XXII Международная конференция "Информатика: проблемы, методы, технологии" (IPMT-2022) и XIII школа-конференция "Информатика в образовании" (INED-2022).

(Information Systems and Computer Modeling

Воронежский государственный университет, 10 февраля 2022 г., Воронеж

Некоторые значимые тренды в развитии цифровой трансформации

Главный научный сотрудник ФИЦ ИУ РАН

Член-корр. Академии Криптографии РФ, д.т.н., профессор

ЗАЦАРИННЫЙ Александр Алексеевич

В докладе

1. Мир в условиях неопределенности. Давос-2022.
2. Цифровая трансформация России. Значимые инициативы Руководства страны.
3. Новые цифровые технологии. Угрозы и риски.
4. Прорыв в стандартизации.
5. Память

Мир сегодня в условиях неопределенностей и рисков

Федеральный исследовательский центр Информатика и Управление Российской академии наук

Из долгосрочного прогноза научно-технологического развития России до 2030г. (prognoz.hse.ru)

«Сквозные» цифровые технологии:

- **большие данные;**
- **нейротехнологии и искусственный интеллект;**
- **системы распределенного реестра;**
- **квантовые технологии;**
- **новые производственные технологии;**
- **промышленный интернет;**
- **компоненты робототехники и сенсорика;**
- **технологии беспроводной связи;**
- **технологии виртуальной и дополненной реальностей**

Глобальные вызовы

- Усиление контроля над информацией в сети Интернет
- Увеличение дисбаланса между требованиями безопасности и личной свободой человека
- Рост киберпреступности и масштаба ее эффектов (технических сбоев и др.)
- Радикальная трансформация рынков ИКТ в условиях смены технологий компонентной базы (прекращение действия закона Мура, развитие новых материалов, фотоники и др.)

Окна возможностей

- Производство и поддержание функционирования суперкомпьютеров
- Работа со сверхбольшими объемами данных (Big Data)
- Создание новых интерфейсов «человек – цифровая среда»
- Конвергенция информационных платформ
- Обеспечение повсеместного высокоскоростного доступа к сетевой инфраструктуре
- Формирование единой управляющей среды
- Новые принципы организации вычислений
- Разработка эффективных форм представления информации, контента и знаний
- Эволюция Интернета («семантический веб», «Интернет вещей»)
- Моделирование человеческого интеллекта, когнитивные модели сознания и поведения
- Разработка биоподобных и антропоморфных робототехнических устройств

2030

Угрозы для России

Ускоренное формирование единого глобального информационного пространства
Обострение «цифрового неравенства»
Неготовность к широкомасштабному предоставлению гражданам медицинских и иных социальных услуг с использованием ИКТ
Возможность использования потенциала ИКТ в целях подрыва национальной безопасности, нарушения государственного и общественного порядка
Необходимость обеспечения эффективного (защищенного) документооборота
Неготовность к массовому применению технологий виртуальной реальности

2030

Нас ожидает лавинообразный рост неопределенности и сложности

Давос-2022 как один из взглядов на глобальные риски

Из-за новой волны коронавируса Всемирный экономический форум (ВЭФ) в Давосе был перенесен на лето.

Организаторы Форума во главе с Клаусом Швабом в начале года представили **доклад о тенденциях развития мировой экономики.**

Коронавирус по-прежнему представляет критическую угрозу для планеты. «Вакцинное неравенство» усугубило социальные разногласия и геополитическую напряженность: в беднейших 52 странах (20% мирового населения) уровень вакцинации составлял всего 6%, тогда как в странах с высокими доходами он превысил 67%.

Поляризация благосостояния в мире усиливается: по оценкам Всемирного банка самые богатые 20% населения мира в 2021 году восстановили половину своих потерь, связанных с пандемией, а беднейшие 20% лишились еще 5% своих доходов.

В докладе определены **4 группы глобальных рисков:**

- **климатические изменения** (на Саммите ООН COP26 в Глазго о единых подходах не договорились, риски применения новых «зеленых» технологий не оценены, под угрозой природа);

- **кибербезопасность** (стремительная цифровизация экономики приводит к глобальному цифровому мошенничеству: только в 2020 году количество атак вредоносных программ и программ-вымогателей увеличилось в 3-4 раза);

- **миграция населения** (даже в условиях локдаунов 2020 года, из-за различных конфликтов, покинули место жительства 34 млн. человек — исторически рекордный показатель);

- **конкуренция в космосе** (в ближайшее десятилетие планируется запуск около 70 тысяч спутниковых устройств, сегодня в космосе уже - 11 тысяч, о космических амбициях заявляют Аргентина, Бразилия, Мексика, Египет, Иран, Турция и др. страны).

Источник: https://ng-ru.turbopages.org/turbo/ng.ru/s/economics/2022-01-16/100_econ16012022.html

Китайский ответ на вызов Давоса: «великая перезагрузка» захлебывается

По приглашению председателя ВЭФ Клауса Шваба **с докладом по видеосвязи из Пекина выступил председатель КНР Си Цзиньпин.**

Китайский лидер охватил целый спектр актуальнейших вопросов современности.

Основное:

1. Единственный верный путь для человечества пролегает через **мир, развитие и взаимовыгодное сотрудничество.**

2. **Развитые экономики** должны первыми выполнять свои обязательства по сокращению выбросов, держать слово и **оказывать финансовую и технологическую поддержку развивающимся странам.**

3. Экономическая глобализация должна развиваться на основе **интересов народов, а не элит.** И особую ответственность в этом несут развитые страны. Си Цзиньпин предложил Западу **вместо стремления к доминированию посвятить себя служению человечеству.**

Планы Китая достичь к 2049 году, к столетию КНР, **«всестороннего строительства социалистической модернизированной страны»,** остаются в вне зависимости от того, какие «встречные планы» и «перезагрузки» будут им противопоставлены.

Очевидно, что **надежды К. Шваба** на возможность «переосмыслить, заново изобрести и перезагрузить наш мир (К.Шваб «COVID-19: Великая перезагрузка», 2020) **не оправдались.**

Федеральный исследовательский центр
Информатика
и Управление
Российской академии наук

Цифровая трансформация России. Значимые инициативы Руководства страны.

Цифровая трансформация в России набирает обороты

- курс на **повышение качества управления** - *«...важнейший вопрос — это новое качество управления»* (М.Мишустин);
- переход к оценке деятельности по **ключевым показателям эффективности (KPI);**
- формирование **института заместителей** федеральных органов, ответственных за цифровую трансформацию (Chief Digital Transformation Officer, CDTO);
- определение в ведущих **ВУЗах страны проректоров**, ответственных за подготовку кадров для цифровой трансформации;
- особая важность **межведомственного взаимодействия**, *«потому что где-то понадобится учитывать в ваших технических заданиях мнения соседствующих ведомств»;*
- **пандемия коронавируса – как фактор ускоренного развития IT;**
- повышение **значимости региональных проектов** в рамках цифровой трансформации.

Последние знаковые события:

Форум «Искусственный интеллект»	- Парк Патриот, Москва, 22-27 августа 2021
Юбилейный Форум «ИТ в ОПК»	- Москва, 16-18 сентября 2021
Международная конференция «ИТ-Стандарт»	- Москва, 24 ноября 2021
Инфофорум-2022	- Москва, 3-4 февраля 2022

Об основах государственной политики в сфере стратегического планирования в Российской Федерации

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Основ государственной политики в сфере стратегического планирования в Российской Федерации

В соответствии с федеральными законами от 28 декабря 2010 г. № 390-ФЗ "О безопасности" и от 28 июня 2014 г. № 172-ФЗ "О стратегическом планировании в Российской Федерации" п о с т а н о в л я ю:

1. Утвердить прилагаемые Основы государственной политики в сфере стратегического планирования в Российской Федерации.

2. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации В.Путин

Москва, Кремль
8 ноября 2021 года
№ 633

Указ определяет цели, задачи, направления и документы стратегического планирования, разрабатываемые в рамках целеполагания на федеральном уровне государственной политики в сфере стратегического планирования

Среди задач государственной политики в сфере стратегического планирования выделим:

Организацию научно-методологического обеспечения стратегического планирования

Научно-методологическое обеспечение стратегического планирования направлено на:

- повышение **качества стратегического управления**
- поддержку процессов выработки и **принятия управленческих решений на вариативной основе**
- **комплексный анализ и прогнозирование** перспектив социально-экономического развития и состояния национальной безопасности
- организацию **мониторинга и контроля реализации документов** стратегического планирования
- формирование **научно обоснованных подходов** к развитию стратегического планирования
- совершенствование **методологии организации и реализации** стратегического планирования
- разработку и внедрение в практику стратегического планирования **методов моделирования, балансовых расчетов, обработки больших объемов данных**

О стратегическом направлении в области цифровой трансформации государственного управления

Председатель правительства М. В. Мишустин подписал Распоряжение Правительства РФ от 22 октября 2021 г. N 2998-р **«Об утверждении стратегического направления в области цифровой трансформации государственного управления»**:

1. Утвердить прилагаемое стратегическое направление в области цифровой трансформации государственного управления.

2. Минцифры России совместно с заинтересованными федеральными органами исполнительной власти и государственными внебюджетными фондами Российской Федерации обеспечить реализацию стратегического направления, утвержденного настоящим распоряжением.

Основанием разработки стратегического направления в области цифровой трансформации государственного управления является перечень поручений Президента РФ по итогам конференции по искусственному интеллекту.

Ответственным за реализацию стратегического направления назначено **Минцифры.** Соисполнители - Минэкономразвития, Минпромторг и др.

Проблемы, решаемыми при цифровизации

- **недостаток достоверных сведений** (данных), доступных в режиме реального времени, необходимых **для принятия управленческих решений**
- **несвязанность контрольно-надзорных мероприятий с реальными рисками** и их трактовка как нагрузка, а не помощь
- затруднение взаимодействия сотрудников органов государственной власти и органов местного самоуправления в связи с **отсутствием унифицированных средств совместной и удаленной работы**, наличие **недостаточного уровня цифровизации кадровой работы государственной службы**
- непрозрачность бюджетного процесса и учета всех органов власти для федерального центра (до 30 процентов рабочего времени сотрудников финансовых подразделений занимает подготовка различных отчетов, **отсутствуют механизмы проверки доведения бюджетных выплат до получателей)**
- наличие **завышенных и дублирующих расходов на создание государственных информационных систем** с идентичным функционалом (например, каждый субъект тратит бюджетные средства на создание систем, предназначенных для предоставления услуг)
- отсутствие средств **объективного контроля за исполнением поставленных задач сотрудникам со стороны руководителей**, в том числе в рамках достижения стратегических задач и целей

Стратегические риски цифровой трансформации государственного управления

- отсутствие **нормативного правового регулирования**, которое может блокировать автоматизированный сбор социально-экономических показателей, так как в настоящее время **коммерческие организации не обязаны предоставлять такую информацию в органы государственной власти** (за исключением налоговой отчетности)
- наличие **малых объемов производства и ограниченного перечня датчиков и приборов объективного контроля российского производства**, неготовность в срок автоматизированных средств агрегации и обработки сведений (данных), полученных дистанционным путем в режиме реального времени
- **недостаточный уровень цифровых компетенций у сотрудников** органов государственной власти и органов местного самоуправления
- **отсутствие заинтересованности в переводе взаимодействия в электронный вид у всех участников такого взаимодействия**
- наличие **зависимости от поставок аппаратной части от зарубежных поставщиков** и сопутствующих этому рисков в области информационной безопасности

Цифровая трансформация вошла в перечень инициатив социально-экономического развития РФ до 2030 года

Федеральный исследовательский центр Информатика и Управление Российской академии наук

Задачами **цифровой трансформации государственного управления** являются повышение качества и системность исполнения следующих государственных функций:

- **государственное регулирование** и выработка государственной политики в отраслях экономики и социальной сфере;
- предоставление **государственных и муниципальных услуг**;
- осуществление **контрольной и надзорной деятельности**;
- **управление государственным имуществом**;
- обеспечение **безопасности государства в целом и граждан в частности.**

Угрозы и риски цифровой трансформации

Угрозы и риски цифровой трансформации

Федеральный исследовательский центр Информатика и Управление Российской академии наук

Четыре группы угроз, связанных с применением информационных технологий (ИТ):

- **угрозы системного характера** – отсутствие системного подхода к описанию архитектуры, алгоритмов функционирования системы и организации процесса использования ИТ.
- **угрозы функционального характера** – неполное соответствие реализуемых алгоритмов функционирования системы при решении пользовательских задач заданным функциональным требований к системе, включая доступность, конфиденциальность и целостность;
- **угрозы алгоритмического характера** – недостаточный контроль реализации функций программных компонент;
- **угрозы технической реализации** – недостаточный контроль реализации механизмов защиты, уязвимости среды функционирования, а также отсутствие технического сопровождения.

Кибербезопасность – приоритетное направление в развитии цифровых технологий

Федеральный исследовательский центр Информатика и Управление Российской академии наук

Для создания методов прогнозирования, выявления и предотвращения кибератак широко используются технологии искусственного интеллекта (ИИ), включая атаки на другие системы ИИ.

1. **Искусственный интеллект** – это принципиально **технологии двойного применения**: они могут использоваться как в мирных, так и в военных целях. Основным двигателем исследований в области ИИ являются военные разработки (США, Китай, Франция, Израиль и др.). Так, в 2021 году появились первые сообщения об автономных дронах-убийцах, которые способны самостоятельно принимать решения о применении оружия против людей.

2. **США в разработках ИИ** рассчитывают создать технологии, которые позволят преодолеть основное военное ограничение 20-21 веков – **паритет в ядерном противостоянии**. Речь идет о создании автономных супербыстрых интеллектуальных образцов вооружения, значительно превышающих возможности противника по реагированию на атаки. В частности, это оружие ориентируется на уничтожение мест базирования (шахт) с баллистическими ракетами до их старта.

В **докладе Комиссии по ИИ для национальной безопасности Конгресса США** отмечается, что ИИ коренным образом изменит способы и инструменты обеспечения безопасности США.

Принят ряд программ.

- Программа национального научного фонда США (NSF) «**Безопасное и доверенное киберпространство**» (Secure and Trustworthy Cyberspace),
- Программы **Управления перспективных исследований разведки** (IARPA) "Virtual User Environment", Secure, Assured, Intelligent Learning Systems (SAILS) и Trojans in Artificial Intelligence (TrojAI) (2018).
- **Управление перспективных исследований и разработок Министерства обороны** (DARPA) анонсировало программу по обеспечению устойчивости искусственного интеллекта к деструктивным воздействиям (Guaranteeing AI Robustness against Deceptions, GARD). (февраль 2019 года).

Совместно эти программы направлены на борьбу с различными видами атак на системы искусственного интеллекта.

Основные проблемы

Проблемы безопасности искусственного интеллекта по мере роста научного и общественного внимания к этому направлению приобретают всё большее значение.

В качестве **основных проблем** выделим:

- **уязвимости систем машинного обучения**, включая использование **недостоверных или заведомо искаженных обучающих выборок**, необходимых для обучения алгоритмов ИИ;

- **преднамеренная деструктивная модификация алгоритмов** обработки данных в системах искусственного интеллекта (наличие «скрытых дверей»);

- необходимость применения **доверенных аппаратно-программных средств** для реализации алгоритмов ИИ;

- обеспечение защиты ИИ от **непреднамеренных ошибок** (например, состязательные атаки);

- **квалификация пользователя**. Во многих случаях эффективность системы искусственного интеллекта существенно зависит от взаимодействия с человеком

Проблемы обеспечения безопасности АИС, использующих технологии ИИ, охватывают как проблемы **защиты функционирования** систем ИИ по назначению, так и проблемы **защиты цифровой инфраструктуры**, в которой эти системы функционируют.

Системы искусственного интеллекта, используемые на объе**ктах критически важных инфраструктур**, должны быть защищены от различного рода преднамеренных кибератак.

Для создания безопасных, надёжных и доверенных АИС с применением систем ИИ необходимо проведение углубленных научных исследований.

О применении технологий искусственного интеллекта в системе защиты информации АИС

Антивирусная защита. Как правило, средства антивирусной защиты базируются на методах сигнатурного поиска участков используемого кода, совпадающих с каким-либо из имеющихся образцов вирусов. В новых антивирусных средствах стали применяться так называемые проактивные методы, которые выявляют возможные вирусные атаки по косвенным признакам, возможным сценариям внедрения и актуализации вирусного кода. Эти методы основаны на использовании технологий искусственного интеллекта.

Мониторинг действий пользователей автоматизированной системы. Составной частью этой подсистемы должна стать интеллектуальная подсистема контентного анализа информационных потоков, позволяющая в ряде случаев выявлять или предупреждать несанкционированные действия инсайдеров. Некоторые элементы технологии ИИ уже используются в активно внедряемых система (SIEM, DLP, Detection System).

Выявление скрытых каналов утечки. Они образуются логическим каналам передачи, образуемым путем модуляции каких-либо легально передаваемых в канал связи сигналов, например, служебной информации связных протоколов (частный случай - скрытый канал, основанный на метках). Для выявления скрытых каналов могут применяться методы искусственного интеллекта для выявления аномалий в канале связи.

Администрирование подсистем защиты. Применительно к территориально распределенным автоматизированным системам задача построения непротиворечивой матрицы доступа является актуальной (особенно с учетом необходимости ее согласования с распределением криптографических ключей шифрования, работой удостоверяющего центра, обеспечивающего использование электронной подписи и т.п.). Отдельные элементы этого направления уже реализуются в системах IDM (Identity Management), управляющих учетными записями зарегистрированных пользователей.

О применении технологий ИИ в АИС

1. **Тиражирование (масштабирование) уже внедренной технологии ИИ** применительно к проектируемой АИС **недопустимо.** Необходимы исследования угроз и рисков этой технологии с учетом требований к функциональной и системной безопасности в каждой конкретной автоматизированной системе и условий ее применения.

2. Использование традиционный подходов обеспечения информационной безопасности в АИС на основе создания замкнутой доверенной среды применительно к АИС с использованием технологий искусственного интеллекта в полном объеме неприемлем. Необходим **переход к концепции мониторинга событий в цифровом пространстве.**

3. Технологию искусственного интеллекта целесообразно использовать в средствах защиты информации для обеспечения мониторинга событий **с учетом угроз функционального и системного характера.**

4. Необходима **корректировка нормативно-методической базы в области безопасности с ориентацией на широкое использование методов мониторинга событий** в цифровом пространстве с выработкой количественных оценок уровней безопасности, основанных на риск-ориентированном подходе.

Три ключевые проблемы, решение которых позволит снизить угрозы и риски

Первая. Создание на основе системного подхода **научно-технической основы** для разработки доверенных систем и средств ИИ как совокупности взаимоувязанных методических, системотехнических и организационных решений.

Вторая. Создание **отечественной аппаратно-программной среды** для разработки, внедрения и применения автоматизированных информационных систем, прежде всего ГИС, с использованием технологий ИИ. Здесь два направления:

- **программное обеспечение** - разработка собственных платформ для нейронных сетей, систем сбора, анализа и обработки данных (примерно 90% нейронных сетей в России сделаны на базе открытых нейронных платформ TensorFlow и PyTorch, принадлежащих Google и Facebook);

- **вычислительные средства** - создание отечественных вычислителей и прежде всего графических карт (сегодня они импортные, дорогие, поставка может ограничиваться санкциями).

Третья. **Подготовка высококвалифицированных специалистов в области ИИ** (большие данные, машинное обучение и др.) и создание комфортных условий для их работы (специалистов мало подготовить, надо их и удержать).

Успешное решение этих проблем возможно на основе **создания на государственном уровне мощного «треугольника успеха»: государственного заказчика – генерального конструктора – научного координатора.**

Требуется разработка **государственной стратегии в области ИИ** с приоритетной ориентацией на интересы **обеспечения национальной безопасности и технологической независимости.** Экономические интересы, включая развитие рынка и применение ИИ коммерческими компаниями, должны учитываться на вторичной основе. Утвержденная в России Национальная стратегия по ИИ привязана к программе «Цифровая экономика».

Россия обладает возможностями для реализации предлагаемого подхода.

Используемые источники

1. Н.И. Касперская. Риски и угрозы Искусственного Интеллекта. Выступление на Консультативном совете Минобороны РФ, 2 июня 2021 г.

2. В.Е. Гаврилов, А.А. Зацаринный. Некоторые системотехнические вопросы использования интеллектуального анализа данных для обеспечения защиты информации в ситуационных центрах. //Системы и средства информатики, №1, 2018г.

3. Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, приказ ФСБ России и ФСТЭК России от 06.05.2019г. № 196

4. А.А. Зацаринный, В.Е. Гаврилов Проблемы нормативно-правового и технического регулирования обеспечения информационной безопасности при создании автоматизированных систем военного назначения. //Материалы 6-й Международной межведомственной научно-практической конференции научного отделения № 10 Российской академии ракетных и артиллерийских наук, Москва, 18.03.21г. Т.2 с.69-75.

5. https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-voennom-protivostoyanii-buduschego/viewer

6.https://in.minenergo.gov.ru/analytics/natsionalnyy-strategicheskiy-plan-issledovaniy-i-razrabotok-v-oblasti-iskusstvennogo-intellekta-aktu

7. ГОСТ Р МЭК 61508-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»

8. В.Е. Гаврилов, А.А. Зацаринный, Исследование проблем нормативно-методического регулирования в области информационной безопасности процессов создания и внедрения информационных технологий, разрабатываемых в рамках программы «Цифровая экономика». // Вестник Воронежского института ФСИН России, 2020, № 3, июль–сентябрь, с. 30-38

9. Варианты аварий самоуправляемых автомобилей https://yablyk.com/873287-varianty-avarij-samoupravlyaemyx-avtomobilej-7-uzhasayushhix-primerov/?utm_referrer=https%3A%2F%2Fzen.yandex.com

10. Eykholt, Kevin, et al. Robust physicalworld attacks on deep learning visual classifi cation. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018.

Используемые источники

11. Knight W. Military artifi cial intelligence can be easily and dangerously fooled. MIT Technology Review от 21.10.2019

12. Нейронные сети компании Google разработали свою собственную систему шифрования данных, https://dailytechinfo.org/infotech/8615-neyronnye-seti-kompanii-google-razrabotali-svoyu-sobstvennuyu-sistemu-shifrovaniya-dannyh.html

13. А.Н.Аверкин, Объяснительный искусственный интеллект (XAI) – преодоление разрыва между коннекционистким и символьным подходами в искусственном интеллекте, , Школа молодых ученых «Высокопроизводительные платформы для цифровой экономики и научных проектов класса мегасайенс

14. Защищаемся от ИИ с помощью ИИ: решения с поддержкой искусственного интеллекта для киберугроз нового поколения, https://www.securitylab.ru/analytics/518993.php

15. Как обманывают искусственный интеллект, 17.02.2020г. https://www.cnews.ru/articles/2020-02-17_kak_obmanyvayut_iskusstvennyj_intellekt

16. ИБ-итоги 2019: Год утечек и социнженеров, 27.12.2019г., https://searchinform.ru/blog/2019/12/27/ib-itogi-2019-god-utechek-i-socinzhenerov

17. Социальные сети: диагноз по "лайкам", 22.06.2021г., https://www.yoki.ru/social/psy/23-01-2015/431160-like-0/

18. Грушо А., Забежайло М., Зацаринный А., Контроль и управление информационными потоками в облачной среде. // Информатика и ее применения, 2015. Т. 9, № 4. С. 95-101.

19. А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина, С.Я. Шоргин. Безопасные архитектуры распределенных систем. //Системы и средства информатики, 2014. Т. 24, № 3. С. 18-31.

20. Alexander Grusho, Nick Grusho and Elena Timonina. Detection of Anomalies in Non-numerical Data, Proceedings of the 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2016

21. А. Грушо, М. Забежайло, А. Зацаринный, В. Писковский, С. Борохов. О возможностях приложений интеллектуального анализа данных в задачах обеспечения информационной безопасности облачных сред, //Научно-техническая информация. 2015. № 11. С. 1-11.

Основные тренды в области стандартизации

Стандартизация как драйвер ускоренного развития цифровых технологий

Руководитель Росстандарта **А.П. Шалаев На XI Международной научной конференции «ИТ-Стандарт» 24.11.2021** отметил:

- **Стандартизация является основой для практического внедрения цифровых решений** и позволяет устранять барьеры применению цифровых моделей и виртуальных испытаний новейших технологий и материалов, оптимизации управления цепочкой поставок.

- За десять лет приняты **более 1000 стандартов в сфере ИТ:** большие данные, робототехника, цифровые двойники.

- По итогам 2020 года **49% утвержденных стандартов разработано за счет компаний** (без привлечения бюджетных средств).

- **Средний срок разработки стандартов** составил 9,2 месяца (в 2012 г. - почти три года). Для сравнения: в Германии время разработки стандарта в среднем 12,5 месяцев, во Франции – около 14 месяцев.

- Отрабатываются подходы к разработке **СМАРТ-стандартов.**

- Важность **международного сотрудничества**, прежде всего с Германией, Францией.

В январе с.г. в режиме видеоконференцсвязи А. Шалаев обсудил с представителями германских предприятий, работающих на российском рынке, вопросы сотрудничества в области технического регулирования и путей **гармонизации цифровых инициатив России и Германии в области стандартизации** – в том числе, стандарты цифровых производств, искусственного интеллекта, цифровых двойников изделий и виртуальных испытаний.

В марте 2022 года состоится **первый российско-германский конгресс по стандартизации** в Ганновере.

SMART-СТАНДАРТ

На заседании Совета ИСО 23 февраля 2021 г. дан старт реализации с 1 марта Стратегии ИСО-2030, основанной на так называемых **SMART-стандартах.**

Это ключевое направление международной стандартизации. Новые понятия: МАШИНОЧИТАЕМЫЕ СТАНДАРТЫ, МАШИНОСЧИТЫВАЕМЫЕ СТАНДАРТЫ, МАШИНОПОНИМАЕМЫЕ СТАНДАРТЫ, МАШИНОПОЧИТАЕМОЕ СОДЕРЖАНИЕ

Умный стандарт (нормативный документ) (SMART (standards machine applicable, readable & transferrable)) – цифровой (машиночитаемый/машинопонимаемый) документ, степень интеграции которого достигла уровня, который делает возможными самоорганизующиеся функции во всех бизнес-процессах, связанных с жизненным циклом документа, а также во всех бизнес-процессах, связанных с жизненным циклом изделия (продукции).

SMART-СТАНДАРТ — ЭТО СЛОЖНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА, которая включает ИНФОРМАЦИОННЫЕ и числовые КАРТЫ (оборудование, материалы и др.), графику (PDF, JPEG, TIF), ВИДЕО И 3D-МОДЕЛИ, ТЕКСТы (XML, HTML,ГИПЕРТЕКСТ), РЕДАКЦИИ (Ретроспектива редакций НД).

SMART-СТАНДАРТ, по существу, - математическая модель, позволяющая на основе ввода в качестве исходных данных требований к АСУ, условий ее функционирования, ограничений (включая финансовые), получать варианты построения АСУ, удовлетворяющие требованиям заказчика.

В структуре ТК/МТК 22 создан **подкомитет «Умные стандарты».**

Классификация машиночитаемых стандартов и информационных систем

Машиночитаемые стандарты — документы, содержание которых легко воспринимается, обрабатывается и передается с помощью компьютерных систем

SMART-стандарты (Standards Machine Applicable, Readable & Transferrable) — стандарты в виде баз данных, моделей и т.д., ключевым потребителем которых является информационная система

Мероприятия в области стандартизации «Искусственный интеллект»

1. В 2021 году разработана и утверждена при согласовании Минэкономразвития России **перспективная программа стандартизации по приоритетному направлению "Искусственный интеллект".**

2. Начиная с 2021 г., ежегодно **ТК 164 «Искусственный интеллект» (председатель – Гарбук С.В.)** направляет доклад в Минэкономразвития России и Росстандарт о разработке и актуализации комплекса стандартов в сфере ИИ.

3. К 2024 г. утверждено и актуализировано **более 100 стандартов** в сфере ИИ.

4. Начиная с 2021 г., представители ТК 164 принимают участие в разработке международных стандартов по ИИ.

Разработка и гармонизация стандартов в области информационной безопасности

ФИЦ ИУ РАН совместно с ИАВЦ в 2020-2021 г.г. (при активном участии специалистов национальных ТК 22 «Информационные технологии», ТК 362 «Защита информации», «Государственного научно-исследовательского испытательного института проблем технической защиты информации ФСТЭК» и др.) по государственному заказу Росстандарта (по лоту 2.1.20) в рамках выполнения федерального проекта «Информационная безопасность» **в течение полутора лет (2019 декабрь – 2021 май)** выполнил комплекс работ по **разработке и гармонизации стандартов в области информационной безопасности и защиты информационных технологий** с учетом современных тенденций их развития.

Разработанные стандарты **(всего 71)** приняты и утверждены приказами Росстандарта с датой введения **в действие 30.11.2021 г.**

В рамках этой работы ФИЦ ИУ РАН разработал комплекс из **29 национальных стандартов системной инженерии по защите информации в типовых процессах жизненного цикла систем в условиях неопределенностей и возможных рисков** (ГОСТ Р 59329 – ГОСТ Р 59357)».

Созданный комплекс стандартов охватывает различного рода системы и реализуемые типовые процессы согласно ГОСТ Р 57193-2016.

Идея – в привязке стандартов к процессам системной инженерии, для возможности их использования как самостоятельно, так и в комбинации с другими стандартами

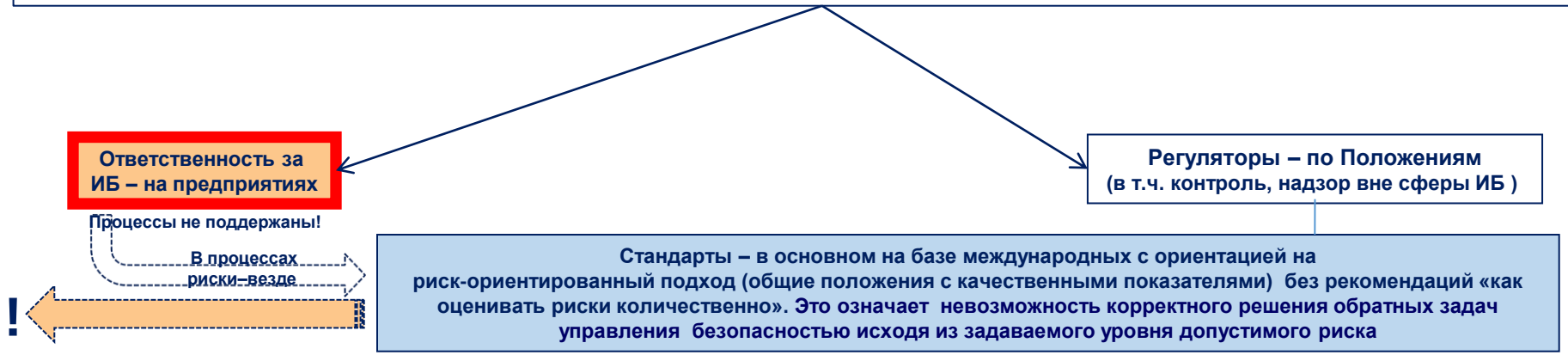
Процессы – по ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем» (ISO/IEC/IEEE 15288, NEQ)

Отличительные особенности

ДО ПРИНЯТИЯ РАЗРАБОТАННЫХ СТАНДАРТОВ

СТИМУЛЫ ДЛЯ ПРЕДПРИЯТИЙ

1. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 31.12.2015 № 683
2. Стратегия научно-технологического развития Российской Федерации, утверждена Указом Президента РФ от 01.12.2016 № 642
3. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ 05.12.2016 № 646
4. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утверждена Указом Президента РФ от 09.05.2017 № 203
5. Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента РФ от 13.05.2017 № 208
6. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017г. № 187-ФЗ
7. Программа «Цифровая экономика РФ», утверждена распоряжением Правительства РФ от 28.07.2017 № 1632-р
8. Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента РФ от 13.05.2019 № 16
9. Концепции создания государственной единой облачной платформы, утвержденной распоряжением Правительства РФ от 28.08.2019 г. №1911-р



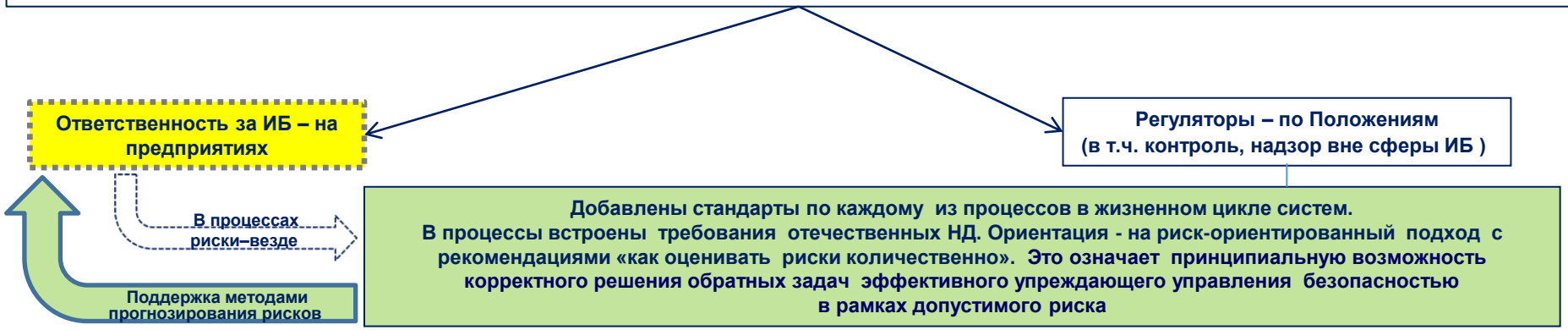
Итог – применение так, «как понимают на местах», риски по ИБ либо вовсе не оценивают, либо оценивают «как могут» (в основном – качественно, количественно - чаще экспертно), нормативы отечественных НД – в системные процессы не встроены, обучение, – зачастую проводится НЕРЕГУЛЯТОРАМИ И ЛИЦАМИ, ИМИ НЕ УПОЛНОМОЧЕННЫМИ (как умеют, без ответственности), гарантий нет, страхование по ИБ не отработано

Отличительные особенности

ПОСЛЕ ПРИНЯТИЯ РАЗРАБОТАННЫХ СТАНДАРТОВ

СТИМУЛЫ ДЛЯ ПРЕДПРИЯТИЙ

1. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 31.12.2015 № 683
2. Стратегия научно-технологического развития Российской Федерации, утверждена Указом Президента РФ от 01.12.2016 №642
3. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ 05.12.2016 № 646
4. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утверждена Указом Президента РФ от 09.05.2017 № 203
5. Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента РФ от 13.05.2017 № 208
6. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017г. № 187-ФЗ
7. Программа «Цифровая экономика РФ», утверждена распоряжением Правительства РФ от 28.07.2017 № 1632-р
8. Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента РФ от 13.05.2019 № 216
9. Концепции создания государственной единой облачной платформы, утвержденной распоряжением Правительства РФ от 28.08.2019 г. №1911-р



Итог – все процессы охвачены, риски по ИБ оцениваются как качественно, так и количественно строго на научной основе. Обучение, сертификация – проводятся по методическим рекомендациям стандартов, гарантии формируются самими предприятиями на основе прогнозирования рисков и корректного решения обратных задач эффективного управления безопасностью, исходя из задаваемого уровня допустимого риска

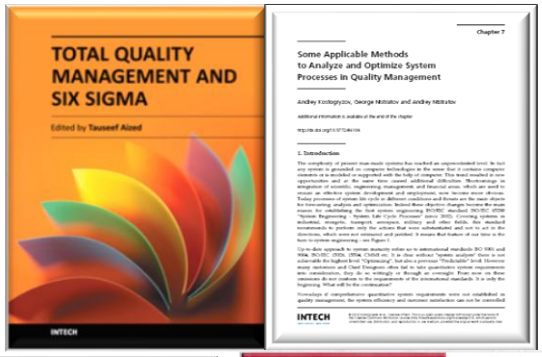
Практическая ценность

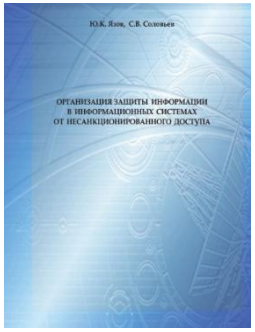
Разработанные **29 стандартов** благодаря рекомендуемым математическим моделям создают условия для:

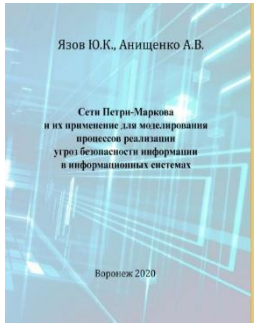
- **обоснования упреждающих мер**, приемлемых для противодействия угрозам по критериям «эффективность - стоимость», «безопасность - стоимость - возможные ущербы»;
- решения **обратных задач**, связанных с обоснованием мер, реализация которых приводит к непревышению допустимых рисков.
- управления рисками при **средне- и долгосрочном планировании**
- **максимизации выигрыша или минимизации ущербов** в каждом из реализуемых процессов на каждом этапе жизненного цикла применительно к каждому значимому компоненту сложной системы и к системе в целом.

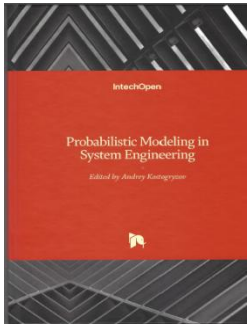
Стандарты являются **методической основой для подготовки обоснованных ответов на вызовы** ближайшего будущего, обусловленные, с одной стороны, ростом неопределенностей и угроз, а с другой, – резким усложнением различного рода систем, возрастанием объемов обрабатываемой информации, построением и эффективным применением систем искусственного интеллекта, внедрением «умных» систем, содержащих много «черных ящиков» (для которых известны входные данные и выходные результаты, но неизвестны внутренности).

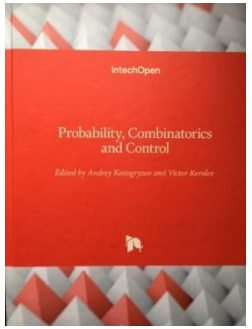
Основой для разработки стандартов явился научно-технический задел ученых ФИЦ ИУ РАН и других научных коллективов











Мы потеряли в прошлом году…

Александр Владимирович СТАРОВОЙТОВ (1940-2021), выдающийся конструктор, ученый и организатор работ в области защищенных информационных технологий, основатель и первый директор ФАПСИ (1992-1998), Герой России, генерал армии, Президент ЦИТИС, Генеральный конструктор специальных систем связи, доктор технических наук, профессор.

Калью Иванович КУКК (1930–2021), выдающийся ученый, конструктор и организатор работ в области военной связи, первый заместитель министра промышленности средств связи СССР, первый заместитель министра связи СССР, вице-президент АО ТЕЛЕКОМ, автор многих научно-исторических трудов в области АСУ и связи, доктор технических наук, профессор

Благодарю за внимание

Здоровья, успехов и удачи

Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН)

Federal Research Center “Computer Science and Control“ of the Russian Academy of Sciences (FRC CSC RAS)

Главный научный сотрудник ФИЦ ИУ РАН
д.т.н., профессор А.А. ЗАЦАРИННЫЙ
119333 Москва, ул. Вавилова, д.44 кор.2
тел./факс (495)135-41-89
e-mail: azatsarinny@ipiran.ru