токи, их поля по своей интенсивности являются близкими к полю источника, а по направлению противоположными ему и в этой связи осуществляется взаимная компенсация полей.

В ходе проектирования и расчетов по электромагнитным экранам для достижения достаточной точности в существующих условиях возможно использование различных идеализированных случаев. Некоторые из них включают:

- Размещение бесконечно плоского экрана на пути плоской волны. В этом случае предполагается, что экран является идеальным проводником и имеет бесконечные размеры в плоскости. Это позволяет достичь приемлемой точности расчетов для плоской волны, которая распространяется параллельно экрану.

- Размещение точечного источника в центре герметичного идеального проводящего экрана с сферической формой. В этом случае экран окружает источник, и предполагается, что экран полностью блокирует электромагнитные поля, создаваемые источником. Это позволяет достичь приемлемой точности расчетов для точечного источника.

- Рассмотрение бесконечно длинного идеально проводящего цилиндра с излучателем в виде бесконечной нити, расположенной на оси цилиндра. В этом случае предполагается, что цилиндр является идеальным проводником и имеет бесконечную длину. Это позволяет достичь приемлемой точности расчетов для излучателя в форме нити, расположенной на оси цилиндра.

В ходе проектирования, когда делают выбор материалов, из которых формируют экраны, тогда ориентируются на определенные условия;

- получение требуемой величины ослабления электромагнитных полей для рассматриваемого рабочего диапазона частот,

- устойчивость материалов экранов по отношению к внешней среде, которая в ряде случаев может быть весьма агрессивной,

- требования к технологичности конструкции экранов при заданной конфигурации.

Активным образом используют листовые материалы (алюминий, медь латунь и др.).

При этом для одинаковых толщин экранов эффективность экранирования для магнитных и немагнитных материалов будет разной. Для электромагнитного режима в полосе частот, в которой эффективность экранирования вследствие отражения будет большей, чем эффективность поглощения, для немагнитных материалов, которые обладаю большей проводимостью, если сравнивать с магнитными, ведут к более высокой эффективности.

Экраны могут быть не только сплошными, а представлять металлические сетки. По массе они будут более легкими, чем листы, их проще изготавливать, удобно собирать и эксплуатировать. Но при этом существуют проблемы с механической прочностью.

Таким образом, использование в комплексе технических материалов, источников электромагнитного излучения позволяет достичь допустимых уровней электромагнитного, а также требования к их измерению в жилых помещениях, что является весьма полезным при разработке соответствующих с санитарных норм.

Список литературы

1. Федорков Е.Д. Об особенностях прогнозирования в ходе проектирования электронных компонентов // Современные материалы, техника и технология: сборник научных статей 10-й Международной научно-практической конференции, Курск, 30 декабря 2020 года. Курск: Юго-Западный государственный университет, 2020. С. 408-412.

2. Губенко В.А., Хатамов А.П. Особенности исследования и моделирования электромагнитных полей внутри жилых помещений // Science and innovation. 2023. № 3. С. 429-433.

3. Алламуратова З.Ж. Сравнительный анализ существующих моделей распределения уровней электромагнитного поля в условиях города // Science and innovation. 2023. № 3. С. 678-680.

4. Гуреев А.В. Энергетические характеристики распространения электромагнитных волн внутри зданий // Известия вузов. Электроника. 2015. № 4. С. 421-430.

5. Зацепин Э.С., Скляр А.Г., Русанов Д.В. Исследование закономерностей распространения электромагнитных волн во внутренних областях помещений // Моделирование, оптимизация и информационные технологии. 2015. № 3(3). URL: https://moit.vivt.ru/ (дата обращения: 15.09.2023).

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ АВТОМАТИЗАЦИИ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Золотарев А.А., Панин Д.В.

Воронежский институт высоких технологий, Воронеж, e-mail: denmilutin@yandex.ru

Люди на протяжении веков и в существующих условиях непрерывно стремились к тому, чтобы автоматизировать разные сферы своей деятельности, ускорить выполнение разных процессов. Это может выражаться в применении соответствующих орудий и средств труда, которые обеспечивают то, что будет частичная механизация или полная автоматизация выполнения работ [1].

В ближайшие годы цифровые решения смогут полностью перевернуть наш привычный мир.

Одним из важных направлений развития автоматизации является цифровизация. Цифровые технологии позволяют упростить процессы, сделать их более эффективными и экономичными.

Компании и страны, которые вовремя осознали неизбежность грядущих изменений и смогут воспользоваться их возможностями, станут ценными поставщиками инновационных решений и получат несравнимое преимущество перед другими игроками, в том числе на международном уровне.

Причем это касается не только таких традиционно чувствительных к цифровым изменениям секторов как медиа и телекоммуникации, ритейл и финансы, но и, в том числе, энергетики [2].

Необходимость в проведении автоматизации энергетической сферы диктуется тем, что есть социально-экономические факторы: повышается производительность в общественном труде, облегчаются и улучшаются условия труда трудящихся, есть нехватка рабочей силы, которая связанна с неблагоприятной демографической ситуацией внутри народного хозяйства и замедляется темп прироста по трудоспособному населению, и т.д.

Сформировавшийся к концу XX столетия пятый технологический уклад, основной технической компонентой которого является микроэлектроника, вычислительная техника, перешел и к началу XXI столетия. Сейчас виден новый технологический уклад.

В нем наблюдаются системы искусственного интеллекта. Они существенным образом могут изменить сферу энергетики.

Для наблюдаемых условий, когда есть автоматизация производств, изменяется содержание и растет сложность труда сотрудников, которые заняты обслуживанием автоматического оборудования в энергетике.

Есть рост роли и значения функций работников, которые обусловлены большими затратами умственной энергии по расчету, контролю, процессам управления, техническому обслуживанию энергетических комплексов, наблюдению за особенностями их работы [3].

В ходе внедрения автоматизации необходимы четкость и бесперебойность функционирования по всем звеньям энергетических комплексов.

Если будут внедрены отдельные автоматические агрегаты, то это не всегда обусловит соответствующий экономический эффект.

Непрерывность в поддержке процессов можно рассматривать как важнейшую предпосылку автоматизации. Она может быть обеспечена за счет того, что применяются малооперационные технологии, сокращаются продолжительности в операциях.

Активным способом применяются информационные технологии для того, чтобы поддерживать автоматизацию IT в энергетической отрасли.

Укажем соответствующие преимущества, связанные с автоматизацией IT в энергетике [4,5]:

– Улучшение показателей, связанных с информационной безопасностью. Среди большинства IT-продуктов, которые используются внутри энергетических компаний, можно отметить весьма большие требования относительно сферы защиты. По такой причине их требуется грамотным способом оптимизировать и распределять.

– Использование резервных центров обработки данных (ЦОД). Происходит накопление больших объемов данных, внутри энергетических компаний. Важно их сохранять в соответствующих местах и обрабатывать. В этой связи важно формировать новые ресурсы и их постоянным образом их модернизировать.

– Применение аутсорсинга. Можно построить IT-структуру в компании таким способом, чтобы потенциалы любых IT-объектов были максимальным образом реализованы. Причем это будет сделано очень быстро.

– Использование перспективных моделей, связанных с техническим обслуживанием и ремонтом оборудования. Кроме оценок состояния в оборудовании, есть возможности для использования функционала по оценкам последствий того, если выйдет из строя какое-то оборудование.

– Проведение оптимизации по бизнес-процессам. Внедрение в рабочие процессы конкретных систем – BPM, СЭД, BI и т.д., которые позволят проводить развитие, модернизацию и замену старых стандартов новыми.

Современные компании сталкиваются с вызовами, связанными с интеграцией различных аппаратных компонентов и программного обеспечения. Это может создавать риски несовместимости технологий:

1. Несовместимость технологий. Разнообразие аппаратных и программных решений может привести к сложностям в их взаимодействии, что увеличивает вероятность возникновения неинтегрируемых технологий.

2. Распределенная генерация и энергоактивные потребители. Развитие распределенной генерации и увеличение энергоактивных потребителей усложняют традиционные профили нагрузок, требуя новых методов прогнозирования энергопотребления.

3. Изменение структуры нагрузок. Промышленные предприятия и домохозяйства изменяют свои потребительские привычки, внося неопределенность в модели прогнозирования нагрузок.

4. Рост удельных издержек. Уменьшение потребления энергии из централизованных источников приводит к увеличению удельных постоянных издержек на производство киловатт-часа электроэнергии, затрагивая всю цепочку централизованной генерации и сетей.

Развитие энергетических систем прямо влияет на конкурентоспособность предприятий. Современные технологии позволяют сократить потребление энергии, улучшить производственные процессы и снизить экологическое воздействие. Автоматизация и использование информационных технологий позволяют предприятиям более точно контролировать и управлять своими энергетическими системами, что ведет к повышению эффективности и снижению затрат.

Инвестирование в современные технологии также способствует улучшению рабочих усло-

вий и безопасности на предприятии, что может привлечь квалифицированных специалистов и повысить уровень производительности. Энергетическая эффективность помогает предприятиям сократить свои операционные расходы и улучшить свою финансовую устойчивость.

Список литературы

1. Соломин С.А., Преображенский Ю.П. Проблемы обеспечения функционирования энергетических систем // Проблемы развития современного общества: сборник научных статей 7-й Всероссийской национальной научно-практической конференции. В 5-ти томах. Том 4. 2022. С. 345-348.

2. Львович И.Я. О возможностях автоматизации при повышении эффективности энергетических систем // Современные материалы, техника и технология. 2020. С. 220-223.

3. Львович И.Я. Проблемы автоматизации управления энергетическими системами // Современные материалы, техника и технология. 2020. С. 216-219.

4. Сафаров И.М., Давлетхузина Э.М., Ишмухаметова Д.М., Баширова Л.И., Садыков Р.Д., Хлебников Д.А. Состояние уровня автоматизации энергетических объектов и решения, направленные на его повышение // Инженерный вестник Дона. 2021. №1 (85). URL: ivdon.ru/ru/magazine/archive/n1y2021/7382 (дата обращения: 07.09.2023).

5. Клаусснер В.А., Демкин В.И. Анализ применения автоматизированной системы коммерческого учета электроэнергии в промышленности // Молодой ученый. 2021. № 5 (347). С. 33-35.

СТОИМОСТНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кислова Д.А., Аветисян Т.В.

Колледж Воронежского института высоких технологий, Воронеж, e-mail: vtatyana_avetisyan@mail.ru

Информационная безопасность включает в себя различные меры по защите информации от несанкционированного доступа. В прошлом, в эпоху до цифровых технологий, люди использовали сейфы для хранения важных документов, нанимали охранников и шифровали свои сообщения на бумаге. В настоящее время защита информации чаще всего относится к цифровой сфере, но основные принципы остаются прежними: специалисты по информационной безопасности создают защищенные виртуальные пространства, устанавливают защитное программное обеспечение, например, антивирусы и используют криптографические методы для шифрования цифровой информации [1].

Информационная безопасность включает в себя защиту трех основных аспектов информации: ее конфиденциальности, целостности и доступности. В рамках концепции информационной безопасности эти аспекты называются принципами информационной безопасности.

Конфиденциальность гарантирует, что информация доступна только тем, кому она предназначена, и не попадает в руки посторонних лиц. Целостность обеспечивает сохранность и неприкосновенность информации, чтобы она не была изменена или повреждена без разрешения. Доступность означает, что информация доступна и используется в нужное время и месте Эти принципы информационной безопасности являются основой для разработки соответствующих мер и политик, направленных на защиту информации от угроз и несанкционированного доступа.

Надежная система защиты должна соответствовать следующим принципам [2,3]:

1) Затраты на внедрение и поддержку системы защиты не должны превышать потенциальные потери от возможных нарушений безопасности;

2) Каждый пользователь обязан иметь доступ только к тем функциям и данным, которые необходимы для выполнения его задач, чтобы минимизировать риски несанкционированного доступа и злоупотребления;

3) Системе защиты необходимо быть удобной и интуитивно понятной для пользователей, чтобы они могли эффективно выполнять свои задачи без излишних препятствий;

4) Система защиты должна иметь механизмы для быстрого отключения или обхода в случае чрезвычайных ситуаций, например, при возникновении угрозы жизни или критических сбоев.

5) Система защиты обязана обеспечивать безопасность всех компонентов и данных, используемых в процессе обработки информации, включая серверы, сети, базы данных и приложения;

6) Разработчики системы защиты не должны иметь привилегированный доступ или контроль над системой, чтобы предотвратить возможность злоупотребления и конфликта интересов.

Стоимостная составляющая надежной системы защиты имеет несколько аспектов [4,5]:

Первый аспект стоимостной составляющей информационной безопасности – это затраты на оборудование и программное обеспечение. Установка и поддержка физической и логической инфраструктуры, таких как серверы, межсетевые экраны, антивирусные программы и системы защиты данных, требует значительных расходов. Компании, особенно крупные организации, должны иметь надежные аппаратные и программные средства для обеспечения безопасности своих информационных ресурсов.

Второй аспект связан с затратами на персонал. Специалисты по информационной безопасности являются ключевыми фигурами в обеспечении безопасности систем и сетей. Это профессионалы, которые не только создают и настраивают системы защиты, но и мониторят их работу, анализируют уязвимости и реагируют на возможные инциденты безопасности. Работа таких высококвалифицированных специалистов требует значительных финансовых ресурсов для их найма и обучения, а также для удержания в компании.