7. *Hoffmann R.* Markov Models of Cyber Kill Chains with Iterations / Proceedings in the 2019 International Conference on Military Communications and Information Systems (ICMCIS). – 2019. – P. 1-6.

8. *Дрянных Ю.Ю., Жуков В.Г.* О необходимости внедрения threat intelligence // Решетневские чтения. – 2017. – №21-2. – С. 398-399.

9. *Левин И.И., Дордопуло А.И., Писаренко И.В., Мельников А.К.* Управление расчетом точных приближений распределений вероятностей значений статистик на гибридных вычислительных системах / XIV Всероссийская мультиконференция по проблемам управления (МКПУ-2021): материалы XIV мультиконференции (27 сентября-2 октября 2021 Дивноморское, Геленджик) в 4 т. / Т. 2. – Управление в распределенных и сетевых системах (УРСС-2021). – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2021. – С. 261-266.

Пискурева Т.А., Махов А.Н.

Цифровая трансформация и импортозамещение во взаимосвязи обеспечения безопасности ядерного объекта

Аннотация: Переход на импортонезависимые решения и цифровая трансформация идут в ногу с обеспечением безопасности на базе использования отечественных программных продуктов и технических средств.

В работе рассматривается взаимосвязь стратегии цифровой трансформации и импортозамещения с задачами по обеспечению безопасности ядерного объекта, обращается внимание на роль человеческого фактора при переходе на использование новых импортонезависимых решений, на важность формирования организационной культуры и культуры безопасности.

Ключевые слова: цифровизация, цифровая трансформация, импотрозамещение, цифровые продукты, системы защиты, ядерный объект, культура безопасности

Изменения, которые происходят в мировом порядке, глобальный кризис и пандемия сформировали новую повестку, следуя которой Россия вступила на путь глубокой цифровой трансформации государства.

Цифровая трансформация – это внедрение цифровых технологий в различные сферы деятельности общества. Что касается организаций, то цифровая трансформация – это, прежде всего, преобразование структуры самой организации, стратегии ее развития, презентации производимых продуктов и услуг, изменение организационной культуры.

Однако нельзя говорить об эффективности такой модели без должной модернизации, разработки и внедрения новых IT-технологий. Откуда же брать эти современные информационные технологии, способные создавать условия, как устойчивого экономического развития, так и эффективную систему безопасности? Это может быть достигнуто только цифровым суверенитетом, включающим в себя модель программного и аппаратного импортозамещения. Вместе с тем, цифровой суверенитет – более широкое понятие, чем импортозамещение. Оно включает в себя обеспечение информационной безопасности, возможность защиты от кибератак и кибершпионажа, обеспечение бесперебойного функционирования сети Интернет. А в условиях массовой глобализации, без политики импортозамещения говорить о 100-процентной кибербезопасности нельзя, да и невозможно.

Государственным структурам и компаниям с госучастим установлен план по переходу на отечественный софт в соответствии с национальной программой «Цифровая экономика РФ»[1]. К 2024 году – более 70% в госорганизациях и не менее 50% в государственных компаниях.

В системе Росатома успешно выполнена трансформация информационных технологий (ИТ), которая обеспечила эффективное протекание бизнес-процессов предприятий отрасли.

Трансформация ИТ была ориентирована на выполнение работ по внедрению корпоративных информационных систем в научно-производственную деятельность предприятий и обеспечение информационной безопасности.

В рамках трансформации ИТ внедрены, тиражированы и используются в научно-производственной деятельности предприятий Росатома различные корпоративные информационных системы, такие как, Единая отраслевая система электронного документооборота на базе EMC Documentum (ЕОСДО), которая обеспечивает скорость прохождения документов, повышает

эффективность работы сотрудников; Информационная система 1С:ERP Росатом, позволяющая эффективно управлять активами; Информационная автоматизированная система по управлению персоналом на базе SAP ERP HCM (ИАСУП), которая позволяет придерживаться единой политики кадрового менеджмента; Информационная система управления отношениями с поставщиками SAP SRM, позволяющая оперативно совершать закупочные процедуры, обеспечивая их контроль и ряд других информационных систем по автоматизации процессов подготовки отчетности, бюджетированию, управлению имущественными активами, энергоэффективностью, инвестиционными проектами, результатами интеллектуальной деятельности, обучением.

Использование информационных систем сокращает сроки подготовки и введения в действия решений, обеспечивает сохранность документов, а также автоматизацию и унификацию бизнес-процессов в соответствии с единой корпоративной учетной политикой.

После завершения цифровой трансформации информационных технологий, предприятия контура Росатома перешли в новую фазу цифровой трансформации самих организаций. С этой целью реализуется Единая цифровая стратегия Росатома, которая ориентируется не только на стратегические цели отрасли, но и на содействие в реализации национальной программы «Цифровая экономика РФ».

В состав Стратегии входят пять взаимосвязанных элементов: «Внутренняя цифровизация», «Цифровые продукты», «Содействие цифровизации-цифровая экономика РФ», «Организационные изменения», «Цифровая культура».

Стратегия состоит из 10 программ и нескольких горизонтов и этапов. В числе ее горизонтов следующие:

- долгосрочный горизонт 2030+ – формирование конкурентоспособной цифровой компании;
- горизонт государственных задач 2024 – достижение задач, зафиксированных в «майских указах» Президента;
- среднесрочный горизонт 2021 – решение задач внутренней цифровизации и создание условий для достижения целей государственного горизонта и видения «Цифровой Росатом» 2030;
- краткосрочный горизонт – решение наиболее важных и срочных бизнес-задач цифровизации на основе дорожных карт.

Основная задача Стратегии – создание устойчивой и безопасной конкурентной инфраструктуры, разработка и внедрение сквозных технологий, использование преимущественно отечественных программных продуктов и обеспечения безопасности информации и информационной инфраструктуры.

Предприятия Росатома идут по пути продуктизации внутренних разработок. Первым цифровым продуктом, выведенным на рынок, стал пакет программ для инженерного анализа и суперкомпьютерного моделирования класса CAE (Computer-Aided Engineering), в который входят модули «Логос Аэро-Гидро», «Логос Тепло» и «Логос Прочность» (расчетные коды), «Волна» – программно-вычислительный комплекс. Разработанная цифровая платформа Multi-D помогает управлять всеми этапами сооружения АЭС и других сложных объектов капитального строительства, система «Призма 2.0» позволяет управлять дискретным производством, связывая конструкторскую документацию и производство в цехах, система «Цифровое предприятие» обеспечивает управление предприятием и производством, платформа «Пилот» обеспечивает контроль и управление доступом для массовых мероприятий, установлена практически на всех стадионах страны, где проводились Олимпийские игры и Чемпионат мира по футболу.

Разработки предназначены как для отраслевого использования, так и для внешнего пользователя, среди них – самый большой в Европе ЦОД «Удомля».

Стоит выделить и разработки в области цифровой энергетики, системы управления спросом, сетевое и телекоммуникационное оборудование, а также ряд платформ – образовательную, «Цифровой добычной комплекс», коммуникационную платформу Atom Space для on-line общения сотрудников предприятий Росатома.

Переход на импортонезависимые решения и цифровая трансформация идут в ногу с обеспечением информационной безопасности на базе использования отечественных программных продуктов и технических средств. Современный рынок продуктов по информационной безопасности позволяет обеспечить защиту государственных интересов, бизнеса и обеспечить защиту информации, циркулирующей в защищаемых ресурсах ядерных

предприятий. Необходимо отметить, что отечественные ИТ-решения не уступают по функционалу и уровню сервиса защиты зарубежным аналогам [2]. Важное преимущество отечественных решений – они создаются с учетом российской специфики и рекомендованы регуляторами. Наиболее используемые решения отечественных производителей в части антивирусной защиты, защиты веб-приложений, защиты от утечек конфиденциальной информации, средств защиты от несанкционированного доступа, анализа защищенности, криптографической защиты информации и другие.

Большое внимание уделяется контролю и предотвращению нарушений информационной безопасности с применением DLP-систем и SIEM-платформ.

Решая вопросы цифровой трансформации и импортозамещения, мы понимаем, что человек был и остается основным гарантом эффективности и безопасности при любых технических и программных усовершенствованиях [3]. Вариативность развития событий, несовершенство инструкций, а главное – социально-психологическая природа человека как субъективного фактора нестабильности и неоднозначности и в восприятии, и в оценке событий – приводит к необходимости учета Человеческого фактора и формирования культуры безопасного внедрения и использования цифровых технологий посредством подбора, отбора, обучения и мотивации персонала. Высокая культура безопасного внедрения и использования информационных технологий, культура информационной безопасности базируется на развитой организационной культуре. С целью единого подхода к развитию культуры безопасности на ядерных объектах реализуется Единая отраслевая политика культуры безопасности. На объектах использования атомной энергии понимают, что культура безопасности должна быть элементом индивидуальных убеждений каждого работника, превалирующим фактором профессионального поведения в любом сегменте деятельности [4].

Крайне важно также отметить, что необходимо максимально открыто обсуждать любой опыт – независимо от того, приобретен ли он ценой достижений или ошибок. Возможность увидеть реальные плюсы и минусы будет мощным мотиватором к внедрению отечественных программных продуктов, а также

механизмом обратной связи, необходимой при переходе к цифровой трансформации и импортозамещению.

Литература:

1. Программа «Цифровая экономика Российской Федерации». Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 10.10.2021).

2. *Гарифуллин Б.М., Зябриков В.В.* Цифровая трансформация бизнеса: модели и алгоритмы // Креативная экономика. – 2018. – Том 12. № 9. – С. 1345-1358.

3. *Пискурева Т.А., Завидова М.Ю., Сергеев М.С.* Вопросы кадровой безопасности. Зоны ответственности при обеспечении комплексной безопасности ядерного объекта / Проблемы управления безопасностью сложных систем. Материалы XXVI Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2018) (19 декабря 2018 г. Москва). – М.: ИПУ РАН, 2018. – С. 364-369.

4. *Piskureva T.A*. Practical Approaches to Nuclear Security Culture Assessment // 1540 COMPASS. – 2015. – Issue 9. – P. 30-33.

Plotnikov N.I.

Method of individual properties soft computing on the example of the civil aviation flight crew safety management

Abstract: Theory and methods of the characteristics of specialists remain uncertain. Statistical data and expertise may be piecewise defined, inaccurate and inconsistent. To calculate the dependability of flight crews based on workload and experience, it is necessary to establish indicators and values of acceptable accuracy, using fuzzy measures. It is proposed soft computing, statistical and expert methods for calculating the properties of a person and social groups in the management of dangerous professions. This makes it possible to calculate the dependability of the pilot properties with an assessment of flight safety risk levels for making management decisions. The results of the work are new standards for the workload of flight crews recommended for civil aviation.