexperiment.html

75. Kaspersky E. Computer Malignity, Peter, St. Petersburg, p. 208, Russia, 2008.

76. Kelic A., Collier Z. A., Brown C., Beyeler W. E., Outkin A. V., Vargas V. N., Ehlen M. A., Judson C., Zaidi A., Leung B., & Linkov I. (2013). Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. *Environment Systems & Decisions*, *33*(4), 544–560.

77. Kenney M., & Zysman J. (2016). The Rise of the Platform Economy. Issues in Science and Technology, 32(3), 61–69.

78. Kolmogorov A. N. Automats and life, In: Berg A. I., Kolman E. (eds.) Cybernetics: Expected and Cybernetics Unexpected, Science, pp. 12–30. Moscow, 1968.

79. Kotenko I. V. Intellectual mechanisms of cybersecurity management. Proceedings of ISA RAS. Risk Manag. Safety, 41, pp. 74–103, Moscow, Russia, 2009.

80. Kott A., Linkov I. (ed.). Cyber Resilience of Systems and Networks (Risk, Systems and Decisions), ISBN 978-3-319-77491-6 and ISBN 978-3-319-77492-3 (eBook), https://doi.org/10.1007/978-3-319-77492-3© 2019 Springer Nature Switzerland AG, part of Springer Nature, 1st ed. 2019 Edition, Kindle Edition, 475 p. 121 illus., 87 illus. in color.

81. Kott A. (2006). *Information warfare and organizational decision-making*. Artech House, Boston, USA.

82. Kott A., & Abdelzaher, T. (2014). Resiliency and robustness of complex systems and networks. *Adaptive Dynamic and Resilient Systems*, *67*, 67–86.

83. Kott A., Alberts D. S., & Wang C. (2015). Will cybersecurity dictate the outcome of future wars? *Computer*, *48*(12), 98–101.

84. Kott A., Ludwig J., & Lange M. (2017). Assessing mission impact of cyberattacks: Toward a model-driven paradigm. *IEEE Security and Privacy*, *15*(5), 65–74.

85. Kott A. et al. (2018). *A Reference Architecture of an Autonomous Intelligent Agent for Cyber Defense* (Technical Report). US Army Research Laboratory, Aberdeen Proving Ground, United States.

86. Simonsk K., Dr. Sharkov G. National Cyber Security Strategy Cyber Resilient Bulgaria 2020, [ITU , ENISA] Regional Cybersecurity Forum, 29-30.11.2016, Sofia, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf

87. Carlson L., Bassett G., Buehring W., Collins M., Folga S., Haffenden B., Petit F., Phillips J., Verner D. and Whitfield R., Resilience: Theory and Applications (ANL/DIS-12-1), January 2012. [Online]. Available: http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

88. Larkin S., Fox-Lent C., Eisenberg D. A., Trump B. D., Wallace S., Chadderton C., & Linkov I. (2015). Benchmarking agency and organizational practices in resilience decision making. *Environment Systems and Decisions*, *35*(2), 185–195.

89. Leslie N. O., Harang R. E., Knachel L. P., & Kott A. (2017). Statistical models for the number of successful cyber intrusions. *The Journal of Defense Modeling and Simulation*, *15*(1), 49–63.

90. Levin I. I., Dordopulo A. I., Kalyaev I. A., Doronchenko Yu. I., Razkladkin M. K. Modern and promising high-performance computing systems with reconfigurable architecture, Proceedings of the international scientific conference "Parallel Computing Technologies (PaVT'2015) ", Ekaterinburg, March 31 — April 2, 2015, Publishing Center of SUSU, pp. 188-199, Chelyabinsk, Russia, 2015.

91. Levy A. 2017. Microsoft's cloud business is growing almost twice as fast as Amazon's, with Google far behind. CNBC Tech. April 27, http://www.cnbc.com/2017/04/27/microsoft-azuregrowing-faster-than-aws-google-cloud-behind.html

92. Linkov I., Eisenberg D. A., Bates M. E., Chang D., Convertino M., Allen J. H., Flynn S. E., & Seager T. P. (2013a). Measurable resilience for actionable policy. *Environmental Science and Technology*, *47*(18), 10108–10110.

93. Linkov I., Eisenberg D. A., Plourde K., Seager T. P., Allen J., & Kott A. (2013b). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476.

94. Linkov I., Bridges T., Creutzig F., Decker J., Fox-Lent C., Kröger W., Lambert J. H., Levermann A., Montreuil B., Nathwani J., Renn O., Scharte B., Scheffler A., Schreurs M.,

Thiel-Clemen T., & Nyer R. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407–409.

95. Linkov I., Fox-Lent C., Allen C. R., Arnott J. C., Bellini E., Coaffee J., Florin M.-V., Hatfield K., Hyde I., Hynes W., Jovanovic A., Kasperson R., Katzenberger J., Keys P. W., Lambert J. H., Moss R., Murdoch P. S., Palma-Oliveira J., Pulwarty R. S., Read L., Sands D., Thomas E. A., Tye M. R., & Woods D. (In press). Tiered Approach to Resilience Assessment. Risk Analysis, DOI: 10.1111/risa.12991.

96. Logan O. Mailloux, Engineering Secure and Resilient Cyber-Physical Systems (2018), Systems Engineering Cyber Center for Research, US Air Force, https://www.caecommunity.org/sites/default/files/symposium_presentations/Engineering_Secure_and_Resilient_Cyber-Physical_Systems.pdf

97. Lomako A. G., Petrenko S. A., Petrenko A. S. Model of the Immune System of Stable Computations, In: Information Systems and Technologies in Modeling and Control. Materials of the all-Russian scientific-practical conference. Russia, 2017. P. 250–254.

98. Lomako A. G., Petrenko S. A., Petrenko A. S. Representation of perturbation dynamics for the organization of computations with memory, In: Remote educational technologies,Materials of the II All-Russian Scientific and Practical Internet Conference. 2017. P. 355–359.

99. Lomako A. G., Petrenko S. A., Petrenko A. S. Realization of the immune system of the stable computations organization, In: Information systems and technologies in modelling and management,Materials of the All-Russian scientific and practical conference. Russia, 2017. P. 255–259.

100. Pendleton M., Garcia-Lebron R. and Xu S. A Survey on Security Metrics. (20 January 2016). [Online]. Available: http://arxiv.org/pdf/1601.05792v1.pdf.

101. Madaya O. The Resilience of Networked Infrastructure Systems: Analysis and Measurement (Systems Research Series — Vol. 3), Hackensack, NJ: World Scientific Publishing Company, 2013.

102. Makoveychuk K. A., Petrenko S. A., Petrenko A. S. Organization of calculations with memory, Information Systems and Technologies in Modeling and Control. Materials of the all-Russian scientific-practical conference. Russia, 2017. P. 260–266.

103. Makoveychuk K. A., Petrenko S. A., Petrenko A. S. Modeling the recognition of destructive effects on computer calculations, Information Systems and Technologies in Modeling and Control. Materials of the all-Russian scientific-practical conference. Russia, 2017. P. 155–161.

104. Makoveychuk K. A., Petrenko S. A., Petrenko A. S. Modeling of self-recovery of computations under perturbation conditions, Information Systems and Technologies in Modeling and Control. Materials of the all-Russian scientific-practical conference. 2017. P. 162–166.

105. Mamaev M. A., Petrenko S. A. Technologies of information protection on the Internet. — St. Petersburg: publishing house «Peter». Russia, St. Petersburg, 2002. P. 848.

106. Mar B. (2017). Supervised V Unsupervised Machine Learning — What's The Difference? Forbes, Tech # BigData, March 16. Web access: https://www.forbes.com/sites/bernardmarr/2017/03/16/supervised-v-unsupervised-machinelearning-whats-the-difference/#6464ce81485d 35

107. Marchese D., Reynolds E., Bates M. E., Morgan H., Clark S. S., & Linkov I. (2018). Resilience and sustainability: Similarities and differences in environmental management applications. *Science of the Total Environment*, *613*, 1275–1283.

108. Markov A., Barabanov A., Tsirlov V. Models for Testing Modifiable Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018. P. 147–168. DOI: 10.5772/intechopen.75126.

109. Markov A., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018. P. 213–231. DOI: 10.5772/intechopen.75232.

110. Markov A. S., Fadin A. A., Tsirlov V. L. Multilevel Metamodel for Heuristic Search of Vulnerabilities in The Software Source Code, *International Journal of Control Theory and Applications*, 2016. Vol. 9. N 30. P. 313–320.

111. Markov A., Luchin D., Rautkin Y., Tsirlov V. (2015). Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements. In *Proceedings of the 11th International Siberian Conference on Control and Communications* (Omsk, Russia, May 21-23, 2015). SIBCON-2015. IEEE, 1-4. DOI: 10.1109/SIBCON.2015.7147139.

112. Markowsky E. (2012). Welcome to the Virtual Factory: American Manufacturing in the 21st Century. ILP Institute Insider, May 10. Web access: http://ilp.mit.edu/newsstory.jsp?id=18006

113. Marz N., Warren J. Big data. Principles and practice of building scalable data processing systems in real time, Williams. Moscow, Russia, 2016. P. 292.

114. Massel L. V. Problems of Smart Grid Creation in Russia from the Perspective of Information Technologies and Cyber Security, Proceedings of the All-Russian Seminar with International Participation, Methodological Issues of Research into the Reliability of Large Energy Systems, Reliability of energy systems: achievements, problems, prospects, ISEM SB RAS. Irkutsk, Russia, 2014. Vol. 64. P. 171–181.

115. McAfee A. and Brynjolfsson E. (2017). Machine, Platform, Crowd: Harnessing Our Digital Future. New York: W. W. Norton & Company.

116. Miller R. (2016). A Look Inside the Rackspace Open Compute Cloud. Data Center Frontier. March 3. Web Access: https://datacenterfrontier.com/rackspace-open-compute-cloud/

117. Meyer T. (2011). Global public goods, governance risk, and international energy. *Duke Journal of Comparative & International Law*, *22*, 319–347.

118. MMC CYBER HANDBOOK 2016 Increasing resilience in the digital economy, https://www.mitteldeutschland.com/sites/default/files/uploads/2016/12/14/mmc-cyber-handbook2016.pdf

119. Musman S. and Agbolosu-Amison S. A Measurable Definition of Resiliency Using "Mission Risk" as a Metric, March 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/resiliencymission-risk-14-0500.pdf.

120. Musman S. and Temin A. A Cyber Mission Impact Assessment Tool (PR 14-3545), in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2015.

121. Navigant Consulting Inc. (2016). Navigant Research. Smart Cities—Smart Technologies and Infrastructure for Energy, Water, Mobility, Buildings, and Government: Global Market Analysis and Forecasts. Last accessed on 12 April 2017, https://www.navigantresearch.com/research/smart-cities.

122. NIST Special Publication 800-160 VOLUME 2. Systems Security Engineering. Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems — (Draft), March 2018, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2018/mar/cs03202018_NIST_Systems_Security.pdf

123. NIST Special Publication 800-160 VOLUME 3. Systems Security Engineering. Software Assurance Considerations for the Engineering of Trustworthy Secure Systems — (Draft), December 20, 2019.

124. NIST Special Publication 800-160 VOLUME 4. Systems Security Engineering. Hardware Assurance Considerations for the Engineering of Trustworthy Secure Systems — (Draft), December 20, 2020.

125. NIST SP 800-34. Rev. 1: Contingency Planning Guide for Federal Information Systems Paperback — February 18, 2014, https://www.amazon.com/NIST-Special-Publication-800-34-Rev/dp/1495983706

126. NIST, Framework for improving critical infrastructure cybersecurity, version 1.1, draft 2, 16 April 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11, or https://doi.org/10.6028/NIST.CSWP.04162018

127. NIST, Framework for Improving Critical Infrastructure Security, Version 1.0, 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

128. NIST. (2012). SP 800–30 Risk Management Guide for Information Technology Systems.

129. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

130. NIST SP 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010.

131. NIST SP 800-53, Rev.3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.

132. NIST SP 800-60, Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

133. NIST SP 800-84, Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities, September 2006.

134. NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.

135. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002.

136. Noel S. and Jajodia S., Metrics Suite for Network Attack Graph Analytics, in *9th Annual Cyber and Information Security Research Conference (CISRC)*, Oak Ridge National Laboratory, TN, 2014.

137. Nordgren J., Stults M., & Meerow S. (2016). Supporting local climate change adaptation: Where we are and where we need to go. *Environmental Science & Policy*, *66*, 344–352.

138. Erol O., Devanandham H. and Sauser B. Exploring Resilience Measurement Methdologies, in *INCOSE International Symposium*, Chicago, IL, 2010.

139. Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation, ISBN 978-3-319-79035-0 and ISBN 978-3-319-79036-7 (eBook), https://doi.org/10.1007/978-3-319-79036-7 © 2018 Springer Nature Switzerland AG, part of Springer Nature, 1st ed. 2018, XXVII, 249 p. 93 illus.

140. Petrenko S. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation,ISBN: 978-87-7022-022-4 (Hardback) and 978-87-7022-021-7 (Ebook) © 2018 River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2018, 490 p. 198 illus.

141. Petrenko A. S., Petrenko S. A., Makoveichuk K. A., Chetyrbok P. V. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT), 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018. P. 950–953.

142. Petrenko A. S., Petrenko S. A., Makoveichuk K. A., Chetyrbok P. V. Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018. P. 945–949.

143. Petrenko S. A., Stupin D. D. Assignment of semantics calculations in invariants of similarity. 2017 IVth International Conference on Engineering and Telecommunication (EnT), 2017. P. 127–129.

144. Petrenko A. S., Petrenko S. A., Makoveichuk K. A., Chetyrbok P. V. About readiness for digital economy. 2017 IEEE II International Conference on Control in Technical Systems (CTS), 2017. P. 96–99.

145. Petrenko S. A., Makoveichuk K. A. Ontology of cyber security of self-recovering smart Grid. CEUR Workshop. 2017. P. 98–106.

146. Petrenko S. A., Makoveichuk K. A. Big data technologies for cybersecurity. CEUR Workshop. 2017. P. 107–111.

147. Petrenko S. A., Petrenko A. S., Makoveichuk K. A. Problem of developing an early-warning cybersecurity system for critically important governmental information assets. CEUR Workshop. 2017. P. 112–117.

148. Petrenko S. A. The Cyber Threat model on innovation analytics DARPA, Trudy SPII RAN, Issue. 39. , Russia, 2015. P. 26–41.

149. Petrenko S. A., Petrenko A. S. New Doctrine of Information Security of the Russian Federation, Information Protection, Inside. N. 1 (73). Russia, 2017. P. 33–39.

150. Petrenko S. A., Kurbatov V. A., Bugaev I. A., Petrenko A. S. Cognitive system of early cyber — attack warning, Protection of information, Inside. Russia, 2016. N 3 (69). P. 74–82.

151. Petrenko S. A., Petrenko A. S. Big data technologies in the field of information security, Protection of information, Inside, Russia, 2016. N 4 (70). P. 82–88.

152. Petrenko A. S., Bugaev I. A., Petrenko S. A. Master data management system SOPKA, Information protection, Inside. Russia, 2016. N 5 (71). P. 37–43.

153. Petrenko S. A., Petrenko A. S. Designing the corporate segment SOPKA, Protection of information, Inside. Russia, 2016. N 6 (72). P. 47–52.

154. Petrenko S. A., Petrenko A. S. Practice of application the GOST R IEC 61508, Information protection, Insider. Russia, 2016. N 2 (68). P. 42–49.

155. Petrenko S. A., Petrenko A. S. From Detection to Prevention: Trends and Prospects of Development of Situational Centers in the Russian Federation, Intellect & Technology. Russia, 2017. N 1 (12). P. 68–71.

156. Petrenko S. A., Stupin D. D. (2017). National Early Warning System on Cyber — attack: a scientific monograph [under the general editorship of SF Boev] "Publishing House" Athena", University of Innopolis; Innopolis. Russia. P. 440.

157. Petrenko S. A., Shamsutdinov T. I., Petrenko A. S. Scientific and technical problems of development of situational centers in the Russian Federation, Information protection, Inside. Russia, 2016. N 6 (72). P. 37–43.

158. Petrenko S. A., Petrenko A. S. The first interstate cyber-training of the CIS countries: Cyber-Antiterror-2016, Information protection, Inside. Russia, 2016. N. 5 (71). P. 57–63.

159. Petrenko S. A., Petrenko A. A. Ontology of the cyber-security of self-healing SmartGrid, Protection of information, Inside. Russia, 2016. N 2 (68). P. 12–24.

160. Petrenko S. A., Petrenko A. A. The way to increase the stability of LTE-network in the conditions of destructive cyber — attacks, Questions of cybersecurity. Russia, 2015. N 2 (10). P. 36–42.

161. Petrenko S. A., Petrenko A. A. Cyberunits: methodical recommendations of ENISA, Questions of cybersecurity. Russia, 2015. N 3 (11). P. 2–14.

162. Petrenko S. A., Petrenko A. A. Research and Development Agency DARPA in the field of cybersecurity, Questions of cybersecurity. Russia, 2015. N 4 (12). P. 2–22.

163. Petrenko S. A. Methods of Information and Technical Impact on Cyber Systems and Possible Countermeasures, Proceedings of ISA RAS, Risk Management and Security, pp. 104–146, Russia, 2009.

164. Petrenko S. A., Petrenko A. A. (2002). Intranet Security audit (Information technologies for engineers), DMK Press, Moscow, Russia, p. 416.

165. Petrenko S. A., Simonov S. V. (2004). Management of Information Risks, Economically justified safety (Information technology for engineers), DMK-Press, Moscow, Russia, p. 384.

166. Petrenko S. A., Kurbatov V. A. (2005). Information Security Policies (Information Technologies for Engineers), DMK Press, p. 400, Russia, Moscow.

167. Petrenko S. A., Petrenko A. S. (2016). Lecture 12, Perspective tasks of information security, Intelligent Information Radiophysical Systems, MSTU, N. E Bauman; [ed. S. F. Boev, D. D. Stupin, A. A. Kochkarov], Moscow, Russia, pp. 155–166.

168. Petrenko S. A., Petrenko A. S. The task of semantics of partially correct calculations in similarity invariants, Remote educational technologies, Materials of the II All-Russian Scientific and Practical Internet Conference, pp. 365–371, Russia, 2017.

169. Petrenko S. A., Petrenko A. A. Information Security Audit Internet/Intranet (Information Technologies for Engineers), 2nd ed, DMK-Press, p. 314, Moscow, Russia, 2012.

170. Perrow C. (1984). *Normal accidents*: *Living with high risk technologies*. Princeton University Press, Princeton, New Jersey.

171. Lin P., Dr. Swimmer M., Urano A., Hilt S., and Vosseler R. Securing Smart Cities: Moving Toward Utopia with Security in Mind. Trend Micro Forward-Looking Threat Research (FTR) Team. A TrendLabs Research PaperAugust 2017.

172. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov — London: IntechOpen, 2018. 287 p. DOI: 10.5772/intechopen.71396.

173. Ford R., Cavalho M., Mayron L. and Bishop M. Antimalware Software: Do We Measure Resilience? in *2013 Workshop on Anti-malware Testing Research (WATeR)*, Montreal, Quebec, 2013.

174. Rajamäki J. Towards a design theory for resilient (sociotechnical, cyber-physical, software-intensive and systems of) systems. In: Zhuang X. Recent advances in information science. WSEAS Press; 2016. p. 29–34.

175. Rajamäki J., Pirinen R. Critical infrastructure protection: towards a design theory for resilient software-intensive systems. In Proceedings of the European Intel-ligence and Security Informatics Conference (EISIC). IEEE Conference Publications; 2015. p. 184.

176. Prasad R. and Ligthart L. P. (ed.) (2018). Towards Future Technologies for Business Ecosystem Innovation. River Publishers.

177. Redmon J., Divvala S., Girshick R. and Farhadi A. 2016. You Only Look Once: Unified, RealTime Object Detection. IEEE Conference on Computer Vision and Pattern Recognition. (CVPR), 2016, pp. 779–788.

178. Reynolds E. 2017. The New Face of Manufacturing Jobs. Boston Globe, Opinion, February 13. Web access: https://www.bostonglobe.com/opinion/2017/02/13/the-new-face-manufacturingjobs/jsozWRgDPwiXo5yJwA3z2M/story.html

179. Graubart R. The MITRE Corporation, Cyber Resiliency Engineering Framework, The Secure and Resilient Cyber Ecosystem (SRCE) Industry Workshop Tuesday, November 17, 2015, https://secwww.jhuapl.edu/SRCE-Workshop/past-events/2015/docs/abstracts/Abstract_Graubart_MITRE.pdf

180. Khatoun R. and Zeadally S. (2016). Communications of the ACM. Smart Cities: Concepts, Architectures, Research Opportunities. Last accessed on 12 April 2017, https://cacm.acm.org/magazines/2016/8/205032-smart-cities/abstract.

181. Roege P. E., Collier Z. A., Chevardin V., Chouinard P., Florin M. V., Lambert J. H., Nielsen K., Nogal M., & Todorovic B. (2017). Bridging the gap from cyber security to resilience. In I. Linkov& J. M. Palma-Oliveira (Eds.), *Resilience and risk*: *Methods and application in environment*, *cyber*, *and social domains* (pp. 383–414). Dordrecht: Springer.

182. Ross R. S., Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 20, 2018,https://doi.org/10.6028/NIST.SP.800-37r2, https://nvlpubs.nist.gov/nistpubs/ Special-Publications/NIST.SP.800-37r2.pdf

183. Ross R. S., McEvilley M., Oren J. C., Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 3-21-2018] March 21, 2018, https://doi.org/10.6028/NIST.SP.800-160v1

184. Rose G. (ed.). (2016). The Fourth Industrial Revolution: A Davos Reader. Council on Foreign Relations.

185. Schneider F. B. (2011). Blueprint for a Science of Cybersecurity. https://www.cs.cornell.edu/fbs/publications/SoS.blueprint.pdf

186. Schwab K. (2016). The Fourth Industrial Revolution. New York: Crown Business.

187. Khou S., Mailloux L. O., Pecarina J. M., Mcevilley M. A Customizable Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks (2017), *Air Force Institute of Technology*, *The MITRE Corporation*, *McLean — USA*, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7979510

188. The BCI Cyber Resilience Report 2018, http://drj.com/fall2018/sessions/BT7-05-Kaltenmark-Lewis-BCI-Cyber-Resilience.pdf

189. The BCI Cyber Resilience Report, https://www.b-c-training.com/img/uploads/resources/BCI-Cyber-Resilience-Report-2018.pdf

190. The Cyber Resilience Blueprint: A New Perspective on Security, Symantec Corporation (2014), https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

191. The nature of effective defense: Shifting from Cybersecurity to Cyber Resilience, Accenture (2018), https://www.accenture.com/t20181016T035332Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en/Accenture-Shifting-from-Cybersecurity-to-Cyber-Resilience-POV.pdf

192. The City of New York. (2017). NYC Environmental Protection. "About Automated Meter Reading (AMR)." Last accessed on 19 April 2017, http://www.nyc.gov/html/dep/html/customer_services/amr_about.shtml.

193. The concept of the state system for detecting, preventing and eliminating the consequences of cyber — attacks on the information resources of the Russian Federation (approved by the President of the Russian Federation on December 12, 2014, No. K 1274).

194. The concept of foreign policy of the Russian Federation (approved by the Decree of the President of the Russian Federation of November 30, 2016 No. 640.

195. The Cyber Resilience Blueprint: A New Perspective on Security, https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

196. The MITRE Corporation (ed.), Fourth Annual Secure and Resilient Cyber Architectures Invitational, 2015. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/2014-Secure-Resilient-Cyber-Architectures-Report-15-0704.pdf.

197. The MITRE Corporation (ed.), Third Annual Secure and Resilient Cyber Architectures Workshop, December 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/13-4210.pdf.

198. Velichkovsky B. M. Cognitive technical systems, Computers, brain, cognition: successes of cognitive sciences, Nauka, pp. 273–292, Moscow, Russia, 2008.

199. Voevodin V. V., Voevodin V. L. Parallel Computing, BHV-Petersburg, p. 609 St. Petersburg, Russia, 2002.

200. Vorozhtsova T. N. Ontology as a basis for the development of an intellectual system for ensuring cybersecurity. Ontol. Des. 4(14), pp. 69–77, Russia, 2014.

201. Vorobiev E. G., Petrenko S. A., Kovaleva I. V., Abrosimov I. K. Analysis of computer security incidents using fuzzy logic, In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24–26 May 2017,), SCM 2017, pp. 349–352, St. Petersburg, Russia, 2017.

202. Vorobiev E. G., Petrenko S. A., Kovaleva I. V., Abrosimov I. K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty, In Proceedings of the 20th IEEE International Conference on Soft Computing

and Measurements (24–26 May 2017). SCM, pp 299–300. DOI: 10.1109/SCM.2017.7970566, St. Petersburg, Russia, 2017.

203. Watson J.-P., et al. «Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the United States.» Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2014-18019 (2014). https://cfwebprod.sandia.gov/cfdocs/CompResearch/docs/EnergyResilienceReportSAN D2014-18019o.pdf

204. World Economic Forum, Partnering for Cyber Resilience: Toward the Quantification of Cyber Risks, 19 January 2015. [Online]. Available: http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

205. World Economic Forum, Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience, 4 November 2014. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf.

206. World Economic Forum, Partnering for Cyber Resilience: Risk and Responsibilities in a Hyperconnected World — Principles and Guidelines, March 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

207. Cheng Y., Deng J., Li J., DeLoach S. A., Singhal A. and Ou X. Metrics of Security, in *Cyber Defense and Situational Awareness*, *Advances in Information Security 62*, Springer International Publishing, 2014, pp. 263–265.

208. Collier Z. A., Panwar M., Ganin A. A., Kott A. and Linkov I., Security Metrics in Industrial Control Systems, in *Cyber Security of Industrial Control Systems*, *Including SCADA Systems*, New York, NY, Springer, 2016.