VI. Автоматизированные системы и средства обеспечения безопасности сложных систем

Грабчак Е.П., Логинов Е.Л.

Обеспечение надежности и безопасности работы информационных систем управления для повышения живучести энергосистемы России

Аннотация: Рассматриваются проблемы обеспечения надежности и безопасности работы информационных систем управления для повышения живучести энергосистемы России. Предлагается формирование сети катастрофоустойчивых межкорпоративных дата-центров соответствующих Tier 3 стандарта TIA-942 с постепенным переходом к Tier 4.

Ключевые слова: энергетика, цифровые технологи, управление, информационная система, дата-центр, надежность, безопасность

Введение

Необходимо обеспечение надежности и безопасности работы информационных систем управления технологическими и бизнес-процессами, в т.ч. информационной безопасности, для повышения живучести энергосистемы России, включая ситуации, когда существенная часть оборудования информационных систем управления в сегменте отрасли будет по любым причинам выведена из строя.

Создание интегрированной катастрофоустойчивой информационной платформы

Предлагается формирование организационной совокупности территориально распределенных информационных ресурсов и информационных систем субъектов энергетики с определенным объемом регулируемого обмена данными путем создания

интегрированной катастрофоустойчивой информационной платформы, в том числе для защищенного хранения информации, адаптированного к любым возможным угрозам ее искажения, повреждения и хищения [1].

Результатом создания интегрированной катастрофоустойчивой информационной платформы станут процедуры защиты осуществления субъектами энергетики оборота и хранения внутренней информации с учетом объемов и структуры генерации данных [2]. Для снижения опасности информационных и аналогичных атак на российские энергетические системы (объекты) важно предусмотреть меры быстрого восстановление связи и вычислительных сервисов управления технологическими и бизнес-процессами для пользователей системы по резервным или вновь установленным каналам связи в условиях выведения из строя традиционно используемых каналов связи [3].

Формирование сети катастрофоустойчивых межкорпоративных дата-центров

Целесообразно в отношении осуществления субъектами энергетики оборота и хранения внутренней информации (с масштабным и стабильным массивом цифровых данных) внедрение сервисов информационно-телекоммуникационной среды нового поколения в рамках сети катастрофоустойчивых межкорпоративных дата-центров. Развитие упомянутых дата-центров может явиться организационно-технической основой внедрения межведомственной конвергентной информационно-вычислительной платформы, в том числе для обеспечения сохранности информации (баз данных и программных пакетов) в условиях, когда информационные системы субъектов энергетики и других компаний ТЭК будут полностью или частично временно выведены из строя.

Формирование сети катастрофоустойчивых межкорпоративных дата-центров создаст предпосылки перехода к формированию в России (в перспективе в рамках Евразийского экономического союза) механизма защищенного хранения информации, адаптированного к любым возможным угрозам ее искажения, повреждения и хищения, которые осуществляются ключевыми ведомствами и энергетическими компаниями с использованием

новых цифровых сервисов работы с информацией, включая технологию Big Data и пр., формирования «цифровых двойников» любых процессов и объектов, в рамках интегрированной катастрофоустойчивой информационной платформы.

Расширение спектра координируемых характеристик различных информационных систем государственных ведомств и энергокомпаний

В настоящее время не существует единой нормативной основы для формирования системно-структурированного подхода к повышению защищенности (информационной безопасности) российской энергетики [4]. Необходимо расширение спектра координируемых характеристик различных информационных систем государственных ведомств и энергокомпаний, и их агрегированных групп на основе стандартизированных ведомственных и межведомственных подходов [5; 6].

В связи с этим остро необходимы новые технологические и бизнес-модели, которые формируют условия и механизмы формирования сетецентрической системы повышенной устойчивости управления энергетикой, опирающейся на распределенную сеть стандартизированных межкорпоративных дата-центров.

Взаимодействие и объединение корпоративных сетевых сред различных собственников, арендаторов и т.п.

Авторами сформулирована бизнес-модель совместного использования государственными ведомствами и коммерческими структурами интегрированной катастрофоустойчивой информационной платформы на основе взаимодействия и объединения корпоративных сетевых сред различных собственников, арендаторов и т.п. в рамках катастрофоустойчивых межкорпоративных дата-центров.

Преимуществом реализации предлагаемой авторами бизнес-модели взаимодействия и объединения корпоративных сетевых сред различных собственников, арендаторов и т.п. для управления сложными совокупностями информационных систем в рамках цифровой энергетики являются качественно более широкие возможности использования реплицированной информации

субъектов энергетики, других компаний ТЭК, органов госуправления различного уровня. Таким образом, результатом реализации бизнес-модели совместного использования государственными ведомствами и коммерческими структурами интегрированной катастрофоустойчивой информационной платформы станет повышение живучести энергосистемы России.

Перспективной технологией для объединения корпоративных сетевых сред представляется полное замещение компьютерных программ иностранного производства для обеспечения информационной безопасности субъектов энергетики, других компаний ТЭК России, органов госуправления на федеральном, региональном и муниципальном уровнях на базе защищенных резервных каналов связи, мощностей для хранения информации, вычислительных мощностей.

Прогнозирование устойчивости или неустойчивости структурированных ансамблей энергетических объектов с интеллектуальными элементами управления

В рассматриваемой системе прогнозирование динамики работы энергосистем, в т.ч. устойчивости или неустойчивости структурированных ансамблей энергетических объектов с интеллектуальными элементами управления, которые могут способствовать выпадению сегментов из цепочек цифровых транзакций в особенности, когда изменение или возмущение превышает базовый порог с учетом количества транзакций, может быть реализовано на базе выявления системно-параметрических взаимосвязей различных фактов, возникающих в рамках замкнутого цикла генерации данных и распределения данных при анализе причин прерывания цепочек цифровых транзакций.

Предлагается формирование расширенного пула ключевых пакетов общеупотребительных и специализированных программ для сетевого предоставления, с определенным объемом генерации данных в рамках интегрированной катастрофоустойчивой информационной платформы, как комбинаторно-регулируемого пространства.

Заключение

Внедрение универсальных оболочек любых бизнес-процессов, начиная с обработки первичных данных до обработки в глубинной области, должно соответствовать Tier 3 стандарта TIA-942 (Telecommunications Industry Association – Telecommunications Infrastructure Standard for Data Centers) с постепенным переходом к Tier 4, которые реализуются в рамках электронного микро-, мезо- и макроконтента, что позволит обеспечить устойчивость цифровой энергетики России в границах оптимальных значений функционирования информационных систем государственных ведомств и энергокомпаний за счет расширения возможностей наблюдения и управления.

Литература:

1. *Агеев А.И., Грабчак Е.П., Логинов Е.Л.* Smart-коллапс в цифровой энергетике будущего: угрозы глобального обрушения информационных систем управления в условиях возможной самоорганизованной информационной блокады//Энергетик. – 2020. – № 6. – С. 10-14.

2. *Агеев А.И.* Подходы к восстановлению элементов государственного управления в энергетике для действий в условиях чрезвычайных ситуаций сложнопрогнозируемого характера //Проблемы безопасности и чрезвычайных ситуаций. – 2020. – № 4. – С. 53-59.

3. *Аюев Б.И., Бинько Г.Ф., Грабчак Е.П., Купчиков Т.В., Логинов Е.Л., Миляев Р.Г., Павлушко С.А., Сацук Е.И., Черезов А.В., Шаров Ю.В.* Проблемы замещения импортного оборудования в электроэнергетике России//Известия НТЦ Единой энергетической системы. – 2020. – №1(82). – С. 109-123.

4. *Грабчак Е.П., Логинов Е.Л.* Определение возможности энергетического объекта выполнять требуемые функции в заданных режимах в условиях нелинейности и дискретности потоков поступающих технологических данных / «Интеллектуальные информационные системы: теория и практика». Сборник научных статей по материалам I Всероссийской конференции. – Курск: Курский государственный университет, 2020. – С. 32-38.

5. *Грабчак Е.П., Логинов Е.Л.* Цифровая энергетика: повышение надежности управления электро- и

теплоэнергетическими системами на основе внедрения цифровых технологий. – М.: МНИИПУ, ИНЭС, 2020. – 222 с.

6. *Грабчак Е.П.* Цифровая трансформация электроэнергетики. – М.: Кнорус, 2018. – 340 с.

7. *Voropai N.I., Stennikov V.A., Barakhtenko E.A.* Integrated Energy Systems: Challenges, Trends, Philosophy//Studies on Russian Economic Development. – 2017. – Vol. 28. 5: 492-499.

Команич Н.В.

Разработка вычислительного устройства, выполненного на основе операционного и управляющего автоматов

Аннотация: Исследована работа операционного и управляющего автоматов вычислительных устройств, которые были реализованы на основе логических схем и ПЗУ. Вычислительное устройство работает под воздействием управляющих сигналов, подаваемых пользователем. Реализована схема реализации необходимой функциональности.

Ключевые слова: операционный автомат, управляющий автомат, деление, дополнительный код, экспоненциальная форма

Операционный автомат представляет собой набор функциональных блоков (таких, как арифметико-логические устройства или операции), которые выполняют обработку данных. Вместе с блоком управления он составляет центральный процессор (ЦП). Операционные устройства (например, микропроцессоры) состоят из операционного автомата и управляющего автомата, при этом большую часть такого устройства занимает управляющий автомат, регулирующий передачу данных между операционным автоматом и памятью. Управляющий автомат в свою очередь, генерирует последовательность управляющих сигналов, предписанную программой и соответствующую значениям логических условий. Тесть он определяет работу операционного автомата [1].

Разработан универсальный делитель, который будет учитывать готовность данных на входе, готовность результата вычисления и