



ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИИ

02 [191] 2023

В. Тютюнник, А. Баканов

Подходы к анализу информационных
процессов в организации **58**

**В. Конторович, А. Кураев, Д. Бобровский,
А. Шелягин, Е. Плешакова, С. Гатауллин**

Противостояние угрозам
телефонного мошенничества средствами
искусственного интеллекта **72**

А. Рыхторова

Открытый доступ: правовые основы
организации доступа к научно-технической
информации в библиотеках **82**



t.me/irr_rea



[/rosenergo.gov.ru](https://rosenergo.gov.ru)



irr@rosenergo.gov.ru

10 ОКТЯБРЯ 2023

ОРГАНИЗАТОР
РЭА
МИНЭНЕРГО РОССИИ



НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ



ТЕРРИТОРИЯ ЭНЕРГЕТИЧЕСКОГО ДИАЛОГА

МЕРОПРИЯТИЕ ПРОВОДИТСЯ
В РАМКАХ МЕЖДУНАРОДНОГО
ФОРУМА «РОССИЙСКАЯ
ЭНЕРГЕТИЧЕСКАЯ НЕДЕЛЯ»



Российская
Энергетическая
Неделя 2023

 РОСКОНГРЕСС
Пространство доверия

tedconf.ru



Содержание

От редакции

- 3 А. Горшкова**
Цифровизация во благо

ТЭК

- 4 С. Козьминых, В. Татаренков**
Обеспечение защиты информации
в промышленной сети
автоматизированной системы
управления технологическим
процессом гидроэлектростанции

- 16 Е. Гниломёдов,
Е. Сухарникова, А. Бачурин**
Создание экосистемы
информационного обмена
результатами научно-технической
деятельности нефтегазовых
компаний России

Транспорт

- 23 К. Климов**
Метод выделения ложных сигналов
АИС на сервисе MarineTraffic



16



50

 **ИНФОРМАЦИОННЫЕ
РЕСУРСЫ РОССИИ**

Строительство

- 31 П. Давыдкин, Л. Адамцевич**
Повышение энергоэффективности
зданий в условиях редевелопмента
городской среды

- 40 Я. Жаров, М. Шабалин, Н. Потехин**
Модернизация информационных систем
каталогизации строительных ресурсов

Цифра

- 50 З. Лященко, О. Игнатьева,
А. Лященко, Д. Глазунов**
Автоматизация рабочего места
машиниста подвижного состава

- 58 В. Тютюнник, А. Баканов**
Подходы к анализу информационных
процессов в организации

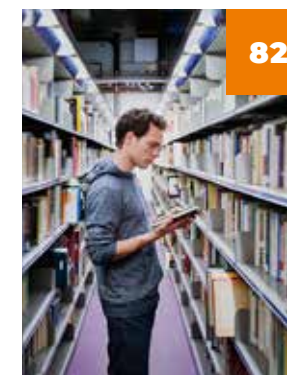
- 72 В. Конторович, А. Кураев, Д. Бобровский,
А. Шелягин, Е. Плешакова, С. Гатауллин**
Противостояние угрозам телефонного
мошенничества средствами
искусственного интеллекта

Библиотеки

- 82 А. Рыхторова**
Открытый доступ: правовые основы
организации доступа к научно-
технической информации в библиотеках



58



82



Founder's word

- 3 A. Gorshkova**
Digitalization for good

FEC

- 4 S. Kozminykh, V. Tatarenkov**
Ensuring the protection of information in the industrial network of the automated process control system of a hydroelectric power plant

- 16 E. Gnilomedov, E. Sukharnikova, A. Bachurin**
Creation of information exchange ecosystem of scientific and technical results activities of oil and gas companies of Russia

Transport

- 23 K. Klimov**
Method for detecting false AIS signals on the Marinetraffic Service



Contents

Building

- 31 P. Davydkin, L. Adamtsevich**
The increasing the energy efficiency of buildings in the context of urban redevelopment

- 40 Ya. Zharov, M. Shabalin, N. Potekhin**
Modernization of information systems for cataloging construction resources

Digitalization

- 50 Z. Lyashchenko, O. Ignatieva, A. Lyashenko, D. Glazunov**
Automation of Rolling Stock Driver's Workplace

- 58 V. Tyutyunnik, A. Bakanov**
Methods for analyzing information processes in an organization

- 72 V. Kontorovich, A. Kuraev, D. Bobrovsky, A. Shelyagin, E. Pleshakova, S. Gataullin**
Phone Fraud Detection and Prevention Based on Voice Recognition with Machine Learning

Library

- 82 A. Rykhtorova**
Open Access: legal basis of organizing access to scientific and technical information for Scientific Libraries



Цифровизация во благо

Никто не будет спорить, что цифровизация и информатизация рабочих процессов, как в офисе, так и на производстве, могут помочь в оптимизации бизнеса. Такие технологии должны обеспечивать слаженность рабочего процесса, синергию и взаимодействие с другими направлениями работ на производстве, более надежное и взвешенное принятие управленческих решений, сокращение рисков ошибок и внештатных ситуаций, снижение количества неквалифицированных сотрудников и срока бюрократических процедур. Но это – ситуация, близкая к идеальной. На деле же переход на цифровые технологии в офисе или на производстве сталкивается с серьезными проблемами, которые вместо оптимизации лишь усложняют бизнес-процессы. Так, процедуры ввода и обработки данных, согласований и утверждения решений могут оказаться более сложными и продолжительными по времени, чем при ручном вводе и бумажном документообороте. Это вызвано такими проблемами, как несовершенство и сложность самих программ, отсутствие высококвалифицированных кадров для проработки разных вариантов функционирования систем и адаптации программ для конкретных работ, инертность и запутанность бизнес-процессов в самих организациях, которые с трудом могут быть оцифрованы, отсутствие прозрачной системы принятия решений, низкая подготовка кадров и недостаточный уровень средств и времени, выделяемых на внедрение цифровых и информационных технологий. Поэтому сейчас, в условиях импортозамещения и ускоренного внедрения отечественных программных продуктов, необходимо более тщательно подходить к анализу работы информационных систем, оперативному устранению выявляющихся ошибок, адаптации к разным видам деятельности и проведению периода подготовки к переходу на цифровизацию.

Главный редактор журнала «ИРР»,
Горшкова Анна



ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОМЫШЛЕННОЙ СЕТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ ГИДРОЭЛЕКТРОСТАНЦИИ

Козьминых Сергей
Профессор Департамента информационной безопасности Финансового университета при Правительстве РФ, профессор кафедры прикладной информатики и информационной безопасности РЭУ им. Г. В. Плеханова, д. т. н., доцент.
E-mail: SlKozminykh@fa.ru, Kozminyh.SI@rea.ru

Татаренков Владислав
Аспирант Департамента информационной безопасности Финансового университета при Правительстве РФ.
E-mail: vt96@mail.ru

Аннотация. В статье анализируется построение защищенной промышленной сети гидроэлектростанции, в которой развернута и функционирует автоматизированная система управления технологическим процессом. Приведены основные документы, регламентирующие обеспечение защиты информации в автоматизированных системах управления технологическим процессом на объектах критической информационной инфраструктуры. Проклассифицированы атаки на автоматизированные системы управления технологическим процессом промышленных объектов, которые демонстрируют актуальность проблемы обеспечения их информационной безопасности (ИБ). Приведены рекомендации выбора средств защиты информации, необходимые для обеспечения должного уровня информационной безопасности. В заключении приводятся предложения по защите промышленной сети автоматизированной системы управления технологическим процессом гидроэлектростанции, удовлетворяющий требованиям ФСТЭК. В качестве вывода сказано, что предлагаемая информационная система с установленными средствами защиты информации (СЗИ) имеет высокий уровень защиты, так как все действия пользователей в СЗИ постоянно контролируются. Отмечено, что необходимо уделять внимание не только высокой технической защищенности системы, но и также другим направлениям обеспечения ИБ на объекте. В частности, необходимы организационные меры обеспечения ИБ, в том числе регулярное обучение персонала для повышения его квалификации и знаний в области ИБ.

Ключевые слова:

автоматизированная система управления технологическим процессом, защищенная промышленная сеть гидроэлектростанции, компьютерные атаки, система обнаружения вторжений, программно-технические средства защиты информации, комплексное обеспечение безопасности.

Защищенность АСУ ТП ГЭС должна соответствовать самому высокому, первому классу, так как степень ущерба от нарушения штатного режима работы ГЭС является очень высокой из-за риска возникновения чрезвычайной ситуации федерального или межрегионального характера

Введение

В настоящее время широко внедряется автоматизация технологических процессов и централизованное управление всем производством, как существующих, так и проектируемых промышленных предприятий. Решением данных задач является внедрение автоматизированной системы управления технологическим процессом (АСУ ТП), которая состоит из вычислительного, сетевого, силового и другого технического оборудования. Применение АСУ ТП на объектах критически важной инфраструктуры, к которым относятся объекты топливно-энергетического комплекса (ТЭК), использование в ее составе различного оборудования от разных производителей, приводит к росту количества инцидентов проникновения в защищенную информационную инфраструктуру. Это позволяет сделать вывод о том, что проблема обеспечения информационной безопасности АСУ ТП на объектах ТЭК является очень важной и актуальной [1]. Кроме того, необходимость создания системы обеспечения безопасности для АСУ ТП на промышленных объектах отражена в требованиях ФЗ № 256 «О безопасности объектов топливно-энергетического комплекса» и ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [2]. Для построения защищенной

промышленной сети АСУ ТП объекта критически важной инфраструктуры обязательно соблюдение требований, указанных в приказе ФСТЭК № 31, приказе ФСТЭК № 235 и приказе ФСТЭК № 239 [3].

В соответствии с ФЗ № 256, приказом Министерства энергетики РФ от 10 февраля 2012 г. № 48 утверждены методические рекомендации по включению объектов топливно-энергетического комплекса в перечень объектов, подлежащих категорированию. В соответствии с этой методикой, в перечень объектов топливно-энергетического комплекса, подлежащих категорированию, в первую очередь включены гидроэлектростанции.

Архитектура АСУ ТП ГЭС

Информационная система (ИС), которой является рассматриваемая АСУ ТП ГЭС, предоставляет необходимый функционал по централизованному управлению электростанцией, а также отслеживанию состояния и показаний ее агрегатов. В информационной системе хранится, обрабатывается и генерируется информация категории «для служебного пользования»: инструкции, отчетные документы, чертежи и т. д. В системе определены следующие виды работников, обеспечивающих ее штатное функционирование: операторы АСУ ТП, сервис-инженеры АСУ ТП, администратор безопасности и администратор