IV Международная научно-практическая конференция

ЦИФРОВИЗАЦИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

В 3-х томах

Том I

Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2024

Министерство науки и высшего образования Российской Федерации
Министерство сельского хозяйства Российской Федерации
Правительство Тамбовской области
Министерство сельского хозяйства Тамбовской области
ФИЦ «Информатика и управление» РАН
ФГБУН «Институт проблем управления им. В. А. Трапезникова» РАН
Евразийская технологическая платформа
«Технологии пищевой и перерабатывающей промышленности АПК – продукты здорового питания»
ООО «Ви Гроу»
Ассоциация инженерного образования России
Тамбовское региональное отделение ООО «СоюзМаш России»
Ассоциация «Объединенный университет им. В. И. Вернадского»
Белорусский государственный аграрный технический университет
Мичуринский государственный аграрный университет
Тамбовский государственный технический университет

IV Международная научно-практическая конференция

«ЦИФРОВИЗАЦИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА»

Сборник научных статей
Тамбов, 23 – 25 октября 2024 г.

В 3-х томах

Том I

Научное электронное издание

IV International Scientific and Practical Conference

“DIGITALIZATION OF AGROINDUSTRIAL COMPLEX”

Proceedings
Tambov, October 23 – 25, 2024

Scientific Electronic Publication

Тамбов
♦ Издательский центр ФГБОУ ВО «ТГТУ» ♦
2024

УДК 631.5
ББК з81+П07
Ц75

Ц75 **Цифровизация** агропромышленного комплекса [Электронный ресурс] : сборник научных статей IV Междунар. науч.-практ. конф. В 3-х т. Тамбов, 23 – 25 октября 2024 г. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2024.

Т. I. – 1 электрон. опт. диск (CD-ROM). – Системные требования : ПК не ниже класса Pentium II ; CD-ROM-дисковод ; 7,0 Mb ; RAM ; Windows 95/98/XP ; мышь. – Загл. с экрана. – ISBN 978-5-8265-2817-4.

Включены материалы секционных докладов, вошедших в программу IV Международной научно-практической конференции «Цифровизация агропромышленного комплекса».

Ц75 **Digitalization** of the agro-industrial complex [Electronic resource] : proceedings of the III International Scientific and Practical Conference. In 3 vol. Tambov, October 23 – 25, 2024. – Tambov : Publishing center TSTU, 2024.

Vol. I. – 1 electron. optical disk (CD-ROM). – System requirements : PC not lower than class Pentium II ; CD-ROM-drive ; 7,0 Mb ; RAM ; Windows 95/98/XP ; mouse. – The title from the screen. – ISBN 978-5-8265-2817-4.

The collection includes materials from section reports that were included in the program of the IV International Scientific and Practical Conference “Digitalization of the Agro-Industrial Complex”.

УДК 631.5
ББК з81+П07

Материалы статей предоставлены в электронном виде и сохраняют авторскую редакцию.

ISBN 978-5-8265-1944-8 (общ.)
ISBN 978-5-8265-2817-4 (т. I)

СОДЕРЖАНИЕ

Секция 1. Цифровые средства и системы управления в агропромышленном комплексе 9

И. И. Аксенов
Контроль высоты опорной пневмоподушки решетного стана 9

А. С. Вишневецкая, В. А. Макушенко, Д. А. Потапова
Цифровизация логистических процессов в сфере перевозки сельскохозяйственных животных 12

Е. Г. Кабулова
Биологическая нейронная сеть для обработки низкоконтрастных изображений БПЛА 15

Е. В. Кошелев
Устойчивость информационных систем управления агропромышленным комплексом к внешним угрозам 18

А. Д. Лавриенко, В. В. Шатских
Использование современных методов шифрования для защиты канала управления беспилотным летательным аппаратом в сельском хозяйстве .. 22

А. Н. Потапов, А. Л. Началов
Подсистема поддержки принятия решений информационного обеспечения эрготехнических систем 26

М. М. Репин, К. В. Стародубов, А. С. Дерябин
Методика анализа рисков деструктивного воздействия на автоматизированные системы агропромышленного комплекса 30

С. А. Савушкин, Д. А. Потапова, С. В. Артемова, А. С. Катруш
Угрозы и риски цифровизации для сельского хозяйства 34

А. Д. Саенко, О. В. Соболева, Д. А. Потапова
Безопасность аналитики и хранения больших данных в агропромышленной отрасли 37

С. В. Артемова, Д. А. Потапова, Е. О. Карамышева, А. С. Спиридонов
Перспективы развития беспилотных систем в агропромышленном комплексе 41

А. М. Хромов, А. А. Гусев
Модернизация каналов управления БПЛА для увеличения дальности связи в сельском хозяйстве 44

М. В. Волчихина
Подход к обеспечению защиты речевой информации при управлении элементами агропромышленных комплексов 47

В. С. Блаженов, Шамсулдин Хайдар Абдулваххаб Х., Алмали Ахмед Аднан Латиф
Регулирование и стандарты безопасности в агропромышленном комплексе 54

С. В. Артемова, Д. А. Потапова, П. И. Карасев, В. Е. Бушуев
Основные киберугрозы для предприятий агропромышленного комплекса и способы их предотвращения 58

А. В. Виноградский, Мустафа Абдулкадим Дхаир Аль-Амиди, Аль-Судани Зайд Али Хуссейн
Проблемы безопасности Интернета вещей в сфере агропромышленного комплекса 62

Г. В. Гвасалия, П. И. Карасев, Г. Ш. Утешева, Алмали Ахмед Аднан Латиф
Информационная безопасность в Умных фермерских хозяйствах: стратегии защиты данных IoT-устройств 66

А. А. Двойных, Мустафа Абдулкадим Дхаир Аль-Амиди, Шамсулдин Хайдар Абдулваххаб Х.
Устойчивость агропредприятий к кибератакам: угрозы и приемы по их предотвращению 69

В. М. Дорошкевич, Г. Ш. Утешева, Аль-Судани Зайд Али Хуссейн
Анализ современных киберугроз, с которыми сталкиваются предприятия агропромышленного комплекса, и стратегии их минимизации 73

И. А. Елизаров, Д. Г. Дмитриев, М. И. Елизарова, Т. А. Черемисин
Использование протокола MQTT при создании автоматизированных систем технического обслуживания оборудования на предприятиях перерабатывающей промышленности 77

П. И. Карасев, Е. А. Ермаков, М. Р. Потемкин, Алмали Ахмед Аднан Латиф
Использование технологии межсетевого экранирования в задачах повышения безопасности предприятия агропромышленного комплекса ... 81

Е. С. Жирнов, Шамсулдин Хайдар Абдулваххаб Х., Мустафа Абдулкадим Дхаир Аль-Амиди
Применение блокчейн-технологий в агропромышленном комплексе 85

А. А. Канцуров, Алмали Ахмед Аднан Латиф, Аль-Судани Зайд Али Хуссейн
Безопасность дистанционного управления аграрными системами 89

Н. Б. Куженова, Б. С. Дмитриевский
Информационная инфраструктура управления производством этилового спирта 92

К. В. Купцов, Шамсулдин Хайдар Абдулваххаб Х., Мустафа Абдулкадим Дхаир Аль-Амиди
Анализ современных систем защиты информации агропромышленного комплекса 95

Н. Ю. Куриленко, С. В. Артемова, Г. Ш. Утешева
Цифровые инструменты для мониторинга устойчивости агросистем к изменениям климата 100

В. А. Лукин
Оценка и оптимизация пользовательского интерфейса мобильного приложения для управления посевными площадями на основе интеграла Шоке 103
В. А. Лукин
Адаптивный мобильный интерфейс для СППР при анализе посевных площадей 107
А. С. Мещеряков
Система автоматического управления дозиметром для оценки радиационной обстановки сельскохозяйственных земель 110
И. С. Михайлов, Д. А. Полещенко
Разработка программного обеспечения для автоматизированного анализа показателей развития сельскохозяйственных культур по изображению с БПЛА 113
В. Н. Палаткин, А. В. Ачкасов
Умные агротехнологические платформы на основе IoT и TinyML для устойчивого сельского хозяйства 116
В. Н. Палаткин, А. В. Ачкасов
Применение КИПиА в точном земледелии 121
В. Г. Матвейкин, П. К. Правин, Б. С. Дмитриевский, А. А. Терехова
Использование модели Грея Маркова для прогнозирования состояний оборудования 126
П. К. Правин
Математическая модель с использованием датчиков Интернета вещей для принятия решений по оптимизации сбора винограда 129
П. И. Карасев, Ф. М. Пыршев, М. А. Ивановский, И. А. Дьяков
Обучение сотрудников основам информационной безопасности для предотвращения внутренних угроз 133
П. И. Карасев, Ф. М. Пыршев, М. А. Ивановский, И. А. Глазкова
Применение сетевых анализаторов и тестов на проникновение при аудите информационной безопасности 126
П. И. Карасев, Ф. М. Пыршев, И. А. Глазкова, И. А. Дьяков
Сравнительный анализ программного обеспечения для защиты от нежелательной рассылки 129
П. И. Карасев, Ф. М. Пыршев, А. И. Елисеев
Цифровизация пермакультурных насаждений 142
С. А. Россман, Алмали Ахмед Аднан Латиф, Аль-Судани Зайд Али Хуссейн
Защита интеллектуальных систем принятия решений в агропромышленном комплексе 145
О. Н. Красуля, А. В. Токарев
Цифровые технологии в производстве мясных и молочных продуктов заданного качества 148

А. И. Шебалкина, Алмали Ахмед Аднан Латиф, Аль-Судани Зайд Али Хуссейн
Оптимизация автоматизированных систем управления агропромышленным комплексом с использованием suckless-подхода 153
А. Р. Эмин, Мустафа Абдулкадим Дхаир Аль-Амиди, Шамсулдин Хайдар Абдулваххаб Х.
Создание безопасной сети для агробизнеса: пример внедрения VPN-технологий в сельском хозяйстве 157
А. А. Терехова, Б. С. Дмитриевский
Совершенствование управления процессом производства сахара..... 161
А. В. Андрющенко, Е. А. Светлишина, С. В. Дронов
Современные технологии автоматизации процесса производства горячей воды в газовой котельной 164
А. Д. Анисимов, А. А. Брюханов, Н. С. Толстошеин, В. В. Шатских
Информационная технология построения учебно-тренировочных средств для подготовки специалистов по применению сельскохозяйственной техники 166
А. В. Бобровских, С. Г. Свиридов, Р. В. Мещеряков
Вариант построения эшелонированной защиты с помощью технологии контейнеризации средств сетевой безопасности информационной инфраструктуры агропромышленного комплекса 169
Д. В. Большунов, А. С. Марков
Разработка технического решения для моделирования безопасной сетевой инфраструктуры АСУ ТП в агропромышленном комплексе..... 172
Н. Г. Буранова
Об одном подходе к разработке алгоритмического обеспечения интеллектуальной системы управления пеллетной котельной..... 175
Р. Н. Бахтиев, Н. В. Гамалеев
Автоматизирование пожаротушения в агропромышленном комплексе как мера повышения безопасности при эксплуатации машин и оборудования 178
А. С. Гордеев, Б. С. Мишин, А. Н. Попов
Цифровой метод контроля зрелости яблок 181
С. В. Дронов, Е. А. Светлишина, А. В. Андрющенко
Современные технологии автоматизации процесса диазотирования при производстве пигмента алого 185
А. В. Душкин, Д. Р. Мусин, И. С. Порсев
Сравнение методов обработки слабоструктурированной информации в условиях сильных шумов с использованием цифровых средств для решения задач безопасности в агропромышленном комплексе 188
М. И. Елизарова
К вопросу выбора технологии передачи данных на объектах агропромышленного комплекса 192

М. И. Елизарова
Макет распределенной системы управления опылением в тепличном комплексе 196
Р. О. Китаев, А. Г. Морозов, Ю. В. Минин
Математическое обеспечение системы управления запасами запасных частей для сельскохозяйственной техники 201
И. Г. Благовещенский, М. М. Клягин, В. А. Холопов
Переход от серийного производства к многономенклатурному мелкосерийному производству в агропромышленном комплексе 204
С. В. Кочергин, С. В. Артемова, В. Ф. Калинин
Моделирование кибератак на систему электроснабжения АПК: анализ уязвимостей и оценка рисков 207
С. Л. Сахаров, А. С. Кравченко
Обнаружения признаков стеганографических вложений в аудиофайлах на основе анализа распределения младших бит 211
Д. С. Лавринов
Методики автоматизации технического обслуживания и ремонта (ТОиР) на производственных предприятиях агропромышленного сектора 215
Д. С. Луцков, А. Н. Грибков
Установка гидротермальной карбонизации биоотходов как объект автоматизации 218
А. С. Мещеряков, В. К. Зольников, А. В. Шпинев
Методы измерения поглощенной дозы ионизирующего излучения для контроля радиационной обстановки сельскохозяйственных земель 221
Д. Р. Мусин, А. В. Душкин
Применение сканеров уязвимостей в информационной инфраструктуре агропромышленного комплекса с целью повышения его защищенности ... 224
Д. Р. Мусин, В. А. Щербаков
Перспективы внедрения модели информационной безопасности Security as a Service в сфере агропромышленного комплекса 227
К. А. Перфильева, Ю. В. Савченко
Внедрение DCAP-системы для защиты информации на предприятии 231
Е. М. Портнов, С. Г. Свиридов, А. В. Бобровских
Методика проведения аудита угроз сетевой безопасности IT-инфраструктуры агропромышленного комплекса 234
В. С. Румянцев, Р. М. Башкиров
Концепция масштабируемой транковой сети с использованием БПЛА-ретрансляторов с технологией роевого интеллекта в сельском хозяйстве 237
К. В. Скоморохов, З. М. Селиванова
Цифровая измерительная система контроля климатических параметров объектов агропромышленного комплекса на базе микроконтроллера и технологии NB-iot 240

М. М. Смотряев, А. В. Облиенко
Принципы безопасности построения прикладного программного обеспечения для устройств с операционной системой Android, используемых в агропромышленном комплексе 244
П. М. Трефилов
Алгоритмическое обеспечение навигационного комплекса малого БПЛА для задач мониторинга сельскохозяйственных угодий 247
А. С. Кравченко, А. М. Тюнина
Цифровизация агропромышленного комплекса 250
К. Б. Фам, В. В. Кушнаренко, В. Н. Богатиков
Управление сельскохозяйственной сушилкой на основе интеллектуального контроллера 253
Р. Ю. Курносов, А. И. Иванин
Применение одноплатных компьютеров для систем стационарных локальных метеокомплексов 258
А. А. Третьяков, Ан. А. Третьяков, И. А. Елизаров, В. Н. Назаров
Разработка программно-технического обеспечения системы сбора данных и управления процессом точного высева многофункциональными посевными комплексами типа ЕМС 262
И. А. Фирсов, Ан. А. Третьяков, А. А. Третьяков
Математическое моделирование процесса пастеризации молока 266
У. Т. Андашев, Р. В. Косов
Формирование «правового фундамента» цифровизации агропромышленного комплекса с учетом реализации задач евразийской интеграции 270
Д. В. Лапин, Д. А. Полубояринов, Т. В. Кожарина, М. В. Соколов
Инновационные подходы к созданию модульной оснастки для погрузчиков: гибкость, эффективность и безопасность 275
А. А. Китаева
Трехмерные объекты и перспективные искажения 278
С. С. Горшкова
Современные методы анализа текстур в компьютерном зрении: подходы, применения и перспективы развития 281
С. А. Родиков, Д. О. Болдырев
Устройство измерения медленной индукции флуоресценции хлорофилла кожицы яблок 285
Е. И. Алгазин, К. А. Лайко, Ю. О. Филимонова, А. С. Разумихин
Об одном методе оценки времени диссипации энергии в цепи с реактивным элементом системы автоматики сельскохозяйственного оборудования 288
Н. В. Саяпин, А. Н. Пахомов
Опыт применения систем точного земледелия и решений для увеличения мощности двигателя в сельскохозяйственных предприятиях 294

Секция 1

ЦИФРОВЫЕ СРЕДСТВА И СИСТЕМЫ УПРАВЛЕНИЯ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

УДК 631.3.03

И. И. Аксенов
(Кафедра электротехники и автоматики,
ФГБОУ ВО «Воронежский государственный аграрный
университет имени императора Петра I», г. Воронеж, Россия,
e-mail: http://vsau.ru, et@agroeng.vsau.ru)

КОНТРОЛЬ ВЫСОТЫ ОПОРНОЙ ПНЕВМОПОДУШКИ РЕШЕТНОГО СТАНА

Аннотация. Установка на раме зерноочистительной машины под продольной осью корпуса по разные стороны от пневмоподушки датчиков, измеряющих расстояние до корпуса, позволяет контролировать изменение высоты пневмоподушки и автоматически изменять давление в ней для обеспечения требуемой высоты.

Ключевые слова: решетный стан, корпус, пневмоподушка, рама, датчик, требуемая высота.

I. I. Axenov
(Department of Electrical Engineering and Automation,
Voronezh State Agrarian University
named after Emperor Peter the Great, Voronezh, Russia)

HEIGHT CONTROL OF THE SUPPORT AIR CUSHION OF THE SIEVE MILL

Abstract. The installation of sensors measuring the distance to the housing on the frame of the grain cleaning machine under the longitudinal axis of the housing on different sides of the air bag allows you to control the height change of the air bag, and automatically change the pressure in it to ensure the required height.

Keywords: grating mill, housing, air gun, frame, sensor, required height.

Использование пневмоподушки в качестве опоры решетного стана зерноочистительной машины позволяет снизить ударные нагрузки и вибрацию машины [1, 3, 4]. Высота пневмоподушки определяется длиной толкателя, расстояниями по горизонтали и вертикали от узла крепления толкателя к корпусу до центра вращения эксцентрика, она

должна быть постоянной при разной нагрузке на пневмоподушку от корпуса. Изменение высоты пневмоподушки, обусловленное изменением нагрузки от корпуса, приводит к смещению корпуса в сторону толкателя при уменьшении нагрузки, или к смещению корпуса в сторону, противоположную от толкателя при увеличении нагрузки. В результате снижается эффективность работы решетного стана.

Для устранения указанного недостатка предложен решетный стан [2], включающий корпус, в котором установлены решета, эксцентрик, вращаемый приводом, толкатель, соединенный одним концом с корпусом, а другим – с эксцентриком, пружину, закрепленную одним концом к корпусу, а другим – к раме, пневмоподушку, установленную на раме. Корпус опирается на пневмоподушку. На раме под продольной осью корпуса по разные стороны от пневмоподушки на расстоянии от нее 1,1R установлены два датчика, измеряющие расстояние до корпуса, где R – радиус эксцентрика. Сигналы датчиков передаются автоматическому устройству управления давлением в пневмоподушке.

Наличие в решетном стане двух датчиков, установленных на раме под продольной осью корпуса по разные стороны от пневмоподушки на расстоянии от нее 1,1R и измеряющих расстояние до корпуса, позволяет контролировать изменение высоты пневмоподушки и автоматически изменять давление в пневмоподушке для обеспечения ее требуемой высоты. Таким образом, независимо от нагрузки, действующей на пневмоподушку от корпуса, за счет автоматического изменения давления в пневмоподушке будет поддерживаться требуемая высота пневмоподушки. Следовательно, повышается эффективность работы решетного стана.

Решетный стан работает следующим образом. Обрабатываемый материал (зерновой ворох) подается на решета, установленные в корпусе. Эксцентрик, вращаемый приводом, посредством толкателя приводит в возвратно-поступательное движение корпус, опирающийся на пневмоподушку, которая сжимается под действием нагрузки от корпуса и изгибается от усилия, создаваемого толкателем, причем максимальный прогиб пневмоподушки составляет не более, чем радиус эксцентрика R. Датчики, установленные на раме под продольной осью корпуса по разные стороны от пневмоподушки, измеряют расстояние до корпуса и выдают сигналы автоматическому устройству управления, которое усредняет результаты измерений датчиков и сравнивает фактическое значение расстояния с требуемым. Усреднение результатов измерений датчиков позволяет исключить влияние вертикальных колебаний корпуса на получаемое значение. Если нагрузка от корпуса на пневмоподушку возрастает, то ее высота уменьшается, а соответственно, уменьшается и расстояние до корпуса, измеряемое датчиками, автоматическое устройство управления выдает

сигнал исполнительному устройству на открытие клапана впуска сжатого воздуха. Давление в пневмоподушке повышается, и ее высота возрастает до требуемого значения, а соответственно, расстояние до корпуса, измеряемое датчиками, также возрастает до требуемого значения, при этом автоматическое устройство управления выдает сигнал исполнительному устройству на закрытие клапана впуска сжатого воздуха. Если нагрузка от корпуса на пневмоподушку снижается, то ее высота увеличивается, а соответственно, повышается и расстояние до корпуса, измеряемое датчиками, автоматическое устройство управления выдает сигнал исполнительному устройству на открытие клапана выпуска воздуха из пневмоподушки. Давление в пневмоподушке снижается, и ее высота уменьшается до требуемого значения, а соответственно, расстояние до корпуса, измеряемое датчиками, также уменьшается, при этом автоматическое устройство управления выдает сигнал исполнительному устройству на закрытие клапана выпуска воздуха из пневмоподушки. Пневмоподушка и пружина обеспечивают гашение горизонтальных сил инерции корпуса.

Список использованных источников

1. Пат. 189555 РФ, МПК B 07 B 1/28 (2006.01). Решетный стан / Оробинский В. И., Корнев А. С., Аксенов И. И. ; заявитель и патентообладатель ФГБОУ ВО «Воронежский ГАУ». – № 2018143170 ; заявл. 05.12.2018 ; опубл. 28.05.2019, Бюл. № 16. – 5 с.
2. Пат. 217360 РФ, МПК B 21 B 07 B 1/28. Решетный стан / Аксенов И. И., Шацкий В. П., Оробинский В. И., Корнев А. С. ; заявитель и патентообладатель ФГБОУ ВО «Воронежский ГАУ». – № 2023101501 ; заявл. 24.01.2023 ; опубл. 29.03.2023, Бюл. № 10. – 5 с.
3. Совершенствование решетного стана зерноочистительной машины / И. И. Аксенов, В. И. Оробинский, Д. Н. Афоничев, А. С. Корнев. – Воронеж : ФГБОУ ВО «Воронежский ГАУ», 2022. – 141 с.
4. Теоретический анализ кинематических параметров решетных станов зерноочистительных машин [Электронный ресурс] / В. П. Шацкий, В. И. Оробинский, Д. Н. Афоничев, И. И. Аксенов, А. С. Корнев // Resources and Technology. – 2021. – № 2, Т. 18. – С. 18 – 31. – URL : https://rt.petrsu.ru/ journal/article.php?id=5703>.

References

1. Patent 189555 of the Russian Federation, IPC B 07 B 1/28 (2006.01). Reshetny Stan / V. I. Orobinsky, A. S. Kornev, I. I. Aksenov ; applicant and patent holder of the Voronezh State Agrarian University. – No. 2018143170 ; application 05.12.2018 ; publ. 28.05.2019, bul. No. 16. – 5 p.
2. Patent 217360 of the Russian Federation, IPC B 21 B 07 B 1/28. Reshetny Stan / I. I. Aksenov, V. P. Shatsky, V. I. Orobinsky, A.S. Kornev; applicant and patent holder of the Voronezh State Agrarian University. – No. 2023101501 ; application 24.01.2023 ; publ. 29.03.2023, bul. No. 10. – 5 p.
3. Improving the sieve mill of a grain cleaning machine / I. I. Aksenov, V. I. Orobinsky, D. N. Afonichev, A. S. Kornev. – Voronezh : Voronezh State Pedagogical University, 2022. – 141 p.
4. Theoretical analysis of kinematic parameters of sieve mills of grain cleaning machines [Electronic resource] / V. P. Shatsky, V. I. Orobinsky, D. N. Afonichev, I. I. Aksenov, A. S. Kornev // Resources and Technology. – 2021. – No. 2, vol. 18. – pp. 18-31. – URL : https://rt.petrsu.ru/journal/article.php?id=5703 >.

УДК 681.5

А. С. Вишневецкая, В. А. Макушенко, Д. А. Потапова
(Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: alexandravishnevetskaya@gmail.com, makushvt@gmail.com)

ЦИФРОВИЗАЦИЯ ЛОГИСТИЧЕСКИХ ПРОЦЕССОВ В СФЕРЕ ПЕРЕВОЗКИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ЖИВОТНЫХ

Аннотация. Рассмотрены возможные применения цифровых технологий, таких как мониторинг температуры и влажности, интеллектуальные системы управления и учета, а также системы отслеживания транспорта и контроля состояния животных в процессе перевозки. Один из ключевых элементов цифровизации – создание автоматизированных систем и защищенных баз данных.

Ключевые слова: цифровизация, логистика, база данных, автоматизированная система, информационная безопасность, сельскохозяйственные животные.

A. S. Vishnevetskaya, V. A. Makushenko, D. A. Potapova
(Department of “Information Protection”,
Federal State Budgetary Educational Institution of Higher Education
RTU MIREA, Moscow, Russia)

DIGITALIZATION OF LOGISTICS PROCESSES IN THE FIELD OF TRANSPORTATION OF FARM ANIMALS

Abstract. The article discusses possible applications of digital technologies, such as temperature and humidity monitoring, intelligent control and accounting systems, as well as transport tracking and animal health monitoring systems during transportation. One of the key elements of digitalization is the creation of automated systems and secure databases.

Keywords: digitalization, logistics, database, automated system, information security, farm animals.

Перевозка сельскохозяйственных животных, как один из элементов агропромышленного комплекса, охватывает широкий спектр задач – от планирования маршрутов до обеспечения комфортных и безопасных условий транспортировки. Рассмотрим подробнее главные аспекты внедрения цифровых технологий в логистические процессы: автоматизированные системы управления, базы данных, Интернет вещей (IoT), а также защиту данных.

Автоматизированные системы управления (АСУ) играют основную роль в цифровизации логистических процессов. Они позволяют оптимизировать различные этапы перевозки животных, от планирования маршрутов до контроля состояния в пути. Современные АСУ

используют алгоритмы для расчета оптимальных маршрутов перевозки. Эти алгоритмы учитывают множество факторов, включая дорожные условия, пробки и временные ограничения. Это позволяет сократить время в пути и снизить затраты на топливо [3]. Они интегрируются с GPS-навигаторами, что позволяет отслеживать местоположение транспортных средств в реальном времени. Эти данные в реальном времени передаются в систему управления, что позволяет принимать меры при отклонениях от нормы.

Электронные базы данных становятся основным инструментом для хранения и управления информацией о животных и их перевозках. Они обеспечивают централизованный доступ к информации и позволяют эффективно ей управлять. Большие объемы данных, собранных в процессе перевозки, могут быть использованы для анализа и выявления трендов. Например, анализ может показать, какие маршруты наиболее эффективны или какие условия перевозки наиболее благоприятны для здоровья животных.

Интернет вещей (IoT) представляет собой сеть подключенных устройств, которые обмениваются данными друг с другом. В контексте перевозки IoT-устройства играют важную роль в мониторинге и управлении состоянием животных и транспортных средств. Устройства IoT могут быть установлены в транспортных средствах и на самих животных. Эти датчики собирают данные и передают их в централизованную систему, что позволяет контролировать состояние животных в реальном времени.

С увеличением объемов и значимости данных, связанных с перевозкой сельскохозяйственных животных, защита информации становится критически важной [1]. Основные меры защиты данных включают шифрование, аутентификацию, контроль доступа, резервное копирование и мониторинг.

Шифрование данных применяется для того, чтобы вся информация, передаваемая между различными компонентами системы (например, между транспортным средством и центром управления, между базами данных и пользователями), была зашифрована. Это включает в себя данные о местоположении транспортных средств, состояния животных и другие важные данные [4].

Аутентификация и авторизация критичны для доступа к системам управления перевозками и базам данных. Системы должны удостоверять личность пользователей с помощью многофакторной аутентификации и предоставлять доступ в зависимости от их роли. Например, оператор может видеть только текущие маршруты и состояние транспортных средств, тогда как менеджер может также иметь доступ к историческим данным и планированию будущих маршрутов. Важно назначить права доступа к различным частям системы на основе ролей

пользователей. Это поможет предотвратить несанкционированные изменения данных или доступ к конфиденциальной информации.

Одним из способов защиты является регулярное создание резервных копий критически важной информации, такой как данные о перевозках, медицинские записи и информация о маршрутах. Необходимо иметь четкие планы и процедуры для восстановления данных после сбоя. Это включает в себя тестирование планов восстановления и регулярные обновления для учета новых данных и изменений в системах. Мониторинг и аудит необходимы для отслеживания активности пользователей и систем, помогают обнаруживать аномалии и потенциальные угрозы в реальном времени.

Как итог, цифровизация логистических процессов в сфере перевозки сельскохозяйственных животных предоставляет новые возможности для повышения эффективности и точности операций [2]. Однако с расширением использования информационных технологий возрастает необходимость в защите данных. Только при комплексном подходе к внедрению и защите цифровых систем можно гарантировать улучшение условий транспортировки и соблюдение всех регуляторных требований.

Список использованных источников

1. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26.07.2017 № 187-ФЗ / Электронное издание, 2017.

2. Современные подходы к организации логистической системы агропромышленного холдинга // Elibrary. – URL : https://www.elibrary.ru/ item.asp?id=23129221 (дата обращения: 07.09.2024).

3. Роль информационно-цифровых технологий в сфере логистики // КиберЛенинка. – URL : https://cyberleninka.ru/article/n/rol-informatsionno-tsifrovyh-tehnologiy-v-sfere-logistiki (дата обращения: 08.09.2024).

4. Методы обеспечения информационной безопасности логистических процессов // КиберЛенинка. – URL : https://cyberleninka.ru/article/n/metody-obespecheniya-informatsionnoy-bezopasnosti-logisticheskih-protsessov (дата обра-щения: 08.09.2024).

References

1. Federal Law No. 187-FZ dated 07/26/2017 “On the Security of the Critical Information Infrastructure of the Russian Federation” // Electronic Edition, 2017.

2. Modern approaches to the organization of the logistics system of an agro-industrial holding. // Elibrary. – URL : https://www.elibrary.ru/item.asp?id= 23129221 (date of application: 07.09.2024).

3. The role of information and digital technologies in the field of logistics // CyberLeninka. – URL : https://cyberleninka.ru/article/n/rol-informatsionno-tsifrovyh-tehnologiy-v-sfere-logistiki (date of application: 09/08/2024).

4. Methods of ensuring information security of logistics processes // CyberLeninka. – URL : https://cyberleninka.ru/article/n/metody-obespecheniya-informatsionnoy-bezopasnosti-logisticheskih-protsessov (date of application: 09/08/2024).

УДК 004.8

Е. Г. Кабулова
(Кафедра «Высшая математика и информатика»,
Старооскольский технологический институт им. А. А. Угарова
(филиал) ФГАОУ ВО «НИТУ «МИСИС»,
г. Старый Оскол, Россия,
e-mail: kabulova.misis@mail.ru)

БИОЛОГИЧЕСКАЯ НЕЙРОННАЯ СЕТЬ ДЛЯ ОБРАБОТКИ НИЗКОКОНТРАСТНЫХ ИЗОБРАЖЕНИЙ БПЛА

Аннотация. Приведена методика сегментации и обработки низкоконтрастных изображений поверхности земли агропромышленных комплексов, полученных с помощью беспилотных летательных аппаратов (БПЛА). Для решения задачи разработан алгоритм, основанный на нейронных сетях и свойствах синхронизации биологических нейронов. В основе алгоритма лежит модель биологической нейронной сети гистерезисной природы.

Ключевые слова: беспилотный летательный аппарат, биологическая нейронная сеть, сегментация.

E. G. Kabulova
(Department “Higher mathematics and Computer Science”,
Stary Oskol Technological Institute named after. A. A. Ugarova
(branch) of the Federal State Autonomous Educational Institution of Higher
Education “National Research Technological University “MISIS”,
Stary Oskol, Russia)

BIOLOGICAL NEURAL NETWORK FOR PROCESSING LOW-CONTRAST UAV IMAGES

Abstract. A technique for segmenting and processing low-contrast images of the earth's surface obtained using unmanned aerial vehicles (UAVs) is presented. To solve the problem, an algorithm has been developed based on neural networks and the synchronization properties of biological neurons. The algorithm is based on a model of a biological neural network of a hysteretic nature.

Keywords: unmanned aerial vehicle, biological neural network, segmentation.

На сегодняшний день беспилотные летательные аппараты (БПЛА) широко применяются во многих областях, включая аграрную промышленность. При решении задачи обнаружения и распознавания объектов на поверхности земли или замаскированных в грунте по инфракрасным (ИК) изображениям, демаскирующим признаком выступает различие в энергетических яркостях объекта и фона. Данные раз-

личия чаще всего обусловлены радиационным тепловым контрастом, который для однородных объектов и фонов определяется через отношение разностей энергетических светимостей объекта и фона к их сумме [1].

Основные параметры, влияющие на образование оптических полей сканируемых поверхностей земли в ИК-диапазоне длин волн, можно представить как: абсолютная температура, коэффициент теплового излучения, спектральный и интегральный коэффициенты отражения, теплофизические свойства объектов и фона. Кроме того, в качестве параметров могут выступать атмосферные явления (облачность, влажность, температура воздуха, давление, скорость ветра), солнечная активность, время года и суток, географические координаты и т.д. При этом, яркость объектов и фона состоит из трех факторов: отраженная энергия, поглощенная (переизлученная) энергия и собственная (внутренняя) энергия [1].

Для повышения эффективности мониторинга земной поверхности в интересах выявления скрытых объектов используют дистанционное измерение теплофизических параметров этих объектов с применением оптико-электронных систем БПЛА.

В связи с этим задача автоматизации оценки качественного показателя изображений важна и актуальна. Требуется на первом этапе сегментировать низкоконтрастные ИК-изображения. Для решения указанной задачи разработана нейронная сеть с синхронизацией биологических нейронов. В основе данного алгоритма лежит модель биологической нейронной сети гистерезисной природы, построенная, в свою очередь, на базе феноменологической модели С. А. Кащенко – В. В. Майорова и модели памяти нейронов А. Н. Радченко [2].

Принципиально новым в предложенной модели является формализация гистерезисных связей на основе модели Боука-Вена, позволяющей за счет своей гибкости наиболее адекватно описывать реальные сложные гистерезисные свойства биологических нейронов [3].

Была решена задача редукции кубоида ИК-изображения, которое получено с БПЛА средней дальности с высоты 4000 м в ночное время суток при съемке одного и того же участка местности с временны́м диапазоном 10 минут в течение 1,5 часов.

На полученных ИК-изображениях различимы постройки, река, кроны деревьев и автомобиль, можно увидеть присутствие воды на крышах зданий, металлические столбы натяжной переправы через реку. Кроме того, применение разработанного алгоритма сегментации ИК-изображений позволяет выделять на термограммах элементы, которые похожи по теплофизическим свойствам [4].

Необходимо отметить, что предложенная модель биологической нейронной сети гистерезисной природы для сегментации низкоконтрастных изображений в совокупности с системами сбора информации с БПЛА может эффективно применяться для мониторинга земной поверхности, а динамика разработанной биологической нейронной сети с гистерезисными свойствами соответствует биологическим данным и корректной сегментации исследуемых изображений.

Список использованных источников

1. The phase ambiguity resolution by the exhaustion method in a single-base interferometer / Y. L. Fateev, D. D. Dmitriev, V. N. Tyapkin, I. N. Ishchuk, E. G. Kabulova // ARPN Journal of Engineering and Applied Sciences. – 2015. – Т. 10, No. 18. – С. 8264 – 8270.

2. Кащенко, С. А. Модели волновой памяти / С. А. Кащенко, В. В. Майоров. – М. : УРСС, 2009. – 288 с.

3. Соловьев, А. М. Модель динамики биологической нейронной сети с гистерезисными связями / А. М. Соловьев, Е. Г. Кабулова, М. Е. Семенов // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии, 2018. – № 1. – С. 133 – 141.

4. Соловьев, А. М. Искусственные нейронные сети с гистерезисной функцией активации / А. М. Соловьев, М. Е. Семенов, М. Ю. Мишин, Е. Г. Кабулова // Теория и техника радиосвязи, 2013. – № 2. – С. 102 – 110.

References

1. The phase ambiguity resolution by the exhaustion method in a single-base interferometer / Y. L. Fateev, D. D. Dmitriev, V. N. Tyapkin, I. N. Ishchuk, E. G. Kabulova, *ARPN Journal of Engineering and Applied Sciences*, 2015. – Т. 10, No. 18. – Pp. 8264 – 8270.

2. Kashchenko, S. A. Modeli volnovoj pamyati / S. A. Kashchenko, V. V. Majorov. – M. : URSS, 2009. – 288 p.

3. Solov'yov, A. M. Model' dinamiki biologicheskoj nejronnoj seti s gisterezisnymi svyazyami / A. M. Solov'yov, E. G. Kabulova, M. E. Semyonov, *Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyj analiz i informacionnye tekhnologii*, 2018. – No. 1. – Pp. 133 – 141.

4. Solov'ev, A. M. Iskusstvennye nejronnye seti s gisterezisnoj funkciej aktivacii / A. M. Solov'ev, M. E. Semenov, M. Yu. Mishin, E. G. Kabulova, *Teoriya i tekhnika radiosvyazi*, 2013. – No. 2. – Pp. 102 – 110.

УДК 004

Е. В. Кошелев
(Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: lyutsian-zzz@yandex.ru)

УСТОЙЧИВОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ АГРОПРОМЫШЛЕННЫМ КОМПЛЕКСОМ К ВНЕШНИМ УГРОЗАМ

Аннотация. Рассмотрены основные методы оценки устойчивости информационных систем к внешним угрозам и приведен общий показатель устойчивости информационной системы управления агропромышленным комплексом.

Ключевые слова: показатель устойчивости, защищенность информационных систем, внешние угрозы.

E. V. Koshelev
(Department of Information Systems and Information Protection,
TSTU, Tambov, Russia)

SUSTAINABILITY OF INFORMATION MANAGEMENT SYSTEMS OF THE AGRO-INDUSTRIAL COMPLEX TO EXTERNAL THREATS

Abstract. The paper considers the main methods for assessing the stability of information systems to external threats and provides a general indicator of the stability of the information management system of the agro-industrial complex.

Keywords: stability indicator, security of information systems, external threats.

Аграрная промышленность играет ключевую роль в экономике каждой страны, обеспечивая продовольственную безопасность и устойчивое развитие сельских территорий. Учитывая растущее население планеты и глобальные изменения климата, важность аграрного сектора неуклонно возрастает, что требует внедрения новых технологий и подходов для повышения его эффективности.

В последние годы наблюдается активное внедрение информационных систем в аграрную промышленность, что значительно улучшает процессы управления, планирования и анализа данных. Использование современных технологий, таких как системы точного земледелия, позволяет фермерам оптимизировать использование ресурсов, минимизи-

руя затраты и увеличивая урожайность. Применение дронов, спутниковых технологий и сенсоров помогает не только в мониторинге состояния посевов, но и в управлении орошением, внесением удобрений и защитой растений от вредителей. Информационные системы также способствуют улучшению цепочки поставок, позволяя более эффективно управлять запасами, отслеживать перемещение продукции и оптимизировать логистику. В перечень информационных систем Минсельхоза России входят:

– Федеральная государственная информационная систем учета и регистрации тракторов, самоходных машин и прицепов к ним (ФГИС УСМТ);

– Система мониторинга и прогнозирования продовольственной безопасности Российской Федерации (СМ ПБ);

– Комплексная информационная система сбора и обработки бухгалтерской и специализированной отчетности сельскохозяйственных товаропроизводителей, формирования сводных отчетов, мониторинга, учета, контроля и анализа субсидий на поддержку агропромышленного комплекса (АИС «Субсидии АПК») и др. [1].

Таким образом, важно осознавать, что будущее аграрной промышленности тесно связано с развитием информационных технологий. Однако с их развитием и внедрением появляются и внешние угрозы:

– кибератаки;
– вирусы и вредоносное программное обеспечение;
– социальная инженерия;
– недостатки в программном обеспечении и др.

Устойчивость информационной системы к внешним угрозам – это важный показатель, который определяет, насколько надежно информационная система защищена от различных видов атак и потенциальных рисков. Оценка устойчивости к угрозам позволяет выявить уязвимости, принять меры для их устранения и, таким образом, минимизировать возможные убытки и потери данных.

Устойчивость системы может быть оценена по различным критериям защищенности. Ниже приведены несколько методов оценки защищенности информационной системы [2].

1. Аудит безопасности. Проведение независимого аудита позволяет выявить слабые места в системе, оценить применяемые меры безопасности и предложить рекомендации по их улучшению. Аудит может включать в себя как технические, так и организационные аспекты безопасности.

2. Пенетрационное тестирование. Этот метод включает в себя проведение контрольных атак на систему в целях проверить ее способности противостоять реальным угрозам. Результаты тестирования помогают определить уязвимости, которые могут быть использованы злоумышленниками.

3. Анализ угроз. Оценка потенциальных угроз и рисков, с которыми может столкнуться система, помогает лучше понять, какие меры необходимо предпринять для защиты. Это может включать анализ различных сценариев атак и оценку их вероятности и последствий.

4. Тестирование на соответствие стандартам. Применение стандартов безопасности, таких как *ISO* 27001 или ГОСТ Р ИСО/МЭК 27002-2021, позволяет оценить защищенность системы в соответствии с установленными требованиями. Процесс сертификации может выявить недостатки и предложить пути их исправления.

5. Мониторинг и аудит логов. Регулярный анализ логов системы позволяет выявлять подозрительные активности и потенциальные атаки на ранних стадиях. Это метод помогает оперативно реагировать на инциденты и корректировать стратегии защиты.

Показатель устойчивости функционирования информационной системы управления агропромышленным комплексом в условиях воздействия *i*-й внешней угрозы примем коэффициент устойчивости $K_{\text{у чi}}$, определяемый по формуле

$$K_{\text{у чi}} = 1 - \frac{\left| K_{\text{тр}} - K_{\text{дф}i} \right|}{K_{\text{тр}}},$$

где $K_{\text{тр}}$ – требуемое значение показателя качества функционирования системы; $K_{\text{дф}i}$ – значение показателя качества функционирования системы в условиях воздействия *i*-й внешней угрозы [3].

Тогда общий показатель устойчивости информационной системы управления агропромышленным комплексом, выражаемый как коэффициент устойчивости $K_{\text{у}}$, определяется выражением

$$K_{\text{у}} = \prod_{i=1}^{I} K_{\text{у чi}},$$

где I – количество учитываемых внешних угроз, оказывающих влияние на информационную систему управления агропромышленным комплексом.

Таким образом, оценка устойчивости информационной системы к внешним угрозам – это важный процесс, который включает в себя комплексный подход и применение различных методов. Проведение таких оценок обеспечивает защиту данных, минимизацию рисков и поддержание доверия клиентов и партнеров.

Список использованных источников

1. Перечень информационных систем Минсельхоза России // Министерство сельского хозяйства Российской Федерации : [сайт]. – 2024. – URL : https://mcx.gov.ru/analytics/infosystems/

2. Полянский, Д. А. Оценка защищенности : учеб. пособие / Д. А. Полянский. – Владимир : Изд-во Владим. гос. ун-та, 2005. – 80 с.

3. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации / В. Л. Бройдо. – 2-е изд. – СПб. : Питер, 2004. – 705 с.

References

1. List of information systems of the Ministry of Agriculture of the Russian Federation // Ministry of Agriculture of the Russian Federation : [website]. – URL : https://mcx.gov.ru/analytics/infosystems/

2. Polyansky, D. A. Assessment of security : studies. the manual / D. A. Polyansky. – Vladimir : Publishing House of the Vladimir State University, 2005. – 80 p.

3. Broido, V. L. Computing systems, networks and telecommunications / V. L. Broido. – 2nd ed. – St. Petersburg : Peter, 2004. – 705 p.

УДК 623.746.-519

А. Д. Лавриенко, В. В. Шатских
(Межвидовой центр подготовки и боевого применения
войск радиоэлектронной борьбы (учебный и испытательный),
Россия, г. Тамбов,
e-mail: nauchnajarota@yandex.ru)

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ШИФРОВАНИЯ ДЛЯ ЗАЩИТЫ КАНАЛА УПРАВЛЕНИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

Аннотация. Содержит краткий обзор роли беспилотных летательных аппаратов (БПЛА) в современном мире, актуальность темы необходимости защиты, каналов управления ими, а также методы шифрования, при помощи которых достигается определенный уровень защищенности канала управления БПЛА.

Ключевые слова: беспилотный летательный аппарат, канал управления БПЛА, методы шифрования, защита сельское хозяйство.

A. D. Lavrienko, V. V. Shatskikh
(Interspecific Center for training and combat use
of electronic Warfare troops (training and testing),
Tambov, Russia)

THE USE OF MODERN ENCRYPTION METHODS TO PROTECT THE CONTROL CHANNEL OF AN UNMANNED AERIAL VEHICLE IN AGRICULTURE

Annotation. This article contains a brief overview of the role of unmanned aerial vehicles (UAVs) in the modern world, the relevance of the topic of the need for protection, their control channels, as well as encryption methods by which a certain level of security of the UAV control channel is achieved.

Keywords: unmanned aerial vehicle, UAV control channel, encryption methods, agriculture protection.

В настоящее время БПЛА достигли своего пика популярности благодаря технологическим достижениям в области микропроцессорных вычислений, навигации, информационных технологий (IT) и искусственного интеллекта (AI).

Одним из главных преимуществ использования беспилотников в сельском хозяйстве является их способность получать информацию с воздуха и добираться в труднодоступные места. Это связано с их компактными размерами, что также помогает снизить производственные затраты.

Защита каналов связи между наземными станциями управления (НСУ) и беспилотными летательными аппаратами (БПЛА) от внешних программных и аппаратных помех в настоящее время является серьезной проблемой [1]. Атаки на беспилотные летательные аппараты могут включать перехват управляющих сигналов, искажение телеметрических данных, вывод из строя транспортного средства, получение или изменение информации, передаваемой полезной нагрузкой, или инициирование дальнейших атак на сетевые системы.

Типы взломов БПЛА

Управление беспилотными летательными аппаратами осуществляется дистанционно посредством спутниковой или иной беспроводной линии передачи данных, вследствие чего возникают такие виды взлома беспилотных летательных аппаратов, как [2]:

– перехват трафика – более трудоемкий метод взлома беспилотного летательного аппарата, требующий применения специальных программ, либо антенны спутниковой связи. С помощью данного вида взламывания можно завладеть как управлением беспилотного летательного аппарат, так и конфиденциальными данными, которые передаются между пунктом управления и беспилотным летательным аппаратом и наоборот;

– имитация и изменение геоданных: GPS-передатчики, используемые беспилотным летательным аппаратом, передают мнимые сигналы, данные, чем нарушают навигационную систему беспилотного летательного аппарата. Данный способ обусловлен нарушением направления траектории беспилотного летательного аппарата для его захвата или посадки.

В качестве перспективных видов взломов беспилотных летательных аппаратов особое место занимают атаки с помощью технологий программно-определяемого радио, которые включают в себя [2]:

– считывание и передачу сигнала на любой частоте: предполагается уязвимость всех частотных диапазонов, используемых для передачи конфиденциальной информации;

– применение универсального передатчика для перехвата и расшифровки радиосигналов: включает в себя не только перехват передаваемых данных от беспилотного летательного аппарата к оператору, и наоборот, но и полное завладение управлением беспилотного летательного аппарата;

– извлечение или расшифровка секретных ключей шифрования для передачи конфиденциальных данных.

Защита канала связи

Чтобы обеспечить конфиденциальность данных, передаваемых беспилотными летательными аппаратами, важно защитить их каналы связи. В настоящее время для этого используются различные методы, такие как периодическая регулировка рабочей частоты псевдослучайным образом, регулировка частот в случае прерываний связи и автоматическая посадка при длительной потере связи. Кроме того, для дальнейшего повышения безопасности каналов связи используются цифровые методы шифрования, включая как симметричное, так и асимметричное шифрование [3].

Схема симметричного шифрования представлена на рис. 1.

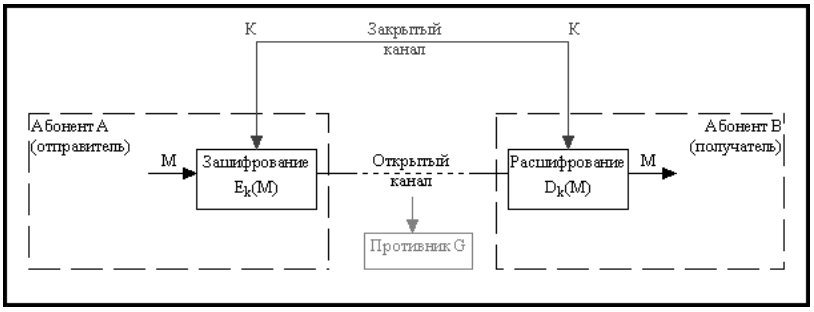


Рис. 1. Общая схема шифрования с закрытым ключом

Несмотря на их широкое использование в различных областях, беспилотные летательные аппараты (БПЛА) подвержены взлому. Это не всегда делается с благими намерениями и может привести к неправильному использованию конфиденциальных данных. Чтобы свести к минимуму риск возникновения подобных ситуаций, важно принять меры для обеспечения безопасности беспилотных летательных аппаратов.

Список использованных источников

1. Оков, И. Н. Способ криптографической защиты каналов связи между наземной станцией управления и одновременно несколькими управляемыми с нее беспилотными летательными аппаратами [Электронный ресурс] / И. Н. Оков, А. А. Устинов // РОССТИП : [патент]. – URL : https://rosstip.ru/patents/... (дата обращения: 20.04.2024).
2. Беспилотная авиация: терминология, классификация, современное состояние / В. С. Фетисов, Л. М. Неугодникова, В. В. Адамовский, Р. А. Красноперов. – Уфа., 2014.
3. Панасенко С. Алгоритмы шифрования / С. Панасенко. – СПб., 2009.

References

1. A method for cryptographic protection of communication channels between a ground control station and simultaneously several unmanned aerial vehicles controlled from it [Electronic resource] / I. N. Okov, A. A. Ustinov // ROSSTYPE: [patent] – URL : https://rosstip.ru/patents /... (date of address: 04/20/2024).
2. Fetisov V. S., Neugodnikova L. M., Adamovsky V. V., Krasnoperov R. A. Unmanned aviation: terminology, classification, current state. – Ufa., 2014.
3. Panasenko S. Encryption algorithms. – St. Petersburg, 2009.

УДК 621.391

А. Н. Потапов, А. Л. Началов
(ФГБОУ ВО «ВГЛУ имени Г. Ф. Морозова», г. Воронеж, Россия,
e-mail: Potapov_il@mail.ru)

ПОДСИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ЭРГОТЕХНИЧЕСКИХ СИСТЕМ

Аннотация. Рассмотрен вопрос разработки архитектуры подсистемы поддержки принятия решений информационного обеспечения эрготехнических систем. Рассмотрена технология обработки информации в подсистеме поддержки принятия решений системы управления информационным обеспечением авиации.

Ключевые слова: управление, архитектура, принятие решений, обеспечение, данные, система, модель.

A. N. Potapov, A. L. Nachalov
(Voronezh State Forestry Engineering University
named after G. F. Morozov, Voronezh, Russia)

SUBSYSTEM OF DECISION SUPPORT FOR INFORMATION SUPPORT OF ERGOTECHNICAL SYSTEMS

Abstract. The paper considers the issue of developing the architecture of the subsystem for decision support of information support for ergotechnical systems. The technology of information processing in the decision support subsystem of the aviation information management system is considered.

Keywords: data Mining, statistics, forecasting, moving average method, sales analysis, time series.

Оперативная аналитическая обработка и интеллектуальный анализ данных – две составные части процесса поддержки принятия решений. Эти два вида анализа должны быть тесно объединены, т.е. системы OLAP должны фокусироваться не только на доступе, но и на поиске закономерностей.

Parsaye K. [1] вводит составной термин «OLAP Data Mining» (многомерный интеллектуальный анализ) для обозначения такого объединения (рис. 1). Средство многомерного интеллектуального анализа данных должно находить закономерности как в детализированных, так и в агрегированных с различной степенью обобщения данных [2].

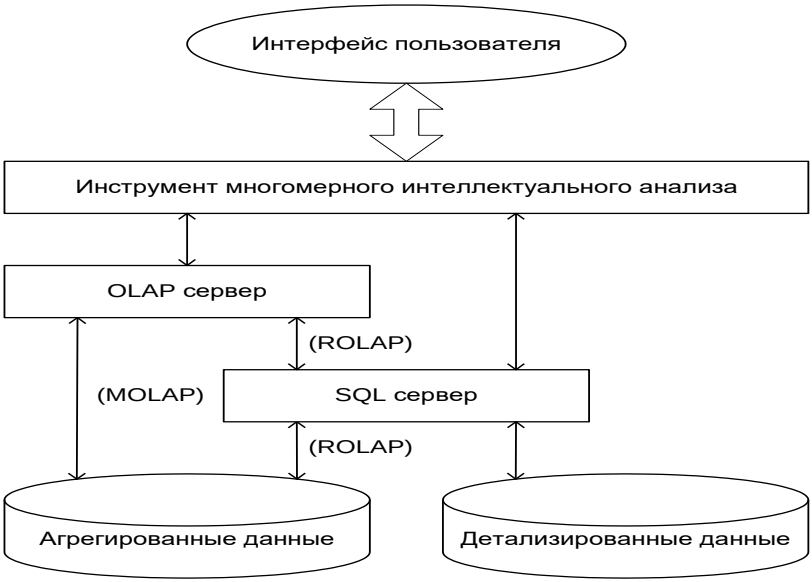


Рис. 1. Архитектура системы многомерного интеллектуального анализа данных

Идеальной целью построения корпоративной информационно-аналитической системы является создание СППР замкнутого цикла. В особенно динамичных сферах, где ситуация меняется ежедневно, своевременное принятие грамотных решений не обеспечивается даже при использовании обычных средств OLAP и ИАД. Они должны быть объединены друг с другом и иметь обратную связь к исходным системам обработки данных, с тем чтобы результаты работы СППР немедленно передавались в виде управляющих воздействий в оперативные системы.

В общем виде такая система поддержки принятия решений (СППР) представляет собой совокупность инструментальных средств, которая используется для манипулирования данными, их анализа и представления результатов анализа конечному пользователю. При этом новая информация заносится в хранилище регулярно и располагается в хронологическом порядке. На рисунке 2 представлена технология обработки информации в СППР, основанной на использовании концепции хранилища данных [3].

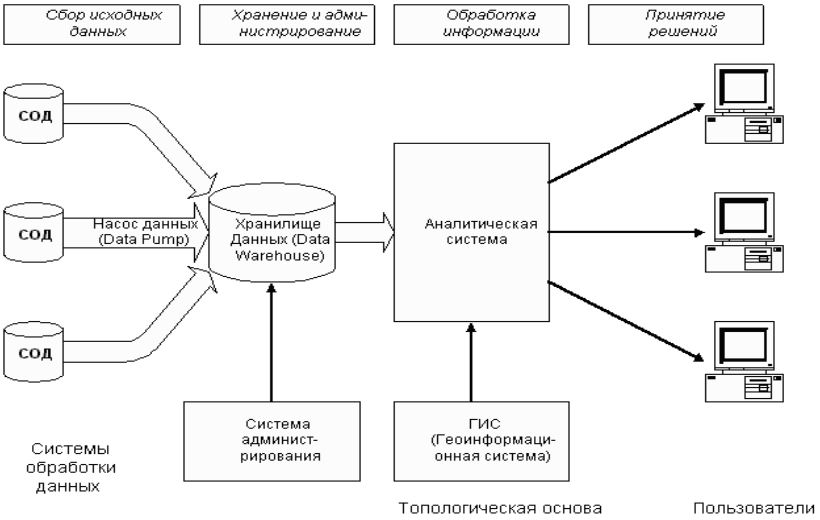


Рис. 2. Технология обработки информации в СППР

В основу модели базы данных хранилища положена концептуальная модель предметной области, которая разрабатывается на основе обработки результатов системного анализа процессов и событий, имеющих место в организации. При этом модель хранилища включает определенную совокупность связанных между собой ассоциативными отношениями информационных объектов, которые соответствуют понятиям (базовым сущностям), имеющим место в предметной области, и представляются в базе данных рядом связанных между собой таблиц. Стержневые (базовые) сущности окружаются наборами справочников и характеристических сущностей.

Справочники используются для кодировки характеризующих сущности атрибутов, по которым впоследствии осуществляются регламентированные выборки. Характеристические сущности выполняют вспомогательную роль в описании многозначных и косвенных свойств сущностей [3].

Список использованных источников

1. Потапов, А. Н. Архитектура математического обеспечения представления разнородных знаний подсистемы поддержки принятия решений проблемно-ориентированной системы управления информационным обеспечением авиации / А. Н. Потапов, Ю. Ю. Громов, А. Л. Началов // Научтехлитиздат. – М. : Промышленные АСУ и контроллеры. – 2023. – № 7. – С. 9 – 15.

2. Сазонова, С. А. Использование объектно-ориентированной среды для создания программ с применением управляющих операторов и циклов / С. А. Сазонова, Н. В. Акамсина, А. В. Лемешкин // Моделирование систем и процессов. – 2022. – Т. 15, № 2. – С. 41 – 54.

3. Шипилова, Е. А. Анализ и моделирование траекторий поведения пользователей онлайн-сервисов с использованием платформы RETENTIONEERING / Е. А. Шипилова, Е. Е. Некрылов, Т. В. Курченкова // Моделирование систем и процессов. – 2022. – Т. 15, № 3. – С. 82 – 93.

References

1. Potapov, A. N. Arkhitektura matematicheskogo obespecheniya predstavleniya raznorodnykh znaniy podsistemy podderzhki prinyatiya resheniy problemno-oriyentirovannoy sistemy upravleniya informatsionnym obespecheniyem aviatsii / A. N. Potapov, Yu. Yu. Gromov, A. L. Nachalov // Nauchtekhlitizdat. – M. : Promyshlennyye ASU i kontrollery. – 2023. – № 7. – S. 9 – 15.

2. Sazonova S. A., Akamsina N. V., Lemeshkin A. V. Ispol'zovaniye ob"yektno-oriyentirovannoy sredy dlya sozdaniya programm s primeneniyem upravlyayushchikh operatorov i tsiklov // Modelirovaniye sistem i protsessov. – 2022. – T. 15, № 2. – S. 41 – 54.

3. Shipilova Ye. A., Nekrylov Ye. Ye., Kurchenkova T. V. Analiz i modelirovaniye trayektoriy povedeniya pol'zovateley onlayn-servisov s ispol'zovaniyem platformy RETENTIONEERING // Modelirovaniye sistem i protsessov. – 2022. – T. 15, № 3. – S. 82 – 93.

УДК 681.5

М. М. Репин, К. В. Стародубов, А. С. Дерябин
(Кафедра КБ-1 «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: Starodubov@mirea.ru)

МЕТОДИКА АНАЛИЗА РИСКОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. В настоящее время актуальным в области АПК является разработка методики, позволяющей анализировать актуальные риски для автоматизированных систем агропромышленного комплекса и осуществлять их объективную оценку с учетом потенциального уровня деструктивного воздействия от их реализации.

Исследованы случаи осуществления атак на автоматизированные системы агропромышленного комплекса, проанализирован уровень нанесенного деструктивного воздействия. Проанализированы существующие методики анализа рисков и выбраны наиболее актуальные для гетерогенного ландшафта информационной инфраструктуры агропромышленного комплекса, а также определены параметры для расчета потенциального уровня деструктивного воздействия от реализации актуальных рисков деструктивного воздействия.

Ключевые слова: агропромышленный комплекс, автоматизированная система, деструктивное воздействие, риск деструктивного воздействия, атака, методика, уязвимость.

M. M. Repin, K. V. Starodubov, A. S. Deryabin
(Department KB-1 “Information Security”,
RSU MIREA, Moscow, Russia)

METHODOLOGY FOR ANALYZING THE RISKS OF DESTRUCTIVE IMPACT ON AUTOMATED SYSTEMS OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. Currently, the development of a methodology that allows analyzing current risks for automated systems of the agro-industrial complex and carrying out their objective assessment taking into account the potential level of destructive impact from their implementation is relevant in the field of the agro-industrial complex.

The cases of attacks on automated systems of the agro-industrial complex are studied, the level of destructive impact inflicted is analyzed. The existing risk analysis methods are analyzed and the most relevant ones for the heterogeneous landscape of the information infrastructure of the agro-industrial complex are selected, and the parameters for calculating the potential level of destructive impact from the implementation of current risks of destructive impact are determined.

Keywords: agro-industrial complex, automated system, destructive impact, risk of destructive impact, attack, methodology, vulnerability.

В настоящее время цифровая трансформация агропромышленного комплекса (АПК) является одним из основных государственных приоритетов.

Согласно открытым источникам, за последнее время на предприятия АПК совершались атаки следующих типов:

- атаки на цепочки поставок, путем внедрения вредоносного программного обеспечения;
- применение вирусов шифровальщиков;
- атаки на IoT (Статья);
- кража данных;
- угрозы интеллектуальной собственности;
- атаки на отказ в обслуживании.

Данные факты свидетельствуют о наличии, на настоящий момент, предпосылок для проведения пересмотра и модернизации системы управления рисками деструктивного воздействия для предприятий АПК, а также потребности в разработке моделей и алгоритмов управления рисками деструктивного воздействия на АС АПК.

Базовые критерии формирования методики анализа рисков деструктивного воздействия

Существующие методики анализа рисков и оценки деструктивного воздействия, рассмотренные в ряде работ [1, 2], и предлагаемое авторами методическое обеспечение не рассматривается в контексте организации анализа рисков информационной безопасности в АПК и не позволяет учитывать все особенности, связанные со всем спектром применяемых технологий.

Чтобы провести обоснованный выбор и адаптацию методики анализа рисков деструктивного воздействия, необходимо определиться с атомарными принципами, которые должны лежать в основе методики анализа рисков деструктивного воздействия в АС АПК.

С учетом критичности рассматриваемой области, а также с учетом того, что необходимо оценивать не столько общий финансовый ущерб от реализации рисков, сколько ущерб, выраженный в степени влияния на индикаторы показателей продовольственной безопасности, целесообразно рассмотреть в качестве первичного такой принцип обеспечения безопасности, как «Снижение вероятности существенного ущерба вследствие атаки в течение определенного периода времени».

В качестве основной стратегии реализации программы по предотвращению деструктивного воздействия целесообразно определить стратегию нулевого доверия. Подобный подход позволит учесть гетерогенность ИТ-ландшафта и применяемых инновационных технологий в сфере АПК.

Таким образом, в качестве базовых критериев формирования методики анализа рисков деструктивного воздействия были определены следующие:

1. Использование принципа «Снижение вероятности существенного ущерба вследствие атаки в течение определенного периода времени» в качестве основного для выбора подходов к обеспечению безопасности АС АПК.

2. Использование стратегии нулевого доверия при реализации программ по предотвращению деструктивного воздействия на АС АПК.

Методика оперативной оценки вероятности реализации риска деструктивного воздействия

Ключевой составляющей одного из базовых принципов является вероятность нанесения существенного ущерба. Таким образом, необходимо сформировать эффективный подход к оценке данных вероятностей.

В то же время, одним из основных требований для методики, применяемой в столь неоднородной и быстро изменяющейся среде, является получение относительно точных оценок, позволяющих оперативно принимать решения и оценивать сложившуюся обстановку.

Данную задачу можно решить, применяя анализ общей вероятности реализации рисков деструктивного воздействия в области АПК к конкретной организации АПК или АС АПК, а затем, анализируя на основе полученных сведений ситуацию именно в данной организации или АС.

После получения частной вероятности риска деструктивного воздействия целесообразно определить границы существенного ущерба. В зависимости от установленного значения параметр вероятности должен корректироваться путем внедрения дополнительных мер, закрывающих области, вызывающих наибольшие опасения в части отражения атак. Кроме того, необходимо учитывать стоимость внедряемых мер, которая должна быть адекватно сопоставима с потенциальным ущербом от деструктивного воздействия. Данная стоимость может быть рассчитана через совокупную стоимость владения или иными методами [2].

Выводы

В рамках данной работы предложена методика анализа рисков деструктивного воздействия на автоматизированные системы агропромышленного комплекса, позволяющая однозначно определять вероятность реализации риска. Заданы ее основные параметры, а также определены параметры для проведения оценки.

Данная методика отходит от общепринятых подходов с использованием детального анализа вероятностей реализации рисков, делая ключевую ставку на оперативность принятия решений с условием допустимых погрешностей.

В методике предлагается использовать общедоступные данные из отчетов компаний и регуляторов, а также сведения о стратегии построения системы защиты в конкретной компании, что позволяет избежать ошибок из-за малой выборки данных, которые существенно влияют на результат анализа.

В качестве дальнейшего развития направления данной работы предлагается рассмотреть формирование рекомендаций по построению комплексной системы защиты от деструктивного воздействия на АС АПК с учетом формирующегося гетерогенного ландшафта технологий и АС.

Список использованных источников

1. Анализ применимости существующих методов оценки рисков в области информационной безопасности / М. М. Репин, Е. А. Пшехотская, А. А. Плоткин, А. А. Кривоногов // Системный администратор. РазделВАК «Наука и технологии». – 2018 – № 1-2. – С. 182–183.

2. Репин, М. М. Построение модели оценки экономической эффективности системы информационной безопасности / М. М. Репин, А. В. Сакулина, Е. А. Пшехотская // Научно-методический журнал, ГБУ ДПО «Региональный центр оценки качества и информатизации образования». – 2017 – № 2(3). – С. 80 – 84.

References

3. Analysis of the applicability of existing risk assessment methods in the field of information security / M. M. Repin, E. A. Pshekhotskaya, A. A. Plotkin, A. A. Krivonogov // System administrator. Section of the Higher Attestation Commission "Science and Technology". – 2018 – No. 1-2. – P. 182–183.

4. Repin, M. M. Construction of a model for assessing the economic efficiency of an information security system / M. M. Repin, A. V. Sakulina, E. A. Pshekhotskaya // Scientific and methodological journal, State Budgetary Educational Institution of Higher Professional Education "Regional Center for Quality Assessment and Informatization of Education". – 2017 – No. 2(3). – P. 80 – 84.

УДК 681.5

С. А. Савушкин, Д. А. Потапова, С. В. Артемова, А. С. Катруш
(Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: serge2109@mail.ru, potapova.daria1998@yandex.ru)

УГРОЗЫ И РИСКИ ЦИФРОВИЗАЦИИ ДЛЯ СЕЛЬСКОГО ХОЗЯЙСТВА

Аннотация. Проанализированы ключевые угрозы нарушения безопасности информации, обрабатываемые в информационных системах, относящихся к агропромышленному комплексу. Выявлено, что наиболее актуальные из них неизменно сопровождают цифровизацию и автоматизацию процессов сбора и анализа данных, необходимых для бесперебойного функционирования сельскохозяйственных комплексов. Определены ключевые риски информационной безопасности для таких комплексов.

Ключевые слова: угроза информационной безопасности, риски информационной безопасности, агропромышленный комплекс, цифровизация, автоматизация процессов, информационные системы.

S. A. Savushkin, D. A. Potapova, S. V. Artemova, A. S. Katrush
(Department of "Information Protection",
Federal State Budgetary Educational Institution of Higher Education
RTU MIREA, Moscow, Russia)

THREATS AND RISKS OF DIGITALIZATION FOR AGRICULTURE

Abstract. The key threats to information security processed in information systems related to the agro-industrial complex were analyzed. It was revealed that the most relevant of them invariably accompany the digitalization and automation of data collection and analysis processes necessary for the smooth functioning of agricultural complexes. The key information security risks for such complexes were identified.

Keywords: information security threat, information security risks, agroindustrial complex, digitalization, process automation, information systems.

Внедрение цифровых технологий стало неотъемлемой частью жизни современного общества и оказывает большое влияние на все сферы деятельности. Сельское хозяйство, являясь одной из главных отраслей экономики, также подвергается изменениям вследствие цифровизации.

Одним из ключевых направлений программы «Цифровая экономика Российской Федерации» является «Цифровое сельское хозяйство».

Данное направление несет в себе множество нововведений, значительно сокращая трудозатраты на выполнение ключевых процессов в области сельского хозяйства [1]. Однако с ростом цифровизации появляется необходимость обеспечения информационной безопасности информационных ресурсов. Поэтому актуальной задачей становится выявление угроз и оценка рисков информационной безопасности агропромышленного комплекса.

Целью данной статьи является анализ угроз и возможных рисков при цифровизации сельского хозяйства в аспекте ее цифровизации.

К цифровизации сельского хозяйства можно отнести создание автономных систем, облачных сервисов, возможность применения анализа данных и машинного обучения. С их помощью собирается, хранится, обрабатывается и передается информация не только на уровне всего хозяйства, но и отдельных полей или гектаров. Так, агрономы и фермеры получают информацию о состоянии растений и их потребностях [2]. Это позволяет выполнять работу более точно и эффективно. Так же цифровизация сельского хозяйства может быть подвержена ряду рисков и угроз. Зависимость от технологий может привести к сбоям в производственных процессах, что может негативно повлиять на урожайность и снизить количество готовой продукции. Сельское хозяйство становится все более уязвимым для кибератак, которые могут нанести серьезный ущерб производству и репутации компании. Злоумышленники могут получить доступ к конфиденциальной информации о фермах, а также нарушить работу систем управления и мониторинга. Вероятность сокращения и потеря рабочих мест тоже возможна при автоматизации и роботизации процессов [3]. Это может вызвать социальные и экономические проблемы в сельском хозяйстве. Чтобы иметь возможность защитить конфиденциальную информацию, можно предпринять несколько решений, таких как внедрение систем шифрования, которые помогут защитить данные от несанкционированного доступа и использования.

Угрозы информационной безопасности, такие как утечка данных и несанкционированный доступ, представляют значительный риск для сельскохозяйственного сектора.

Утечка данных происходит, когда конфиденциальная информация попадает к неавторизованным лицам или третьим сторонам. В сельском хозяйстве это могут быть данные о состоянии полей, урожайности, финансовых показателях и даже личная информация сотрудников. Такие утечки могут привести к целому ряду негативных последствий, включая потерю конкурентных преимуществ, нарушение конфиденциальности и потенциальные финансовые потери. Например, доступ к данным о передовых сельскохозяйственных технологиях и методах может быть использован конкурентами для усовершенствования соб-

ственных процессов, что поставит под угрозу положение компании на рынке и ее прибыльность. Чтобы предотвратить утечку данных, необходимо внедрить надежное шифрование данных, контролировать доступ к данным с помощью многофакторной аутентификации и регулярно проводить аудит безопасности для выявления и устранения потенциальных уязвимостей.

Неавторизованный доступ представляет собой еще одну серьезную угрозу, когда злоумышленники получают доступ к системам и данным без соответствующих разрешений. Это может включать физический доступ к оборудованию или удаленный доступ к программному обеспечению и базам данных. В сельском хозяйстве несанкционированный доступ может позволить злоумышленникам изменить настройки системы, что приведет к неправильным действиям, таким как неправильное распределение ресурсов или манипулирование урожайностью. Такой доступ также может быть использован для кражи конфиденциальной информации или уничтожения данных, что приведет к серьезному нарушению сельскохозяйственных операций. Для защиты от несанкционированного доступа необходимо внедрять системы контроля доступа, включая замки и наблюдение для физической защиты оборудования, и использовать системы аутентификации и авторизации для защиты информационных систем.

Подводя итог, комплексный подход к защите данных, включающий надежное шифрование, контроль доступа и регулярные проверки безопасности, помогут минимизировать риски утечки данных и несанкционированного доступа, тем самым обеспечивая безопасность и надежность современных сельскохозяйственных технологий.

Список использованных источников

1. Федеральный проект «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации».

2. Дятлова, А. Ф. Цифровизация в сельском хозяйстве: преимущества и проблемы внедрения / А. Ф. Дятлова // Московский экономический журнал. – С. 20.

3. Алтухов, А. И. Развитие цифровизации аграрного сектора экономики России / А. И. Алтухов, В. И. Нечаев, А. И. Трубилин // Экономика сельского хозяйства России. – 2018. – № 3. – С. 2 – 10.

References

1. Federal project "Digital public administration" of the national program "Digital economy of the Russian Federation".

2. Dyatlova A. F. Digitalization in agriculture: advantages and problems of implementation // Moscow Economic Journal. – 20.

3. Altukhov A. I., Nechaev V. I., Trubilin A. I. Development of digitalization of the agricultural sector of the Russian economy // Economics of agriculture of Russia. – 2018. – No. 3. – P. 2 – 10.

УДК 681.5

А. Д. Саенко, О. В. Соболева, Д. А. Потапова
(Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: potapova.daria1998@yandex.ru, Wertygool.work@gmail.com)

БЕЗОПАСНОСТЬ АНАЛИТИКИ И ХРАНЕНИЯ БОЛЬШИХ ДАННЫХ В АГРОПРОМЫШЛЕННОЙ ОТРАСЛИ

Аннотация. Цифровизация агропромышленного комплекса в России ведет к активному использованию больших данных для повышения эффективности производства, оптимизации процессов и принятия более точных решений. Однако безопасность аналитики и хранения этих данных является критической задачей, требующей новых подходов для минимизации рисков утечек и кибератак. В статье рассматриваются основные угрозы, связанные с большими данными, а также предлагаются инновационные решения, такие как использование блокчейн-технологий для защиты и управления данными в агропромышленной отрасли.

Ключевые слова: безопасность данных, большие данные (Big Data), агропромышленный комплекс, блокчейн-технологии, кибербезопасность, хранение данных, аналитика данных, смарт-контракты, цифровизация сельского хозяйства, информационная безопасность.

A. D. Saenko, O. V. Soboleva, D. A. Potapova
(Department of “Information Protection”,
Federal State Budgetary Educational Institution of Higher Education
RTU MIREA, Moscow, Russia)

SECURITY OF BIG DATA ANALYTICS AND STORAGE IN THE AGRO-INDUSTRIAL SECTOR

Abstract. The digitalization of the agro-industrial complex in Russia is leading to the active use of big data to improve production efficiency, optimize processes, and make more accurate decisions. However, ensuring the security of data analytics and storage is a critical task that requires new approaches to minimize the risks of data leaks and cyberattacks. This article examines the main threats related to big data, as well as proposes innovative solutions, such as the use of blockchain technologies for data protection and management in the agro-industrial sector.

Keywords: data security, big data, agro-industrial complex, blockchain technologies, cybersecurity, data storage, data analytics, smart contracts, digitalization of agriculture, information security.

Современные агропромышленные предприятия РФ активно внедряют цифровые технологии для управления производственными процессами. Одним из ключевых факторов успешного использования

таких технологий является работа с большими данными, которые предоставляют возможности для прогнозирования урожайности, улучшения условий выращивания сельскохозяйственных культур и оптимизации логистических процессов. Однако с ростом объемов данных возрастают и угрозы, связанные с их безопасностью. Недостаточная защита данных может привести к серьезным экономическим потерям и угрожать репутации компаний.

Большие данные в агропромышленности собираются из множества источников, таких как сенсоры, беспилотники, спутники и аналитические платформы. Основные проблемы, которые возникают при работе с этими данными, включают:

– угрозы кибератак. Хакеры могут получить доступ к ценным данным, которые включают информацию о планировании урожая, коммерческую информацию и другие конфиденциальные сведения;

– нарушения конфиденциальности. Использование персональных данных фермеров, работников и третьих сторон требует строгих мер по защите этих данных;

– недостаточная защита инфраструктуры хранения данных. Большие данные хранятся на серверах или в облачных системах, которые могут стать объектом атак или быть подвержены техническим сбоям;

– отсутствие общепринятых стандартов безопасности. В отрасли недостаточно разработанных стандартов по защите данных, что приводит к разнородности подходов на предприятиях.

Оригинальное решение: использование блокчейн-технологий для защиты данных

Для обеспечения более высокого уровня безопасности больших данных в агропромышленной отрасли предлагается внедрение блокчейн-технологий. Блокчейн обладает несколькими преимуществами, которые делают его подходящим инструментом для защиты данных.

Преимущества блокчейна:

1. Неизменяемость данных. Все данные, записанные в блокчейн, невозможно изменить или удалить задним числом, что гарантирует их целостность и защищает от подделок.

2. Прозрачность. Все участники системы могут видеть действия, связанные с данными, что обеспечивает высокий уровень доверия и предотвращает внутренние манипуляции.

3. Децентрализация. Блокчейн не зависит от одного центра хранения, что снижает риски атак на центральные серверы и обеспечивает надежность всей системы.

4. Автоматизация через смарт-контракты. Интеллектуальные контракты (смарт-контракты) могут автоматизировать процессы на основе собранных данных, таких как контроль за состоянием почвы и автоматический запуск систем орошения.

Предположим, крупный агрохолдинг собирает данные о состоянии полей с помощью дронов, спутниковых снимков и сенсоров. Эти данные хранятся в распределенной системе на базе блокчейна. Каждый раз, когда обновляются данные о состоянии почвы или уровня влажности, эта информация записывается в блокчейн и становится доступной для всех участников агропромышленной цепочки – фермеров, менеджеров и контролирующих органов.

Другие методы защиты

Помимо использования блокчейна, предприятия могут применять следующие меры для повышения безопасности данных:

1. Шифрование данных при хранении и передаче для предотвращения их перехвата.

2. Многофакторная аутентификация для ограничения доступа только авторизованным пользователям.

3. Регулярное резервное копирование данных для предотвращения их потери при технических сбоях.

4. Использование систем мониторинга и анализа угроз, основанных на технологиях искусственного интеллекта и машинного обучения, для раннего обнаружения потенциальных атак.

Обеспечение безопасности больших данных в агропромышленной отрасли России является важным условием для дальнейшего цифрового развития отрасли. Внедрение инновационных решений, таких как блокчейн, вместе с традиционными методами защиты, позволит минимизировать риски утечек и атак, обеспечивая сохранность данных и их целостность. Актуализация стандартов безопасности и обучение сотрудников также будут способствовать созданию надежной инфраструктуры для работы с большими данными. Это создаст прочный фундамент для успешного использования цифровых технологий в агробизнесе.

Список использованных источников

1. Уткин, А. В. Безопасность больших данных в агропромышленном комплексе: вызовы и перспективы / А. В. Уткин, И. Г. Иванов // Журнал информационной безопасности. – 2022.

2. Петренко, М. С. Применение блокчейн-технологий в агропромышленном секторе / М. С. Петренко // Труды конференции по цифровой трансформации сельского хозяйства. – 2021.

3. ISO/IEC 27001:2013. Стандарты управления информационной безопасностью.

4. Лебедев, П. Проблемы кибербезопасности в агробизнесе / П. Лебедев // Экспертное мнение. – 2023.

References

1. Utkin, A. V., Ivanov, I. G. "Big data security in the agro-industrial complex: challenges and prospects". Information Security Journal, 2022.

2. Petrenko, M. S. "Application of blockchain technologies in the agro-industrial sector". Proceedings of the Conference on Digital Transformation of Agriculture, 2021.

3. ISO/IEC 27001:2013. Information security management standards.

4. Lebedev, P. "Cybersecurity problems in agribusiness". Expert opinion, 2023.

УДК 681.5

С. В. Артемова, Д. А. Потапова, Е. О. Карамышева, А. С. Спиридонов
(Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: potapova.daria1998@yandex.ru, spiridonov.a.s@edu.mirea.ru)

ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕСПИЛОТНЫХ СИСТЕМ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрен потенциал беспилотных систем, таких как беспилотники, автономные тракторы и роботизированные комбайны, для повышения эффективности сельскохозяйственного сектора. В нем подчеркивается критическая важность решения проблем информационной безопасности, подчеркивается необходимость защиты данных и систем от потенциальных кибератак в условиях растущей цифровизации.

Ключевые слова: беспилотные системы, дроны, автономные тракторы, роботизированные комбайны, эффективность сельского хозяйства, информационная безопасность, кибербезопасность, цифровизация в сельском хозяйстве, точное земледелие, защита данных.

S. V. Artyomova, D. A. Potapova, E. O. Karamysheva, A. S. Spiridonov
(Department of “Information Protection”,
Federal State Budgetary Educational Institution of Higher Education
RTU MIREA, Moscow, Russia)

PROSPECTS FOR THE DEVELOPMENT OF UNMANNED SYSTEMS IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. This article examines the potential of unmanned systems such as drones, autonomous tractors and robotic harvesters to improve the efficiency of the agricultural sector. It highlights the critical importance of addressing information security issues, emphasizing the need to protect data and systems from potential cyberattacks in an increasingly digitalized world.

Keywords: unmanned systems, drones, autonomous tractors, robotic harvesters, agricultural efficiency, information security, cybersecurity, digitalization in agriculture, precision farming, data protection.

Современные тенденции развития агропромышленного комплекса сигнализируют о возрастающей потребности внедрения инновационных технологий, которые будут направлены на повышение эффективности сельскохозяйственного производства [1]. Одной из таких технологий является потенциальное использование беспилотных систем,

которые могут включать в себя летательные дроны, беспилотные тракторы, роботизированные автономные комплексы полива и сбора урожая. Данные решения уже показали свою эффективность в ряде стран путем обеспечения высокой точности операций, оптимизацией и сокращением затрат на производственные ресурсы.

Целью данной статьи является всесторонний анализ перспектив развития беспилотных систем в агропромышленном комплексе с акцентом на информационную безопасность. В ходе исследования рассмотрены современные тенденции и достижения в данной области, а также возможные риски и способы их минимизации.

Беспилотные системы становятся неотъемлемой частью современного агропромышленного сектора, предлагая решения, которые значительно повышают эффективность и автоматизируют ключевые сельскохозяйственные процессы. В настоящее время беспилотники широко используются для мониторинга урожая, оценки состояния растений, анализа почвы и точного внесения удобрений [2]. Автономные тракторы и комбайны автоматизируют такие задачи, как посев, обработка почвы и сбор урожая, что значительно сокращает трудозатраты и повышает производительность.

Использование беспилотных систем в сельском хозяйстве уже демонстрирует свою экономическую эффективность. Снижение трудозатрат, повышение точности и минимизация потерь за счет использования беспилотных технологий ведут к повышению рентабельности сельскохозяйственных предприятий [3].

Несмотря на ряд очевидных преимуществ, внедрение и активное использование беспилотных систем в агропромышленном комплексе сопряжено с рядом серьезных проблем, одной из которых является обеспечение информационной безопасности [4]. В условиях массовой цифровизации беспилотные аппараты все чаще становятся объектами потенциальных кибератак, способных привести к серьезным последствиям. Такие угрозы могут не только снизить эффективность использования новых технологий, но и вызвать значительные экономические и социальные риски, особенно в сельских регионах.

С учетом этих факторов интеграция беспилотных систем в агропромышленный комплекс требует всестороннего подхода, который включает не только технические аспекты их разработки и внедрения, но и обеспечение высокого уровня информационной безопасности. Это становится критически важным, поскольку от уровня защищенности данных и систем будет зависеть не только экономическая эффективность их использования, но и безопасность всего агропромышленного комплекса.

Подводя итог, для успешного внедрения и развития беспилотных систем в сельском хозяйстве необходим комплексный подход, включающий технические, экономические, социальные и правовые аспекты, а также обеспечивающий высокий уровень информационной безопасности.

Список использованных источников

1. Использование беспилотных летательных аппаратов в сельском хозяйстве // КиберЛенинка. – URL : https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-selskom-hozyai-stve (дата обращения: 03.09.2024).

2. Беспилотные летательные аппараты в сельском хозяйстве // Карнеев.com. – URL : https://www.karneev.com/stati/bpla-v-selskom-khozyaystve/ (дата обращения: 03.09.2024).

3. Дроны в сельском хозяйстве // TAdviser. – URL : https://www.tadviser.ru/index.php/Статья:Дроны_в_сельском_хозяйстве (дата обращения: 03.09.2024).

4. Мехтиев, Ш. Некоторые вопросы безопасности применения дронов / Ш. Мехтиев, А. Мехдиев // Информационная безопасность: актуальные многодисциплинарные научно-практические проблемы : материалы IV Республиканской конференции. – Баку : Институт Информационных Технологий НАНА, 2018. – С. 91.

References

1. Use of unmanned aerial vehicles in agriculture // CyberLeninka. – URL : https://cyberleninka.ru/article/n/ispolzovanie-bespilotnyh-letatelnyh-apparatov-v-selskom-hozyai-stve (date of reference: 03.09.2024).

2. Unmanned aerial vehicles in agriculture // Karneev.com. – URL : https://www.karneev.com/stati/bpla-v-selskom-khozyaystve/ (date of address: 03.09.2024).

3. Drones in agriculture // TAdviser. – URL : https://www.tadviser.ru/index.php/Статья:Дроны_в_сельском_хозяйстве (date of address: 03.09.2024).

4. Mehdiyev, S. Some safety issues of drone application / S. Mehdiyev, A. Mehdiyev // Information security: actual multidisciplinary scientific and practical problems: materials of the IV Republican Conference. – Baku: Institute of Information Technologies of ANAS, 2018. – C. 91.

УДК 621.396.43

А. М. Хромов, А. А. Гусев
Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный),
г. Тамбов, Россия,
e-mail: nauchnajarota@yandex.ru)

МОДЕРНИЗАЦИЯ КАНАЛОВ УПРАВЛЕНИЯ БПЛА ДЛЯ УВЕЛИЧЕНИЯ ДАЛЬНОСТИ СВЯЗИ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

Аннотация. Рассмотрены ключевые стратегии и технологические решения для увеличения дальности связи систем беспилотных летательных аппаратов (БПЛА).

Ключевые слова: система связи, дальность связи, антенные системы, ретрансляторы, меш-сети, спутниковая связь, сельское хозяйство.

A. M. Khromov, A. A. Gusev
(Interspecific Center for Training and Combat Use of Electronic Warfare Troops (Training and Testing), Tambov, Russia)

MODERNIZATION OF UAV CONTROL CHANNELS TO INCREASE THE RANGE OF COMMUNICATION IN AGRICULTURE

Annotation. This article discusses key strategies and technological solutions for increasing the communication range of unmanned aerial vehicle (UAV) systems.

Keywords: communication system, communication range, antenna systems, repeaters, mesh networks, satellite communications, agriculture.

Беспилотные летательные аппараты (БПЛА) становятся неотъемлемой частью многих отраслей промышленности, таких как мониторинг окружающей среды, сельское хозяйство и коммерческое судоходство. Эффективность работы беспилотного летательного аппарата в значительной степени зависит от качества и дальности действия систем связи, которые позволяют передавать данные и управляющие сигналы между транспортным средством и оператором или автоматизированной системой управления.

Значение дальности действия систем связи

Дальность связи беспилотного летательного аппарата напрямую влияет на дальность его работы, определяя потенциальные области

применения, для которых он может быть использован. За счет увеличения дальности связи беспилотник может работать на больших расстояниях от своего пункта управления, что делает его идеальным для использования в отдаленных или труднодоступных районах [1].

Физические и технические ограничения

1. Полоса пропускания и частота передачи: диапазон частот, в котором работает система связи беспилотного летательного аппарата, напрямую влияет на дальность действия и качество сигнала. Например, высокочастотные сигналы обеспечивают бóльшую полосу пропускания для передачи данных, но имеют меньшую дальность действия и более чувствительны к физическим препятствиям.

2. Мощность передатчика: мощность сигнала, излучаемого передатчиком, напрямую влияет на то, на какое расстояние он может быть передан. Однако увеличение мощности передатчика приводит к увеличению потребления энергии, что может стать серьезной проблемой для беспилотных летательных аппаратов с ограниченными запасами энергии.

3. Чувствительность приемника: способность приемника обнаруживать слабые сигналы играет важную роль в расширении диапазона связи беспилотных летательных аппаратов. Повышение чувствительности приемника может значительно увеличить расстояние, на котором беспилотные летательные аппараты могут надежно принимать команды и передавать данные.

Технологические решения для увеличения дальности связи

Расширение диапазона связи беспилотных летательных аппаратов (БПЛА) требует использования передовых технологических решений для оптимизации передачи сигнала и повышения общей производительности системы связи [2]. В этой статье будут рассмотрены несколько ключевых технологий и методологий, которые могут помочь в достижении этих целей.

Применение усовершенствованных антенных систем и повышение мощности передатчика

1. Усовершенствованные антенные системы: использование направленных или адаптивных антенных технологий может помочь сфокусировать сигнал в определенном направлении, значительно расширяя его диапазон и снижая потери. Антенны с бóльшим коэффициентом усиления могут улучшить прием и передачу данных на большие расстояния.

2. Повышенная мощность передатчика: увеличение мощности радиосигнала обеспечивает связь на большие расстояния и улучшает проникновение сигнала через препятствия. Однако это также влечет

за собой увеличение энергопотребления, что требует соблюдения баланса между мощностью передатчика и энергоэффективностью беспилотного летательного аппарата (БПЛА).

Спутниковая связь как альтернативное решение

Для расширения возможностей системы связи с беспилотными летательными аппаратами (БПЛА) спутниковая связь предлагает мощную альтернативу. Эта технология обеспечивает глобальное покрытие и надежную связь, что имеет решающее значение для операций в отдаленных и труднодоступных районах [3].

Расширение возможностей системы связи с БПЛА (беспилотным летательным аппаратом) открывает новые возможности для ее применения в критических и стратегически важных задачах по всему миру. Текущие исследования и разработки в этой области по-прежнему являются главным приоритетом для исследователей и инженеров, стремящихся максимально использовать потенциал передовых беспилотных технологий.

Список использованных источников

1. Иванов, И. И. Усовершенствование антенных систем для увеличения дальности связи БПЛА / И. И. Иванов, П. П. Петров. – М. : Технополис, 2023. – 210 с.

2. Смирнова, Е. А. Ретрансляторы и меш-сети в системах связи беспилотных летательных аппаратов / Е. А. Смирнова // Журнал телекоммуникационных исследований. – 2022. – № 4. – С. 34 – 42.

3. Васильев, В. В. Интеграция спутниковых технологий в системы связи БПЛА / В. В. Васильев, К. К. Михайлов. – СПб. : Политехника, 2021. – 176 с.

References

1. Ivanov, I. I. Improvement of antenna systems to increase the communication range of UAVs / I. I. Ivanov, P. P. Petrov. – M. : Technopolis, 2023. – 210 p.

2. Smirnova, E. A. Repeaters and mesh networks in communication systems of unmanned aerial vehicles / E. A. Smirnova // Journal of Telecommunication Research. – 2022. – No. 4. – P. 34 – 42.

3. Vasiliev, V. V. Integration of satellite technologies into UAV communication systems / V. V. Vasiliev, K. K. Mikhailov. – St. Petersburg : Polytechnic, 2021. – 176 p.

УДК 004.942

М. В. Волчихина
(ФГБОУ ВО «ТГТУ», г. Тамбов,
e-mail: mariyamoiseeva@mail.ru)

ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ЭЛЕМЕНТАМИ АГРОПРОМЫШЛЕННЫХ КОМПЛЕКСОВ

Аннотация. В современных условиях сотрудники коммерческих, в том числе, агропромышленных предприятий, различных организаций и компаний вынуждены проводить переговоры и обрабатывать конфиденциальную информацию в условиях, которые не обеспечивают защищенность конфиденциальной речевой информации на заданном уровне, определяемом нормативно-правовыми актами.

Ключевые слова: информационная безопасность, конфиденциальная информация, защита конфиденциальной информации, акустовибрационный канал утечки речевой информации.

M. V. Volchikhina
(TSTU, Tambov, Russia)

AN APPROACH TO ENSURING THE PROTECTION OF SPEECH INFORMATION WHEN MANAGING ELEMENTS OF AGRO-INDUSTRIAL COMPLEXES

Abstract. In modern conditions, employees of commercial enterprises, including agro-industrial enterprises, various organizations and companies are forced to conduct negotiations and process confidential information in conditions that do not ensure the security of confidential speech information at a given level determined by regulatory and legal acts.

Keywords: information security, confidential information, protection of confidential information, acoustic-vibrational channel of speech information leakage.

В существующих средствах защиты информации (СЗИ) отсутствует своевременный мониторинг параметров речевых сигналов субъектов переговоров, что снижает маскирующие свойства применяемых помеховых сигналов. Кроме того, задачи по снижению уровня шума, создаваемого СЗИ, стали ставиться и решаться относительно недавно, поэтому в настоящее время отсутствуют модели и алгоритмы для решения задачи защиты конфиденциальной речевой информации в офисном помещении от утечки по техническим каналам с учетом ограниченности контролируемой зоны офисного помещения, монито-

ринга изменения параметров речевых сигналов субъектов переговоров и необходимости соответствия уровня генерируемого помехового сигнала требованиям условий труда по уровню шума. Это обусловило отсутствие не только приемлемых организационных мер, препятствующих утечке конфиденциальной речевой информации, но и средств ее защиты от утечки по акустовибрационному каналу, в которых адаптивно меняется уровень и частотный диапазон генерируемого помехового сигнала в зависимости от изменения параметров речевых сигналов субъектов переговоров. В связи с этим разработан подход к сохранению бизнес-интересов организаций в нестандартных условиях, основанный на применении в СЗИ адаптивной речевой помехи [1]. Реализация данного подхода в СЗИ обеспечит надежную защиту конфиденциальной речевой информации от утечки по техническим каналам не только в офисном помещении, но и в нестандартных условиях (полуоткрытые, временные, мобильные офисы и т.п.).

В [1] обращено внимание на то, что в существующих ранее постановках задач на защиту конфиденциальной речевой информации (КРИ) не учитывалось, что в процессе переговоров меняется не только громкость речи субъектов переговоров, но и тембр, субъектами переговоров являются не только мужчины, но и женщины. В этой статье не указано, что то же самое относится и к изменению количества участников переговоров и смене языка их ведения. Это также должно учитываться при разработке модели адаптивной речеподобной помехи. Предельно допустимый интегральный уровень помехового сигнала должен соответствовать гигиеническим нормативам по уровню шума в офисном помещении и нормируется нормативно-правовыми актами, в частности, стандартом ИСО 3382 2009 «Измерение параметров акустики помещений», ГОСТ 30494–2011 «Акустика. Звукоизоляция помещений зданий», СНиП 23.03.2003 «Защита от шума».

Для реализации рассмотренного подхода к активной защите конфиденциальной речевой информации в офисном помещении от утечки по техническим каналам, построена математическая модель адаптивной речеподобной помехи (РПП), в которой учитывается разнообразие голосов субъектов переговоров, пол и возраст, количество и язык – т.е. изменение речевой обстановки и снижение интегрального уровня помехового сигнала в офисном помещении согласно требованиям нормативно-правовых актов по уровню шума при выполнении требований защищенности конфиденциальной информации.

В источнике [1] представлена постановка задачи и приведены математические выражения для модели адаптивной РПП. В данной статье эти математические выражения представлены в более удобном для понимания виде. Постановка задачи на разработку модели сфор-

мулирована следующим образом. Злоумышленник принимает смесь сигналов, состоящую из речевого сигнала $S(t)$, компенсирующей помехи $S'(t)$, обеспечивающей за счет сложения в противофазе с защищаемым сигналом снижение его амплитуды, адаптивной РПП $S_d^{\text{РПП}}(t)$ и помехового сигнала $g(t)$, обусловленного сторонними источниками акустического сигнала. После аналогово-цифровых преобразований, совокупность речевого и помеховых сигналов в виде их гармонических моделей с дискретным представлением во времени может быть записана следующим образом:

$$z_d(i\Delta t) = S_d(i\Delta t) + S'_d(i\Delta t) + S_d^{\text{РПП}}(i\Delta t) + g_d(i\Delta t), \qquad (1)$$

где $S_d(i\Delta t)$, $S'_d(i\Delta t)$, $S_d^{\text{РПП}}(i\Delta t)$ и $g_d(i\Delta t)$ – дискретное представление защищаемого речевого сигнала, компенсирующей помехи, РПП и помехового сигнала от сторонних источников в момент времени $t = i\Delta t,\ i = \overline{1, I},\ I = \dfrac{T}{\Delta t}$; T – время наблюдения сигнала; Δt – интервал дискретизации, с которым осуществляется аналогово-цифровое преобразование сигналов в ЭВМ,

$$S_d(i\Delta t) = \sum_{k=1}^{K} A_k(i\Delta t)\cos[\varphi_k(i\Delta t)]; \qquad (2)$$

$$S'_d(i\Delta t) = \sum_{k=1}^{K} B_k(i\Delta t)\cos[\varphi_k(i\Delta t) + \varphi_k(0) + \delta]; \qquad (3)$$

$$S_d^{\text{РПП}}(i\Delta t) = \sum_{n=1}^{N}\sum_{k=1}^{K} C_{kn}(i\Delta t)\cos[\varphi_k(i\Delta t) + \varphi_k(0) + \varphi_{kn}(i\Delta t)] + \sum_{n=1}^{N} r_n(i\Delta t); \qquad (4)$$

$$g_d(i\Delta t) = \sum_{k=1}^{K} G_k(i\Delta t)\cos[\varphi_k(i\Delta t)]; \qquad (5)$$

где $A_k(i\Delta t)$, $B_k(i\Delta t)$, $G_k(i\Delta t)$ – амплитуды k-й гармоники соответственно защищаемого речевого сигнала, компенсирующей помехи и помехи от сторонних источников в момент времени, равный $i\Delta t$; $C_{kn}(i\Delta t)$ – амплитуды k-й гармоники в n-м канале ($n = \overline{1, N}$) генератора РПП в момент времени, равном $i\Delta t$; $\varphi_k(i\Delta t)$ – фаза k-й гармонической составляющей звука, нарастающая с течением времени, в дискретном виде,

$$\varphi_k(i\Delta t) = \sum_{i=1}^{I} 2\pi f_k(i\Delta t) + \varphi_k(0), \qquad (6)$$

где $f_k(i\Delta t)$ – значение частоты k-й гармоники; $\varphi_k(0)$ – значение фазы k-й гармонической составляющей звука в начальный момент времени; $\varphi_{kn}(i\Delta t)$ – набег фазы k-й гармонической составляющей звука, обусловленный распространением сигнала в n-м канале генератора РПП; δ – параметр фазы, учитывающий задержку компенсирующей помехи относительно исходного сигнала, обусловленную различным пространственным положением генераторов компенсирующей помехи в помещении; $r_n(i\Delta t)$ – значение амплитуды шума дискретизации речевого сигнала в n-м канале генератора РПП, обусловленного аналогово-цифровым преобразованием сигнала; K – количество энергетически значимых (с ненулевой амплитудой) гармонических составляющих звука.

Оценка эффективности применения компенсирующей помехи осуществлялась по значению сигнала ошибки как индикатора качества процесса активного шумоподавления. Сигнал ошибки определялся как сумма исходного речевого сигнала и компенсирующей помехи.

Своевременный мониторинг сигнала ошибки позволяет изменять параметры компенсирующей помехи в процессе работы СЗИ. Эта процедура мониторинга сигнала ошибки положена в основу контроля качества процесса адаптации параметров помехового сигнала СЗИ к изменению параметров речевых сигналов субъектов переговоров [2].

Кроме того, использована модель активного шумоподавления, согласно которой противоположный сигнал (компенсирующая помеха) формируется за счет автоматической регулировки параметров этого сигнала относительно параметров речевого сигнала, исходящего от субъектов переговоров.

Формирование речеподобной помехи происходит путем преобразования исходного сигнала, поступающего на N линий задержек генератора РПП. Таким образом, для речеподобной помехи получено выражение:

$$S_{\text{РПП}}(N, k, i\Delta t) = \sum_{j=1}^{N} \sum_{k=1}^{K} A_{kj}(i\Delta t) \times$$
$$\times \cos\left(\sum_{i=1}^{i_{\max}} 2\pi f_k(i\Delta t) + \varphi_k(0) + \varphi_{kj}(i\Delta t) + \sum_{j=1}^{N} r_j(i\Delta t)\right), \qquad (7)$$

где j – порядковый номер канала в генераторе РПП; N – количество каналов в генераторе РПП; $A_{kj}(i\Delta t)$ – амплитуда k-й гармонической составляющей звука в j-м канале генератора РПП, дБ; $r_j(i\Delta t)$ – помехо-

вый сигнал, обусловленный другими (кроме участников переговоров) источниками акустического сигнала в j-м канале генератора РПП, дБ; $\varphi_{kj}(i\Delta t)$ – набег фазы, обусловленный распространением сигнала в j-м канале генератора РПП, рад.

РПП формируется на основе речевых сигналов, приходящих на вход СЗИ от каждого субъекта переговоров с различной фазовой задержкой ($\varphi_{kj}(i\Delta t)$).

Таким образом, разработанная модель адаптивной речеподобной помехи, представленная выражениями (1) – (7), реализует два параллельных процесса: формирование компенсирующей помехи и формирование речеподобной помехи. Модель адаптивной РПП обеспечивает подстройку параметров сигнала СЗИ в соответствии с изменениями параметров речи субъектов переговоров.

Процесс формирования адаптивной речеподобной помехи представлен следующими этапами:

– на микрофон подаются речевые сигналы субъектов переговоров $S(t)$, представленные выражением (2);

– из речевого сигнала, после аналого-цифрового преобразования, формируется речеподобная помеха $S_{\text{РПП}}(N, k, i\Delta t)$ в соответствии с выражением (6) путем наложения фрагментов скрываемого речевого сигнала с различными уровнями, поступающих с N каналов (достаточное количество каналов определено экспериментально);

– организуется процедура прерывания излучения помехового сигнала при отсутствии речевого;

– речеподобная помеха $S_{\text{РПП}}(N, k, i\Delta t)$ подается на звуковую карту ЭВМ, с линейного выхода которой она может быть подана или на звуковую колонку, или на внешний вход генератора шума средства акустовибрационной защиты.

В процессе исследования установлено оптимальное количество каналов, равное шести [2]. В ходе исследования получены спектры речевого сигнала и, синтезированной генератором, речеподобной помехи (рис. 1), а также временные диаграммы речеподобной помехи и ее смеси с исходным речевым сигналом (рис. 2). Результаты моделирования показали достаточную схожесть данных спектров. Также подтверждено, что спектральный состав речи в значительной степени зависит от пола, возраста и индивидуальных особенностей говорящего, а для различных людей отклонение уровней сигналов, измеренных в октавных полосах, от типовых уровней составило до 6 дБ.

Результаты исследования модели адаптивной РПП показали, что уровень РПП, при одинаковых показателях словесной разборчивости, значительно ниже уровня помеховых сигналов, используемых в современных СЗИ.

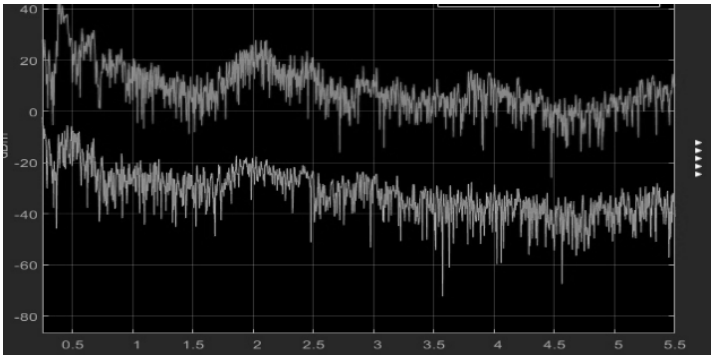


Рис. 1. Спектры речевого сообщения и речеподобной помехи

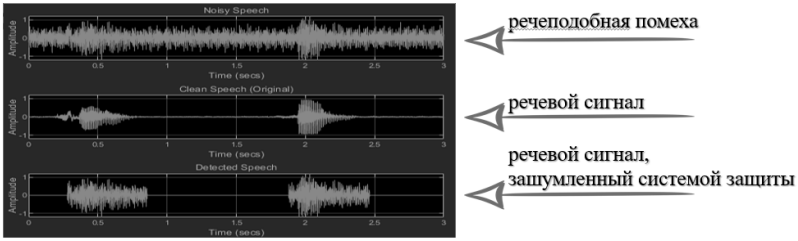


Рис. 2. Результаты исследования работы генератора речеподобной помехи

В процессе проведения натурного эксперимента установлено, что за счет разности хода волн исходного сигнала и помехи наблюдается небольшой сдвиг по фазе, вследствие чего возможна погрешность в 2…3°. Это было учтено, что обеспечило достижение поставленной цели моделирования.

Результат суммирования речевого и помехового сигналов, оцениваемый сигналом ошибки, показал практически нулевое его значение, что свидетельствует о подавлении адаптивной РПП речевого сигнала на границе контролируемой зоны.

Разработанную модель целесообразно применять в системах активной защиты речевой информации от утечки по акустовибрационному каналу в соответствии с нормативно-методическим документом по защите конфиденциальной информации СТР-К. В системе управления элементами агропромышленных комплексов разработанная модель обеспечивает скрытность управления и сохранение коммерческой тайны.

Список литературы

1. Волчихина, М. В. Модель адаптации параметров средства защиты информации к параметрам речи субъектов переговоров в помещении офисного типа / М. В. Волчихина, А. В. Фурсова // Вестник Воронежского института МВД. – 2024. – № 1. – С. 108 – 115.
2. Азаров, И. С. Непрерывное и дискретное гармонические преобразования для декомпозиции речевого сигнала на периодическую и шумовую компоненты / И. С. Азаров, А. А. Петровский // Доклады БГУИР. – Минск : БГУИР, 2008. – № 4(34). – С. 92 – 105.
3. Волчихина, М. В. Метод адаптации параметров средств защиты информации на основе дискретного изменения амплитуды и тембра субъектов переговоров / М. В. Волчихина // Вестник Тамбовского государственного технического университета. – 2022. – Т. 28, № 2. – С. 226 – 234.

References

1. Volchikhina, M. V. Model of adaptation of parameters of information security tool to speech parameters of subjects of negotiations in an office-type room / M. V. Volchikhina, A. V. Fursova // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs. – 2024. – No. 1. – P. 108 – 115.
2. Azarov, I. S. Continuous and discrete harmonic transformations for decomposition of speech signal into periodic and noise components / I. S. Azarov, A. A. Petrovsky // Reports of BSUIR. – Minsk : BSUIR, 2008. – No. 4(34). – P. 92 – 105.
3. Volchikhina, M. V. Method of adapting the parameters of information security tools based on discrete changes in the amplitude and timbre of negotiating parties / M. V. Volchikhina // Bulletin of TSTU. – 2022. – V. 28, No. 2. – P. 226 – 234.

УДК 681.5

В. С. Блаженов[1], Шамсулдин Хайдар Абдулваххаб Х.[2], Алмали Ахмед Аднан Латиф[2]
([1]Кафедра КБ-1 «Защита информации»,
РТУ МИРЭА, Москва, Россия);
[2]г. Багдад, Ирак)

РЕГУЛИРОВАНИЕ И СТАНДАРТЫ БЕЗОПАСНОСТИ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрен подход к регулированию и стандартам безопасности в сфере агропромышленного комплекса. Приведены примеры стандартов, дана их краткая характеристика.

Ключевые слова: безопасность, стандарты, агрокомплекс, защита информации.

V. S. Blazhenov[1], Shamsuldaeen Haidar Abdulwahhab H.[2], Almali Ahmed Adnan Lateef
([1]Department of Information Security,
RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq)

REGULATION AND SAFETY STANDARDS IN THE AGRICULTURAL SECTOR

Abstract. An approach to the regulation and safety standards in the agricultural sector is considered. Examples of standards are given and their brief characteristics are given.

Keywords: safety, standards, agricultural complex, information protection.

Введение. Агропромышленный комплекс (АПК) является одной из ключевых отраслей экономики многих стран, обеспечивающей продовольственную безопасность и устойчивое развитие. В условиях глобализации, изменения климата, а также изменения политической обстановки вопрос безопасности в АПК становится все более актуальным. Регулирование и стандарты безопасности играют важную роль в обеспечении стабильной работы и качества продукции АПК.

В настоящее время практически каждое производство имеет собственную ИТ-инфраструктуру, которая требует непрерывного обеспечения информационной безопасности. Метрики, по которым будут определяться критерии защищенности и степень их выполнения, описываются в различных документах. В перечень этих документов могут

входить как нормативные и нормативно-правовые акты, так и внутренние стандарты компаний, которые конкретизируют общую документацию.

Исходя из вышесказанного, можно утверждать, что для обеспечения требуемого уровня безопасности, следует провести исследование широкого набора стандартов, соответствующих отрасли и общих стандартов для построения системы информационной безопасности.

Регулирование безопасности. Система регулирования безопасности в агропромышленном комплексе включает в себя как международные, так и национальные, нормы и стандарты. На международном уровне важную роль играют такие организации, как Всемирная организация здравоохранения (ВОЗ) и Продовольственная и сельскохозяйственная организация ООН (ФАО). Эти организации разрабатывают рекомендации и практические руководства, которые помогают странам адаптировать свои законодательства к международным требованиям.

На национальном уровне регулирование безопасности в агропромышленном комплексе осуществляется через различные государственные структуры и министерства, которые разрабатывают законы и постановления, касающиеся производства, переработки и продажи сельскохозяйственной продукции.

Стандарты безопасности в АПК определяют несколько ключевых аспектов:

– безопасность процесса производства. Данный аспект объединяет все меры по защите процесса производства и обеспечения информационной безопасности компании, осуществляющей деятельность в составе агропромышленного комплекса.

– безопасность продукции (пищевых продуктов). В России основным документом, регламентирующим безопасность пищевых продуктов, является Федеральный закон «О качестве и безопасности пищевых продуктов». Данный Федеральный закон устанавливает требования к производственным процессам, контроль за качеством и безопасностью, а также ответственность за нарушение норм.

Примеры стандартов. Начальным шагом для обеспечения информационной безопасности можно назвать проектирование и создание системы менеджмента информационной безопасности (далее – СМИБ) в организации. Требования и меры по созданию и поддержанию СМИБ устанавливаются в семействе международных стандартов ГОСТ Р ИСО/МЭК 27000, которое состоит из множества документов. Рассмотрим некоторые из них.

– ГОСТ Р ИСО/МЭК 27001–2021.

Стандарт устанавливает общие требования по созданию, внедрению, поддержке и постоянному улучшению СМИБ в контексте деятельности организации. Стандарт также содержит требования по оценке и обработке рисков информационной безопасности с учетом потребностей организации.

– ГОСТ Р ИСО/МЭК 27002–2021.

В настоящем стандарте содержатся рекомендации по созданию и практическому использованию в организации СМИБ, включая вопросы выбора, внедрения и применения полноценного набора мер обеспечения ИБ, соответствующих совокупности имеющихся в данной организации рисков ИБ.

– ГОСТ Р ИСО/МЭК 27003–2021.

Настоящий стандарт содержит руководство по реализации требований к СМИБ, приведенных в ИСО/МЭК 27001, и предоставляет рекомендации, возможности и допустимое действие в отношении этих требований.

Данное семейство стандартов содержит множество документов, представленные в данной статье документы являются основными, но в случае возникновения вопросов по содержанию мер или требований существует возможность обратиться к прочим представителям семейства этих стандартов.

В процессе проектирования и создания СМИБ следует учитывать такое характерное условие компаний агропромышленного комплекса как бизнес-ориентированность. Достижение равномерно высокой зрелости ИБ по всем бизнесам компании может потребовать итерационного подхода к разработке СМИБ и составления бизнес-ориентированной модели СМИБ.

Вывод. Регулирование и стандарты безопасности имеют большое влияние на построение процессов в компаниях агропромышленного комплекса. Но несмотря на обширность нормативной базы каждый случай требует индивидуального подхода к использованию описанных в стандартах мер и способов их реализации.

Список использованных источников

1. Балджи, Ю. А. Современные аспекты контроля качества и безопасности пищевых продуктов : монография / Ю. А. Балджи. – М. : Лань, 2019.

2. Официальный сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р ИСО/МЭК 27001–2021. – URL : https://protect.gost.ru/document1.aspx?control=31&id=242006

3. Официальный сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р ИСО/МЭК 27002-2021. – URL : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=1&year=2015&search=27002&id=240766

4. Официальный сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р ИСО/МЭК 27003-2021. – URL : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=496&month=3&year=2015&search=%D0%93%D0%BE%D1%81%D1%82&id=240709

References

1. Balji, Yu. A. Modern aspects of quality control and food safety : monograph / Yu. A. Balji. – M. : Lan, 2019.

2. Official website of the Federal Agency for Technical Regulation and Metrology GOST R ISO/IEC 27001-2021. – URL : https://protect.gost.ru/document1.aspx?control=31&id=242006

3. Official website of the Federal Agency for Technical Regulation and Metrology GOST R ISO/IEC 27002-2021. – URL : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=0&month=1&year=2015&search=27002&id=240766

4. Official website of the Federal Agency for Technical Regulation and Metrology GOST R ISO/IEC 27003-2021. – URL : https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=496&month=3&year=2015&search=%D0%93%D0%BE%D1%81%D1%82&id=240709

УДК 681.5

С. В. Артемова, Д. А. Потапова, П. И. Карасев, В. Е. Бушуев
(Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: potapova.daria1998@yandex.ru, bushuev.v.e@edu.mirea.ru)

ОСНОВНЫЕ КИБЕРУГРОЗЫ ДЛЯ ПРЕДПРИЯТИЙ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Аннотация. Рассмотрены цели киберпреступников при атаках на чувствительные области агропромышленного комплекса. Приводятся примеры кибератак и их последствия. Даны рекомендации по снижению киберугроз.

Ключевые слова: кибератака, киберугроза, злоумышленник, получение финансовой выгоды, программа-шифровальщик, кража.

S. V. Artemova, D. A. Potapova, P. I. Karasev, V. E. Bushuev
(Department of Information Security,
RTU MIREA, Moscow, Russia)

THE MAIN CYBER THREATS TO ENTERPRISES IN THE AGRO-INDUSTRIAL COMPLEX AND WAYS TO PREVENT THEM

Abstract. The article examines the goals of cybercriminals when attacking sensitive areas of the agro-industrial complex. Examples of cyber attacks and their consequences are given. Recommendations for reducing cyber threats are given.

Keywords: cyber attack, cyber threat, intruder, obtaining financial benefits, encryption program, theft.

Киберугроза – это любая потенциальная угроза, направленная на нарушение конфиденциальности, целостности и доступности информационных систем, сетей и данных.

Киберугрозы могут исходить от хакеров, инсайдеров, преступных группировок и даже сотрудников организации. Основные виды киберугроз:

- Вредоносное ПО: вирусы, черви, трояны, шпионские программы, вымогатели, которые наносят ущерб, уничтожают данные или предоставляют несанкционированный доступ.
- Фишинг: попытки мошенников получить конфиденциальную информацию, например, пароли, путем маскировки вредоносных файлов или ссылок.

- Атаки типа «отказ в обслуживании»: перегружают системы, делая их недоступными для пользователей.
- Кража данных: несанкционированное копирование и использование конфиденциальных данных.
- Социальная инженерия: манипуляции, чтобы получить информацию путем обмана пользователей.

Для предприятий агропромышленного комплекса по статистике основными киберугрозами являются:

1. Программы-вымогатели: блокируют доступ к системе или данным, требуя выкуп для разблокировки.
2. Вредоносные почтовые рассылки: фишинговые письма, маскирующиеся под сообщения от популярных брендов или сервисов, ведущие на вредоносные сайты.
3. Атаки на корпоративные сети: несанкционированный доступ к конфиденциальной информации через социальную инженерию, вирусы или уязвимости в безопасности.
4. Утечки баз данных компаний: несанкционированная передача конфиденциальных данных из базы данных компании третьим лицам.
5. Атаки, связанные с взломом датчиков: нарушение работы датчиков, что может привести к сбоям в производственных процессах и финансовым потерям.

Основные цели злоумышленников при кибератаках на предприятия агропромышленного комплекса:

1. Промышленный шпионаж. Злоумышленники пытаются выяснить, что производят в компании, кому продают, в каком количестве, основные цепочки поставок и так далее, все это делается с целью передачи информации конкурентам.
2. Получение финансовой выгоды. Злоумышленники пытаются получить доступ к системам управления производственными процессами, а также к персональным данным и документам, содержащим конфиденциальную информацию, после чего начинают шантажировать руководство.
3. Нарушение работы предприятия. Злоумышленники оказывают воздействие на технологический процесс с целью приостановки работы предприятия – например, останавливают станок, меняют температуру воздуха в холодильнике или вызывают аварию при помощи перегрева оборудования.

Вот несколько примеров кибератак злоумышленников на предприятия агропромышленного комплекса РФ:

1. В марте 2022 года агрохолдинг «Мираторг» подвергся атаке шифровальщика BitLocker. В результате этой атаки были зашифрова-

ны файлы, которые использовали 18 предприятий компании, и они долгое время не могли оформлять производственные и транспортные ветеринарные документы на продукцию.

2. Уже в марте 2023 в Ростовской области в результате атаки была временно остановлена работа завода «Тавр». Вредоносным программным обеспечением были атакованы серверы, рабочие станции, информационные системы предприятия.

3. В феврале 2023 злоумышленники попытались испортить 40 т продукции в агрохолдинге «Селятино»: получив несанкционированный доступ к ключевым системам, преступники изменили температуру хранения замороженной продукции на плюсовую.

4. В качестве примера атаки программы шифровальщика, показателен случай, который произошел на «Агрокомплексе им. Н. И. Ткачева». В апреле 2024 года все IT-системы компании подверглись атаке. Инцидент привел к краже и шифрованию данных на серверах организации. В результате сайт агрокомплекса не работал 8 и 9 апреля. По мнению экспертов, целью хакеров была не только остановка работы организации, но и выкуп за украденные данные. Запрос составил около 500 миллионов рублей. Доступ к данным агрокомплекса мог быть получен через фишинг, уязвимости в публичных приложениях или протокол удаленного рабочего стола.

Чтобы предотвратить кибератаки на агропромышленный комплекс, можно предпринять следующие меры:

1. Обучить сотрудников основам кибербезопасности. Также регулярно проводить тренинги, чтобы привить сотрудникам полезные привычки: проверять ссылки, адреса электронной почты, хорошо подумать, прежде чем отправлять конфиденциальную информацию.

2. Создать резервные копии данных. Это позволит, даже в случае нарушения информационной безопасности предприятия и потере или зашифровке чувствительных данных, выйти предприятию «сухим из воды». Такие копии должны быть изолированы от исходных файлов, чтобы злоумышленники не смогли зашифровать их при своей атаке.

3. Сегментировать сеть. Логически разделенные части корпоративной инфраструктуры могут быть изолированы в случае обнаружения подозрительной активности в одной части сети. Это позволит в гораздо быстрые сроки полностью вернуть сеть в работу.

4. Регулярно исправлять и обновлять программное обеспечение, такое как антивирусы и сетевые экраны. При выявлении уязвимостей в компьютерных системах и программном обеспечении вендоры регулярно дорабатывают их и обновляют системы для защиты своих клиентов.

5. Внедрить оптимальную политику паролей. Сотрудникам следует использовать надежные пароли, состоящие из букв, цифр и специальных символов, а также чаще обновлять их. Рекомендуется внедрить многофакторную аутентификацию для предотвращения несанкционированного доступа к устройствам и, по возможности, использовать биометрические системы контроля доступа.

Список использованных источников

1. Вострецова, Е. В. Основы информационной безопаснсти : учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал, ун-та, 2019. – С. 68 – 79.

2. F.A.C.C.T. защитит мясокомбинаты от кибератак // anti-malware.ru. – URL : https://www.anti-malware.ru/success_stories/2023-05-26/41262 (дата обращения: 07.09.2024).

3. Top Russian meat producer hit with Windows BitLocker encryption attack // bleepingcomputer.com. – URL : https://www.bleepingcomputer.com/news/security/top-russian-meat-producer-hit-with-windows-bitlocker-encryption-attack/ (дата обращения: 07.09.2024).

References

1. Vostretsova, E. V. Fundamentals of information security : a tutorial for university students / E. V. Vostretsova. – Ekaterinburg : Ural University Publishing House, 2019. – P. 68 – 79.

2. F.A.C.S.T. will protect meat processing plants from cyber attacks // anti-malware.ru. – URL : https://www.anti-malware.ru/success_stories/2023-05-26/41262 (accessed: 09/07/2024).

3. Top Russian meat producer hit with Windows BitLocker encryption attack // bleepingcomputer.com. – URL : https://www.bleepingcomputer.com/news/security/top-russian-meat-producer-hit-with-windows-bitlocker-encryption-attack/ (date of access: 09/07/2024).

УДК 681.5

А. В. Виноградский[1], Мустафа Абдулкадим Дхаир Аль-Амиди[2], Аль-Судани Зайд Али Хуссейн[2]
([1]Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия;
[2]г. Аль-Кадисия, Ирак)

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ В СФЕРЕ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Рассмотрены основные проблемы безопасности при применении технологии Интернета вещей в Агропромышленном комплексе, а также возможные негативные последствия, которые могут быть вызваны данными проблемами.

Ключевые слова: умный сад, технологии в агропромышленном комплексе, Интернет вещей, IoT.

A. V. Vinogradskiy[1], Mustafa Abdulkadhim Dhahir Al-Ameedee[2], Al-Soudany Zaid Ali Hussein[2]
([1]Department of Information security
RTU MIREA, Moscow, Russia;
[2]Al-Qadisiyah, Irag)

SECURITY PROBLEMS OF THE INTERNET OF THINGS IN THE FIELD OF AGRO-INDUSTRIAL COMPLEX

Abstract. An approach to the construction of an intensive garden management system using LoRa wireless technology is considered. The used technical means are given, their brief characteristic is given.

Keywords: smart garden, technologies in agro-industrial complex, Internet of Things, IoT.

Введение. Интернет вещей (IoT) как технология стремительно проникает в различные отрасли и сферы. Идея создания «умного сада», а также использования «умных» устройств в агропромышленном комплексе уже давно не является чем-то новым. Умные сенсоры, устройства мониторинга и автоматизированные системы управления могут значительно повысить эффективность в сельскохозяйственной промышленности. Технология Интернета вещей способна значительно упростить многие процессы в сфере аграрной промышленности, но также данная технология создает большой простор для проблем с информационной безопасностью. В данной статье будут рассмотре-

ны основные проблемы, связанные с безопасностью IoT в агропромышленном комплексе.

Уязвимости устройств – одна из основных проблем, свойственных технологии Интернета вещей. Здесь серьезную роль играет экономия производителей на безопасности. Заинтересованность производителей, в первой очередь в разработке устройств за наименьшую себестоимость в кратчайшие сроки. Так как такой продукт направлен на массового потребителя, не погруженного в вопросы безопасности, большинство производителей просто пренебрегают внедрением достаточных ресурсов и систем безопасности, в силу их дороговизны. По тем же причинам многие устройства Интернета вещей имеют ограниченные ресурсы, что затрудняет последующее внедрение сложных механизмов защиты. Часто они используют устаревшие операционные системы или программное обеспечение с известными уязвимостями. Это делает их легкой мишенью для злоумышленников, которые могут получить доступ к системам управления и манипулировать ими. Данная проблема особенно актуальна на крупных агропромышленных предприятиях, где нарушение работы даже одного устройства может сильно повлиять на процессы.

Сбор и передача данных – это ключевые аспекты работы IoT в агросекторе. Безопасность этих данных закономерно часто оказывается под угрозой. Исходя из слабой защищенности и значительных объемов информации в IoT-системах, технология представляет большую область для возможных утечек информации. Такая информация, как необработанные данные о состоянии почвы, погодных условиях или здоровье животных могут быть перехвачены, что может привести к утечке конфиденциальной информации. Все это может привести к промышленному шпионажу со стороны конкурентов и даже к последующим финансовым потерям для фермеров.

Существуют также серьезные инфраструктурные риски. Интернет вещей в агропромышленном комплексе зависит от сложной инфраструктуры, включающей в себя облачные сервисы и локальные сети. Атаки на эти инфраструктуры могут привести к серьезным сбоям в работе как отдельных устройств, так и целой экосистемы. Самым простым примером послужит ситуация, если злоумышленники получат доступ к центральной системе управления экосистемой, тогда они могут отключить полив или нарушить температурный режим, что повредит урожай.

Очевидным решением для обеспечения безопасности является создание нормативов, которым должны соответствовать IoT-системы. В сфере IoT существует проблема отсутствия законодательных актов,

норм, стандартов и правил. На данный момент практически отсутствуют стандарты и законодательные акты, которые могли бы урегулировать процесс создания безопасных устройств и их внедрения, что крайне затрудняет оценку рисков и выработку общих рекомендаций по защите. То же самое применимо и к процессу построения IoT-инфраструктур в агропромышленном комплексе, из-за чего крайне сложно обеспечить должный уровень безопасности даже на крупном агропромышленном предприятии. Без четких регуляторных норм и стандартов агробизнесы рискуют сталкиваться с различными угрозами, которые могут привести к потере данных или даже саботажу операций.

Одной из актуальных проблем также является проблема совместимости устройств. Существует большое разнообразие устройств и протоколов связи, используемых в IoT. Из-за такого разнообразия, а также отсутствия нормативов и стандартов по построению IoT-систем образуются серьезные проблемы для совместимости устройств, а также интеграции новых. Все эти факторы также затрудняют интеграцию систем безопасности и могут создавать «белые пятна», которые злоумышленники могут использовать для своих атак. Без стандартов безопасности и сертификации устройства могут оказаться уязвимыми.

Как и любая экосистема, IoT требует постоянного обслуживания и обновления. Данная концепция относительно нова и специалистов в области данной технологии недостаточно, при этом существующим специалистам часто не хватает знаний в области информационной безопасности, из-за чего даже настроенная правильно система может иметь множество проблем с безопасностью. Проблема обслуживания вызвана не только недостатком квалифицированных специалистов, но и сложностями с обеспечением безопасности ПО и при дальнейшем обновлении IoT-устройства. На данный момент только растет количество выпускаемых решений для IoT. Отсюда следует и следующая проблема – обеспечить безопасность при установке обновлений к IoT достаточно сложно, как правило специфика пользовательских интерфейсов, доступных пользователям, не позволяет использовать традиционные механизмы обновления.

Необходимо также учитывать и социальные аспекты внедрения IoT в агропромышленный комплекс. Большинство работников не имеют должных знаний и компетенций при работе с технологиями Интернета вещей. Этот фактор также часто усугубляется отсутствием необходимых мероприятий и правил в условиях агропромышленного сектора. Отсутствие правил и политики безопасности при работе

с IoT-устройствами вызывают значительные проблемы и увеличивают вероятность человеческого фактора при работе с IoT-устройствами.

Заключение. Технологии IoT предоставляют большой спектр возможностей для реализации полезных функций в сфере агропромышленного комплекса. Но несмотря на все преимущества, которые предоставляет Интернет вещей в агропромышленном комплексе, проблемы безопасности остаются актуальными и требуют значительного внимания. Концепция на данный момент крайне слабо защищена, и проблемы, которые могут возникнуть в процессе ее эксплуатации могут быть очень серьезны при применении ее в сфере агропромышленного комплекса. Для решения этих проблем нобходимо разрабатывать и внедрять комплексные меры по защите устройств и данных, обеспечивать обучение сотрудников и проводить соответствующие мероприятия в области кибербезопасности и сотрудничать с производителями оборудования для улучшения безопасности их продуктов. Только так можно будет минимизировать риски и обеспечить устойчивое развитие IoT-технологий в агропромышленном комплексе.

Список использованных источников

1. Мырзабекова, А. М. Обзор современных систем для хранения зерновых культур / А. М. Мырзабекова // Информационно-измерительная техника и технологии : материалы VI науч.-практ. конф. – Томск : Изд-во ТПУ, 2015. – С. 95 – 101.

2. Федотов, Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М. : Юридический Мир, 2007. – 432 с.

3. Росляков, А. В. Интернет вещей : учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. – Самара : ПГУТИ, 2015. – 136 с.

References

1. Myrzabekova, A. M. Review of modern systems for storing cereals, Information and measuring equipment and technologies : materials of the VI scientific-practical conference / A. M. Myrzabekova. – Tomsk : Publishing house TPU, 2015. – P. 95 – 101.

2. Fedotov, N. N. Forensics – computer forensics / N. N. Fedotov. – M. : Yuridicheskiy Mir, 2007. – 432 p.

3. Roslyakov, A. V. Internet of Things : textbook / A. V. Roslyakov, S. V. Vanyashin, A. Yu. Grebeshkov. – Samara : PGUTI, 2015. – 136 p.

УДК 004.94

Г. В. Гвасалия[1], П. И. Карасев[1], Г. Ш. Утешева[2], Алмали Ахмед Аднан Латиф[3]
([1]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия,
e-mail: gvasaliagv@bk.ru, karasev@mirea.ru;
[2]Западно-Казахстанский инновационно-технологический
университет, г. Уральск, Казахстан;
[3]г. Багдад, Ирак)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УМНЫХ ФЕРМЕРСКИХ ХОЗЯЙСТВАХ: СТРАТЕГИИ ЗАЩИТЫ ДАННЫХ IoT-УСТРОЙСТВ

Аннотация. Рассмотрены вопросы обеспечения информационной безопасности Интернет вещей агропромышленного комплекса и отдельных ферм. Приведены основные угрозы, уязвимости, которые могут возникнуть на устройствах, в сети и внутренней инфраструктуре комплекса. Также обсуждаются рекомендации по повышению уровня информационной безопасности в условиях цифровизации агропромышленного комплекса. В качестве дополнительных мер защиты рассматриваются многофакторная аутентификация (MFA) и политика создания надежных паролей.

Ключевые слова: интернет вещей, политика паролей, агропромышленный комплекс, информационная безопасность, защита информации.

G. V. Gvasalya[1], P. I. Karasev[1], G. S. Uteseva[2], Almali Ahmed Adnan Lateef[3]
([1]Department of Information Systems and Information Protection,
RTU MIREA, Moscow, Russia;
[2]West Kazakhstan University of Innovation
and Technology, Uralsk, Kazakhstan;
[3]Baghdad, Iraq)

DIGITALIZATION OF PERMACULTURE PLANTATIONS

Abstract. The article discusses the issues of ensuring the information security of the Internet of Things of the agro-industrial complex and individual farms. The main threats and vulnerabilities that can occur on devices, in the network and in the internal infrastructure of the complex are presented. Recommendations on improving the level of information security in the context of digitalization of the agro-industrial complex are also discussed. Multi-factor authentication (MFA) and a strong password creation policy are considered as additional security measures.

Keywords: Internet of Things, password policy, agro-industrial complex, information security, information protection.

Введение. Информационные технологии активно, но поспешно внедряются в аграрную промышленность, чтобы оптимизировать ее и сделать фермерское хозяйство более умным. Эти хозяйства используют различные устройства Интернета вещей (IoT) и внутреннюю сеть, которая обеспечивают сбор, обработку и передачу данных, автоматизируя и упрощая процесс. Однако с ростом таких устройств и внутренней сети в различных фермах и в агропромышленном комплексе возникает проблема их безопасности и безопасности данных.

Угрозы и уязвимости интеллектуальных систем. Интеллектуальные системы, используемые в агропромышленном комплексе, как и любые системы, основанные на технологиях Интернета вещей (IoT), подвержены множеству угроз и уязвимостей. Угрозы, возникающие в агропромышленном комплексе, повреждают, ограничивают или изменяют информацию, которая хранится на устройствах и во внутренней сети. Атаки на устройства происходят с помощью незащищенных соединений, из-за устаревшего программного обеспечения, низкого уровня политики создания паролей и отсутствия дополнительной аутентификации. Недостаточная защищенность данных может быть использована как внутренним, так и внешним нарушителем, который может повредить автоматизированный процесс в агропромышленном комплексе.

Методы защиты интеллектуальных систем. Для эффективной защиты интеллектуальных систем, используемых в агропромышленном комплексе, необходимо внедрение комплексного подхода, который включает технические и организационные меры, связанные с политикой создания паролей и дополнительной аутентификации. На данный момент пароль, состоящий из восьми символов с цифрами и буквами в разных регистрах можно забрутфорсить за 60 часов, но если добавить знаки препинания и различные символы, которые есть на клавиатуре, то время подбора пароля увеличиться до 70 дней, что составляет 2700%.

Вторым вариантом для защиты информации в сети и на устройствах может послужить многофакторная аутентификация, которая может состоять из пароля с рисунком, отпечатком пальцев или любой модальностью, которая зарегистрирована для идентификации человека в Российской Федерации и в Единой биометрической системе. Эти методы повысят эффективность защиты и снизят риски утечек информации.

Примеры успешной защиты интеллектуальных систем в агропромышленном комплексе. Одним из примеров является проект «Умные теплицы» в Китае: В Китае реализован проект умных теплиц,

где системы управления климатом и поливом интегрированы с IoT-устройствами. В качестве защиты активно используются политика создания паролей и дополнительная аутентификация, которые позволяют выявлять аномалии в работе оборудования и предотвращать потенциальные кибератаки.

Заключение. Информационная безопасность в агропромышленном комплексе становится все более важным аспектом при цифровизации и внедрении технологий Интернета вещей. В условиях растущего количества угроз и уязвимостей необходимо внедрять комплексные меры защиты, которые включают создания политики паролей и внедрение дополнительной аутентификации. Примеры успешной защиты интеллектуальных систем показывают, что применение современных решений и подходов позволяет снизить риски и повысить надежность работы фермерских хозяйств.

Список использованных источников

1. IoT Internet of Things, Jade Carter (accessed 05.09.2024).

2. Authentication Theory and practice of ensuring secure access to information resources, A. A. Afanasyev, L. T. Veenyev, A. A. Voronov, E. R. Gazizova, A. L. Dookhov, A.V. Kryashkov, O. Y. Poyanskaya, A. G. Sabanov, M. A. Skiäa, S. N. Khayyapin, A. A. Sheupanov (accessed: 05.09.2024).

3. Chudosvetova, D. Y. The potential of permaculture for the development of agriculture / D. Y. Chudosvetova // Sustainable development of rural areas: the view of young scientists : materials of the All-Russian Scientific and Practical Conference of Young Scientists (December 10 – 12, 2020) – Novosibirsk : Novosibirsk State Agrarian University un-t. − 2020. – 112 p.

4. Durdymyadov Allamyrat, Toylyev Nurmukhammet, Gurbanberdiev Gurbanberdi. Main characteristics of soil types in agriculture / Durdymyadov Allamyrat // IN SITU. – 2023. – No. 10.

5. Abdusalamova, R. R. Soil Resources of Russia / R. R. Abdusalamova, Z. M. Balamirzoeva // Herald of Sleep. – 2020. – No. 1(33).

УДК 681.5

А. А. Двойных[1], Мустафа Абдулкадим Дхаир Аль-Амиди[2], Шамсулдин Хайдар Абдулваххаб Х.[3]
([1]Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия;
[2]г. Аль-Кадисия, Ирак;
[3]г. Багдад, Ирак)

УСТОЙЧИВОСТЬ АГРОПРЕДПРИЯТИЙ К КИБЕРАТАКАМ: УГРОЗЫ И ПРИЕМЫ ПО ИХ ПРЕДОТВРАЩЕНИЮ

Аннотация. Рассмотрена важность устойчивости агропредприятий к кибератакам в условиях цифровизации агропромышленного комплекса. Обсуждены основные угрозы, с которыми сталкиваются компании, и предлагаются практические рекомендации для повышения уровня кибербезопасности.

Ключевые слова: кибератаки, агропредприятие, безопасность, сельское хозяйство.

A. A. Dvoynykh[1], Mustafa Abdulkadhim Dhahir Al-Ameedee[2], Shamsuldaeen Haidar Abdulwahhab H.[3]
(Department of Information security,
RTU MIREA, Moscow, Russia;
[2]Al-Qadisiyah, Irag;
[3]Baghdad, Iraq)

RESILIENCE OF AGRICULTURAL ENTERPRISES TO CYBER ATTACKS: THREATS AND TECHNIQUES FOR THEIR PREVENTION

Abstract. The article discusses the importance of the resistance of agricultural enterprises to cyber attacks in the context of digitalization of the agro-industrial complex. The main threats that companies face are discussed and practical recommendations are offered to improve the level of cybersecurity.

Keywords: cyber attacks, agribusiness, security, agriculture.

Введение. Продолжительное время сельское хозяйство не было бизнесом, привлекательным для инвесторов, в связи с длинным производственным циклом, подверженным природным рискам и большим потерям урожая при выращивании, сборе и хранении, невозможностью автоматизации биологических процессов и отсутствием прогресса в повышении производительности и инноваций. Использование ИТ в сельском хозяйстве ограничивалось применением компьютеров и ПО

в основном для управления финансами и отслеживания коммерческих сделок. Не так давно фермеры начали использовать цифровые технологии для мониторинга сельскохозяйственных культур, домашнего скота и различных элементов сельскохозяйственного процесса. В настоящее время агропредприятия сталкиваются с возрастающей угрозой кибератак, что обусловлено стремительной цифровизацией сельского хозяйства. Внедрение современных технологий, таких как Интернет вещей, автоматизация процессов и использование больших данных, значительно улучшает эффективность и продуктивность в агросекторе.

Агробизнес в России достиг определенной зрелости, о чем свидетельствуют стабилизация уровня инвестиций в сельское хозяйство и рост конкуренции среди производителей сельхозпродукции. Но у повышения уровня автоматизации производственных и бизнес-процессов есть и обратная сторона – рост числа киберпреступлений, связанных с хищением данных, вымогательством и даже остановкой производственных циклов. Сложно представить себе более важный сектор экономики, чем сельское хозяйство. Эта отрасль оказывает прямое влияние на жизнь каждого жителя планеты. Именно поэтому зависимость мировой экономики от налаженных цепочек поставок продовольствия формирует фактор уязвимости и привлекает внимание хакеров.

Последствия кибератак на агропредприятие. *Экономические потери*: прямые финансовые убытки от атак могут быть значительными. Например, остановка производственных процессов или утечка конфиденциальных данных может привести к снижению доходов.

Ущерб репутации: потеря доверия со стороны клиентов и партнеров может иметь долгосрочные последствия для бизнеса. Репутационные потери могут затруднить привлечение новых клиентов и инвестиций.

Правовые последствия: нарушение законодательства о защите данных может привести к штрафам и юридическим издержкам. Агропредприятия обязаны защищать данные своих клиентов и сотрудников.

Для того, чтобы минимизировать ущерб от кибератак рассмотрим несколько приемов, которые могут быть актуальны в борьбе со злоумышленниками в аграрном секторе.

Развитие нужных компетенций у работников. Возможно, наиболее эффективной мерой является обучение своих сотрудников основам кибербезопасности. Подавляющее большинство кибератак начинается с применения методов социальной инженерии – для этого

в первую очередь используется электронная почта. За последнее время фишинговые письма стало трудно отличить от обычных легитимных электронных. Пользователи, которые были хорошо обучены в распознавании явных признаков вредоносных мейлов, составляют первый уровень защиты компании. Для повышения уровня знаний компании на регулярной основе проводят обучение в формате видеолекций с тестом для оценки знаний. В целях тренировки и проверки навыков случается, что внутренние службы компании целенаправленно отправляют среди сотрудников письма с подозрительными темой, адресом или содержимым: таким образом можно быстро определить, кому из сотрудников стоит пройти дополнительное обучение.

Резервное копирование данных. С помощью программ-вымогателей хакеры внедряют вредоносное ПО, предназначенное для блокировки доступа компаний к их критически важным данным. Регулярное создание резервных копий данных поможет восстановить информацию в случае кибератаки, такой как шифрование данных программами-вымогателями.

Сегментация сети. Отделяя технологические сети от локальных бизнес-сетей и дробя их на более мелкие части, ИТ-подразделения могут повысить уровень информационной безопасности компании. Логически разделенные части корпоративной инфраструктуры могут быть изолированы в случае обнаружения подозрительной активности в одной части сети. Даже сегментированная инфраструктура уязвима для вредоносных программ, внедряемых в один из сегментов сети, например, при обновлении программ. Однако сегментация может предотвратить распространение вредоносного ПО во всей компании

Использование антивирусного ПО на всех устройствах пользователей и в сети компании. Вредоносное ПО предназначено для нанесения ущерба, кражи данных, шифрования файлов или получения незаконного доступа к электронным системам. Среди таких «вредителей» – трояны, черви и программы-вымогатели. Для блокировки вредоносного ПО антивирусы используют механизм обнаружения сигнатур, поведенческий анализ и даже элементы искусственного интеллекта. Крайне важно, чтобы на каждом устройстве в сети, будь то персональный компьютер, ноутбук или смартфон, было установлено антивирусное ПО. В современном мире, где активно используется подход bring your own devices повсеместное внедрение таких средств защиты информации становится непростой задачей. Решение задачи требует комплексного подхода и хорошей осведомленности работников об опасности кибератак.

Регулярное исправление и обновление ПО. При выявлении уязвимостей в компьютерных системах и ПО вендоры регулярно дорабатывают их и обновляют системы для защиты своих клиентов. К сожалению, зачастую пользователи пренебрегают обновлением своих систем, что позволяет хакерам использовать недоработки ПО, уже «залеченные» доступными обновлениями.

Разработка плана реагирования на инциденты. Наличие четкого плана действий в случае кибератаки поможет быстро и эффективно реагировать на инциденты, минимизируя ущерб.

Экспертиза с привлечением сторонних компаний. Взаимодействие с компаниями, специализирующимися на кибербезопасности, может предоставить доступ к передовым технологиям и знаниям, что значительно повысит уровень защиты.

Заключение. Устойчивость агропредприятий к кибератакам является важной задачей в условиях растущей цифровизации сектора. Необходимость защиты информации и систем управления требует комплексного подхода, включающего обучение сотрудников, инвестиции в технологии и разработку стратегий реагирования на инциденты. Только так можно минимизировать риски и обеспечить стабильную работу агропромышленного комплекса в условиях современных вызовов.

Список использованных источников

1. URL : https://vc.ru/tech/571559-o-kiberbezopasnosti-v-selskom-hozyaistve – Информационная статья «О кибербезопасности в сельском хозяйстве» (дата обращения: 10.09.2024).

2. URL : https://www.tadviser.ru/index.php/Статья:Цифровизация_в_агропромышленном_ комплексе_России – Информационная статья «Цифровизация в агропромышленном комплексе России» (дата обращения: 10.09.2024).

3. URL : https://habr.com/ru/companies/radcop/articles/782398/ – Информационная статья «Нужна ли «Кибердеревне» кибербезопасность: ИИ, IoT и роботизация в сельском хозяйстве» (дата обращения: 10.09.2024).

References

1. URL : https://vc.ru/tech/571559-o-kiberbezopasnosti-v-selskom-hozyaistve – Information article “On cybersecurity in agriculture” (date of access: 09/10/2024).

2. URL : https://www.tadviser.ru/index.php/Article:Digitalization_in_the_agro-industrial_complex_of_Russia – Information article “Digitalization in the agro-industrial complex of Russia” (date of access: 09/10/2024).

3. URL : https://habr.com/ru/companies/radcop/articles/782398/ – Information article “Does the Cyber Village need cybersecurity: AI, IoT and robotization in agriculture” (date of access: 09/10/2024).

УДК 681.5

В. М. Дорошкевич[1], Г. Ш. Утешева[2],
Аль-Судани Зайд Али Хуссейн[3]
([1]Кафедра КБ-1 «Защита информации»,
РТУ МИРЭА, Москва, Россия;
[2]Западно-Казахстанский инновационно-технологический
университет, г. Уральск, Казахстан;
[3]г. Багдад, Ирак)

АНАЛИЗ СОВРЕМЕННЫХ КИБЕРУГРОЗ, С КОТОРЫМИ СТАЛКИВАЮТСЯ ПРЕДПРИЯТИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА, И СТРАТЕГИИ ИХ МИНИМИЗАЦИИ

Аннотация. Рассмотрены современные киберугрозы, относящиеся к агропромышленным комплексам, возможные потери и способы по минимизации рисков киберугроз.

Ключевые слова: агропромышленный комплекс, киберугрозы, минимизация киберугроз.

V. M. Doroshkevich[1], G. S. Utesheva[2],
Al-Soudany Zaid Ali Hussein[3]
([1]Department of Information security
RTU MIREA, Moscow, Russia;
[2]West Kazakhstan University of Innovation
and Technology, Uralsk, Kazakhstan;
[3]Baghdad, Iraq)

ANALYSIS OF MODERN CYBER THREATS FACED BY ENTERPRISES OF THE AGRO-INDUSTRIAL COMPLEX AND STRATEGIES FOR THEIR MINIMIZATION

Abstract. This article examines modern cyber threats related to agro-industrial complexes, possible losses and ways to minimize the risks of cyber threats.

Keywords: agro-industrial complex, cyber threats, minimization of cyber threats.

Введение. В последние годы агропромышленный комплекс стал одной из ключевых отраслей, активно использующих цифровые технологии для оптимизации процессов. Однако, с увеличением цифровизации, предприятия АПК сталкиваются с различными киберугрозами, которые могут нанести серьезный ущерб как экономически, так и репутационно. В данной статье будут рассмотрены основные киберугро-

зы, с которыми сталкиваются компании АПК, и предложения стратегии их минимизации.

В современном мире атаки на агропромышленные комплексы стали происходить чаще. Это связано с несколькими факторами, включая увеличение зависимости от цифровых технологий и глобальной геополитической напряженностью. В таких условиях необходимо принять ряд мер для защиты предприятий агропромышленного комплекса, чтобы не допустить проблем с продовольствием и товарами.

Атаки на АПК могут быть выполнены по следующим причинам:

1. Экономические интересы. В нынешнее время атаки на агропромышленные комплексы направлены для дестабилизации экономики. Успешная атака может привести к потерям и задержкам в поставках сельскохозяйственной продукции, что создаст проблемы как на внутреннем, так и на внешнем рынках, что негативно скажется на экономическом положении страны.

2. Уязвимость территорий. Сельское хозяйство считается уязвимой отраслью из-за изменений климата. Из-за зависимости от природных условий, агропромышленные комплексы могут быть подвержены атакам, направленным на уничтожение или заражение урожая, а также на распространение болезней среди животных и получаемых от них продуктов.

3. Технологические уязвимости. Злоумышленники нацеливаются на системы управления, с целью нарушения их работоспособности, что может повлиять на системы управления, которые контролируют производственные процессы, а также на программное обеспечение, используемое для мониторинга и анализа данных, вследствие чего, могут произойти сбои в производстве и логистике.

Данные атаки на агропромышленный комплекс могут быть осуществлены с помощью различных видов кибератак. Далее будут рассмотрены несколько основных примеров таких атак, их последствия, а также способы борьбы с ними.

DDoS-атака. Данные атаки направлены на перегрузку серверов и сетевой инфраструктуры, что приводит к недоступности разных сервисов. В агропромышленном комплексе это может привести к затруднению работы систем управления, что повлияет на производственные процессы и логистику. Например, данная атака на сервера может вызвать проблемы на этапе закупки товаров, оплаты или задержки в доставке продукции. Для борьбы с DDoS-атаками необходимо внедрять системы защиты, которые способны производить мониторинг трафика. Данные программы позволяют быстро реагировать на аномальное поведение трафика, что позволит быстро среагировать на них.

Также стоит настроить фильтрации трафика, которые позволяют блокировать подозрительные IP-адреса и типы трафика.

Фишинг и социальная инженерия. Данные атаки направлены на сотрудников компаний с целью получения их логинов и паролей к системам управления и программному обеспечению. Обычно сотрудникам компаний могут высылать письма на электронную почту, которые выглядят как официальные запросы от руководства, директора и других вышестоящих сотрудников компании. При переходе по ссылке из письма могут быть скомпрометированы данные для входа в систему сотрудника агропромышленного комплекса, вследствие чего может быть произведена утечка базы данных сотрудников, технических характеристик техники и устройств, установленных в производстве. Все это может привести к потере репутации, денег и штрафам. Для того чтобы избежать этого, следует обучить персонал, ввести программное обеспечение, которое не позволит открывать посторонние и подозрительные ссылки, фотографии и прочее. Для создания пароля также следует ввести правила, такие как: увеличение минимального числа символов, прописные и заглавные буквы, специальные символы. Также необходимо оставлять все личные устройства при входе в комплексы.

Внедрение вредоносного программного обеспечения. При заражении устройства, злоумышленник получает доступ к огромному количеству информации. Данные могут включить в себя финансовую информацию, электронные письма, пароли. В агропромышленном комплексе такие атаки могут привести к утечке данных о производственных процессов и технологиях, находящихся у данной компании. Также утечки могут привести к сбоям техники, что замедляет производство товара, что вызовет проблемы с поставками. Из-за этого, компания будет вынуждена потратить деньги на восстановление работы производства. Для защиты от вредоносного программного обеспечения следует внедрить современные системы безопасности, включая антивирусы и системы обнаружения вторжений. Обучение сотрудников также является необходимым этапом для предотвращения заражения вредоносным программным обеспечением, так как часто заражение происходит из-за открытия подозрительных ссылок или иных приложений из недостоверных источников.

Несанкционированный доступ к информации. Некоторые сотрудники, которые не согласны с начальством или недовольны заработной платой, могут использовать свои полномочия для доступа к разной информации, ее кражи и последующей продажи для получения прибыли. Такие действия могут нанести не только материальной ущерб,

но и репутационные риски, из-за чего компания может понести потери. Для предотвращения таких ситуаций следует создать ограничение доступа, чтобы получить информацию могли только определенные люди. Стоит ввести регулярные аудиты и мониторинги доступа, которые позволяют выявить подозрительную активность.

Заключение. В эпоху технологического прогресса и перехода агропромышленного комплекса на цифровые технологии, киберугрозы становятся более актуальными проблемами. Фишинг, DDoS-атаки, вредоносное программное обеспечение и другие уязвимости представляют собой важные аспекты, требующие внимания для обеспечения надежного производства и защиты. Для эффективного противодействия киберугрозам, предприятиям следует внедрят современные системы защиты. Регулярное обновление программного обеспечения, обучение персонала и создание резервных копий может существенного снизить риски, связанные с киберугрозами.

Список использованных источников

1. Хоружий, Л. И. Анализ и оценка рисков информационной безопасности организаций АПК / Л. И. Хоружий, Н. Ю. Трясцина, А. Ю. Данильченко // Бухучет в сельском хозяйстве. – 2018. – № 11. – С. 48 – 58.

2. Хоружий, Л. И. Анализ рисков предприятий АПК / Л. И. Хоружий, Н. Ю. Трясцина, Т. Ю. Крутова // Бухучет в сельском хозяйстве. – 2018. – № 1. – С. 72 – 80.

References

1. Khoruzhy, L. I. Analysis and assessment of information security risks of agro-industrial complex organizations / L. I. Khoruzhy, N. Yu. Tryastsina, A. Yu. Danilchenko // Accounting in agriculture. – 2018. – No. 11. – P. 48 – 58.

2. Khoruzhy, L. I. Risk analysis of agricultural enterprises / L. I. Khoruzhy, N. Yu. Tryastsina, T. Yu. Krutova // Accounting in agriculture. – 2018. – No. 1. – P. 72–80.

УДК 681.5

И. А. Елизаров[1], Д. Г. Дмитриев[1],
М. И. Елизарова[2], Т. А. Черемисин[3]
([1]Кафедра «Информационные процессы и управление»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]Институт компьютерных наук и кибербезопасности,
ФГАОУ ВО «СПбПУ Петра Великого», г. Санкт-Петербург, Россия,
e-mail: elial68@yandex.ru, 7ddg7@mail.ru, elizarova2002@ yandex.ru;
[3]МАОУ «Лицей № 6»)

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА MQTT ПРИ СОЗДАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ ОБОРУДОВАНИЯ НА ПРЕДПРИЯТИЯХ ПЕРЕРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

Аннотация. Рассмотрен подход к построению автоматизированной системы технического обслуживания и диагностики нештатных ситуаций с использованием протокола MQTT.

Ключевые слова: система мониторинга состояния оборудования, промышленный Интернет вещей IIoT, протокол MQTT.

I. A. Elizarov[1], D. G. Dmitriev[1],
M. I. Elizarova[2], T. A. Cheremisin[3]
([1]Department of Information Processes and Control,
TSTU, Tambov, Russia;
[2]Peter the Great SPbPU, St. Petersburg, Russia;
[3]Lyceum № 6)

THE USE OF THE MQTT PROTOCOL IN THE CREATION OF AUTOMATED EQUIPMENT MAINTENANCE SYSTEMS IN THE PROCESSING INDUSTRY

Abstract. An approach to the construction of an automated system for maintenance and diagnostics of emergency situations using the MQTT protocol is considered.

Keywords: equipment condition monitoring system, industrial Internet of Things, MQTT protocol.

Особенностью подавляющего большинства российских промышленных предприятий перерабатывающей промышленности является «лоскутная автоматизация». На предприятиях присутствует определенное количество разработанных в разное время, разными компаниями и практически несвязанных друг с другом локальных автоматизированных систем управления отдельными участками технологических

процессов. В то же время на этих предприятиях в результате «оптимизации» кадровых ресурсов наблюдается централизация служб, осуществляющих техническое обслуживание и ремонт технологического оборудования и средств автоматизации. Это приводит к существенному увеличению времени реагирования на поломки и нештатные ситуации.

При появлении неполадки или неисправности (например, выход из строя некоторого датчика в АСУТП), оператор (аппаратчик) фиксирует проблему. Далее информация передается вверх по инстанции, начальнику смены, далее начальнику цеха. Начальник цеха доводит информацию до начальника службы КИП (контрольно-измерительных приборов). Начальник службы КИП определяет свободного специалиста, за которым закрепляется решение задачи. Далее специалист КИП направляется в цех для идентификации причины появления неисправности (сгорел датчик, обрыв линии связи и т.п.). Если диагностируется, что датчик вышел из строя, то начальник производственного цеха или службы КИП делается запрос на склад на поиск подходящего для замены датчика из состава ЗИП. При его наличии датчик выдается специалисту КИП и им осуществляется его замена. В итоге длительность процесса от появления неполадки до ее устранения может быть недопустимо большой. Все эти потери времени могут привести к простою производства, что, в свою очередь, приведет к материальным потерям.

Одним из подходов, который позволяет существенно сократить цепочку передачи информации, и, как следствие, время оповещения специалистов по техническому обслуживанию, является подход, основанный на применении технологии промышленного Интернета вещей (IIoT), в частности протокола MQTT.

В программируемый логический контроллер, который осуществляет управление технологическим процессом, добавляется программный модуль диагностики и выдачи сообщений о состоянии технических средств автоматизации (датчиков, исполнительных механизмов, клапанов, частотных преобразователей, модулей ввода-вывода и др.). Этот программный модуль (далее МДГС – модуль диагностики и генерации сообщений) постоянно в режиме реального времени осуществляет диагностику состояния оборудования и при выявлении неисправности автоматически отправляет сообщение всем заинтересованным службам (оператору, начальнику смену, начальнику цеха, начальнику службы КИП, ответственному специалисту КИП, на склад). Сообщение содержит полную информацию о диагностируемой проблеме, месте и времени ее появления. В итоге существенно сокращается путь

передачи информации, и она поступает до исполнителя практически в момент появления проблемы.

Также МДГС дополнительно осуществляет учет времени наработки технических средств автоматизации (ТСА) и технологического оборудования (насосов, мешалок и др.) и при приближении к назначенному ресурсу заранее информирует интересующие службы о необходимости проведения планово-предупредительных работ (ППР), при этом в качестве коммуникационного протокола используется протокол MQTT (Message Queue Telemetry Transport). Структура системы мониторинга состояния оборудования, построенная с использованием MQTT, представлена на рис. 1.

Встраиваемый в контроллер программный модуль МДГС и MQTT-модуль обеспечивают передачу данных посредством протокола MQTT брокеру, который обрабатывает, сортирует и отправляет информацию конкретным пользователям, подписанным на необходимые им топики. При информационном взаимодействии используется спорадический тип опросов, что значительно разгружает сеть. То есть информация об ошибках отправляется по мере их возникновения (инициатором передачи выступает сам контроллер), а не циклически передается как при периодическом опросе в традиционных системах.

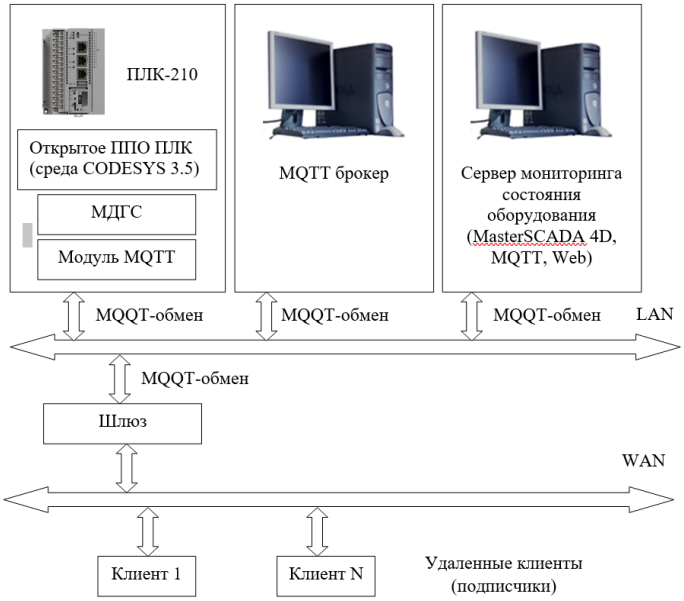


Рис. 1. Структура системы

Модуль МДГС осуществляет автоматический контроль и выявление неисправностей технологического оборудования и средств автоматизации: датчики – обрыв, короткое замыкание; запорные клапана – неоткрытие или незакрытие за заданное время, несрабатывние конечных выключателей; приводы насосов и мешалок – невключение или невыключение; протечки и разрывы трубопроводов и др.

Модуль МДГС генерирует соответствующее сообщение по диагностируемой ошибке, аварии или неисправности и это сообщение в формате MQTT-протокола отправляется на MQTT-брокер Mosquitto, который развернут на отдельном компьютере в сети АСУТП предприятия. На сервере брокера производится обработка, сортировка, хранение, распределение информации и отправка ее «подписчикам» – удаленным клиентам, которые подписались на соответствующие топики.

При построении системы максимально используется существующая IT-инфраструктура предприятия и проводной Ethernet. При его отсутствии или невозможности использования, коммуникационные взаимодействия можно организовать посредством беспроводных технологий Wi-Fi.

Предлагаемая система мониторинга и технического обслуживания позволяет сократить время диагностики и устранения неисправностей технологического оборудования и оборудования АСУТП, что позволяет снизить число нештатных ситуаций, сократить простои оборудования, и, как следствие, – повысить экономическую эффективность производства.

Список использованных источников

1. Андреев, Ю. С. Промышленный интернет вещей / Ю. С. Андреев. – СПб. : Университет ИТМО, 2019. – 54 с.

References

1. Andreev, Y. S. Industrial Internet of Things / Y. S. Andreev. – St. Petersburg : ITMO University, 2019. – 54 p.

УДК 681.5

П. И. Карасев[1], Е. А. Ермаков[1], М. Р. Потемкин[1],
Алмали Ахмед Аднан Латиф[2]
([1]Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: karasev@mirea.ru,e_erm@bk.ru, potemkinmr@gmail.com;
[2]г. Багдад, Ирак)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ В ЗАДАЧАХ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Рассмотрены задачи повышения безопасности предприятия агропромышленного комплекса с использованием технологий межсетевого экранирования.

Ключевые слова: межсетевое экранирование, беспроводные технологии, агропромышленный комплекс.

P. I. Karasev[1], E. A. Ermakov[1], M. R. Potemkin[1],
Almali Ahmed Adnan Lateef[2]
([1]Department of Information Security,
RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq)

THE USE OF INTER-NETWORK SHIELDING TECHNOLOGY IN THE TASKS OF IMPROVING THE SAFETY OF AN AGRO-INDUSTRIAL COMPLEX ENTERPRISE

Abstract. The tasks of improving the safety of an agro-industrial complex enterprise using inter-network shielding technologies are considered.

Keywords: inter-network shielding, wireless technologies, agro-industrial complex.

Введение. В условиях развития информационных технологий предприятия агропромышленного комплекса (далее – АПК) активно внедряют цифровые технологии для эффективности производства сельского хозяйства. Они занимаются производством сельскохозяйственных продуктов, в которых активно используются информационные системы для управления и взаимодействия ресурсов. Данное развитие влечет за собой и новые проблемы, среди которых главенствующую роль занимает обеспечение информационной безопасности.

В связи с этим, межсетевое экранирование становится важным элементом защиты информационных систем предприятий АПК от киберугроз.

Определения.

Межсетевой экран – это программно-аппаратное или программное решение для контроля сетевого трафика и его фильтрации в соответствии с определенными правилами.

Существует несколько видов межсетевых экранов, каждый из которых имеет свои особенности:

- **Пакетные фильтры**: Простейший тип межсетевых экранов, который анализирует трафик на уровне сетевых пакетов. Эти экраны могут блокировать или разрешать трафик в зависимости от IP-адресов и портов, однако не предоставляют полной защиты от более сложных угроз.
- **Межсетевые экраны на уровне сеансов**: Эти экраны отслеживают активные сеансы связи и могут обеспечивать более глубокий контроль за трафиком. Они эффективны для предотвращения атак на уровне приложений.
- **Межсетевые экраны нового поколения (NGFW)**: Объединяют в себе функции традиционных межсетевых экранов, системы обнаружения вторжений (IDS) и других средств безопасности. NGFW способны анализировать трафик на более высоком уровне, что делает их идеальным выбором для защиты сложных информационных систем предприятий АПК.

Значение межсетевого экранирования для агропромышленных предприятий.

АПК становятся привлекательными целями для киберпреступников по нескольким причинам:

- Увеличение уровней автоматизации.
- Системы управления производственными процессами могут содержать критически важную информацию.

Наиболее распространенные угрозы включают в себя вирусы-шифровальщики, программы-вымогатели, атаки «отказ в обслуживании» (DDoS).

Для АПК важность межсетевого экранирования обусловлена следующими факторами:

- **Защита производственных процессов**: Нарушение работы информационных систем может привести к сбоям в производстве, что, в свою очередь, повлияет на качество и количество продукции.

- **Защита коммерческой тайны**: Конкурентоспособность предприятий АПК во многом зависит от сохранения конфиденциальности информации о производственных процессах, рецептурах и других критически важных данных.
- **Соответствие нормативным требованиям**: Межсетевые экраны помогают соответствовать предприятию нормативным требованиям информационной безопасности.

Основные функции МЭ для повышения безопасности.

Межсетевое экранирование играет центральную роль в создании многоуровневой защиты на предприятиях АПК. Оно обеспечивает следующие функции:

- Контроль трафика: межсетевые экраны позволяют фильтровать трафик на основе заданных политик безопасности.
- Логирование и мониторинг: многие современные межсетевые экраны имеют функции логирования, которые регистрируют все попытки доступа и действия в сети, что упрощает последующий анализ инцидентов.
- Интеграция с другими системами безопасности: межсетевые экраны могут быть интегрированы с системами предотвращения вторжений (IPS), антивирусами и другими решениями для повышения общей защиты.

Реализация межсетевого экранирования на предприятиях АПК. Для успешной реализации межсетевого экранирования на предприятии АПК необходимо учитывать несколько ключевых аспектов:

- Анализ инфраструктуры: важно провести всесторонний аудит существующей инфраструктуры, чтобы определить точки доступа и потенциальные уязвимости.
- Разработка политик безопасности: необходимо сформулировать четкие политики безопасности, основанные на бизнес-процессах и актуальных угрозах. Каждая политика должна учитывать специфику работы предприятия и учитывать важные аспекты, такие как доступ к данным, использование мобильных устройств и удаленный доступ.
- Выбор решений: на рынке представлено множество решений по межсетевому экранированию. Выбор следует основывать не только на функционале, но и на стоимости, а также на уровне технической поддержки.
- Постоянный мониторинг и обновления: киберугрозы постоянно эволюционируют, поэтому необходимо регулярно обновлять поли-

тики и правила на межсетевых экранах, а также проводить мониторинг трафика и инцидентов.

Заключение. Межсетевое экранирование представляет собой важный компонент системы информационной безопасности на предприятиях агропромышленного комплекса. Его применение позволяет защитить критически важные информационные системы от множества киберугроз. Важно не только внедрять технологии межсетевого экранирования, но и развивать комплексный подход к безопасности, который учитывает как технические, так и организационные меры.

Список использованных источников

1. Лапонина, О. Р. Межсетевое экранирование / О. Р. Лапонина. – 2-е изд. – М. : ИНТУИТ, 2016. – 465 с.

References

1. Laponina, O. R. Inter-network shielding / O. R. Laponina. – 2nd ed. – M. : INTUIT, 2016. – 465 p.

УДК 681.5

Е. С. Жирнов[1], Шамсулдин Хайдар Абдулваххаб Х.[2], Мустафа Абдулкадим Дхаир Аль-Амиди[3]
([1]Кафедра «Защита информации», «Информационная безопасность», РТУ МИРЭА, Москва, Россия,
e-mail: Zhirnov@bk.ru, karasev@mirea.ru;
[2]г. Багдад, Ирак;
[3]г. Аль-Кадисия, Ирак)

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрены возможности применения блокчейн-технологий в агропромышленном комплексе. Описаны ключевые направления использования блокчейна для отслеживания цепочки поставок, обеспечения качества продукции и автоматизации сделок. Выделены преимущества и трудности внедрения технологии.

Ключевые слова: блокчейн, агропромышленный комплекс, прозрачность, смарт-контракты, отслеживание цепочки поставок, сельское хозяйство, цифровая трансформация, безопасность данных.

E. S. Zhirnov[1], Shamsuldaeen Haidar Abdulwahhab H.[2], Mustafa Abdulkadhim Al-Ameedee Dhahir[3]
([3]Department of Information systems and information protection, RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq;
[3]Al-Qadisiyah, Irag)

APPLICATION OF BLOCKCHAIN TECHNOLOGIES IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The possibilities of blockchain technologies application in the agro-industrial complex are considered. The key areas of blockchain use for tracking the supply chain, ensuring product quality and automating transactions are described. The advantages and difficulties of the technology implementation are highlighted.

Keywords: blockchain, agribusiness, transparency, smart contracts, supply chain tracking, agriculture, digital transformation, data security.

Применение блокчейн-технологий в агропромышленном комплексе. Блокчейн-технологии за последние годы приобрели широкую известность благодаря своему применению в таких отраслях, как финансы, логистика и здравоохранение. Агропромышленный ком-

плекс также не остался в стороне, так как блокчейн может повысить прозрачность, эффективность и доверие на всех уровнях производственно-сбытовой цепочки. В данной статье рассматриваются основные аспекты применения блокчейна в аграрном секторе, его преимущества и потенциальные трудности.

Основные принципы и возможности блокчейн-технологий. Блокчейн – это распределенный реестр данных, где информация хранится в виде непрерывной цепи блоков. Каждый блок содержит запись о конкретной операции или событии, а изменение данных в блоках невозможно, что обеспечивает высокий уровень безопасности. Все участники системы имеют доступ к обновленной информации в реальном времени, что исключает необходимость посредников. Это особенно актуально для агропромышленного комплекса, где блокчейн можно применять на всех этапах – от производства и переработки до поставок и продаж.

Одним из ключевых направлений является прозрачность и отслеживаемость цепочки поставок. В рамках блокчейн-системы каждый участник (фермер, переработчик, дистрибьютор, продавец) может вносить данные о продукте, что позволяет отслеживать его путь от фермы до потребителя. Это повышает доверие к продуктам, ведь потребители могут проверить, где и кем был произведен товар, с помощью, например, QR-кода. В случае выявления проблем с качеством продукции, блокчейн позволяет быстро отследить ее путь и оперативно отозвать с рынка, минимизируя риски для потребителей.

Смарт-контракты и финансовые решения в агропромышленном комплексе. Еще одно важное направление – использование смарт-контрактов для автоматизации сделок. Смарт-контракт – это программа, которая автоматически выполняется при наступлении заранее оговоренных условий. В агропромышленном комплексе такие контракты можно применять для автоматизации взаимодействия между фермерами, поставщиками, логистическими компаниями и продавцами, что снижает риск мошенничества и ошибок, связанных с человеческим фактором.

Блокчейн также может способствовать улучшению финансовых решений для фермеров. Оценка урожайности, климатических условий и других факторов, фиксируемых в блокчейне, позволит банкам и страховым компаниям более точно оценивать риски и предоставлять кредитные и страховые услуги на более выгодных условиях. Фермеры могут создавать цифровую историю своей деятельности, что облегчает доступ к финансовой поддержке и страхованию.

Прозрачность распределения субсидий и дотаций. Государственные субсидии и дотации играют важную роль в поддержке сельского хозяйства, однако их распределение часто сталкивается с бюрократическими задержками и недостатком прозрачности. С применением блокчейн-технологий каждая транзакция, начиная от подачи заявки до перевода средств, фиксируется в реестре, что делает процесс более прозрачным и справедливым.

Преимущества и недостатки блокчейн-технологий в агропромышленном комплексе. К основным преимуществам блокчейна в агропромышленном комплексе относятся прозрачность и доверие между участниками рынка, возможность исключить посредников, а также высокая безопасность данных. Кроме того, автоматизация через смарт-контракты ускоряет процессы расчетов и поставок, что особенно важно в условиях сезонности производства.

Однако внедрение блокчейна в агропромышленном комплексе сталкивается с рядом трудностей. Это включает техническую сложность и необходимость высокоуровневой инфраструктуры, что может быть препятствием для небольших фермеров. Первоначальные затраты на внедрение блокчейн-решений могут оказаться значительными, что отпугивает малый и средний бизнес. Также существует недостаточная правовая база для регулирования использования блокчейна в сельском хозяйстве, что создает неопределенность. Некоторые участники цепочки поставок могут опасаться потери контроля или прибыли при внедрении блокчейна, что вызывает сопротивление.

Заключение. Применение блокчейн-технологий в агропромышленном комплексе открывает большие возможности для повышения прозрачности, безопасности и эффективности производства и логистики сельскохозяйственной продукции. Однако для успешного внедрения необходимо преодолеть ряд технических и организационных трудностей. В будущем блокчейн может стать важным элементом цифровой трансформации агропромышленного комплекса, способствуя развитию более устойчивого и прозрачного сельского хозяйства.

Список использованных источников

1. Барсукова, С. В. Блокчейн как инструмент цифровой трансформации агропромышленного комплекса / С. В. Барсукова, А. В. Ильина // Вестник цифровой экономики. – 2022. – № 3. – С. 45 – 59.

2. Иванов, А. А. Использование блокчейн-технологий для повышения прозрачности цепочек поставок в сельском хозяйстве / А. А. Иванов,

В. П. Смирнов // Современные технологии в агропромышленном комплексе. – 2021. – № 4. – С. 73 – 82.

3. Кузнецова, Л. В. Интеллектуальные контракты и их применение в агробизнесе / Л. В. Кузнецова // Инновационные технологии в сельском хозяйстве. – 2020. – № 7. – С. 90 – 105.

4. Марков, И. В. Блокчейн в системе агрологистики: вызовы и перспективы / И. В. Марков // Логистика и управление цепями поставок. – 2021. – № 2. – С. 123 – 136.

References

1. Barsukova, S. V. Blockchain as a tool for digital transformation of the agro-industrial complex / S. V. Barsukova, A. V. Ilyina // Vestnik of Digital Economy. – 2022. – No. 3. – P. 45 – 59.

2. Ivanov, A. A. The use of blockchain technologies to increase the transparency of supply chains in agriculture / A. A. Ivanov, V. P. Smirnov // Modern Technologies in Agroindustrial Complex. – 2021. – No. 4. – P. 73 – 82.

3. Kuznetsova, L. V. Smart contracts and their application in agribusiness / L. V. Kuznetsova // Innovative technologies in agriculture. – 2020. – No. 7. – P. 90 – 105.

4. Markov, I. V. Blockchain in the system of agro-logistics: challenges and prospects / I. V. Markov // Logistics and Supply Chain Management. – 2021. – No. 2. – P. 123 – 136.

УДК 004.94

А. А. Канцуров[1], Алмали Ахмед Аднан Латиф[2],
Аль-Судани Зайд Али Хуссейн[2]
([1]Кафедра «Информационные системы и защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: proa1210@gmail.com, karasev@mirea.ru;
[2]г. Багдад, Ирак)

БЕЗОПАСНОСТЬ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ АГРАРНЫМИ СИСТЕМАМИ

Аннотация. Статья посвящена безопасности дистанционного управления аграрными системами, такими как: умные теплицы, дроны и автоматические производства. Мы рассматриваем основные угрозы IoT и облачных платформ, в том числе несанкционированный доступ и кибератаки.

Ключевые слова: безопасность аграрных систем, автоматизированные системы, IoT, кибербезопасность, аграрные технологии, защита данных.

A. A. Kanzurov[1], Almali Ahmed Adnan Lateef[2],
Al-Soudany Zaid Ali Hussein[2]
([1]Department of Information Systems and Information Protection,
RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq)

SAFETY OF REMOTE CONTROL OF AGRICULTURAL SYSTEMS

Abstract. This article is devoted to the safety of remote control of security systems such as smart greenhouses, drones and automatic production. We look at the main threats to IoT and cloud platforms, including unauthorized access and cyber attacks.

Keywords: security of agricultural systems, automated systems, IoT, cybersecurity, agricultural technologies, data protection.

Введение. В этой статье мы рассмотрим SIEM-системы, одно из их главных преимуществ которых – обработка большого количества данных. Аграрные системы могут представлять не очень большую инфраструктуру, но с развитием IoT она состоит из огромного количества умных датчиков, камер и других элементов, каждый из них нужно защищать.

SIEM (система управления событиями и информацией безопасности) выполняет две ключевые задачи: сбор и анализ данных о событиях безопасности (SEM), а также управление этими данными (SIM).

Она собирает журналы событий с различных устройств и сетей, проводит анализ в реальном времени и выявляет отклонения от нормы. В случае обнаружения угроз, таких как несанкционированный доступ, DDoS-атаки или утечка данных, система незамедлительно уведомляет администратора.

Использование SIEM в агропромышленных комплексах помогает централизованно контролировать безопасность всех устройств, анализировать взаимосвязи между событиями и оперативно выявлять кибератаки, что особенно важно для бесперебойной работы автоматизированных систем.

Работа на примере SIEM от Solar. Рассмотрим SIEM от Solar, она имеет ряд преимуществ.

Соответствие российским стандартам: Solar Dozor соответствует законодательным требованиям РФ, включая ФЗ-152 и правила защиты критической информационной инфраструктуры (КИИ). Это делает ее идеальным выбором для отечественных агропредприятий, стремящихся соблюдать местные нормы безопасности.

Локальная поддержка: Solar Dozor предоставляет качественную техническую поддержку на русском языке, что упрощает ее использование и адаптацию для российских аграрных предприятий.

Интеграция с облачными сервисами: Система поддерживает интеграцию с российскими облачными платформами, что обеспечивает удобное хранение и обработку данных от устройств, таких как теплицы и дроны.

Масштабируемость: Solar Dozor легко адаптируется к нуждам различных предприятий – от мелких фермерских хозяйств до крупных агропромышленных комплексов. Благодаря интеграции с IoT-устройствами и автоматизированными системами, она является эффективным инструментом для сельского хозяйства.

Solar Dozor собирает и анализирует логи и события с различных устройств в аграрных системах, таких как умные теплицы, дроны и IoT-сенсоры. Система централизует обработку этих данных, выявляя аномалии и подозрительные действия.

Заключение. SolarWinds SIEM (Solar Dozor) является важным инструментом для обеспечения безопасности аграрных систем в условиях растущих киберугроз. Благодаря соответствию российским нормативам, локальной поддержке и возможности интеграции с разнообразными IoT-устройствами и облачными сервисами, эта система подходит как для небольших фермерских хозяйств, так и для крупных агрохолдингов. Solar Dozor не только помогает выявлять и блокиро-

вать потенциальные угрозы в реальном времени, но и обеспечивает оперативную защиту критических процессов, таких как управление теплицами и дронами.

Список использованных источников

1. Мырзабекова, А. М. Обзор современных систем для хранения зерновых культур / А. М. Мырзабекова // Информационно-измерительная техника и технологии : материалы VI науч.-практ. конф. – Томск : Изд-во ТПУ, 2015. – С. 95 – 101.
2. Кузнецов, А. В. Использование систем SIEM для защиты аграрных IoT-устройств / А. В. Кузнецов // Информационная безопасность в АПК. – 2020. – № 2. – С. 38 – 44.
3. Обзор систем SolarWinds SIEM для защиты критической инфраструктуры // Сайт SolarWinds Russia. – URL : https://www.solarwinds.com/ru/siem (дата обращения: 05.09.2024).

References

1. Mirzabekova, A. M. Review of modern systems for storing grain crops / A. M. Murzabekova // Information and measuring equipment and technologies : materials of the VI scientific and practical conference. – Tomsk : TPU Publishing House, 2015. – P. 95 – 101.
2. Kuznetsov, A. V. Using the SIEM system to protect agricultural IoT devices / A. V. Kuznetsov // Information security in agriculture. – 2020. – No. 2. – P. 38 – 44.
3. Overview of the SolarWinds SAM system for the protection of critical information // SolarWinds Russia website. – URL : https://www.solarwinds.com/ru/siem (date of application: 09/05/2024).

УДК 681.5

Н. Б. Куженова, Б. С. Дмитриевский
(Кафедра «Информационные процессы и управление»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: ipu_tstu@mail.ru)

ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ ЭТИЛОВОГО СПИРТА

Аннотация. Рассмотрены элементы инфраструктуры, подход к разработке соответствующих управленческих решений, выявление очередности реализации управленческих решений для этих элементов.

Ключевые слова: инфраструктура, цифровизация, система управления, модель, принятие решений.

N. B. Kuzhenova, B. S. Dmitrievsky
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

INFORMATION INFRASTRUCTURE FOR ETHYL ALCOHOL PRODUCTION MANAGEMENT

Abstract. The elements of infrastructure, an approach to the development of appropriate management decisions, and the identification of the order of implementation of management decisions for these elements are considered.

Keywords: monitoring infrastructure, digitalization, management system, model, decision-making.

Система деятельности предприятия, производящего продукцию, определяется тремя подсистемами: производительной, административной и их обеспечения. Первая подсистема выполняет работу, связанную с превращением входных величин в выходные величины. Вторая подсистема выдает решения, как должна работать вторая подсистема. В нее входят: администрация, общий отдел, отдел кадров, бухгалтерия и плановый отдел. Третью подсистему образуют подразделения предприятия, выполняющие функции, которые необходимы для работы первых двух подсистем. Эта подсистема включает службы, обеспечивающие жизнедеятельность: эксплуатация зданий и помещений, инженерных коммуникаций и прилегающих территорий.

Обеспечивающая инфраструктура является основой социально-экономического развития предприятия, обеспечивает функционирование производственных подсистем. Она состоит из капиталовложений, определяющих будущее предприятия. Обособленно выделяют информационную инфраструктуру и рассматривают ее отдельно.

Для эффективного функционирования предприятия мало знать все составные элементы инфраструктуры, необходимо еще грамотно ими управлять. Поэтому подобная задача сейчас очень актуальна в производстве этилового спирта. Управление сервисными подразделениями сводится к координации работ в этих подразделениях, и основано на выполнении конкретных целей. Эти различающиеся подразделения должны работать как единая система.

Сервисная часть предприятия представляет механический набор служб, которые выполняют узкопрофессиональные работы. Это и есть причина того, что многие направления деятельности предприятия просто уходят из поля зрения сервисных подразделений. Только при слаженном функционировании возможно достижение поставленных задач. Одной из них является периодическое снижение внутренних издержек производства. Это и является основным моментом в деятельности специалиста по управлению подразделениями обеспечения.

Производственная инфраструктура обладает новым качеством, заключающимся в том, что она превращается в развивающуюся отрасль и вид деятельности. Функционирование инфраструктуры имеет двойной смысл: первый – обслуживание материального производства, второй – воспроизводство трудовых ресурсов, т.е. фактор, который непосредственно участвует в производстве.

Инновационной деятельностью следует управлять как системой динамических бизнес-процессов. Состояние системы в динамике определяется входными и выходными величинами, функцией управления, обратными связями и ресурсами.

Изучение элементов инфраструктуры, разработка соответствующих управленческих решений, выявление очередности реализации управленческих решений для этих элементов позволит повысить эффективность работы организации в целом. Каждый из элементов инфраструктуры оказывают свое влияние на ее развитие, но только их совокупность может обеспечить эффективное управление.

Модель управления инфраструктурой и формируемые на ее основе программы действий определяют последовательность выполнения планируемых управленческих процессов, сроки их реализации, список лиц, ответственных за их выполнение, то есть все этапы с момента принятия решения о совершенствовании элемента инфраструктуры до использования этого элемента в производственном процессе. Цифровую систему управления инфраструктурой условно можно представить состоящей из трех функционально обособленных систем: системы интеллектуальной поддержки управления, системы автоматизированного документооборота и системы информационной поддержки управления.

В условиях цифровизации для эффективной реализации своих специфических функций каждое подразделение должно располагать специальным математическим обеспечением управления – комплексом интеллектуализированных программных средств и алгоритмов определения различных вариантов решений, которые в совокупности образуют систему интеллектуальной поддержки управления производством.

Технологически реализация сформулированных ниже предложений выглядит следующим образом. Должностные лица в каждом подразделении формируют все, без исключения, свои документы (как для внешнего, так и для внутреннего использования) исключительно в рамках специально разработанных для них программных оболочек. Алгоритмы, лежащие в основе таких оболочек, таковы, что вся введенная через них информация (в случае необходимости!) автоматически структуризируется и вводится в общую базу данных.

При разработке программы построения инфраструктуры необходимо использовать принцип: отдельное подразделение вводит в общую систему только ту информацию, которая возникает в процессе его функционирования, а использует информацию всей инфраструктуры. Вопросы формирования запросов отделены от процессов наполнения базы данных.

Важнейшим шагом в построении системы управления является создание системы автоматизированного документооборота. Функционирование этой системы создаст предпосылки для всеобъемлющей цифровизации.

Принципиально важным является реализация следующих принципов.

1. Работа в рамках единого информационного пространства. Все должностные лица реализуют свои функции в рамках информационной среды, технической основой которой является полномасштабная телекоммуникационная сеть с выходом в Internet.

2. Безбумажная технология управления. Каждое должностное лицо в рамках своей компетенции формирует проекты документов, ведет учет документов и всей необходимой ему информации исключительно компьютерными средствами, входящими в общую сеть.

Разработанная система управления координирует информационное пространство вместе с работой и людьми на предприятии, использует передовые управленческие принципы с новыми профессиональными знаниями для повышения эффективности работы производства.

УДК 681.5

К. В. Купцов[1], Шамсулдин Хайдар Абдулваххаб Х.[2], Мустафа Абдулкадим Дхаир Аль-Амиди[3]
([1]Кафедра «Защиты информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: ipu@mail.ahp.tstu.ru, postmaster@nauka.tstu.ru;
[2]г. Багдад, Ирак;
[3]г. Аль-Кадисия, Ирак)

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Рассмотрены различные средства защиты информации, которые применяются в агропромышленном комплексе. Описаны возможности этих средств и их применение в различных областях этой сферы. Важным моментом, на который необходимо обратить внимание, является важность выбора средств защиты информации в зависимости от конкретных задач и требований безопасности системы. Понимание контекста и потребностей поможет эффективней обеспечить безопасность информации в одной из важнейших отраслей в нашей стране. Каждая из перечисленных средств защиты играет важную роль в обеспечении целостности, конфиденциальности и доступности данных. Выбор оптимальных средств защиты информации для конкретной задачи позволит эффективно обеспечить безопасность информации в системе в целом.

Ключевые слова: защита информации, СЗИ, АПК, средства, шифрование, брандмауэр, несанкционированный доступ, ЗИ.

K. V. Kuptsov[1], Shamsuldaeen Haidar Abdulwahhab H.[2], Mustafa Abdulkadhim Dhahir Al-Ameedee[3]
([1]Department of Information Security,
RTU MIREA, Moscow, Russia,
[2]Baghdad, Iraq;
[3]Al-Qadisiyah, Irag)

ANALYSIS OF MODERN INFORMATION SECURITY SYSTEMS OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. This article examines the various information security tools that are used in the agro-industrial complex. She describes the possibilities of these tools and their application in various areas of this field. An important point to pay attention to is the importance of choosing information security tools depending on the specific tasks and security requirements of the system. Understanding the context and needs will help effectively ensure the security of information in one

of the most important industries in our country. Each of the listed security measures plays an important role in ensuring the integrity, confidentiality and availability of data. Choosing the optimal means of information protection for a specific task will effectively ensure the security of information in the system as a whole.

Keywords: information protection, SPI, APK, tools, encryption, firewall, unauthorized access, IP.

Для начала следует разобраться со отличительными особенностями земледелия. Это подразумевает груду секций, от выращивания агропродукции вплоть до ее утилизации, спецхранения и доставки потребителю. Информационные технологии в любой агроотрасли имеют большое значение на основании автоматизирования череды процессов, а также оптимизируя производство и повышая эффективность. Здесь также появляются недостатки, так как все упомянутое несет неисследованные угрозы информационной безопасности, которые Ит-специалист обязан решить.

Специфика угроз в АПК состоит из нескольких факторов:

– критическая инфраструктура, в связи с тем, что перебои работы базы данных аграрного комплекса таят в себе угрожающий исход для пищевой безопасности и экономики;

– распределенность и разнообразие объектов, зачастую они уязвимы, что может привести к их взлому и к ущербу компании.

Физическая защита охватывает меры по охране территорий и хозяйства вместе с системами контроля доступа, какие-либо служат для идентификации, предотвращения и нейтрализации угроз:

– нередкое использование смартфонов в угоду регулирования производственных процессов наращивает шанс заражения вредоносным ПО;

– нужда в унифицированном стандарте информационной безопасности, исходя из нужности достаточных политик безопасности на предприятиях АПК;

– затруднительное положение за неимением опытных специалистов по ИБ;

– кибератаки, которые оказывают угрозу для систем управления и спецоборудования;

– неавторизованный доступ с позиции персонала предприятия или хакера;

– технические сбои или промахи пользователей наряду с катаклизмами, которые были способны сделать негодным систему, что породит после себя утерю важной информации.

Важно отметить в наши дни всевозможные средства ЗИ, подразумевающие антивирусное ПО, сетевые устройства, средства контроля доступа и остальные. СЗИ имеет в своем составе аппаратные и программные средства, обеспечение и допоборудование, спроектированные ради недопущения угрозы и гарантии безопасности данных, ввиду их пользования.

Аппаратные средства защиты информации предопределены ради защиты информации от ее утраты и незаконного доступа с помощью ТСЗИ. Программные средства имеют в своем составе защиту от наносящего вред ПО и сканирование систем, обеспечение шифрования данных. Теперь обратим внимание на актуальные средства защиты информации в АПК:

– антивирусное программное обеспечение, необходимое для специализированных решений вопросов сельскохозяйственного оборудования;

– сетевые устройства и устройства их защиты. Они предназначены для управления сетевым трафиком и блокировки незаконного подключения;

– системы обнаружения и предотвращения вторжений для защиты на сетевом уровне;

– брандмауэры нужны ради лимита доступа к информационным активам;

– средства контроля доступа незаменимы в целях управления возможностью входа пользователей в соответствии с правилами безопасности;

– ТСЗИ необходимы для предотвращения недопущения в подсистему;

– системы управления доступом, незаменимые для отладки права доступа;

– шифрование данных необходимое для противодействия несанкционированному доступу;

– резервное копирование также необходимо в случае каких-либо чрезвычайных ситуаций для восстановления данных в случае их потери;

– системы мониторинга и управления нужны для контроля за состоянием информационных систем, выявлением аномальных активностей;

– обучение сотрудников нужно для повышения осведомленности о возможных опасностях ИБ, регламентах информбезопасности;

– системы управления доступом, позволяющие сузить подступ к данным через роли пользователей в базе данных предприятия.

Специфические решения для АПК необходимы для решения ключевых задач, а именно для повышения эффективности производства, улучшения качества продукции, упрощения управления организацией, а также снижения рисков, которые влияют на производство. В них входят:

– системы управления производственными усилиями незаменимы во избежание несанкционированного доступа к документации об агропроизводственных процессах;

– системы мониторинга и управления сельского оснащения сделают возможным гарантию от несанкционированного управления техникой, предотвращение кражи данных;

– в системе контроля качества сельхозпродукции не обойтись без безопасности и подлинности данных о качестве продукции;

– системы автоматизации агрокомплекса имеют необходимость в избавлении от кибератак в системах настройки поливом, спецосвещением, температурным режимом;

– системы контроля доступа к сельскохозяйственным объектам нужны для ограничения доступа к фермам, складам и другим объектам.

В завершение обсуждения, стоит подчеркнуть важность наличия и актуального апгрейда систем защиты информации в АПК. Также важно внедрять дообучение персонала структурного подразделения, поскольку это имеет влияние на поднятие эффективности труда, проверку информационной безопасности. Необходимо задействовать как технические, так и организационные меры защиты. Регулярное отработка систем безопасности и обучение сотрудников с учетом их отрасли также хорошо влияет на повышение безопасности. Внедрение новых технологий повышает степень защиты информации в отрасли поднимает производительность труда.

Список использованных источников

1. Абидарова, А. А. Физические средства защиты информации / А. А. Абидарова, // Наука, образование и культура. – 2019. – № 2(36). – С. 19–20.

2. Михеев, Р. Э. Современное состояние и перспективы развития методов и средств защиты информации в компьютерных сетях / Р. Э. Михеев. – М. : Проблемы науки, 2018. – С. 55–56.

3. Мещерякова, Т. В. Метод и программные средства оценки надежности средств защиты информации от несанкционированного доступа / Т. В. Мещерякова, И. Г. Дровникова, Е. А. Рогозин. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2023. – 96 с.

4. Кирин, Д. А. Методы и программно-аппаратные средства защиты информации от несанкционированного доступа в сети Интернет / Д. А. Кирин, В. В. Сааков // Инновационные научные исследования. – 2021. – № 9-1(11). – С. 31 – 37.

References

1. Abidarova, A. A. Physical means of information protection // Science, education and culture / A. A. Abidarova. – 2019. – No. 2(36). – P. 19–20.

2. Mikheev, R. E. The current state and prospects of development of methods and means of information protection in computer networks / R. E. Mikheev. – M. : Problems of Science, 2018. – P. 55–56.

3. Meshcheryakova, T. V. Method and software tools for assessing the reliability of information protection against unauthorized access / T. V. Meshcheryakova, I. G. Drovnikova, E. A. Rogozin. – Voronezh : Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, 2023. – 96 p.

4. Kirin, D. A. Methods and software and hardware protection of information from unauthorized access to the Internet / D. A. Kirin, V. V. Saakov // Innovative scientific research. – 2021. – No. 9-1(11). – P. 31 – 37.

УДК 681.5

Н. Ю. Куриленко[1], С. В. Артемова[1], Г. Ш. Утешева[2]
([1]Кафедра «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: karasev@mirea.ru, kurilenko.n.y@edu.mirea.ru;
[2]Западно-Казахстанский инновационно-технологический
университет, г. Уральск, Казахстан)

ЦИФРОВЫЕ ИНСТРУМЕНТЫ ДЛЯ МОНИТОРИНГА УСТОЙЧИВОСТИ АГРОСИСТЕМ К ИЗМЕНЕНИЯМ КЛИМАТА

Аннотация. Статья посвящена исследованию цифровых инструментов для мониторинга устойчивости агросистем к изменениям климата. Климатические изменения оказывают значительное влияние на сельское хозяйство, требуя новых подходов к управлению агросистемами. Digital инструменты, такие как дистанционное зондирование, геоинформационные системы (ГИС) и сенсоры предоставляют новые возможности для оценки состояния агросистем, предсказания изменений и разработки адаптивных стратегий. В статье представлены примеры эффективного использования цифровых технологий, а также рекомендации по их интеграции в аграрную практику.

Ключевые слова: устойчивость, агросистемы, изменения климата, цифровые инструменты, мониторинг, дистанционное зондирование, геоинформационные системы, адаптация, сельское хозяйство.

N. Y. Kurilenko[1], S. V. Artemova[1], G. S. Utesheva[2]
(Department of “Information Protection”,
RTU MIREA, Moscow, Russia;
West Kazakhstan University of Innovation
and Technology, Uralsk, Kazakhstan)

DIGITAL TOOLS FOR MONITORING RESILIENCE OF AGROSYSTEMS TO CLIMATE CHANGE

Abstract. This paper investigates digital tools for monitoring the resilience of agro-systems to climate change. Climate change has a significant impact on agriculture, requiring new approaches to agro-system management. Digital tools such as remote sensing, geographic information systems (GIS) and sensors provide new opportunities for assessing the state of agrosystems, predicting changes and developing adaptive strategies. The article presents examples of effective use of digital technologies, as well as recommendations for their integration into agrarian practices.

Keywords: resilience, agrosystems, climate change, digital tools, monitoring, remote sensing, GIS, adaptation, agriculture.

Цифровые инструменты для мониторинга устойчивости агросистем к изменениям климата играют ключевую роль в адаптации сельского хозяйства к современным вызовам. Эти технологии позволяют собирать, анализировать и интерпретировать данные о состоянии окружающей среды, почвах и агрокультуре, что способствует более информированному принятию решений.

Системы дистанционного зондирования и геоинформационные технологии предоставляют возможность отслеживать изменения в микроклимате и воздействие экстремальных погодных условий на урожайность. Модели предсказания позволяют агрономам оценивать риски, связанные с изменением климата, и разрабатывать стратегии управления, направленные на снижение потенциальных потерь.

Кроме того, использование мобильных приложений и платформ для обмена данными способствует быстрому распространению информации среди фермеров и исследователей, что улучшает координацию действий в вопросах повышения устойчивости агросистем. В результате комплексный подход к применению цифровых инструментов не только повышает продуктивность сельского хозяйства, но и способствует устойчивому развитию агроэкосистем, позволяя адаптироваться к изменяющимся климатическим условиям и обеспечивать продовольственную безопасность.

Важным аспектом применения цифровых технологий является интеграция данных из различных источников, что позволяет формировать целостное представление о состоянии агросистем. С помощью аналитических платформ возможно объединение данных о почвах, климатических условиях и агрометеорологических показателях, создавая мощные инструменты для прогнозирования. Это, в свою очередь, помогает фермерам более точно планировать посевные и сборные кампании, минимизируя сезонные риски и максимизируя урожайность.

Одним из значительных преимуществ цифровых инструментов является способность к быстрой адаптации к изменениям в окружающей среде. Постоянный мониторинг микроклимата и состояния культуры позволяет агрономам оперативно реагировать на неблагоприятные условия, такие как засухи или наводнения. Это, в свою очередь, минимизирует потери и сохраняет рентабельность хозяйств. Например, системы автоматического полива, интегрированные с метеорологическими данными, обеспечивают оптимальное увлажнение почвы, что критично при резких колебаниях погоды.

Также стоит подчеркнуть значимость применения алгоритмов машинного обучения в агрономии. Эти алгоритмы имеют возможность обрабатывать огромные объемы данных, выявляя скрытые закономер-

ности и тенденции, которые могут оставаться незамеченными при традиционном анализе. Это позволяет фермерам оптимизировать процесс внесения удобрений и применение пестицидов, что, в свою очередь, приводит к снижению затрат и минимизации негативного воздействия на окружающую среду.

В конечном счете, использование цифровых инструментов для мониторинга устойчивости агросистем не только помогает справляться с вызовами, связанными с изменением климата, но и формирует систему умного сельского хозяйства, где каждое решение основывается на точных данных и научных знаниях. Это становится залогом устойчивого продовольственного обеспечения для будущих поколений.

Список использованных источников

1. Климатическая безопасность аграрного сектора: угрозы и проблемы адаптации // КиберЛенинка. – URL : https://cyberleninka.ru/article/n/klimaticheskaya-bezopasnost-agrarnogo-sektora-ugrozy-i-problemy-adaptatsii (дата обращения: 06.09.2024).

2. ГИС-технологии как эффективный инструмент для оценки негативных природно-климатических факторов, лимитирующих развитие аграрного природопользования // КиберЛенинка. – URL : https://cyberleninka.ru/article/n/gis-tehnologii-kak-effektivnyy-instrument-dlya-otsenki-negativnyh-prirodno- klimaticheskih-faktorov-limitiruyuschih-razvitie-agrarnogo (дата обращения: 07.09.2024).

References

1. Climatic security of agrarian sector: threats and adaptation problems // CyberLeninka. – URL : https://cyberleninka.ru/article/n/klimaticheskaya-bezopasnost-agrarnogo-sektora-ugrozy-i-problemy-adaptatsii (date of address: 06.09.2024).

2. GIS-technologies as an effective tool for assessment of negative natural-climatic factors limiting the development of agrarian nature management // CyberLeninka. – URL : https://cyberleninka.ru/article/n/gis-tehnologii-kak-effektivnyy-instrument-dlya-otsenki-negativnyh-prirodno-klimaticheskih-faktorov-limitiruyuschih-razvitie-agrarnogo (date of address: 07.09.2024).

УДК 004.5

В. А. Лукин
(Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: vlad@kerby.ru)

ОЦЕНКА И ОПТИМИЗАЦИЯ ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ УПРАВЛЕНИЯ ПОСЕВНЫМИ ПЛОЩАДЯМИ НА ОСНОВЕ ИНТЕГРАЛА ШОКЕ

Аннотация. Рассмотрены критерии, необходимые для выбора оптимального пользовательского интерфейса мобильного приложения для управления посевными площадями. Описано использование интеграла Шоке в многокритериальных задачах, в особенности при выборе пользовательского интерфейса.

Ключевые слова: пользовательский интерфейс, мобильное приложение, Flutter, интеграл Шоке, UI/UX, многокритериальные задачи.

V. A. Lukin
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

EVALUATION AND OPTIMIZATION OF THE USER INTERFACE OF A MOBILE APPLICATION FOR MANAGING ACREAGE BASED ON THE SHOKE INTEGRAL

Abstract. The criteria necessary for choosing the optimal user interface of a mobile application for managing acreage are considered. The use of the Shoke integral in multi-criteria tasks is described, especially when choosing a user interface.

Keywords: user interface, mobile application, Flutter, Integral Shock, UI/UX, multi-criteria tasks.

В современном мире агробизнеса эффективное управление посевными площадями становится ключевым фактором успеха. Мобильные приложения играют все более важную роль в этом процессе, предоставляя оперативный доступ к критически важной информации и инструментам управления. Однако разработка оптимального пользовательского интерфейса для таких приложений представляет собой сложную многокритериальную задачу.

Актуальность данного исследования обусловлена растущей потребностью в эффективных и удобных мобильных решениях для агро-

холдингов. Традиционные методы оценки и оптимизации пользовательских интерфейсов часто не учитывают сложные взаимосвязи между различными критериями, что может привести к субоптимальным решениям. В условиях, когда качество интерфейса напрямую влияет на эффективность управления сельскохозяйственными ресурсами, разработка более точных методов оценки и оптимизации становится критически важной.

Научная новизна работы заключается в применении интеграла Шоке для оценки и оптимизации пользовательского интерфейса мобильного приложения в контексте агробизнеса. Этот подход позволяет учесть нелинейные взаимодействия между различными критериями оценки интерфейса, такими как скорость работы, информативность, удобство использования и адаптивность. Использование интеграла Шоке в данном контексте представляет собой инновационное решение, позволяющее более точно моделировать сложные предпочтения пользователей и оптимизировать интерфейс с учетом специфики агробизнеса.

При проектировании интерфейса мобильного приложения необходимо учитывать многие критерии, такие как удобство пользования, скорость работы приложения, интуитивность, информативность, адаптивность как к разным операционным системам, так и к разным соотношениям сторон дисплея или же разрешения.

Скорость работы приложения является четким параметром, который можно измерить различными инструментами (BrowserStack, Appium). При этом данный критерий является достаточно важным, но им можно немного пренебречь в пользу более важных критериев.

Адаптивность к дисплеям и операционным системам является критерием, который нельзя опустить при проектировании, так как у всех пользователей должна быть возможность работать с приложением. При этом обязательно адаптировать приложение для популярных ОС, таких как Android и iOS, которые в сумме занимают практически 99% мобильных операционных систем.

Информативность также нельзя опускать при выборе интерфейса, ведь при недостаточном объеме данных пользователи могут получать неполную информацию и делать из нее в корне неверные выводы. Это может повлечь за собой серьезные последствия, особенно если пользователями являются участники высшего руководства компании.

При этом такие критерии, как удобство и интуитивность пользовательского интерфейса, являются нечеткими и субъективными.

Из-за этого мы не можем достоверно оценить пользовательский интерфейс и следует опираться на мнение пользователей, которые, в свою, очередь будут выставлять оценки исходя из своего пользовательского опыта.

Учитывая многокритериальность задачи и наличие как четких, так и нечетких критериев, становится очевидной необходимость использования более сложного инструмента для оценки и оптимизации интерфейса. Интеграл Шоке представляется идеальным решением для агрегации этих разнородных критериев, позволяя учесть их взаимодействие и относительную важность.

Интеграл Шоке, изначально разработанный в теории вероятностей, со временем нашел широкое применение в области многокритериального принятия решений. За последние годы его использование значительно расширилось, особенно в сложных задачах, требующих учета взаимодействия между различными критериями. В контексте многокритериальных задач интеграл Шоке предоставляет мощный инструмент для моделирования предпочтений лица, принимающего решения, позволяя учитывать нелинейные взаимосвязи между критериями. Рассмотрим применение этого метода на конкретном примере.

При использовании интеграла Шоке для оценки интерфейса мобильного приложения важно учитывать его неаддитивную природу. Это свойство несколько усложняет анализ и интерпретацию модели. В отличие от традиционных методов, где мы рассматриваем «веса» отдельных критериев, в случае с интегралом Шоке необходимо учитывать все возможные комбинации критериев.

Например, при оценке интерфейса мы не можем просто суммировать важность скорости работы, информативности и удобства использования. Вместо этого мы должны рассмотреть, как эти критерии взаимодействуют друг с другом в различных сочетаниях.

Для проведения такого комплексного анализа обычно применяется вектор Шепли, широко известный в теории кооперативных игр. В контексте нашего мобильного приложения для агрохолдинга, вектор Шепли поможет определить реальный вклад каждого критерия в общую оценку интерфейса.

Значения вектора Шепли лежат в интервале [0, 1], а их сумма равна единице. Это позволяет нам интерпретировать полученные результаты как относительную важность каждого аспекта интерфейса. Например, мы можем определить, что в нашем приложении информативность имеет значение 0,4, удобство использования – 0,3,

а скорость работы – 0,2, при этом их совместное влияние составляет оставшиеся 0,1.

Такой подход обеспечивает более точную и нюансированную оценку интерфейса, учитывающую сложные взаимосвязи между различными критериями, что особенно важно при разработке специализированных приложений для агробизнеса.

В работе детально рассмотрены критерии выбора оптимального пользовательского интерфейса мобильного приложения СППР при анализе посевных площадей, проведена аналитика ценности критериев для разных групп пользователей и использован интеграл Шоке для комплексной оценки и оптимизации интерфейса. Применение интеграла Шоке позволило учесть нелинейные взаимодействия между различными критериями, что обеспечило более точное моделирование предпочтений пользователей.

Список использованных источников

1. Garenne Bigby. Top 15 Tools for Measuring Website or Application Speed. – URL : https://dynomapper.com/blog/21-sitemaps-and-seo/457-top-15-tools-for-measuring-website-or-application-speed

2. Тимонин, М. В. Методы поиска экстремальных значений интеграла Шоке и их применение в задачах принятия решений / М. В. Тимонин. – 2018.

References

1. Garenn Bigby. The 15 best tools for measuring the speed of a website or application. – URL : https://dynomapper.com/blog/21-sitemaps-and-seo/457-top-15-tools-for-measuring-website-or-application-speed

2. Timonin, M. V. Methods of searching for extreme values of the Shoke integral and their application in decision-making problems / M. V. Timonin. – 2018.

УДК 004.5

В. А. Лукин
(Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: vlad@kerby.ru)

АДАПТИВНЫЙ МОБИЛЬНЫЙ ИНТЕРФЕЙС ДЛЯ СППР ПРИ АНАЛИЗЕ ПОСЕВНЫХ ПЛОЩАДЕЙ

Аннотация. Рассмотрены особенности требований к мобильному интерфейсу для системы помощи принятия решений при анализе посевных площадей, а также описан необходимый набор базовых функций.

Ключевые слова: пользовательский интерфейс, мобильное приложение, Flutter, UI/UX, агрохолдинг, СППР.

V. A. Lukin
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

ADAPTIVE MOBILE INTERFACE FOR DECISION SUPPORT SYSTEM FOR ANALYSIS OF CROP AREAS

Abstract. The features of the requirements for a mobile interface for a decision-making assistance system for analyzing acreage are considered, and the necessary set of basic functions is described.

Keywords: user interface, mobile application, Flutter, UI/UX, agricultural holding, DSS.

Внедрение инновационных IT-решений открывает новые возможности для оптимизации бизнес-процессов, повышения эффективности использования ресурсов, снижения издержек и роста производительности агрохолдингов. Переход на цифровые платформы, автоматизация операций, применение технологий больших данных, искусственного интеллекта и Интернета вещей становятся ключевыми факторами конкурентоспособности в агропромышленной отрасли. Вместе с тем, внедрение инноваций сопряжено с рядом вызовов, требующих комплексного подхода с учетом специфики деятельности агрохолдингов.

В проведенном исследовании акцент сделан на вопросах цифровой трансформации агропромышленного комплекса, оптимизации бизнес-процессов и внедрении инновационных ИТ-решений, которые активно исследуются отечественными и зарубежными учеными. Однако разработка конкретных программных продуктов, ориентированных

на автоматизацию деятельности агрохолдингов, остается малоизученной областью и требует дальнейших научных изысканий.

Научной новизной является интеграция современных мобильных технологий с задачами агропромышленного комплекса, что открывает новые возможности для повышения производительности труда агрономов, оптимизации использования ресурсов и улучшения общей эффективности сельскохозяйственного производства. Разработанное приложение представляет собой уникальный инструмент, объединяющий передовые достижения в области информационных технологий и специфические требования агропромышленной отрасли.

Оптимизация бизнес-процессов в агрохолдинге позволяет повысить его эффективность и производительность. Например, автоматизация и внедрение новых технологий в производственные процессы позволяет снизить затраты на рабочую силу, значительно увеличить выход продукции и повысить качество. Анализ и оптимизация логистических процессов помогает улучшить управление запасами, сократить временные затраты на доставку и повысить надежность поставок.

Самым важным критерием для мобильного приложения от агрохолдинга является возможность работы без подключения к Интернету.

Возможность работы мобильного приложения для агрохолдинга без подключения к Интернету является критически важной функцией, особенно когда речь идет о работе в полевых условиях. Сельскохозяйственные угодья часто расположены в отдаленных районах с ограниченным или нестабильным доступом к Интернету. В таких ситуациях наличие офлайн-режима обеспечивает бесперебойную работу приложения, позволяя сотрудникам выполнять свои задачи без перерывов и задержек, связанных с отсутствием подключения к сети.

Офлайн-режим позволяет пользователям получать доступ к ранее загруженным данным, таким как карты полей, информация о посевах, истории операций и другие важные сведения, необходимые для принятия решений и выполнения повседневных задач. Это обеспечивает непрерывность рабочего процесса и повышает эффективность работы сотрудников в полевых условиях. Кроме того, возможность вводить данные и обновлять информацию в автономном режиме с последующей синхронизацией при восстановлении подключения к Интернету гарантирует целостность и актуальность данных в системе агрохолдинга. Это особенно важно для своевременного принятия решений и планирования дальнейших действий на основе точной и обновленной информации.

Основные функции, которые необходимы мобильному приложению в СППР в управлении посевными площадями:

- Просмотр всех посевных площадей. На общей карте должны быть нанесены полигоны площадей, чтобы пользователь мог видеть общую картину расположения и как поля расположены относительно друг друга.
- Детальная страница посевных площадей. Должна быть возможность просмотра полной информации по полю, с возможностью изменения как общей информации, так и изменения засаженной культуры.
- Управление журналом работ на полях. В большинстве случаев на полях проводят такие работы как удобрение, управление семенным материалом и обработка почвы. Все акты данных работ должны быть сохранены в приложении и должна быть возможность их просмотра, управления и добавления новой записи.

В работе были детально рассмотрены текущие интерфейсы СППР для анализа посевных площадей, поставлены требования к необходимому функционалу, с помощью интеграла Шоке был выбран оптимальный интерфейс для основных пользователей в лице агрономов и управленцев, а также рассмотрены и построены модели классов в виде диаграмм в нотации UML.

Список использованных источников

1. Подповетная, Ю. В. Агрохолдинг: совершенствование и автоматизация / Ю. В. Подповетная, А. С. Орлова // Управление в современных системах. – 2018. – № 4(20).

2. Шагайда, Н. Характеристика агрохолдингов и их роль в сельском хозяйстве / Н. Шагайда // Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. – URL : https://www.ranepa.ru/sobytiya/novosti/rol-agroholdingov-v-rossijskom-selskom-hozyajstve

3. Реинжиниринг бизнес-процессов: этапы разработки и реализации // Клерк. – URL : https://www.klerk.ru/boss/articles/299721/

References

1. Podpovetnaya, Yu. V. Agroholding: improvement and automation / Yu. V. Podpovetnaya, A. S. Orlova // Management in modern systems. – 2018. – No. 4(20).

2. Shagaida, N. Characteristics of agricultural holdings and their role in agriculture / N. Shagaida // Russian Academy of National Economy and Public Administration under the President of the Russian Federation. – URL : https://www.ranepa.ru/sobytiya/novosti/rol-agroholdingov-v-rossijskom-selskom-hozyajstve

3. Business process reengineering: stages of development and implementation // Clerk: URL: https://www.klerk.ru/boss/articles/299721 /.

УДК 004

А. С. Мещеряков
(ВГЛТУ им. Г. Ф. Морозова, г. Воронеж, Россия,
e-mail: asm13052004@mail.ru)

СИСТЕМА АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ ДОЗИМЕТРОМ ДЛЯ ОЦЕНКИ РАДИАЦИОННОЙ ОБСТАНОВКИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ЗЕМЕЛЬ

Аннотация. Рассмотрена модель дозиметра, использующая эффект деградации электропараметров транзистора. При воздействии ионизирующего излучения на детектор система автоматического управления анализирует изменения в характеристиках транзистора и преобразует их в показания уровня радиации. Описан состав модели, принцип работы, преимущества, а также потенциальные области применения.

Ключевые слова: детектор, дозиметр, радиация, ионизирующие излучения, система автоматического управления.

A. S. Meshcheriakov
(VSUFT named after G. F. Morozov, Voronezh, Russia)

AN AUTOMATIC DOSIMETER CONTROL SYSTEM FOR ASSESSING THE RADIATION SITUATION OF AGRICULTURAL LANDS

Abstract. This article discusses a dosimeter model using the degradation effect of transistor electrical parameters. When exposed to ionizing radiation on the detector, the automatic control system analyzes changes in the characteristics of the transistor and converts them into radiation level readings. The composition of the model, the principle of operation, advantages, as well as potential applications are described.

Keywords: detector, dosimeter, radiation, ionizing radiation, automatic control system.

Дозиметры – это устройства, предназначенные для измерения уровня ионизирующего излучения. Большинство дозиметров основаны на счетчике Гейгера-Мюллера или ионизационных камерах, которые, как правило, являются громоздкими и дорогими. В последние годы в мире растет интерес к созданию более компактных и доступных дозиметров, которые основаны на полупроводниковых детекторах. В таких дозиметрах основным компонентом средств измерения дозы является программное обеспечение, которое в автоматизированном режиме будет способно по изменению электропараметров транзистора

определить поглощенную дозу с высокой точностью. Оно способно рассчитать дозу по изменению электропараметров прибора с учетом нелинейного характера зависимости, температуры окружающей среды, условий работы, технологического разброса детекторов, что обеспечивает высокую точность измерений.

Модель дозиметра, основанная на деградации электропараметров транзистора, включает в себя следующие основные элементы [1]:

1) КМОП – транзистор, подобранный для определения высокой чувствительности к воздействию ионизирующего излучения. Где под воздействием радиации деградируют его электропараметры, такие как пороговое напряжение ($U_{пор}$), которое служит основой для измерения уровня радиации (рис. 1, формула (1))

$$U_{пор} = F(D), \quad (1)$$

где $U_{пор}$ – пороговое напряжение; D – поглощенная доза ионизирующего излучения.

2) Измерительная схема предназначена для определения выбранного электропараметра транзистора.

3) Аналого-цифровой преобразователь (АЦП), который преобразует аналоговый сигнал с измерительной схемы в цифровой формат, удобный для обработки микропроцессором.

4) Микропроцессор – центральный элемент системы управления. Он обрабатывает данные, полученные от АЦП, выполняет калибровку, сравнивает текущие данные с эталонными значениями, вычисляет уровень радиации и управляет функциями дозиметра.

5) Сигнализация предупреждает оператора о превышении допустимого уровня радиации. Она может быть звуковой, световой, вибрационной.

6) Система управления реализует алгоритмы автоматического управления дозиметром. Она может включать: автоматическую калибровку, которая сравнивает электропараметры транзистора с эталонными значениями для компенсации дрейфа параметров; автоматическое управление сигналом тревоги, который активирует сигнализацию при превышении допустимого уровня радиации; автоматическую запись данных для последующего анализа.

Принцип работы:

В контактное устройство дозиметра помещается детектор с накопленной дозой ионизирующего излучения. Измерительная схема определяет на сколько деградировали электропараметры ($U_{пор}$) транзистора. АЦП преобразует аналоговый сигнал измерительной схемы в цифровой формат. Микропроцессор обрабатывает данные, получен-

ные от АЦП, сравнивает их с эталонными значениями, определяет уровень радиации в выбранных единицах измерения и выдает график на дисплей.

Если измеренный уровень радиации превышает допустимый уровень, автоматически включается звуковое оповещение (звуковой сигнал).

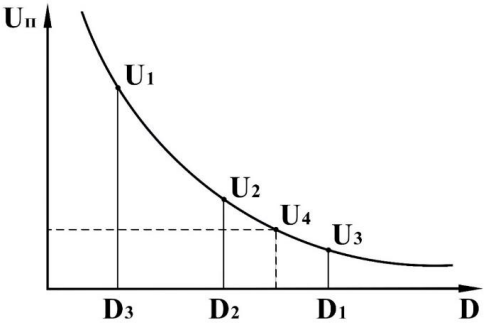


Рис. 1. График зависимости порогового напряжения от поглощенной дозы ионизирующего излучения

Таким образом дозиметр, основанный на деградации электропараметров транзистора, является интересным решением для измерения уровня радиации. Он обладает рядом преимуществ, таких как высокая чувствительность и низкая стоимость, но требует учета факторов, которые могут влиять на стабильность характеристик транзистора.

Список использованных источников

1. Таперо, К. И. Радиационные эффекты в кремниевых интегральных схемах космического применения / К. И. Таперо, В. Н. Улимов, А. М. Членов. – М. : БИНОМ. Лаборатория знаний, 2020. – 304 с.

References

1. Tapero, K. I. Radiation effects in silicon integrated circuits for space purposes / K. I. Tapero, V. N. Ulimov, A. M. Chlenov. – M. : BINOM. Laboratory of Knowledge, 2020. – 304 p.

УДК 004.89

И. С. Михайлов, Д. А. Полещенко
(Кафедра автоматизированных и информационных систем
управления им. Ю. И. Еременко,
СТИ НИТУ «МИСИС», г. Старый Оскол, Россия,
e-mail: mikhaylov.is@yandex.ru, po-dima@yandex.ru)

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО АНАЛИЗА ПОКАЗАТЕЛЕЙ РАЗВИТИЯ СЕЛЬСКОХОЗЯЙСТВЕННЫХ КУЛЬТУР ПО ИЗОБРАЖЕНИЮ С БПЛА

Аннотация. Разработан инструмент, предоставляющий возможность автоматизированного анализа изображений, полученных с беспилотных летательных аппаратов (БПЛА), и представления данных о развитии сельскохозяйственных культур в удобной для пользователя форме. Использование программного обеспечения способствует более эффективному мониторингу и управлению сельским хозяйством.

Ключевые слова: показатели развития сельскохозяйственных культур, индекс листовой поверхности.

I. S. Mikhailov, D. A. Poleshchenko
(Y. I. Eremenko Automated and information control systems chair,
STI NUST MISIS, Stary Oskol, Russia)

SOFTWARE DEVELOPMENT FOR AUTOMATED ANALYSIS OF CROP DEVELOPMENT INDICATORS BASED ON UAV IMAGES

Abstract. The research has developed a tool that allows for automated analysis of images taken by unmanned aerial vehicles (UAVs) and presents data on crop development in a user-friendly format. The use of this software contributes to more efficient monitoring and management of agricultural operations.

Keywords: Indicators of crop development, leaf area index.

Введение. В современных условиях сельского хозяйства автоматизация процессов становится ключевым фактором в улучшении производительности и обеспечении высокого качества продукции. Одним из наиболее перспективных направлений в этой области является применение беспилотных летательных аппаратов (БПЛА) в сочетании с передовым программным обеспечением для анализа изображений сельскохозяйственных угодий. Этот подход привлекает внимание множества исследователей по всему миру, подчеркивая его актуальность и потенциал.

В работе [1] рассматриваются различные методы оценки индекса листовой поверхности с использованием RGB-изображений, данных LiDAR и гиперспектральных изображений (HSI), полученных с БПЛА. Результаты исследования показали, что метод на основе гиперспектральных данных обеспечивает наивысшую точность, хотя и отличается высокой стоимостью. В связи с этим авторы предлагают комбинировать различные методы для достижения оптимальных результатов.

Исследование [2] посвящено оценке состояния почвенного покрова на экспериментальных участках с хлопком, сорго и сахарным тростником, используя изображения и ортофотопланы, полученные с БПЛА.

В работе [3] представлены результаты исследования по созданию системы автоматизированного контроля за развитием сельскохозяйственных культур на примере подсолнечника. Для этого использовались изображения, снятые с БПЛА, и нейронные сети, построенные на архитектурах YOLOv5 и U-Net. В рамках исследования предложены алгоритмы для оценки плотности всходов и индекса листовой поверхности.

Настоящее исследование продолжает развитие идей, предложенных в работе [3], и направлено на создание инструмента визуализации, обеспечивающего удобное взаимодействие с пользователем.

Разработка программного обеспечения. Было разработано программное обеспечение для определения показателей развития сельскохозяйственных культур. Для пользователя доступен следующий функционал: загрузка изображений исследуемых участков; просмотр и сканирование загруженных изображений; просмотр полученных показателей; просмотр местоположения исследуемого участка на карте по координатам.

В ПО реализовано окно главной формы (см. рис. 1), где показан доступный функционал и вывод количества загруженных изображений и состояние сканирования изображений.

Загружаемые в систему изображения проходят обработку и результат отображается на форме «Результат сканирования», представленной на рис. 2. Реализован просмотр изображения после детектирования и сегментации, координаты места съемки, а также показатели развития.

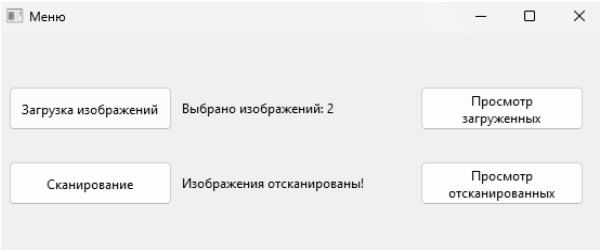


Рис. 1. Экранная форма «Меню»

Рис. 2. Экранная форма «Результат сканирования»

На данной форме показываются координаты снимка, также можно посмотреть место на Яндекс Картах, где была сделана данная фотография, нажав кнопку «Показать на карте».

Заключение. В работе разработано программное обеспечение, которое позволяет пользователям анализировать изображения и получать информацию о развитии сельскохозяйственных культур в удобной и наглядной форме.

Список использованных источников

1. Potato leaf area index estimation using multi-sensor unmanned aerial vehicle (uav) imagery and machine learning / T. Yu et al. // Remote Sensing. – 2023. – T. 15. – No. 16. – P. 4108.

2. Comparison of ground cover estimates from experiment plots in cotton, sorghum and sugarcane based on images and ortho-mosaics captured by UAV / T. Duan et al. // Functional Plant Biology. – 2016. – T. 44. – No. 1. – P. 169 – 183.

3. Poleshchenko, D. Development of a System for Automated Control of Planting Density, Leaf Area Index and Crop Development Phases by UAV Photos / D. Poleshchenko, V. Petrov, I. Mikhailov // 2023 7th International Conference on Information, Control, and Communication Technologies (ICCT). – IEEE, 2023. – P. 1 – 6.

4. ten Harkel, J. Biomass and crop height estimation of different crops using UAV-based LiDAR / J. ten Harkel, H. Bartholomeus, L. Kooistra // Remote Sensing. – 2019. – T. 12. – No. 1. – P. 17.

УДК 681.5

В. Н. Палаткин, А. В. Ачкасов
(ФГБОУ ВО «ВГЛТУ им. Г. Ф. Морозова», г. Воронеж, Россия,
e-mail: goodmorning5243@gmail.com, achkasov@list.ru**)**

УМНЫЕ АГРОТЕХНОЛОГИЧЕСКИЕ ПЛАТФОРМЫ НА ОСНОВЕ IoT И TINYML ДЛЯ УСТОЙЧИВОГО СЕЛЬСКОГО ХОЗЯЙСТВА

Аннотация. Проведен анализ современных подходов к разработке и внедрению умных агротехнологических платформ на основе технологий Интернета вещей (IoT) и машинного обучения на периферийных устройствах (TinyML) для повышения эффективности и устойчивости сельскохозяйственного производства. Рассматриваются ключевые компоненты таких платформ, их преимущества и потенциальные области применения. Особое внимание уделяется использованию TinyML для обработки данных.

Ключевые слова: Интернет вещей, IoT, TinyML, устойчивое сельское хозяйство, мониторинг почвы, беспроводные сенсорные сети, периферийные вычисления.

V. N. Palatkin, A. V. Achkasov
(Voronezh State University of Forestry and Technologies
named after G. F. Morozov, Voronezh, Russia)

SMART AGROTECH PLATFORMS BASED ON IoT AND TINYML FOR SUSTAINABLE AGRICULTURE

Abstract. The article analyzes modern approaches to the development and implementation of smart agrotech platforms based on the Internet of Things (IoT) and edge machine learning (TinyML) to improve the efficiency and sustainability of agricultural production. The key components of such platforms, their advantages and potential applications are considered. Particular attention is paid to the use of TinyML for data processing.

Keywords: Internet of Things, IoT, TinyML, sustainable agriculture, soil monitoring, wireless sensor networks, edge computing.

Введение. Современное сельское хозяйство сталкивается с множеством вызовов, включая изменение климата, истощение природных ресурсов и растущий спрос на продовольствие. В этих условиях внедрение умных технологий становится критически важным для повышения эффективности и устойчивости сельскохозяйственного производства. Интернет вещей (IoT) и технологии машинного обучения

на периферийных устройствах (TinyML) открывают новые возможности для создания интеллектуальных агротехнологических платформ, способных осуществлять мониторинг и оптимизацию сельскохозяйственных процессов в режиме реального времени [1].

Компоненты умных агротехнологических платформ. Современные умные агротехнологические платформы включают в себя несколько ключевых компонентов:

1. Сенсорные узлы: Различные датчики для измерения параметров почвы, климата и состояния растений. Это могут быть датчики температуры, влажности, pH почвы, освещенности и др.
2. Коммуникационная инфраструктура: Беспроводные сети для передачи данных от сенсорных узлов к центральному узлу или облачной платформе. Часто используются технологии LoRaWAN или NB-IoT, обеспечивающие большой радиус действия и низкое энергопотребление [2].
3. Центральный узел или шлюз: Устройство для сбора и первичной обработки данных с сенсорных узлов.
4. Облачная платформа: Серверная инфраструктура для хранения, анализа и визуализации данных.
5. Алгоритмы машинного обучения: Модели для анализа данных и принятия решений, которые могут работать как в облаке, так и на периферийных устройствах (TinyML).
6. Пользовательский интерфейс: Мобильные приложения или веб-интерфейсы для взаимодействия пользователей с системой.

Преимущества использования IoT и TinyML в сельском хозяйстве. Внедрение умных агротехнологических платформ на основе IoT и TinyML предоставляет ряд существенных преимуществ. Точный мониторинг состояния почвы и растений позволяет оптимизировать использование воды, удобрений и других ресурсов [3]. Интеграция с системами орошения, внесения удобрений и другим оборудованием позволяет автоматизировать многие сельскохозяйственные операции. Непрерывный мониторинг позволяет обнаруживать заболевания растений, вредителей или неблагоприятные условия на ранних стадиях. Оптимизация условий выращивания на основе данных и рекомендаций системы может значительно повысить урожайность культур. Более эффективное использование ресурсов и снижение применения химикатов способствует уменьшению негативного воздействия на окружающую среду [4]. Анализ исторических данных и текущих условий позволяет более точно прогнозировать урожайность и планировать производство.

Применение TinyML в умных агротехнологических платформах. Технология TinyML, позволяющая запускать модели машинного обучения на микроконтроллерах и других устройствах с ограниченными вычислительными ресурсами, открывает новые возможности для создания интеллектуальных сельскохозяйственных систем. Основные преимущества использования TinyML в агротехнологических платформах включают:

1. Низкое энергопотребление: Модели TinyML могут работать на устройствах с батарейным питанием в течение длительного времени, что критически важно для сенсорных узлов в полевых условиях.

2. Обработка данных в реальном времени: Анализ данных непосредственно на сенсорных узлах позволяет принимать решения и реагировать на изменения условий без задержек.

3. Снижение нагрузки на сеть: Обработка данных на периферийных устройствах уменьшает объем передаваемых данных, что особенно важно в условиях ограниченной пропускной способности сельских сетей.

4. Повышение приватности: Локальная обработка данных снижает риски, связанные с передачей и хранением конфиденциальной информации в облаке [5].

Примеры применения TinyML в умных агротехнологических платформах включают:

– классификация заболеваний растений на основе анализа изображений листьев;

– прогнозирование потребности в орошении на основе данных о влажности почвы и погодных условиях;

– обнаружение вредителей с помощью акустических сенсоров;

– оптимизация внесения удобрений на основе анализа состояния растений и почвы.

Проблемы и перспективы развития. Несмотря на значительный потенциал, внедрение умных агротехнологических платформ сталкивается с рядом проблем:

– начальные инвестиции в оборудование и инфраструктуру могут быть значительными, особенно для небольших фермерских хозяйств;

– эксплуатация и обслуживание таких систем требует определенных технических навыков, которых может не хватать традиционным фермерам;

– системы должны быть способны работать в сложных полевых условиях, включая экстремальные температуры, влажность и механические воздействия;

– отсутствие единых стандартов затрудняет интеграцию компонентов от разных производителей;

– защита собираемых данных от несанкционированного доступа и кибератак является критически важной задачей [6].

Перспективные направления развития умных агротехнологических платформ включают: разработку более энергоэффективных и долговечных сенсорных узлов, способных работать автономно в течение нескольких сезонов; развитие методов федеративного обучения для улучшения моделей машинного обучения без централизованного сбора данных [7]; интеграцию с БПЛА для мониторинга больших площадей и труднодоступных участков; использование технологий компьютерного зрения и гиперспектральной съемки для более точной оценки состояния растений; создание открытых платформ и стандартов для облегчения интеграции и обмена данными между различными системами.

Заключение. Умные агротехнологические платформы на основе IoT и TinyML представляют собой мощный инструмент для повышения эффективности и устойчивости сельскохозяйственного производства. Они позволяют оптимизировать использование ресурсов, повысить урожайность и снизить негативное воздействие на окружающую среду. Интеграция технологий TinyML открывает новые возможности для создания интеллектуальных систем, способных работать в сложных полевых условиях с минимальным энергопотреблением.

Список использованных источников

1. Яхяев, М. А. Применение технологий Интернета вещей в сельском хозяйстве / М. А. Яхяев, А. В. Петров // Цифровые технологии в АПК: состояние, потенциал и перспективы развития : сб. науч. тр. I Всерос. науч.-практ. конф. – Махачкала : ДГТУ, 2019. – С. 137 – 142.

2. Кузнецов, Н. В. Умные технологии в растениеводстве: перспективы внедрения / Н. В. Кузнецов, Е. А. Скворцова // Инновации в сельском хозяйстве. – 2020. – № 2(35). – С. 84 – 91.

3. Смирнов, А. Г. Разработка IoT-платформы для мониторинга параметров почвы / А. Г. Смирнов, И. В. Козлов // Вестник аграрной науки. – 2021. – № 3(90). – С. 115 – 123.

4. Федоров, В. М. Применение технологии TinyML в системах точного земледелия / В. М. Федоров // Достижения науки и техники АПК. – 2022. – Т. 36, № 4. – С. 73 – 79.

5. Ковалева, Е. Н. Анализ эффективности использования IoT-решений в сельском хозяйстве / Е. Н. Ковалева, С. А. Иванов // Экономика сельского хозяйства России. – 2023. – № 1. – С. 54 – 61.

6. Морозов, Д. С. Энергоэффективные решения для автономных сельскохозяйственных IoT-устройств / Д. С. Морозов // Техника и технологии АПК. – 2023. – № 2(38). – С. 28 – 35.

7. Соколова, А. В. Перспективы развития умных агротехнологических платформ в России / А. В. Соколова // Экономика сельскохозяйственных и перерабатывающих предприятий. – 2023. – № 5. – С. 45 – 52.

References

1. Yakhyaev, M. A. Application of the Internet of Things technologies in agriculture / M. A. Yakhyaev, A. V. Petrov // Digital technologies in the agro-industrial complex: state, potential and development prospects : collection of scientific papers of the I All-Russian scientific and practical conference. – Makhachkala : DSTU, 2019. – P. 137 – 142.

2. Kuznetsov, N. V. Smart technologies in crop production: implementation prospects / N. V. Kuznetsov, E. A. Skvortsova // Innovations in agriculture. – 2020. – No. 2(35). – P. 84 – 91.

3. Smirnov, A. G. Development of an IoT platform for monitoring soil parameters / A. G. Smirnov, I. V. Kozlov // Bulletin of agricultural science. – 2021. – No. 3(90). – P. 115 – 123.

4. Fedorov, V. M. Application of TinyML technology in precision farming systems / V. M. Fedorov // Achievements of science and technology of the agro-industrial complex. – 2022. – V. 36, No. 4. – P. 73 – 79.

5. Kovaleva, E. N. Analysis of the efficiency of using IoT solutions in agriculture / E. N. Kovaleva, S. A. Ivanov // Economics of agriculture in Russia. – 2023. – No. 1. – P. 54 – 61.

6. Morozov, D. S. Energy-efficient solutions for autonomous agricultural IoT devices / D. S. Morozov // Equipment and technologies of the agro-industrial complex. – 2023. – No. 2(38). – P. 28 – 35.

7. Sokolova, A. V. Prospects for the development of smart agrotechnological platforms in Russia / A. V. Sokolova // Economy of agricultural and processing enterprises. – 2023. – No. 5. – P. 45 – 52.

УДК 681.5

В. Н. Палаткин, А. В. Ачкасов
(ФГБОУ ВО «ВГЛТУ им. Г. Ф. Морозова», г. Воронеж, Россия»,
e-mail: goodmorning5243@gmail.com, achkasov@list.ru)

ПРИМЕНЕНИЕ КИПиА В ТОЧНОМ ЗЕМЛЕДЕЛИИ

Аннотация. Рассмотрены современные тенденции внедрения точного земледелия, основанного на использовании контрольно-измерительных приборов и автоматики (КИПиА) для оптимизации сельскохозяйственных процессов. Проведен анализ ключевых элементов КИПиА, обеспечивающих сбор и анализ данных о состоянии почвы, растений и окружающей среды. Оценены перспективы и динамика роста применения подключенных устройств в сельском хозяйстве.

Ключевые слова: точное земледелие, контрольно-измерительные приборы и автоматика (КИПиА), информационные технологии, подключенные устройства, сельское хозяйство, оптимизация процессов, данные о почве и растениях.

V. N. Palatkin, A. V. Achkasov
(Voronezh State University of Forestry and Technologies named
after G. F. Morozov, Voronezh, Russia)

APPLICATION OF INSTRUMENTATION AND AUTOMATION (KIPiA) IN PRECISION AGRICULTURE

Abstract. The article examines modern trends in the implementation of precision agriculture based on the use of instrumentation and automation (KIPiA) to optimize agricultural processes. An analysis of the key elements of KIPiA that ensure the collection and analysis of data on the condition of soil, plants, and the environment is provided. The prospects and growth dynamics of the application of connected devices in agriculture are also assessed.

Keywords: precision agriculture, instrumentation and automation (KIPiA), information technology, connected devices, agriculture, process optimization, soil and plant data.

Введение. Точное земледелие представляет собой современный подход к управлению сельскохозяйственным производством, основанный на использовании информационных технологий, спутниковой навигации, автоматизированных систем и датчиков для оптимизации производственных процессов. Ключевым элементом точного земледелия является применение контрольно-измерительных приборов и автоматики (КИПиА), которые позволяют собирать, анализировать

и использовать данные о состоянии почвы, растений и окружающей среды для принятия обоснованных управленческих решений [1].

В последние годы наблюдается стремительный рост внедрения КИПиА в сельском хозяйстве. По данным отчета Global Connected Agriculture Market, в 2022 году в мире насчитывалось около 23 млн подключенных устройств в сельском хозяйстве, а к 2030 году ожидается увеличение этого показателя до 187 млн, при этом годовой темп прироста в растениеводстве составляет 41% [2]. Это свидетельствует о высокой актуальности и перспективности применения КИПиА в точном земледелии.

Основные типы КИПиА в точном земледелии. Датчики состояния почвы являются одним из наиболее распространенных типов КИПиА в точном земледелии. Они позволяют измерять такие параметры, как влажность, температура, pH, электропроводность и содержание питательных веществ в почве. По оценкам экспертов, к 2025 году мировой рынок датчиков для сельского хозяйства достигнет 2,5 млрд долларов, при этом датчики состояния почвы будут составлять около 30% этого рынка [3]. Агротехнологические платформы позволяют фермерам получать точную информацию о состоянии почвы в режиме реального времени и принимать обоснованные решения по управлению посевами.

Метеорологические станции также играют важную роль в точном земледелии, предоставляя данные о погодных условиях, которые влияют на рост и развитие сельскохозяйственных культур. Современные метеостанции оснащены датчиками температуры воздуха, влажности, скорости и направления ветра, количества осадков и солнечной радиации. По данным исследования, проведенного в 2023 году, около 65% крупных сельскохозяйственных предприятий в развитых странах используют автоматизированные метеостанции для мониторинга погодных условий на своих полях [4]. Это позволяет им более точно планировать сроки посева, полива и внесения удобрений, а также прогнозировать риски, связанные с неблагоприятными погодными явлениями.

Системы дистанционного зондирования, включающие спутниковые снимки и беспилотные летательные аппараты (БПЛА), становятся все более популярными в точном земледелии. Они позволяют получать информацию о состоянии посевов на больших площадях, выявлять проблемные участки и оценивать эффективность агротехнических мероприятий. Согласно исследованию, проведенному в 2022 году, мировой рынок БПЛА для сельского хозяйства оценивался в 1,2 млрд долларов, и ожидается, что к 2028 году он достигнет 5,7 млрд долларов

при среднегодовом темпе роста 31,1% [5]. Это свидетельствует о растущем интересе к использованию БПЛА в сельском хозяйстве для сбора данных и мониторинга состояния посевов.

Системы точного внесения удобрений и средств защиты растений позволяют оптимизировать использование ресурсов и минимизировать негативное воздействие на окружающую среду. Они включают в себя датчики, определяющие потребность растений в питательных веществах, и автоматизированные системы внесения, способные регулировать дозировку в зависимости от конкретных условий на каждом участке поля. По данным отчета Global Precision Agriculture Market, к 2025 году мировой рынок систем точного внесения удобрений и средств защиты растений достигнет 10,2 млрд долларов, при этом ежегодный рост составит около 13% [6].

Преимущества применения КИПиА в точном земледелии. Использование КИПиА в точном земледелии обеспечивает ряд существенных преимуществ для сельскохозяйственных производителей:

1. Точное управление внесением удобрений и средств защиты растений на основе данных, полученных с помощью КИПиА, позволяет повысить урожайность на 10…15% [7].

2. Применение систем точного внесения удобрений и средств защиты растений позволяет сократить их расход на 20…30%, что снижает затраты и уменьшает негативное воздействие на окружающую среду [6].

3. Мониторинг состояния почвы и растений с помощью КИПиА позволяет оптимизировать условия выращивания и повысить качество сельскохозяйственной продукции.

4. Использование метеорологических станций и систем прогнозирования позволяет минимизировать риски, связанные с неблагоприятными погодными условиями.

Проблемы и перспективы развития КИПиА в точном земледелии. Несмотря на очевидные преимущества, внедрение КИПиА в точном земледелии сталкивается с рядом проблем:

1. Высокая стоимость оборудования и технологий, особенно для малых и средних фермерских хозяйств.

2. Необходимость обучения персонала работе с новыми технологиями.

3. Проблемы совместимости и интеграции различных устройств и систем.

4. Обеспечение надежности и долговечности оборудования в полевых условиях.

5. Вопросы информационной безопасности и защиты данных.

Однако, несмотря на эти проблемы, перспективы развития КИПиА в точном земледелии остаются очень высокими. Ожидается, что к 2030 году мировой рынок технологий точного земледелия достигнет 23,1 млрд долларов, при этом значительная часть этого рынка будет приходиться на КИПиА [8].

Заключение. Применение КИПиА в точном земледелии представляет собой перспективное направление развития сельскохозяйственного производства, позволяющее повысить эффективность использования ресурсов, увеличить урожайность и качество продукции, а также снизить негативное воздействие на окружающую среду. Несмотря на существующие проблемы, связанные с внедрением новых технологий, ожидается дальнейший рост рынка КИПиА для точного земледелия, что будет способствовать повышению эффективности и устойчивости сельскохозяйственного производства в глобальном масштабе.

Список использованных источников

1. Интеллектуальные системы в точном земледелии: обзор и перспективы / М. В. Щербаков, А. Бребельс, Н. Л. Щербакова, А. П. Тюков // Известия Волгоградского государственного технического университета. – 2021. – № 3(250). – С. 7 – 14.

2. Global Connected Agriculture Market Report. (2023). Counterpoint Research: сайт. – URL : https://www.counterpointresearch.com/insights/global-connected-agriculture-market-shipments-2022/ (дата обращения: 15.09.2024).

3. Sharma, R., Kumar, S. (2022). Soil sensors for precision agriculture: A comprehensive review. Sensors, 22(3), 1024.

4. Johnson, L., & Smith, K. (2023). The impact of automated weather stations on modern agriculture. Journal of Agricultural Technology, 15(2), 123 – 135.

5. Agricultural Drones Market Size, Share & Trends Analysis Report. (2022). Grand View Research: сайт. – URL : https://www.grandviewresearch.com/industry-analysis/agriculture-drones-market (дата обращения: 15.09.2024).

6. Global Precision Agriculture Market Report. (2021). MarketsandMarkets : сайт. – URL : https://www.marketsandmarkets.com/Market-Reports/precision-farming-market-1243.html (дата обращения: 15.09.2024).

7. Петров, А. В. Эффективность применения технологий точного земледелия в растениеводстве / А. В. Петров, Е. Н. Иванова // Аграрный научный журнал. – 2020. – № 5. – С. 14 – 18.

8. Precision Farming Market – Growth, Trends, COVID-19 Impact, and Forecasts (2023 – 2028). (2023). Mordor Intelligence : сайт. – URL : https://www.mordorintelligence.com/industry-reports/global-precision-farming-market-industry (дата обращения: 15.09.2024).

References

1. Intelligent systems in precision agriculture: Review and prospects / M. V. Shcherbakov, A. Brebels, N. L. Shcherbakova, A. P. Tyukov // Izvestia of the Volgograd State Technical University. – 2021. – No. 3(250). – P. 7 – 14.

2. Global Connected Agriculture Market Report. (2023). Counterpoint Research : сайт. – URL : https://www.counterpointresearch.com/insights/global-connected-agriculture-market-shipments-2022/ (date: 15.09.2024).

3. Sharma, R., Kumar, S. (2022). Soil sensors for precision agriculture: A comprehensive review. Sensors, 22(3), 1024.

4. Johnson, L., & Smith, K. (2023). The impact of automated weather stations on modern agriculture. Journal of Agricultural Technology, 15(2), 123 – 135.

5. Agricultural Drones Market Size, Share & Trends Analysis Report. (2022). Grand View Research: сайт. – URL : https://www.grandviewresearch.com/industry-analysis/agriculture-drones-market (date: 15.09.2024).

6. Global Precision Agriculture Market Report. (2021). MarketsandMarkets : сайт. – URL : https://www.marketsandmarkets.com/Market-Reports/precision-farming-market-1243.html (date: 15.09.2024).

7. Petrov, A. V., Ivanova, E. N. (2020). The effectiveness of precision agriculture technologies in crop production. Agrarian Scientific Journal, 5, 14 – 18.

8. Precision Farming Market – Growth, Trends, COVID-19 Impact, and Forecasts (2023-2028). (2023). Mordor Intelligence : сайт. – URL : https://www.mordorintelligence.com/industry-reports/global-precision-farming-market-industry (date: 15.09.2024).

УДК 681.5

В. Г. Матвейкин, П. К. Правин, Б. С. Дмитриевский, А. А. Терехова
(Кафедра «Информационные процессы и управление»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: terehova-95@yandex.ru)

ИСПОЛЬЗОВАНИЕ МОДЕЛИ ГРЕЯ МАРКОВА ДЛЯ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЙ ОБОРУДОВАНИЯ

Аннотация. Рассмотрена модель Грея Маркова для прогнозирования отказов оборудования из-за человеческой ошибки. Принимается во внимание, что отказы носят динамический характер и модель корректируется для повышения точности. Получен критерий разделения состояний и дана матрица вероятности перехода состояний. Проверена точность предложенной модели.

Ключевые слова: математическая модель, модель Грея Маркова, прогнозирование, отказ, состояние системы.

V. G. Matveykin, P. K. Praveen, B. S. Dmitrievsky, A. A. Terekhova
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

USING THE GRAY MARKOV MODEL TO PREDICT EQUIPMENT CONDITIONS

Abstract. The Gray Markov model for predicting failures due to human error is considered. It is taken into account that the failures are dynamic and the model is adjusted to improve accuracy. A criterion for the separation of states is obtained and a probability matrix for the transition of states is given. The accuracy of the proposed model has been verified.

Keywords: mathematical model, Gray Markov model, forecasting, failure, system state.

Поскольку человеческие ошибки не поддаются обобщению, мы можем сказать, что данные об ошибках являются случайными. Мы выбрали модель Грея Маркова [1] для прогнозирования или оценки ошибок по следующим причинам:

A. Ошибка не является регулярной и ее нельзя обобщить.

B. Она разбросана случайным образом.

C. Информация о необработанных данных ограничена.

D. Информация не является ни идеальной, ни определенной.

Принимая во внимание случайность данных, отказ во временном ряду может быть выражен как последовательность, сгенерированная с близким средним значением.

Согласно методу прогнозирования облачности системы Grey, модель прогнозирования может быть выражена дифференциальным уравнением первого порядка. Чтобы повысить точность прогнозирования и максимально приблизить его к реальной ситуации, модель корректируется.

Данные для статистики отказов из-за отсутствия технического обслуживания могли бы быть больше, а поскольку поведение человека крайне неопределенно, следовательно, регулярность может быть слабой по своей природе или не очень сильной. Чтобы повысить точность прогнозирования и максимально приблизить его к реальной ситуации, модель корректируется для повышения точности.

Измененный принцип и алгоритм заключаются в следующем. При первом получении последовательности данных остатков получается следующее прогнозируемое значение и фактическое значение. Если в первый раз поправка к остаткам не смогла обеспечить точность требуемого прогноза, то должна быть выполнена вторая поправка к остаткам и так далее до тех пор, пока не будут выполнены требуемые требования к точности.

Кривая, которую мы получим из прогноза, по существу, будет экспоненциальной кривой, а результатом предсказания будет плавная кривая. Марковская модель принята для прогнозирования тенденций состояния посредством передачи вероятности, которую она может адаптировать к случайности и изменчивости состояния.

Сбои в оборудовании из-за отсутствия технического обслуживания могут меняться ежегодно и представляют собой динамический нестационарный случайный процесс. Следовательно, показатели точности, соответствующие прогнозу, также должны быть переменными и случайными, поскольку границы и значение различных годовых состояний могут меняться. Следовательно, необходимо получить критерий адаптивного разделения состояний, и этот критерий должен соответствовать основной временной тенденции отказов оборудования из-за отсутствия технического обслуживания.

Когда мы говорим, что состояние разделено, количество различных интервалов может быть разумно разделено в соответствии с реальной ситуацией. Если наши исходные данные будут меньше, то интервальное деление должно быть меньше, чтобы увеличить количество переводов между различными группами, и, таким образом, закон о передаче должен быть более объективно отражен между группами.

И наоборот, если исходных данных будет больше, интервальное деление должно быть меньше, чтобы извлечь больше информации

из большого количества данных для повышения точности прогнозирования. Целесообразно адаптировать метод кластерной классификации для определения номера класса и интервалов классификации из-за меньшего количества данных и неопределенного статуса отказов оборудования из-за отсутствия технического обслуживания в результате человеческой ошибки.

Матрица вероятности перехода состояния отражает все статистические закономерности перехода состояния и управление будущим состоянием системы может быть предсказано путем исследования матрицы. При фактическом анализе процесса обычно рассматривается только матрица вероятности перехода на один шаг.

Будущее состояние системы будет определено путем исследования матрицы вероятностей перехода состояния, и также будет определен интервал изменения первого приближения относительного прогнозируемого значения в будущие моменты времени.

Чтобы проверить точность предлагаемой модели, необходимы испытания оборудования для определения погрешности между прогнозируемым значением и фактическим значением. Для оценки точности модели используется относительная ошибка. Относительная погрешность сравнивает реальные и прогнозируемые значения в определенный момент времени. Общая точность модели может быть определена по средней относительной погрешности.

Результаты анализа, основанные на модели прогнозирования, показывают, что если произойдет халатность при обслуживании оборудования из-за человеческой ошибки, это приведет к отказам оборудования. Индекс точности Грея предполагает, что он может предсказать близкие к точным результатам отказа оборудования для указанных условий.

Список использованных источников

1. Xiang-cheng JIANG, Senfa CHEN, Application of Weighted Markov SCGM (1,1) c Model to Predict Drought Crop Area, Systems Engineering // Theory & Practice. – 2009. – V. 29, Is. 9. – P. 179 – 185. – URL : https://doi.org/10.1016/S1874-8651(10)60072-5

УДК 681.5

П. К. Правин
(ТОО биологических и решений в области безопасности,
Мумбаи, Индия,
e-mail: Praveen.singh.rajput21@gmail.com)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ С ИСПОЛЬЗОВАНИЕМ ДАТЧИКОВ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ ПО ОПТИМИЗАЦИИ СБОРА ВИНОГРАДА

Аннотация. В статье обсуждаются оптимальные сроки сбора винограда в арена Нашик в штате Махараштра в Индии, который известен как «Винная столица Индии», крупный регион по производству винограда в Индии. Сроки сбора урожая существенно влияют как на качество, так и на урожайность винограда, что напрямую влияет на рентабельность виноградников.

Ключевые слова: Виноград, Сбор урожая, Скрытая Марковская модель, Байесовский вывод, Монте-Карло, Интернет вещей, Датчики, ленивый алгоритм Витерби.

P. K. Praveen
(AGG Lifesciences and Safety Solutions LLP, Mumbai, India)

MATHEMATICAL MODEL INTRODUCING IOT SENSORS FOR DECISION MAKING OF THE OPTIMIZATION OF THE GRAPE HARVEST

Abstract. This article discusses about the optimal timing to harvest the grapes in the arena of Nashik in the state of Maharashtra in India which is popularly known as «Wine Capital of India», a major region for the production of grapes in India. Harvest timings significantly influence both the quality and yield of grapes, which directly affects the profitability of vineyards.

Keywords: Grape, Harvest, Hidden Markov Model, Bayesian Inference, Monte Carlo, IoT, Sensors, Lazy Viterbi Algorithm.

Выращивание винограда в Нашике регулярно сталкивается с трудностями из-за колебаний погодных условий, таких как перепады температуры, количества осадков и влажности, которые влияют на созревание винограда. Точные сроки сбора урожая имеют решающее значение для обеспечения максимального качества винограда и его урожайности. Традиционные методы часто включают ручную проверку и принятие решений на основе опыта, основанного на дегустации, осмотре, наблюдении:

A. Цвет кожицы окрашенного винограда меняется с зеленого на красный, синий или черный.

B. Ягоды винограда начинают размягчаться, белый виноград становится более прозрачным.

C. Уровень сахара начинает повышаться.

D. Кислотность начинает снижаться.

E. pH сока начинает повышаться.

F. Цвет сока начинает меняться. Белый цвет – от зеленоватого до беловатого. Красные – начинают приобретать некоторый кожичный пигмент.

G. Танины в кожице начинают полимеризоваться.

H. Начинают усиливаться сортовые вкусовые качества.

I. Рахис начинает созревать.

J. Между плодоножкой (плодоножкой виноградной ягоды) и ягодой винограда начинает развиваться зона абсцесса.

K. Семена начинают созревать.

Вышеприведенные методы не учитывают различные факторы окружающей среды. Предлагается математическая структура, которая объединяет датчики Интернета вещей для мониторинга состояния виноградников в режиме реального времени, вероятностное моделирование для оценки скрытых стадий созревания винограда и передовые методы, такие как байесовский вывод и анализ чувствительности методом Монте-Карло.

Мы используем марковскую модель (HMM), которая моделирует процесс созревания винограда с течением времени. Математическая модель включает датчики Интернета вещей для сбора данных в режиме реального времени, байесовский вывод для динамического обновления параметров модели и анализ чувствительности для оценки надежности процесса принятия решений.

Модель (HMM) отражает стохастический процесс созревания винограда, при котором фактическое состояние спелости не поддается непосредственному наблюдению, но наблюдаемые переменные предоставляют косвенную информацию об этих состояниях. HMM определяется следующими компонентами:

Скрытые состояния St представляют истинные стадии созревания винограда в момент времени t, которые непосредственно не наблюдаются:

$$St \in \{S1, S2, S3, S4\},$$

где S1 – незрелый виноград; S2 – приближается к спелости; S3 – оптимальная спелость; S4 – перезрелый виноград.

Переменные наблюдения Ot: Вектор наблюдения Ot состоит из измеримых факторов, собранных датчиками Интернета вещей, установленными на винограднике: Tt: Температура (°C). Rt: Количество осадков (мм). Bt: Уровень сахара по шкале Брикса. ph: Уровень кислотности. Mt: Содержание влаги в почве (%).

Датчики Интернета вещей, установленные по всему винограднику, постоянно отслеживают условия окружающей среды и показатели спелости винограда. Эти датчики измеряют такие переменные, как температура, количество осадков, содержание сахара (уровень Брикса), кислотность (уровень pH) и влажность почвы. Данные, собранные с датчиков в режиме реального времени, формируют вектор наблюдения Ot.

Мы предполагаем предварительное распределение Дирихле для каждой строки матрицы перехода A. Чтобы определить наиболее вероятную последовательность скрытых состояний (S1, S2, ..., ST) на основе наблюдений (O1, O2, ..., OT), мы используем ленивый алгоритм Витерби. Этот алгоритм эффективно вычисляет наиболее вероятную последовательность состояний, динамически пересчитывая только при необходимости. Как только определено конечное состояние в момент времени t, путем обратного поиска по сохраненным вероятностям состояний получается наиболее вероятная последовательность состояний.

Решение о сборе урожая основывается на вероятности того, что виноград находится в состоянии «оптимальной спелости» S3. Представим эту вероятность в момент времени t. При этом учитывается пороговое значение, которое выбирается исходя из практических соображений, таких как рыночные условия, прогнозы погоды и логистические ограничения. Кроме того, мы учитываем затраты на ранний или поздний сбор урожая в процессе принятия решений.

Чтобы оценить надежность модели в условиях неопределенности, мы проводим анализ чувствительности методом Монте-Карло. Для этого необходимо многократно запускать модель, каждый раз беря за основу апостериорные распределения вероятностей перехода и выбросов, а также распределения внешних условий, таких как температура и количество осадков.

Для каждого выбранного набора параметров запускается алгоритм ленивого Витерби, чтобы оценить наиболее вероятную последовательность скрытых состояний. Интересующие результаты, такие как вероятность достижения состояния S3 «оптимальной зрелости» и общая ожидаемая стоимость, регистрируются для каждой итерации по методу Монте-Карло.

После выполнения моделирования методом Монте-Карло в течение большого числа итераций (например, 10 000) мы анализируем чувствительность модели к изменениям входных параметров, вычисляя коэффициенты корреляции между выбранными параметрами и результатами. Кроме того, мы используем методы анализа чувствительности, основанные на дисперсии, для количественной оценки вклада каждого параметра в дисперсию результатов.

Разработанная модель позволяет управляющим виноградниками оптимизировать сроки сбора урожая, тем самым повышая качество и урожайность винограда и сводя к минимуму риски преждевременного или запоздалого сбора урожая.

УДК 004.56

П. И. Карасев[2], Ф. М. Пыршев[2], М. А. Ивановский[1], И. А. Дьяков[1]
([1]Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия,
e-mail: fpyrshiev@bk.ru, karasev@mirea.ru)

ОБУЧЕНИЕ СОТРУДНИКОВ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРЕДОТВРАЩЕНИЯ ВНУТРЕННИХ УГРОЗ

Аннотация. Настоящая статья представляет анализ методов обучения и повышения осведомленности сотрудников о принципах информационной безопасности, а также их влияние на снижение внутренних угроз для предприятий.

Ключевые слова: информационная безопасность, обучение сотрудников, человеческий фактор, внутренние угрозы, повышение осведомленности.

P. I. Karasev[2], F. M. Pyrshev[2], M. A. Ivanovskiy[1], I. A. Dyakov[1]
([1]Department of Information Systems and Information Protection,
TSTU, Tambov, Russia;
[2]Department of Information Security, RTU MIREA, Moscow, Russia)

TRAINING EMPLOYEES IN THE BASICS OF INFORMATION SECURITY TO PREVENT INTERNAL THREATS

Abstract. This article presents an analysis of methods of training and raising awareness of employees about the principles of information security, as well as their impact on reducing internal threats to enterprises.

Keywords: information security, employee training, human factor, internal threats, awareness raising.

Введение. В эпоху цифровизации бизнес-процессов и постоянного роста объемов цифровой информации, информационная безопасность выходит на передний план как один из приоритетных аспектов устойчивого развития и конкурентоспособности предприятий [1]. Защита информационных активов от несанкционированного доступа, вредоносных атак, утечек данных и других угроз становится не просто задачей IT-отдела, но стратегической задачей управления на всех уровнях организации. Помимо технических средств защиты, значительную роль в обеспечении информационной безопасности играет

человеческий фактор. Таким образом, систематическое обучение и повышение осведомленности персонала по вопросам информационной безопасности являются неотъемлемыми элементами стратегии защиты информационных ресурсов предприятия.

Основная часть. В современном обществе, информация становится одним из ключевых активов для любой организации или индивида. Защита этой информации является критически важной для поддержания конфиденциальности, целостности и доступности данных [2]. Обучение сотрудников имеет решающее значение для защиты данных. Правильное обучение поможет выстроить первую линию обороны от утечек информации, кражи данных и других видов атак.

Обучение помогает повысить осведомленность сотрудников о возможных угрозах, научить их распознавать подозрительные ситуации и действия, а также правильно реагировать на них.

Краткий обзор основных угроз информационной безопасности, связанных с человеческим фактором.

Человеческий фактор играет значительную роль в обеспечении информационной безопасности [3]. Ошибки сотрудников, недостаточная осведомленность о принципах безопасности и целенаправленные вредоносные действия внутренних лиц могут стать причиной серьезных угроз для организаций. Среди ключевых угроз, связанных с человеческим фактором, выделяют: социальную инженерии, фишинг, несанкционированный доступ, внутренние угрозы.

Защита от этих и других угроз требует комплексного подхода, включая технические средства защиты, обучение персонала основам информационной безопасности и разработку эффективных политик безопасности [4].

Методы обучения сотрудников по информационной безопасности: онлайн-курсы и вебинары, корпоративные тренинги и семинары, симуляция фишинга, обучение на примерах из реальной жизни, тестирование знаний и навыков.

Преимущества обучения сотрудников: повышение уровня осведомленности сотрудников, улучшение навыков сотрудников, создание атмосферы ответственности и доверия в компании, снижение вероятности возникновения внутренних угроз со стороны сотрудников, как намеренных, так и случайных, улучшение репутации компании и повышение доверия клиентов и партнеров, сокращение потенциальных финансовых потерь и репутационных убытков, повышение профессионального уровня сотрудников, обеспечение соответствия компании требованиям законодательства и стандартам безопасности данных.

Вывод. В заключении можно сделать вывод: обучение и повышение осведомленности сотрудников в области информационной безопасности является ключевым аспектом защиты организации от внутренних и внешних угроз. Важно подходить к процессу обучения комплексно, сочетая различные методы и инструменты для охвата широкого круга тем и сценариев. Эффективное обучение должно включать как теоретические аспекты безопасности, так и практические упражнения, моделирующие реальные угрозы и ситуации. Использование игровых элементов и реалистичных симуляций может значительно усилить вовлеченность и интерес сотрудников, повышая эффективность учебного процесса. Наконец, регулярное тестирование и обновление знаний помогут поддерживать высокий уровень осведомленности и готовности сотрудников к действиям в условиях изменяющейся информационной среды.

Список использованных источников

1. Васильков, А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков. – М. : ФОРУМ: ИНФРА-М, 2013. – 368 с.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин – СПб. : СПбНИУИТМО, 2014. – 173 с.

3. Малюк, А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк. С. В. Пазизин, Н. С. Погожин. – М. : Горячая линия – Телеком, 2001. – 148 с.

4. Мельников, В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. – М. : Финансы и статистика, 2003. – 368 с.

References

1. Vasilkov, A. V. Security and access control in information systems / A. V. Vasilkov. – M. : FORUM: INFRA-M, 2013. – 368 p.

2. Zhigulin, G. P. Organizational and legal provision of information security / G. P. Zhigulin. – St. Petersburg : St. Petersburg State University ITMO, 2014. – 173 p

3. Malyuk, A. A. Introduction to information security in automated systems / A. A. Malyuk. S. V. Pazizin, N. S. Pogozhin. – M. : Hotline – Telecom, 2001. – 148 p.

4. Melnikov, V. V. Information security in automated systems / V. V. Melnikov. – M. : Finance and Statistics, 2003. – 368 p.

УДК 004.051

П. И. Карасев[2], Ф. М. Пыршев[2],
М. А. Ивановский[1], И. А. Глазкова[1]
([1]Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия,
e-mail: fpyrshiev@bk.ru, karasev@mirea.ru)

ПРИМЕНЕНИЕ СЕТЕВЫХ АНАЛИЗАТОРОВ И ТЕСТОВ НА ПРОНИКНОВЕНИЕ ПРИ АУДИТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Рассмотрена возможность аудита информационной безопасности с использованием сетевых анализаторов и тестов на проникновение в рамках современных условий рынка.

Ключевые слова: тестирование на проникновение, сетевые анализаторы, уязвимость, кибератаки.

P. I. Karasev[2], F. M. Pyrshev[2],
M. A. Ivanovskiy[1], I. A. Glazkova[1]
([1]Department of Information systems and information protection, TSTU,
Tambov, Russia;
[2]Department of Information Security,
RTU MIREA, Moscow, Russia)

AUDIT OF INFORMATION SECURITY OF ORGANIZATIONS USING NETWORK ANALYZERS AND PENETRATION TESTS

Abstract. The article considers the possibility of auditing information security using network analyzers and penetration tests within the framework of modern market conditions.

Keywords: penetration testing, network analyzers, vulnerability, cyber-attacks.

Введение. Актуальность аудита информационной безопасности в современных условиях обусловлена ростом числа кибератак, с каждым годом количество кибератак увеличивается, что делает информационную безопасность одной из главных забот для бизнеса и государственных учреждений. Развитие технологий приводит к усложнению ИТ-инфраструктур, что требует более тщательного подхода к обеспечению безопасности. Таким образом, аудит информационной безопасности остается актуальным и необходимым инструментом для обеспе-

чения безопасности данных и защиты интересов компаний и организаций в условиях постоянно растущих киберугроз [1].

Основная часть. В само понятие аудита информационной безопасности входит процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определенными критериями и показателями безопасности. Задачами аудита является анализ текущего состояния информационной безопасности организации с последующим выявлением уязвимостей и потенциальных угроз, разработкой рекомендаций по улучшению системы информационной безопасности и контроль за их выполнением. Таким образом, аудит информационной безопасности дает возможность организациям оценить готовность системы и персонала к возможным атакам, а также выявить слабые места и устранить их. Аудит информационной безопасности включает в себя различные методы и подходы, направленные на оценку текущего состояния системы защиты информации и выявление возможных уязвимостей. В данной статье рассматриваются методы, включающие в себя использование сетевых анализаторов и тестов на проникновение.

Сетевые анализаторы – это инструменты, предназначенные для анализа сетевого трафика в реальном времени. Они выполняют функции, аналогичные сетевым мониторам, но дополнительно помогают выявлять причины неполадок в сети и устранять их. Они бывают нескольких видов: Анализаторы протоколов (Protocol Analyzers) – инструменты, позволяющие просматривать и анализировать данные, передаваемые по сети, на уровне отдельных протоколов. Примеры: Wireshark, TCPDump. Сетевые мониторы (Network Monitors) – обеспечивают мониторинг сетевого трафика, но не всегда предоставляют детализированный анализ данных. Примеры: Zabbix, Nagios. Системы обнаружения вторжений (Intrusion Detection Systems, IDS) – специализированы на выявлении несанкционированных действий в сети, таких как попытки взлома. Примеры: Snort, Suricata.

Принцип работы сетевых анализаторов заключается в том, чтобы перехватить весь трафик или его часть, который идет между сервером и клиентом, декодировать его содержимое и структуру, и проанализировать данный трафик на предмет каких-либо подозрительных активностей или аномалий. Таким образом, сетевые анализаторы позволяют обнаруживать и устранять проблемы до того, как они приведут к серьезным сбоям или утечке данных.

Тесты на проникновение (пентест) – это метод оценки безопасности компьютерных систем или сетей путем моделирования атаки зло-

умышленника. Цель пентеста – оценить возможность осуществления атаки и спрогнозировать экономические потери в случае успешного проникновения. Есть внутренний и внешний пентест, первый направлен на оценку безопасности системы со стороны внешнего потенциального злоумышленника, а второй со стороны внутреннего сотрудника, имеющего доступ к системе. По итогу тестирования составляются документы, содержащие описание проведенных тестов, выявленные уязвимости и рекомендации по их устранению, что помогает обеспечить информационную безопасность системы, позволяя предотвратить возможные атаки [3].

Вывод. Таким образом, в совокупности, использование сетевых анализаторов и тестов на проникновение позволяют аудиторам и специалистам по информационной безопасности получить более детальную картину состояния сетевой системы организации, делая процесс аудита более оптимизированным и эффективным, что в свою очередь позволяет предотвратить потенциальные кибератаки, минимизировать ущерб от уже произошедших инцидентов и поддерживать высокий уровень доверия клиентов и партнеров.

Список использованных источников

1. Кибербезопасность в 2023–2024 гг.: тренды и прогнозы [Электронный ресурс]. Часть третья : [сайт]. – URL : https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (дата обращения: 09.09.2024).

2. Шарифов, Б. А. Методика проведения аудита с использованием информационных технологий и персональных компьютеров / Б. А. Шарифов // Молодой ученый. – 2021. – № 3(345). – С. 332 – 335.

3. Макаренко, С. И. Анализ стандартов и методик тестирования на проникновение / С. И. Макаренко Г. Е. Смирнов // Системы управления, связи и безопасности. – 2020. – № 4.

References

1. Cybersecurity in 2023–2024: trends and forecasts. Part three / [Electronic resource] // positive technologies : [website]. – URL : https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya / (date of reference: 09.09.2024).

2. Sharifov, B. A. Audit methodology using information technology and personal computers / B. A. Sharifov // A young scientist. – 2021. – No. 3(345). – P. 332 – 335.

3. Makarenko, S. I. Analysis of standards and methods of penetration testing / S. I. Makarenko G. E. Smirnov // Management, communication and security systems. – 2020. – No. 4.

УДК 004. 051

П. И. Карасев[2], Ф. М. Пыршев[2], И. А. Глазкова[1], И. А. Дьяков[1]
([1]Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия,
e-mail: fpyrshiev@bk.ru, karasev@mirea.ru)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЗАЩИТЫ ОТ НЕЖЕЛАТЕЛЬНОЙ РАССЫЛКИ

Аннотация. Данная работа посвящена сравнительному анализу программного обеспечения для защиты от нежелательной рассылки по электронной почте. В работе был использован тестовый набор данных, содержащий 4993 электронных письма.

Ключевые слова: информационная безопасность, спам, электронная почта.

P. I. Karasev[2], F. M. Pyrshev[2], I. A. Glazkova[1], I. A. Dyakov[1]
([1]Department of Information systems and information protection,
TSTU, Tambov, Russia;
[2]Department of Information Security,
RTU MIREA, Moscow, Russia)

COMPARATIVE ANALYSIS OF ANTI-SPAM SOFTWARE

Abstract. This work is devoted to the comparative analysis of software for protection against unsolicited e-mail. A test dataset containing 4,993 emails was used in the work.

Keywords: information security, spam, e-mail.

Введение. В наше время, когда электронная почта является неотъемлемой частью нашей жизни, одной из основных проблем, с которой мы сталкиваемся, является нежелательная рассылка. Для борьбы с нежелательными сообщениями было создано множество антиспам-приложений. В данной работе будет проведен сравнительный анализ пяти из них: Apache SpamAssassin, Kaspersky Internet Security, MailWasher, SPAMfighter и Norton 360 Standard.

Основная часть. Прежде чем приступить непосредственно к анализу, необходимо провести краткий обзор самих приложений и методик сравнения.

Apache SpamAssassin (SA) – это бесплатное клиент-серверное средство с открытым исходным кодом, которое используется для фильтрации спама на почтовых серверах. Оно предоставляет множество настраиваемых параметров для улучшения работы фильтрации спама.

Kaspersky Internet Security (KIS) – это линейка программных продуктов для защиты компьютера от различных видов угроз. Данное приложение использует технологии машинного обучения для идентификации и блокирования спам-сообщений.

MailWasher (MW) – это антиспам-программа, которая работает как промежуточное звено между почтовым сервером и пользователем.

SPAMfighter (SF) – это ПО для фильтрации спама, которое используется на почтовых серверах и на компьютерах пользователей. Программа основана на едином фильтре, который позволяет пользователям помогать друг другу, сообщая о спаме.

Norton 360 Standard (NS) – это комплексное приложение для защиты компьютера от различных видов угроз в интернете, включая защиту от спама. Norton использует технологии машинного обучения и анализа текстовых сообщений для идентификации и блокирования спам-сообщений. Приложение также имеет множество дополнительных функций, таких как защита от вирусов, фишинга и вредоносных программ.

Для каждого продукта был выделен отдельный сервер, на котором производилось тестирование. В качестве MTA использовался Postfix. Для сравнения эффективности мы будем использовать тестовый датасет из 4993 электронных сообщений, которые были классифицированы как спам или не спам. Помимо этого, будет сравниваться ценовая категория и сколько памяти программа требует для работы.

Из результатов эффективности в табл. 1 можно сделать вывод, что все пять ПО имеют высокую точность классификации электронных сообщений. Разница между ними может быть вызвана внутренней настройкой.

При этом Kaspersky и Norton имеют наивысшее потребление оперативной памяти. Это связанно с тем, что они являются комплексными антивирусными программами, то есть помимо функции антиспам они также занимаются, например, обеспечением безопасного соединения в интернете. Остальные же программы используют достаточно малое потребление ресурсов компьютера.

Также можно заметить, что Apache SpamAssassin является единственной полностью бесплатной программой. Все остальные относятся к условно-бесплатным или полностью платным (Kaspersky Internet Security и Norton 360 Standard). По сравнению с другим ПО (помимо SpamAssassin), Norton имеет наименьшую цену.

1. Результаты метрик

Название	Точность	Полнота	F-мера
SA	0,98	0,92	0,95
KIS	0,99	0,93	0,96
MW	0,95	0,84	0,89
SF	0,97	0,93	0,95
NS	0,96	0,85	0,90

Вывод. Таким образом, выбор наилучшего ПО зависит от индивидуальных потребностей пользователя или компании. Если вы хотите получить в комплекте не только качественный антиспам-продукт, то Kaspersky является наиболее оптимальным решением. Данный программный продукт на момент написания статьи имеет сертификаты ФСТЭК и ФСБ.

Однако, если у вас есть отдельный почтовый сервер и вы ищете стабильно работающее ПО, то, как минимум, стоит обратить внимание на Apache SpamAssassin, который потребляет не так много ресурсов машины и работает ничуть не хуже средства выше.

Список использованных источников

1. Brunton, F. Spam: A Shadow History of the Internet / F. Brunton. – MIT Press, 2015. – 296 p.

2. Частикова, В. А. Обзор актуальных проблем основных методов фильтрации спама и анализ их эффективности / В. А. Частикова, К. В. Козачек // Вестник Адыгейского государственного университета.

3. Абдуллаев, В. Г. Защита от спама в Интернет пространстве / В. Г. Абдуллаев // Радиоэлектроника и информатика. – 2014. – № 2(65).

References

1. Brunton, F. Spam: A Shadow History of the Internet / F. Brunton. – MIT Press, 2015. – 296 p.

2. V. A. Chastikova, Review of current problems of the main spam filtering methods and analysis of their effectiveness / V. A. Chastikova, K. V. Kozachek // Bulletin of the Adygea State University.

3. Abdullaev, V. G. Protection from spam in the Internet space / V. G. Abdullaev // Radioelectronics and informatics. – 2014. – No. 2(65).

УДК 004.94

П. И. Карасев[2], Ф. М. Пыршев[2], А. И. Елисеев[1]
([1]Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия,
e-mail: fpyrshiev@bk.ru, karasev@mirea.ru)

ЦИФРОВИЗАЦИЯ ПЕРМАКУЛЬТУРНЫХ НАСАЖДЕНИЙ

Аннотация. Рассмотрен подход к цифровизации пермакультурных насаждений, предложены модели элементов системы насаждений и обозначены преимущества и недостатки данного метода.

Ключевые слова: моделирование, пермакультура, сельское хозяйство, цифровизация, цифровые технологии.

A. I. Eliseev[1], P. I. Karasev[2], F. M. Pyrshev[2]
([1]Department of Information systems and information protection,
TSTU, Tambov, Russia;
[2]Department of Information Security,
RTU MIREA, Moscow, Russia)

DIGITALIZATION OF PERMACULTURE PLANTATIONS

Abstract. An approach to digitalization of permacultural plantations is considered, models of elements of the planting system are proposed and the advantages and disadvantages of this method are outlined.

Keywords: modeling, permaculture, agriculture, digitalization, digital technologies.

Введение. В современном мире достаточно остро стоит вопрос экологичности всех сфер жизни, включая сельское хозяйство. В данной сфере для улучшения экологической ситуации было придумано использовать пермакультуру.

Пермакультура – сельскохозяйственная система, которая предполагает наиболее рациональное использование плодородных площадей. При этом должны соблюдаться следующие принципы:

- взаимосвязанность – все элементы системы должны благотворно влиять друг на друга, повышая таким образом продуктивностью всей системы;
- функциональность – каждый элемент системы должен выполнять какую-либо функцию;

- дублирование – для выполнений какой-либо функции не должен использоваться единственный элемент системы;
- многоуровневость – необходимо эффективно использовать весь объем территории, на которых находятся насаждения [1].

Из этого исходит то, что пермакульура – результат построения модели экосистемы на заданной площади. Но возникает проблема того, что необходимо подбирать растения с разлучными характеристиками, которые будут благотворно влиять друг на друга, при этом необходимо закладывать инфраструктуру для обслуживания насаждений. Данная работа написана с целью исследования возможности цифровизации процесса моделирования пермакультурного комплекса. Для этого необходимо рассмотреть характеристики растений, сформировать модели конкретных растений и использовать эти модели для построения модели премакультурной системы.

Основная часть. Необходимо рассмотреть основу любых сельскохозяйственных насаждений – почву. Именно от ее характеристик зависит то, какие именно культуры можно использовать в рамках системы, а также какие дополнительные элементы необходимы для обеспечения функционирования этой системы. Среди основных характеристик можно выделить следующие: тип почвы, влажность почвы, питательные вещества в почве и уровень загрязнения почвы [2].

Среди типов почв встречаются следующие: глинистая, песчаная, суперпесчаная, суглинистая, известковая и торфяная. Различные типы почв по-разному подходят для ведения сельского хозяйства, а также на этих почвах можно выращивать различные типы культур [3].

Уровни влажности, содержания органических и минеральных веществ можно обозначить в виде процента в содержании почве. Все эти уровни влияют на то, какие именно культуры можно эффективно выращивать на данных почвах [2].

Уровень загрязнения почвы можно обозначить так же, как и остальные, но данный уровень показывает на то, насколько почва безопасна для растений.

Для роста растений необходимы следующие компоненты: свет, вода, почва, температура, питательные вещества и биотические факторы. Некоторые компоненты были рассмотрены при формировании модели почвы, но все равно необходимо указывать данные параметры, чтобы проверять соблюдение необходимых условий.

Свет и температура определяются как определенный показатель окружающей среды, которые можно назвать освещенностью и температурой. При этом в самом растении необходимо указать, какой промежуток значений является оптимальным для этих растений.

Следующие факторы определяют то, насколько уместно размещение различных растений в непосредственной близости друг от друга, а также то, какие дополнительные биологические элементы необходимы для обеспечения роста различных культур. Для эффективного моделирования требуется подбирать матрицу дискреционной модели, но при построении первых моделей можно обойтись мандатной моделью взаимодействия различных групп культур.

Вывод. Из этого следует то, что модель премакультурной системы состоит из 3 элементов. То, каким образом данные модели формируются, было описано в рамках статьи. Данный способ позволяет упростить формирование насаждений, но для эффективной работы этого метода необходимо очень подробно прорабатывать модели, что является сложной задачей.

Список использованных источников

1. Чудосветова, Д. Ю. Потенциал пермакультуры для развития сельского хозяйства / Д. Ю. Чудосветова // Устойчивое развитие сельских территорий: взгляд молодых ученых : материалы Всерос. науч.-практ. конф. молодых ученых (10 – 12 декабря 2020 г.) ; Новосиб. гос. аграр. ун-т. – Новосибирск, 2020. – 112 с.

2. Дурдымядов, А. Основные характеристики типов почв в сельском хозяйстве / А. Дурдымядов, Н. Тойлыев, Г. Гурбанбердиев // IN SITU. – 2023. – № 10.

3. Абдусаламова, Р. Р. Почвеные ресурсы России / Р. Р. Абдусаламова, З. М. Баламирзоева //Вестник СПИ. – 2020. – № 1(33).

References

1. Chudosvetova, D. Yu. The potential of permaculture for the development of agriculture / D.Yu. Chudosvetova // Sustainable development of rural areas : the view of young scientists: materials of the All-Russian Scientific and Practical Conference of Young Scientists (December 10 – 12, 2020) ; Novosibirsk State Agrarian University. un-T. – Novosibirsk, 2020. – 112 p.

2. Durdymyadov A., Main characteristics of soil types in agriculture / A. Durdymyadov, N. Toylyev, G. Gurbanberdiev // IN SITU. – 2023. – No. 10.

3. Abdusalamova, R. R. Soil resources of Russia / R. R. Abdusalamova, Z. M. Balamirzoeva //Herald of SLEEP. – 2020. – No. 1(33).

УДК 681.5

С. А. Россман[1], Алмали Ахмед Аднан Латиф[2],
Аль-Судани Зайд Али Хуссейн[2]
([1]Кафедра «Информационная безопасность»,
РТУ МИРЭА, Москва, Россия;
[2]г. Багдад, Ирак,
e-mail: rossmansa@bk.ru, zaidali83@gmail.com)

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПРИНЯТИЯ РЕШЕНИЙ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрены вопросы обеспечения информационной безопасности интеллектуальных систем принятия решений в агропромышленности. Приведены основные типы угроз и уязвимостей, характерные для данных систем, такие как атаки на данные и алгоритмы, а также атаки на инфраструктуру. Обсуждены методы защиты, включающие шифрование данных, использование блокчейн-технологий и обучение моделей искусственного интеллекта на защищенных данных. Приведены примеры успешной реализации мер безопасности в сельскохозяйственном секторе. Рассмотрены рекомендации по повышению уровня информационной безопасности в условиях цифровизации агропромышленного комплекса.

Ключевые слова: интеллектуальные системы, агропромышленный комплекс, информационная безопасность, блокчейн, шифрование данных.

S. A. Rossman[1], Almali Ahmed Adnan Lateef[2],
Al-Soudany Zaid Ali Hussein[2]
(Department of Information systems and information protection;
RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq)

PROTECTION OF INTELLIGENT DECISION-MAKING SYSTEMS IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The article discusses the issues of ensuring information security of intelligent decision-making systems in the agro-industry. The main types of threats and vulnerabilities specific to these systems are presented, such as attacks on data and algorithms, as well as attacks on infrastructure. Security methods are discussed, including data encryption, the use of blockchain technologies and the training of artificial intelligence models on protected data. Examples of successful implementation of safety measures in the agricultural sector are given. Recommendations on improving the level of information security in the context of digitalization of the agro-industrial complex are considered.

Keywords: intelligent systems, agro-industrial complex, information security, blockchain, data encryption.

Интеллектуальные системы становятся все более распространенными в агропромышленном комплексе, они положительно влияют на эффективность производства и управления аграрными предприятиями. Такие системы широко применяются для анализа данных, предсказания урожайности, оптимизации использования ресурсов и автоматизации процессов принятия решений. Однако, с ростом распространения этих технологий увеличиваются и риски, связанные с информационной безопасностью. Интеллектуальные системы становятся объектами киберугроз, которые способны привести к различным рискам, таким как финансовые потери, снижению урожайности и даже к нарушению продовольственной безопасности.

Интеллектуальные системы принятия решений в агропромышленном комплексе являются уязвимыми перед большим количеством киберугроз. Среди них можно выделить атаки на данные, атаки на алгоритмы и атаки на инфраструктуру. Атаки на данные подразумевают использование поддельных или измененных данных для обучения моделей искусственного интеллекта, что может привести к ошибочным решениям, негативно влияющим на производство и управленческие процессы. Атаки на алгоритмы включают изменения в алгоритмах, инъекции вредоносного кода или манипуляции с параметрами, что значительно влияет на точность и надежность принимаемых решений. Атаки на инфраструктуру основаны на несанкционированном доступе к серверам и системам хранения данных, что может создать риск утечки конфиденциальной информации. Недостаточная защищенность данных и алгоритмов может быть использована злоумышленниками для нанесения значительного ущерба агропромышленным предприятиям.

Для эффективной защиты интеллектуальных систем принятия решений в агропромышленном комплексе необходимо использовать комплексный подход мер безопасности, который включает как технические, так и организационные мероприятия. Одним из основных методов защиты является шифрование данных. Современные методы шифрования обеспечивают защиту данных на всех этапах их обработки и хранения, предотвращая несанкционированный доступ и манипуляции информацией. Другое перспективное направление – использование технологий блокчейн. Применение блокчейна обеспечивает неизменность и подлинность данных и исключает возможность манипуляций с информацией, что увеличивает уровень доверия к принимаемым решениям.

Кроме того, важно применять методы защиты данных, такие как дифференциальная конфиденциальность, и использовать защищенные данные для обучения моделей искусственного интеллекта. Это позволяет минимизировать риски утечек и манипуляций, а также повышает общую надежность интеллектуальных систем.

Одним из таких примеров успешной реализации защиты интеллектуальных систем является использование блокчейн-технологий в системе управления цепочкой поставки агропродукции. Данный инструмент позволяет обеспечить высокий уровень прозрачности и защиты данных о происхождении продукции и качестве агропродукции, что способствует предотвращению манипуляций и распространения контрафакта.

В условиях растущей цифровизации агропромышленного комплекса вопросы информационной безопасности интеллектуальных систем приобретают особую значимость. Для эффективной защиты от киберугроз важно применять комплексные меры, включая современные методы шифрования, блокчейн-технологии и защиту данных. Будущее агропромышленности тесно связано с безопасностью использования интеллектуальных систем, что требует их постоянного усовершенствования и адаптации к новым вызовам и угрозам.

Список использованных источников

1. Интеллектуальные системы в управлении экономикой агропромышленного комплекса КБР с применением CALS-технологий // Cyberleninka. – URL : https://cyberleninka.ru/article/n/intellektualnye-sistemy-v-upravlenii-ekonomikoy-agropromyshlennogo-kompleksa-kbr-s-primeneniem-cals-tehnologiy (дата обращения: 04.09.2024).

2. Система информационной безопасности предприятия агропромышленного комплекса // Cyberleninka. – URL : https://cyberleninka.ru/article/n/sistema-informatsionnoy-bezopasnosti-predpriyatiya-agropromyshlennogo-kompleksa (дата обращения: 04.09.2024).

3. Интернет вещей в сельском хозяйстве // Cyberleninka. – URL : https://cyberleninka.ru/article/n/internet-veschey-v-selskom-hozyaystve (дата обращения: 04.09.2024).

References

1. Intelligent systems in the management of the economy of the agro-industrial complex of the CBD using CALS technologies // Cyberleninka. – URL : https://cyberleninka.ru/article/n/intellektualnye-sistemy-v-upravlenii-ekonomikoy-agropromyshlennogo-kompleksa-kbr-s-primeneniem-cals-tehnologiy (date of application: 04.09.2024).

2. Information security system of the agro-industrial complex enterprise // Cyberleninka. – URL : https://cyberleninka.ru/article/n/sistema-informatsionnoy-bezopasnosti-predpriyatiya-agropromyshlennogo-kompleksa (date of request: 04.09.2024).

3. Ensuring information security of industrial enterprises // Cyberleninka. – URL : https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-predpriyatiy-promyshlennosti (date of access: 04.09.2024).

УДК 637

О. Н. Красуля[1], А. В. Токарев[2]
([1]Кафедра Технологии хранения и переработки продуктов животноводства, ФГБОУ ВО «РГАУ–МСХА имени К. И. Тимирязева», Москва, Россия;
[2]ООО «ФудСофт», г. Воронеж, Россия,
e-mail: okrasulya@mail.ru, e-mail:info@foodsoft.org)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ МЯСНЫХ И МОЛОЧНЫХ ПРОДУКТОВ ЗАДАННОГО КАЧЕСТВА

Аннотация. Раскрывается информация о новаторских автоматизированных гибридных экспертных системах, а именно «МультиМит Эксперт» и «МультиМилк Эксперт», разработанных впервые на территории России. Эти системы являются уникальными программными комплексами, специализированными на решении разнообразных технологических и учетных задач в мясной и молочной промышленности в реальном времени. Их использование приводит к автоматизации производственных процессов, управлению качеством продукции, снижению временных и финансовых затрат, а также оптимизации разработки новых продуктов.

Основой программных комплексов является «Базовый» модуль, дополненный несколькими инновационными модулями, такими как «Оптимизация и моделирование рецептур» и «Экспертная система диагностики и анализа качества». Эти модули обладают уникальным функционалом, который позволяет оптимизировать состав продуктов, выявлять проблемы на этапе моделирования технологических процессов и получать рекомендации для их устранения. Важно отметить, что программные комплексы «МультиМит Эксперт» и «МультиМилк Эксперт» не имеют аналогов на рынке программного обеспечения, как в России, так и за рубежом.

Ключевые слова: экспертная система, программное обеспечение, оптимизация, моделирование, рецептура, цифровизация, проектирование, продукты питания, автоматизация, производственный учет, пищевая промышленность.

O. N. Krasulya[1], A. V. Tokarev[2]
([1]Department of Technologies for Storage and Processing of Livestock Products, Russian State Agrarian University – Moscow Agricultural Academy named after K. I. Timiryazev, Moscow, Russia;
[2]CTO of Food Soft LLC, Voronezh, Russia)

DIGITAL TECHNOLOGIES IN THE PROCESSING OF LIVESTOCK PRODUCTS

Abstract. The lecture presents information about the automated hybrid expert systems “MultiMeatExpert” and “MultiMilkExpert” developed for the first time in the domestic practice, which are specialised software complexes designed to solve a wide range of technological and accounting tasks at the enterprises of meat

and dairy industry in real time. Their application allows automating the process of production of meat and dairy products, to manage the technological process in order to obtain products of a given composition and properties, to reduce time and financial costs of the enterprise, as well as the cost of developing a new assortment.

The programme complex consists of “Basic” and several additional modules. Technological modules “Optimisation and modelling of recipes” and “Expert system of diagnostics and analysis of quality” contain unique functionality, which allows to calculate the recipe of products of a given quality with minimum cost, to identify at the stage of modelling technological problems and to receive recommendations for their elimination. MultiMitExpert and MultiMilkExpert software systems have no analogues in the foreign and domestic software market.

Keywords: software, expert system, optimization, modeling, recipe, digitalization, design, food, automation, production accounting, food industry.

Искусственный интеллект, в частности, экспертные системы, представляет собой одно из важных направлений в научной дисциплине искусственного интеллекта. Введение ЭС в практику началось в начале 1980-х годов прошлого века и с тех пор активно развивается. Основным фокусом ЭС является работа с знаниями: их сбор, представление и использование.

Экспертные системы состоят из нескольких основных компонентов, включая базу данных, базу знаний, механизм логического вывода и интерфейс пользователя. Они работают по принципу условия «ЕСЛИ X, то Y», где X – условие, а Y – действие, выполняемое, если условие X истинно.

На российском рынке продукции животноводства присутствует информационная неопределенность, обусловленная различными факторами, такими как колебания цен и качества сырья, а также спроса на продукцию. Для решения этих проблем активно используются цифровые технологии, включая экспертные системы, которые позволяют координировать работу предприятий и оптимизировать производственные процессы.

Целью данной работы являлась разработка экспертных систем для цифровизации процессов проектирования рецептур и управления технологическим процессом в режиме реального времени на предприятиях мясной и молочной промышленности. Для достижения этой цели использовались методы целочисленного линейного и нелинейного программирования, а также алгоритмы пошагового построения решений.

В настоящее время на мясоперерабатывающих предприятиях России и странах ЕАЭС успешно эксплуатируется экспертная система «МультиМит Эксперт», разработанная совместно компанией «ФудСофт» и РГАУ–МСХА имени К. А. Тимирязева. За период своей

долгой эксплуатации данная система продемонстрировала высокую технологическую и экономическую эффективность. Дополнительную информацию о ее работе можно найти на сайте multimeat.ru, а также в монографиях и периодических изданиях.

В 2023 году была разработана еще одна инновационная экспертная система под названием «МультиМилк Эксперт», предназначенная для решения широкого спектра технологических и учетных задач на предприятиях молочной промышленности. Это программное обеспечение также создано компанией «ФудСофт», в сотрудничестве с РГАУ–МСХА имени К. А. Тимирязева и РТУ–МИРЭА.

Особенностью этих экспертных систем является их модульная концепция, обеспечивающая гибкую настройку интерфейса и функционала под требования каждого конкретного предприятия. Это позволяет адаптировать систему и вносить изменения в соответствии с потребностями заказчика. Кроме того, функционал системы предоставляет возможность интеграции с различными управленческими и бухгалтерскими программами.

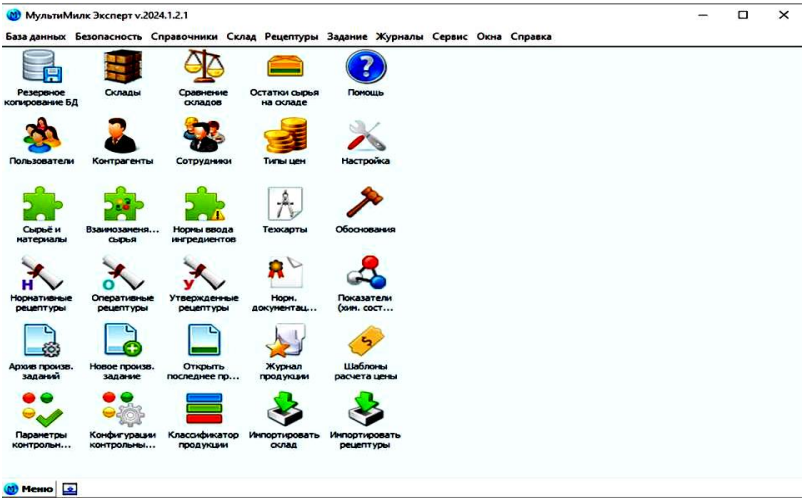


Рис. 1. Главное окно программного комплекса «МультиМилк Эксперт»

Обе системы, «МультиМит Эксперт» и «МультиМилк Эксперт» включают в себя базовый модуль и дополнительные, предназначенные для решения конкретных задач. Например, в «МультиМит Эксперт» и «МультиМилк Эксперт» предусмотрены модули производственного задания и учета, оптимизации и моделирования рецептур, экспертной диагностики и анализа качества, а также интеграции с экспресс-

анализаторами. В «МультиМит Эксперт» также доступны модули для убоя скота, обвалки и жиловки мяса.

Эти инновационные решения представляют собой современные инструменты для решения сложных задач в мясной и молочной промышленности, способствуя автоматизации производственных процессов и оптимизации бизнеса в режиме реального времени.

Программный модуль «Базовый» является основным модулем ЭС. Он обеспечивает не только контроль за качеством и ценой продукции, но и представляет собой мощный инструмент для работы с рецептурами молочных продуктов. Этот модуль осуществляет аналитику рецептур и производит расчет стоимостных показателей готовой продукции, включая себестоимость, рентабельность и цену реализации. Кроме того, он также осуществляет складской учет, обеспечивая полную информацию о запасах сырья и готовой продукции.

Программный модуль «Оптимизация и моделирования рецептур» предоставляет возможность для оптимизации рецептур различных молочных продуктов в условиях информационной неопределенности. Этот модуль способствует снижению себестоимости продукции на 5…10% при сохранении высоких стандартов качества. Более того, его функционал уникален на рынке программного обеспечения как в отечественном, так и в зарубежном сегменте.

Программный модуль «Экспертная система диагностики и анализа качества» предназначен для выявления технологических проблем и предложения решений по оптимизации процесса. Он осуществляет анализ рецептур с учетом различных физико-химических, функционально-технологических и структурно-механических свойств сырья. Данный модуль также выполняет уникальную операцию по определению оптимального набора пищевых добавок для корректировки качества продукции, что помогает избежать технологического брака.

Программный модуль «Производственное задание и учет» обеспечивает организацию единого информационного пространства для управления учетной деятельностью на предприятиях молочной промышленности. Он позволяет формировать производственные задания, планировать выпуск продукции, анализировать деятельность производства и контролировать качество выпускаемой продукции.

Программный модуль «Интеграция с экспресс-анализатором химического состава сырья» автоматизирует импорт результатов анализа химического состава сырья и ингредиентов, что позволяет получать данные о качестве сырья в режиме реального времени. Это обеспечивает более точные расчеты оптимизации и моделирования рецептур на основе фактических данных.

Из представленной выше информации можно сделать ряд выводов, подчеркивающих значимость и преимущества разработанных программных продуктов в мясной и молочной промышленности:

- Экспертные системы «МультиМит Эксперт» и «МультиМилк Эксперт» представляют собой передовые решения для автоматизации технологических и учетных задач на предприятиях данного сектора экономики. Они позволяют оптимизировать весь цикл производства, начиная от обработки сырья и заканчивая выпуском готовой продукции.
- Внедрение этих экспертных систем способствует существенной экономии времени и снижению финансовых издержек предприятия за счет повышения эффективности производственных процессов. Это позволяет компаниям оптимизировать планирование и управление производством в реальном времени, что является ключевым фактором в современной конкурентной среде.
- «МультиМит Эксперт» и «МультиМилк Эксперт» представляют не только инструменты для решения текущих технологических задач, но и обеспечивают поддержку в принятии оптимальных управленческих решений как в обычном режиме работы, так и в условиях критических ситуаций на производстве.

Эти программные продукты обладают гибкостью и масштабируемостью, что позволяет их использование как на небольших предприятиях, так и на крупных производствах. Они совместимы с различными операционными системами, что упрощает их интеграцию и использование на различных платформах.

Таким образом, «МультиМит Эксперт» и «МультиМилк Эксперт» представляют собой инновационные инструменты, способствующие современной автоматизации и оптимизации производства в мясной и молочной промышленности. Их внедрение может значительно повысить эффективность и конкурентоспособность предприятий данного сектора экономики.

УДК 681.5

А. И. Шебалкина[1], Алмали Ахмед Аднан Латиф[2],
Аль-Судани Зайд Али Хуссейн[2]
([1]Кафедра КБ-1 «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: shebalkina@bk.ru, karasev@mirea.ru;
[2]г. Багдад, Ирак)

ОПТИМИЗАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ АГРОПРОМЫШЛЕННЫМ КОМПЛЕКСОМ С ИСПОЛЬЗОВАНИЕМ SUCKLESS-ПОДХОДА

Аннотация. Современные системы управления в агропромышленном комплексе все больше зависят от сложных цифровых решений, что создает дополнительные риски, связанные с уязвимостями и сложностью администрирования. Применение философии suckless и принципа KISS («Keep it simple, stupid») в управлении цифровыми процессами позволяет значительно снизить риски, одновременно повышая надежность и безопасность систем управления. В статье рассматривается, как минималистичные и простые цифровые решения могут упростить управление сельскохозяйственными процессами, облегчить их мониторинг и контроль, а также повысить устойчивость к киберугрозам.

Ключевые слова: агропромышленный комплекс, сельское хозяйство, информационная безопасность, комплексная безопасность, suckless, KISS, UNIX-подход, АСУ ТП.

A. I. Shebalkina[1], Almali Ahmed Adnan Lateef[2],
Al-Soudany Zaid Ali Hussein[2]
([1]RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq)

OPTIMIZATION OF AUTOMATED MANAGEMENT SYSTEMS FOR THE AGRO-INDUSTRIAL COMPLEX USING THE SUCKLESS APPROACH

Abstract. Modern management systems in the agro-industrial complex are increasingly dependent on complex digital solutions, which introduces additional risks associated with vulnerabilities and administrative complexity. Applying the suckless philosophy and the KISS principle (“Keep it simple, stupid”) in digital process management can significantly reduce risks, while enhancing the reliability and security of control systems. This article examines how minimalist and simple digital solutions can streamline the management of agricultural processes, facilitate their monitoring and control, and improve resistance to cyber threats.

Keywords: Agro-industrial complex, agriculture, Information security, Comprehensive security, suckless, KISS, UNIX-way, PAS.

Введение. Агропромышленный комплекс сталкивается с необходимостью все более активного использования цифровых систем управления, начиная с мониторинга урожайности и заканчивая контролем за автоматизированными машинами и оборудованием. Однако с ростом сложности этих систем возникают дополнительные риски, связанные с кибератаками, нестабильностью и сложностью их сопровождения. Применение принципов suckless – минималистичного и простого подхода к проектированию систем – может стать решением этих проблем.

Философия suckless подразумевает использование минимально необходимых технологий для достижения максимального контроля над системой. В условиях агропромышленного комплекса это позволяет создать более надежные и управляемые системы, где сложность снижена до необходимого минимума, что делает их менее уязвимыми к сбоям и угрозам безопасности.

1. Применение принципов suckless в агропромышленном комплексе

1.1. Принцип минимализма в управлении цифровыми системами

Минималистичный подход, лежащий в основе философии suckless, идеально подходит для агропромышленного комплекса, где избыточные функции в системах управления могут привести к усложнению работы и возникновению дополнительных уязвимостей. Использование простых инструментов, выполняющих строго необходимые функции, позволяет снизить вероятность ошибок и упрощает мониторинг процессов.

Внедрение таких решений может повысить прозрачность системы управления сельскохозяйственными процессами, снизив зависимость от сторонних модулей и сложных программных систем. Например, использование узкоспециализированных программ для мониторинга состояния почвы или контроля работы сельскохозяйственных машин с минимальной функциональностью может обеспечить не только высокую эффективность, но и надежную защиту от внешних воздействий.

1.2. Преимущества UNIX-подхода в агропромышленном комплексе

Использование UNIX-подхода в агропромышленном комплексе позволяет создавать надежные, гибкие и масштабируемые системы управления процессами. Простота и модульность программного обес-

печения значительно уменьшают количество ошибок и уязвимостей, а также повышают производительность системы. Это критично для агропромышленности, где ошибки или сбои в работе цифровых систем могут привести к серьезным экономическим потерям.

Кроме того, минимизация кода и использование модульных решений способствует более эффективному использованию ресурсов системы, что позволяет сократить затраты на ее сопровождение и модернизацию. В результате агропромышленные предприятия могут значительно повысить эффективность управления своими процессами, снижая затраты на инфраструктуру и минимизируя риски, связанные с кибератаками и сбоями в системах.

2. Преимущества применения философии suckless для агропромышленного комплекса

2.1. Оптимизация затрат на внедрение и эксплуатацию

Одним из ключевых преимуществ минималистичных цифровых решений является их экономическая эффективность. Простые системы требуют меньших затрат на внедрение, настройку и дальнейшую эксплуатацию. В агропромышленном комплексе это особенно важно, так как предприятия могут экономить на технологической инфраструктуре, не жертвуя при этом надежностью и безопасностью процессов.

2.2. Улучшение прозрачности и возможности аудита

Простота систем, основанных на философии suckless, позволяет легче проводить аудит их безопасности и повышает прозрачность процессов. Это важно для выполнения нормативных требований и для защиты данных, используемых в агропромышленном комплексе. Системы становятся легче для аудита и мониторинга, что обеспечивает лучшее понимание их функционирования и снижает риски несанкционированного доступа.

Заключение. Применение философии suckless и принципов KISS в системах управления агропромышленного комплекса позволяет оптимизировать управление цифровыми процессами, снизить уязвимости и повысить уровень безопасности.

Стремление к минимализму и устранению избыточной функциональности может привести к снижению числа уязвимостей, упрощению аудита безопасности и увеличению контроля над системой.

Простота и минимализм помогают предприятиям сократить затраты на обслуживание и повысить контроль над операциями. Внедрение таких подходов является перспективным направлением для обеспечения устойчивого и безопасного функционирования цифровых систем в агропромышленном комплексе.

Список использованных источников

1. Frederick T Grampp, Robert H Morris The UNIX System: UNIX Operating System Security // AT&T Bell Laboratories Technical Journal. – 1984. – No. 63(8). – P. 1649 – 1672.

2. Gianni J Ruiz, Md Minhaz Chowdhury, Shadman Latif A Comparative Study of OS Security // 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). – 2021. – P. 1 – 6.

3. Denny Cherry Computer Operating System Security // Enterprise-Grade IT Security for Small and Medium Businesses: Building Security Systems, in Plain English. – 2022. – P. 71 – 81.

4. Yusuf Perwej, Syed Qamar Abbas, Jai Pratap Dixit, Nikhat Akhtar, Anurag Kumar Jaiswal A systematic literature review on the cyber security // International Journal of scientific research and management. – 2021. – No. 9(12). – P. 669 – 710.

УДК 681.5

А. Р. Эмин[1], Мустафа Абдулкадим Дхаир Аль-Амиди[2], Шамсулдин Хайдар Абдулваххаб Х.[3]
([1]Кафедра «Защита информации», РТУ МИРЭА, Москва, Россия, e-mail: artem8emin@gmail.com;
[2]г. Аль-Кадисия, Ирак;
[3]г. Багдад, Ирак)

СОЗДАНИЕ БЕЗОПАСНОЙ СЕТИ ДЛЯ АГРОБИЗНЕСА: ПРИМЕР ВНЕДРЕНИЯ VPN-ТЕХНОЛОГИЙ В СЕЛЬСКОМ ХОЗЯЙСТВЕ

Аннотация. В условиях растущей цифровизации агропромышленного комплекса обеспечение информационной безопасности становится критически важным. Внедрение виртуальных частных сетей (VPN) представляет собой эффективное решение для защиты данных фермеров и агропредприятий. Данная статья рассматривает преимущества использования VPN, такие как шифрование данных и безопасный доступ к корпоративным ресурсам, а также примеры успешного внедрения в российском агросекторе. Вместе с тем, обсуждаются потенциальные недостатки, включая сложности настройки и возможное снижение скорости интернета. Анализируя актуальные проблемы и решения в области кибербезопасности, статья предоставляет рекомендации для фермеров по созданию безопасной сети, что способствует защите их информации и повышению устойчивости бизнеса.

Ключевые слова: Виртуальные частные сети (VPN), Информационная безопасность, Агропромышленный комплекс, Защита данных, Шифрование данных, Цифровизация агробизнеса.

A. R. Emin[1], Mustafa Abdulkadhim Dhahir Al-Ameedee[2], Shamsuldaeen Haidar Abdulwahhab H.[3]
([1]Department of Information security, RTU MIREA, Moscow, Russia;
[2]Baghdad, Iraq;
[3]Al-Qadisiyah, Irag)

CREATING A SECURE NETWORK FOR AGRIBUSINESS: AN EXAMPLE OF IMPLEMENTING VPN TECHNOLOGIES IN AGRICULTURE

Abstract. With the increasing digitalization of the agro-industrial complex, ensuring information security becomes critically important. Implementing Virtual Private Networks (VPN) offers an effective solution for protecting the data

of farmers and agricultural enterprises. This article examines the benefits of using VPNs, such as data encryption and secure access to corporate resources, along with examples of successful implementation in the Russian agricultural sector. Additionally, it discusses potential drawbacks, including setup complexities and possible internet speed reductions. By analyzing current issues and solutions in cybersecurity, the article provides recommendations for farmers on creating a secure network, contributing to the protection of their information and enhancing business resilience.

Keywords: Virtual Private Networks (VPN), Information Security, Agro-industrial Complex, Data Protection, Data Encryption, Digitalization of Agribusiness.

Фермеры и агропредприятия все чаще используют цифровые технологии для управления процессами. Однако с увеличением цифровизации возрастает и риск кибератак, утечек данных и несанкционированного доступа.

Решение: Внедрение виртуальных частных сетей (VPN) позволяет создать безопасное соединение между устройствами и серверами. VPN шифрует данные, что предотвращает их перехват злоумышленниками.

Преимущества использования VPN:

– Защита конфиденциальности: шифрование данных делает их недоступными для посторонних.

– Безопасный доступ: фермеры могут безопасно подключаться к корпоративным ресурсам из удаленных мест.

– Устойчивость к кибератакам: использование VPN помогает предотвратить атаки типа «человек посередине».

Примеры внедрения: Некоторые российские агропредприятия уже используют VPN для обеспечения безопасности своих данных. Например, компания, занимающаяся точным земледелием, может подключать датчики и дроны к защищенной сети, что гарантирует защиту данных о состоянии полей от киберугроз, таких как:

1. Атаки типа «человек посередине»: Злоумышленники могут перехватывать данные, передаваемые между дронами и серверами, что может привести к утечке информации о состоянии полей.

2. Несанкционированный доступ: без защиты данные о состоянии полей могут быть доступны для неавторизованных пользователей, что может привести к манипуляциям с данными или кражам интеллектуальной собственности.

3. Вредоносное ПО: Злоумышленники могут пытаться внедрить вирусы или трояны через уязвимости в системах управления дронами

и датчиками, что может привести к повреждению оборудования или утечке данных.

4. Фишинг: Сотрудники могут получать поддельные электронные письма с просьбой предоставить доступ к системам. Если доступ получен, злоумышленники могут манипулировать данными о состоянии полей.

5. DDoS-атаки: Киберпреступники могут устраивать атаки на системы управления, что может привести к остановке работы дронов и системы мониторинга.

6. Утечка данных: Недостаточная защита может привести к случайной утечке данных о состоянии полей, что может быть использовано конкурентами.

7. Социальная инженерия: Злоумышленники могут пытаться манипулировать сотрудниками для получения доступа к системам, что может привести к компрометации данных.

Использование защищенной сети, такой как VPN, помогает минимизировать эти риски и обеспечивает безопасность данных.

Рекомендации: Фермерам стоит рассмотреть возможность внедрения VPN-систем, а также проводить регулярное обучение сотрудников по вопросам информационной безопасности.

Также хочу необходимо отметить недостатки, с которыми можно столкнуться – это Сложность настройки: Внедрение и настройка VPN может потребовать технических знаний, что может быть трудным для некоторых фермеров и малых предприятий.

Снижение скорости интернета: Использование VPN может замедлить скорость подключения из-за шифрования данных и дополнительного маршрутизации.

Зависимость от интернет-соединения: Эффективность VPN-системы зависит от качества интернет-соединения, что может быть проблемой в удаленных или сельских районах.

Стоимость: Некоторые надежные VPN-услуги могут быть дорогими, что может быть затруднительно для небольших фермерских хозяйств.

Уязвимости: хотя VPN защищает данные, не все VPN-сервисы одинаково безопасны. Неправильный выбор провайдера может привести к утечкам данных или недостаточной защите.

Обновления и поддержка: Необходимость регулярного обновления программного обеспечения и мониторинга безопасности может быть трудоемкой задачей для фермеров.

Ограниченные ресурсы: Некоторые устройства и системы могут не поддерживать VPN, что может ограничить их использование в агробизнесе.

Использование защищенной сети, такой как VPN, является важным шагом для обеспечения информационной безопасности в агросекторе. Несмотря на некоторые недостатки, преимущества в виде защиты данных и безопасного доступа перевешивают риски. Компании, занимающиеся точным земледелием, должны тщательно оценить свои потребности и возможности, чтобы эффективно внедрить VPN и минимизировать угрозы данных.

Список использованных источников

1. Мырзабекова, А. М. Обзор современных систем для хранения зерновых культур / А. М. Мырзабекова // Информационно-измерительная техника и технологии : материалы VI науч.-практ. конф. – Томск : Изд-во ТПУ, 2015. – С. 95 – 101.

References

1. Myrzabekova, A. M. Review of modern systems for storing cereals, Information and measuring equipment and technologies: materials of the VI scientific-practical conference / A. M. Myrzabekova. – Tomsk : Publishing house TPU, 2015. – P. 95 – 101.

УДК 681.5

А. А. Терехова, Б. С. Дмитриевский
(Кафедра «Информационные процессы и управление»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: terehova-95@yandex.ru)

СОВЕРШЕНСТВОВАНИЕ УПРАВЛЕНИЯ ПРОЦЕССОМ ПРОИЗВОДСТВА САХАРА

Аннотация. Рассмотрен подход к построению системы управления сахарным производством. Приведены характерные особенности производства с точки зрения управления. Для комплексного управления производством необходимо моделирование как отдельных участков производства, так и всего предприятия в целом.

Ключевые слова: система управления, производственный процесс, цифровизация.

A. A. Terekhova, B. C. Dmitrievsky
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

IMPROVING THE MANAGEMENT OF THE SUGAR PRODUCTION PROCESS

Abstract. An approach to the construction of a sugar production management system is considered. The characteristic features of production from the point of view of management are given. For integrated production management, it is necessary to model both individual production sites and the entire enterprise as a whole.

Keywords: management system, production process, digitalization.

Сотрудники предприятия, работающие непосредственно в цеховом помещении, сталкиваются со следующими физически опасными и вредными производственными факторами: повышенным уровнем шума, повышенной температурой, влажностью окружающей среды, воздействием электрического тока и статического электричества, недостаточной освещенностью рабочей зоны. Воздействие этих факторов ведет к снижению работоспособности и росту вероятности производственного травматизма. Труд работников должен быть организован таким образом, чтобы каждый из них имел строго закрепленное свое рабочее место, позволяющее использовать свою специальность и квалификацию с максимальным эффектом.

При выборе средств контроля технологических параметров сахарного производства учитывают возможность их работы в разных

средах и при разных режимах. Система управления сахарным производством строится как двухуровневая распределенная система [1].

Нижняя часть включает в себя аппаратную часть – различные датчики, регулирующие клапаны, программируемые контроллеры и программное обеспечение контроллеров.

Программируемые контроллеры решают задачи нижнего уровня:

– контроль технологических параметров;

– регулирование параметров;

– обмен информацией с верхним уровнем: прием команд установок и выдача информации о протекании технологического процесса.

Верхний уровень представляется автоматизированным рабочим местом (АРМ), разработанным на базе одной из популярных SCADA-систем.

АРМ решает задачи верхнего уровня:

– сбор и отображение информации о технологическом процессе;

– сигнализация возникновения критических состояний и аварийных ситуаций с регистрацией времени и места возникновения данной ситуации;

– учет количества выпущенной продукции за смену, сутки и месяц и др.

Цифровизация процесса управления позволяет успешно изменять одновременно множество переменных. Следовательно, источниками эффективности управляющих систем для сложных процессов является изменение промежутка времени, расходуемого на переход от одного рабочего режима к другому, а также сокращение числа нарушений процесса, вызываемых настройкой с целью компенсации возмущений. Скорость протекания или сложность процесса могут быть такими, что ручное управление заданиями регуляторов невозможно осуществлять достаточно быстро, чтобы поддерживать режимы вблизи нужных рабочих точек. Цифровизация обеспечивает повышение качества управления, благодаря своей способности быстро реагировать на возмущения и вырабатывать управляющие воздействия, в котором учитывается взаимное влияние настроек.

Анализ систем управления диффузионными аппаратами в сахарном производстве показал, что используемые методы управления не обеспечивают увеличение и стабилизацию концентрации сахарозы в выходящем диффузионном соке и не эффективны в условиях возмущений (качество сырья, площади свекловичной стружки, температура поступающей свеклы, нестационарности и инерционности технологических процессов).

Выявленные недостатки известных способов управления процессом получения диффузионного сока показали, что при большой инерционности обеспечивается необходимое качество регулирования только при малых возмущениях. Главная причина состоит в неумении преодоления инерционности объекта.

Системный анализ процессов производства сахара показал, что для совершенствования управления производством сахара, являющимся сложной системой, с большой размерностью и большим количеством возмущающих и управляющих воздействий, с повышенными требованиями к качеству продукта, необходимо формирование методологической основы для создания информационной базы для принятия управленческих воздействий.

Для совершенствования управления сахарным производством, как сложным многомерным производством, с целью повышения выхода сахара из корнеплодов свеклы в условиях переменного качества сырья разработана система управления, основанная на использовании оперативных данных от наиболее важных функциональных подсистем и имеет обратную связь.

Оперативное управление осуществлено за счет координации планов и ресурсов. От процессов сахарного производства через подсистемы передается информация о их состоянии лицу, принимающему решение. На основе анализа альтернатив в полученных отчетах принимаются решения по управлению производством.

Задача управления производством сахара сформулирована следующим образом: найти оптимальные управляющие воздействия на всех этапах жизненного цикла продукции, при которых достигается максимум выхода сахара из 1 тонны сахарной свеклы в течение производственного сезона (год) с учетом внешней и внутренней среды и ограничениями на ресурсы.

Список использованных источников

1. Разработка системы управления многосвязными технологическими процессами на примере пищевых производств / В. Г. Матвейкин, Б. С. Дмитриевский, А.А. Терехова, и др. // Вестник Тамбовского государственного технического университета. – 2023. – Т. 29, № 3. – С. 352 – 362.

References

1. Development of a management system for multicommunicated technological processes on the example of food production / V. G. Matveikin, B. S. Dmitrievsky, A. A. Terekhova, et al. // Bulletin of the Tambov State Technical University. – 2023. – V. 29, No. 3. – P. 352 – 362.

УДК 681.5

А. В. Андрющенко, Е. А. Светлишина, С. В. Дронов
(ФГБОУ ВО «ТГТУ», г. Тамбов, Россия
e-mail: 15.05.02.al@gmail.com)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ПРОЦЕССА ПРОИЗВОДСТВА ГОРЯЧЕЙ ВОДЫ В ГАЗОВОЙ КОТЕЛЬНОЙ

Аннотация. Предложен подход к построению распределенной АСУ ТП производства горячей воды в газовой котельной. Представлена структура АСУ ТП производства, построенная с использованием «интеллектуальных» датчиков и исполнительных механизмов.

Ключевые слова: производство горячей воды, распределенная система управления, автоматизированная система управления.

A. V. Andryushchenko, E. A. Svetlishina, S. V. Dronov
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

MODERN AUTOMATION TECHNOLOGIES PROCESS OF HOT WATER PRODUCTION IN A GAS BOILER

Abstract. An approach to the construction of a distributed automated process control system for hot water production in a gas boiler house is proposed. The structure of the automated process control system for production, built using “smart” sensors and actuators, is presented.

Keywords: hot water production, distributed control system, automated control system.

Технологический процесс производства горячей воды является сложным и требует эффективного управления с использованием современных средств и принципов автоматизации. В последнее время для производства горячей воды применяются газовые модульные котельные. Для управления процессом, протекающим в котельной, часто используются распределенные системы управления, благодаря которым улучшаются эксплуатационные характеристики оборудования. Распределенные системы управления включают в себя датчики, исполнительные механизмы, в которых установлен микропроцессорный модуль, который обеспечивает возможность дистанционного управления, самодиагностики, калибровки и поверки. Верхний уровень системы управления представлен автоматизированным рабочим местом оператора или сенсорной панелью оператора, а нижний уровень – интеллектуальными датчиками и исполнительными механизма-

ми с программируемыми логическими контроллерами. Разработанная система управления позволит повысить экономическую и технологическую эффективность производства горячей воды, снизит процент брака.

Использование распределенной системы управления в процессе производства горячей воды обеспечивает возможность оперативного контроля и управления процессом производства, что позволяет предотвращать возможные аварийные ситуации и обеспечивать стабильную работу оборудования. Благодаря автоматизации и централизации управления, производственные процессы становятся более прозрачными и эффективными, что, в свою очередь, повышает качество производимой продукции.

Важным элементом распределенной системы управления является возможность удаленного мониторинга и управления процессом, что позволяет операторам быстро реагировать на изменения и корректировать параметры производства в реальном времени. Такой подход упрощает работу персонала, сокращает временные затраты на наладку и настройку оборудования, а также уменьшает вероятность ошибок и сбоев в процессе.

В целом, применение современных технологий и принципов автоматизации в процессе производства горячей воды позволяет улучшить качество продукции, снизить затраты и повысить конкурентоспособность предприятия на рынке.

Список использованных источников

1. Промышленные вычислительные сети : учебное пособие/ И. А. Елизаров, П. М. Оневский, В. А. Погонин, А. А. Третьяков. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2012. – 152 с.

2. Интегрированные системы проектирования и управления. SCADA-системы : учебное пособие / И. А. Елизаров, А. А. Третьяков, А. Н. Пчелинцев и др. – Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2015. – 160 с.

References

1. Promyshlennye vychislitel'nye seti : uchebnoe posobie / I. A. Elizarov, P. M. Onevskij, V. A. Pogonin, A. A. Tret'yakov. – Tambov: Izd-vo FGBOU VPO “TGTU”, 2012. – 152 s.

2. Integrirovannye sistemy proektirovaniya i upravleniya. SCADA-sistemy : uchebnoe posobie / I. A. Elizarov, A. A. Tret'yakov, A. N. Pchelincev i dr. – Tambov : Tambovskij gosudarstvennyj tekhnicheskij universitet, EBS ASV, 2015. – 160 c.

УДК 681.5

А. Д. Анисимов, А. А. Брюханов, Н. С. Толстошеин, В. В. Шатских
(Межвидовой центр подготовки и боевого применения войск
радиоэлектронной борьбы (учебный и испытательный),
г. Тамбов, Россия,
e-mail: nauchnajarota@yandex.ru)

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПОСТРОЕНИЯ УЧЕБНО-ТРЕНИРОВОЧНЫХ СРЕДСТВ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ПРИМЕНЕНИЮ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ТЕХНИКИ

Аннотация. Представлена информационная технология построения учебно-тренировочных средств на основе модульной технологии для подготовки специалистов по применению сельскохозяйственной техники, которая позволяет повысить качество подготовки специалистов перед началом работы на используемой в производстве технике.

Ключевые слова: информационная технология, учебно-тренировочное средство, подготовка специалистов.

A. D. Anisimov, A. A. Bryukhanov, N. S. Tolstoshein, V. V. Shatskikh
(Interspecific Center for Training and Combat Use
of Electronic Warfare Troops (Training and Testing),
Tambov, Russia)

INFORMATION TECHNOLOGY OF CONSTRUCTION EDUCATIONAL AND TRAINING FACILITIES TO TRAIN SPECIALISTS IN THE USE OF AGRICULTURAL MACHINERY

Annotation. The paper presents an information technology for the construction of educational and training facilities based on modular technology for training specialists in the use of agricultural machinery, which allows to improve the quality of training of specialists before starting work on equipment used in production.

Keywords: information technology, educational and training tool, training of specialists.

Развитие аграрной промышленности подразумевает использование все большего числа разнообразной сельскохозяйственной техники, что влечет за собой увеличение количества времени, необходимого для обучения использования техники. Это создает трудности в доступности средств, на которых проводится обучение. Прежде чем использо-

вать сельскохозяйственную технику, необходимо пройти теоретическое и практическое обучение, как правильно производить необходимые операции для ее работы.

Подготовка специалистов на реальной технике может сопровождаться нанесением ей ущерба, например, обучаемый ошибается в порядке выполнения шагов эксплуатации техники, из-за чего возникают проблемы с ее дальнейшей эксплуатацией или здоровьем специалистов. Данные проблемы возможно решить с использованием учебно-тренировочных средств (УТС), предотвращая ремонт дорогостоящей техники. Так же УТС позволят повысить качество и скорость подготовки специалистов.

Для подготовки специалистов необходимо выделить технику, используемую для работы. Однако, количество обучаемых превышает количество техники, что при наличии одного образца займет значительное количество времени. Это ведет к снижению качества полученных знаний обучаемых при работе с техникой.

После проведения теоретических занятий обучаемому необходимо на практике закрепить полученные знания. Но, если теория будет доводиться отдельно от практических занятий, полноценного прогресса в освоении техники не возникнет. В УТС возможно настроить различные режимы освоения, в которых будет доводиться порядок работы с техникой и контролироваться итоговая подготовка обучаемого.

В основе создания УТС лежат технологии 3D-моделирования и виртуальной реальности. Для создания 3D-моделей компонентов сельскохозяйственной техники и окружающего мира может использоваться программа Cinema 4D, позволяющая создавать и текстурировать высокоточные модели.

Симуляции возможно создавать с использованием приложения Unity – игрового движка, который позволяет объединять разработанные 3D-модели в единую среду, а также визуально редактировать разрабатываемое УТС.

При создании УТС используется модульный подход, который выражается в построении следующих моделей:

– процесса усвоения информации специалистом;
– реального объекта (сельскохозяйственной техники);
– окружающей среды.

В итоге УТС представляет собой модульную систему, которая легко разбивается на параллельные процессы. Модули разрабатываются и отлаживаются максимально независимо. Данный подход к построению УТС на основе принципов модульности позволяет обеспечить решение следующих задач:

– одноразовая разработка и многократное использование компонентов УТС для подготовки специалистов;

– легкость модернизации УТС;
– коллективное использование УТС;
– сокращение сроков построения УТС;
– сбережение ресурсов и сокращение стоимости построения УТС.

УТС предоставляет возможность выбирать различные условия работы с техникой, характеристики окружающей среды, вести контроль действий обучаемого специалиста и фиксацию допускаемых ошибок.

Также для повышения качества освоения техники специалистом в УТС возможно смоделировать ситуации поломки техники или нарушения ее работы. В подобном сценарии обучаемый может лично увидеть признаки неисправности техники, и визуально запомнить порядок действий, необходимых для устранения неполадки.

После прохождения курса освоения сельскохозяйственной техники с использованием УТС специалист будет иметь представление о необходимых операциях для работы техники и о возможных неисправностях и путях решения данных проблем. Подготовленный оператор, при непосредственной работе на производстве, будет иметь виртуальный опыт работы с техникой и нахождения в нештатной ситуации.

УТС возможно использовать в учебных заведениях, в частности, при подготовке операторов сельскохозяйственной техники как для получения навыков управления и обслуживания техники, так и для проведения лабораторных исследований с использованием УТС.

Описанный опыт успешно применяется при разработке УТС двойного назначения в Межвидовом центре подготовки и боевого применения войск радиоэлектронной борьбы (учебном и испытательном).

Список использованных источников

1. Юрков Н. К., Интеллектуальные компьютерные обучающие системы / Н. К. Юрков. – Пенза : Изд-во ПГУ, 2010. – 304 с.

2. Зеленовская, Н. В. Возможности обучения с использованием виртуальных учебных имитаций (симуляторов) / Н. В. Зеленовская, Н. С. Филимонов // Инновационные технологии в инженерной графике: проблемы и перспективы : сб. тр. Междунар. науч.-практ. конф. (Брест, 21 апреля 2017 г.). – Новосибирский государственный архитектурно-строительный университет, 2017. – С. 114 – 116.

3. Шлее, М. Qt 5.10. Профессиональное программирование на C++ / М. Шлее. – СПб. : БХВ-Петербург, 2018. – 1072 с.

4. Тарасов, И. Е. ПЛИС Xilinx. Языки описания аппаратуры VHDL и Verilog, САПР, приемы проектирования / И. Е. Тарасов. – М. : Горячая линия – Телеком, 2022. – 538 с.

УДК 004.056

А. В. Бобровских, С. Г. Свиридов, Р. В. Мещеряков
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: a_dushkin1@mail.ru)

ВАРИАНТ ПОСТРОЕНИЯ ЭШЕЛОНИРОВАННОЙ ЗАЩИТЫ С ПОМОЩЬЮ ТЕХНОЛОГИИ КОНТЕЙНЕРИЗАЦИИ СРЕДСТВ СЕТЕВОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Показана возможность разработки следующих контейнеризированных средств сетевой безопасности: межсетевой экран с DNS-фильтром, прокси-сервер, балансировщик нагрузки и средство мониторинга.

Ключевые слова: информационная инфраструктура, межсетевой экран, фильтр, сетевая безопасность, мониторинг.

A. V. Bobrovskikh, S. G. Sviridov, R. V. Meshcheryakov
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

AN OPTION FOR CONSTRUCTING ECHELONED PROTECTION USING CONTAINERIZATION TECHNOLOGY FOR NETWORK SECURITY TOOLS FOR THE INFORMATION INFRASTRUCTURE OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. This article demonstrates the possibility of developing the following containerized network security tools: a firewall with a DNS filter, a proxy server, a load balancer, and a monitoring tool.

Keywords: information infrastructure, firewall, filter, network security, monitoring.

Основой защиты любой сетевой инфраструктуры организации являются средства сетевой безопасности, включающие в себя межсетевые экраны, прокси-серверы, балансировщики нагрузки. Главная проблема заключается в том, что зачастую данное оборудование узкоспециализировано, имеет высокую цену, минимальные сроки технической поддержки и быстро устаревает, что делает масштабирование данных устройств невыгодным. Виртуализация сетевых функций позволяет избежать значительных затрат и повысить сетевую безопасность путем построения, например, эшелонированной защиты [1].

Учитывая, что для обеспечения безопасности функции не должны зависеть друг от друга, то их предлагается запускать в изолированном окружении с помощью программного обеспечения Docker.

Программное обеспечение Docker – это программное обеспечение, позволяющее операционной системе запускать процессы в изолированном окружении с помощью специально созданных образов. В качестве образа сетевой операционной системы использована операционная система специального назначения (ОССН) «Astra Linux Special Edition» версии 1.7.

Для изоляции процессов используется технология контейнеризации, которая обеспечивает запуск приложений в контейнерах [2]. Контейнеры представляют собой виртуализированную среду с заложенной в нее функцией и позволяет воспроизвести функцию(-и) работы дорогостоящего сетевого оборудования. После создания контейнера провести изменение среды невозможно. Таким образом, обеспечивается высокий уровень целостности контейнера. При необходимости внесения изменений в конфигурацию контейнера, его останавливают, изменяют конфигурацию и создают заново.

Контейнеризация межсетевого экрана с функцией контентной фильтрации сетевого трафика позволяет предотвратить несанкционированный доступ к конфиденциальной информации, которая может быть передана через Интернет, блокировать потенциально опасные сайты, а также ресурсы, не связанные с работой и ввести административный контроль за пользователями в корпоративной сети. Для имитации работы межсетевого экрана с функцией контентной фильтрации сетевого трафика была использована утилита iptables, входящая в состав ОССН «Astra Linux», и специальный bash-скрипт, который позволил осуществить фильтрацию сетевого трафика в соответствии с настроенной политикой безопасности. Подключение к облачному DNS-серверу осуществляется путем изменения конфигурации системных настроек операционной системы Astra Linux 1.7.

Контейнеризация межсетевого экрана с функцией ограничения доступа к сетевым ресурсам на основе прокси-сервера. Для имитации работы межсетевого экрана с функцией ограничения доступа к сети Интернет по протоколу HTTP на основе прокси-сервера было использовано программное обеспечение SQUID, входящее в состав ОССН «Astra Linux». Данное виртуальное сетевое оборудование при определенных конфигурациях способно кешировать данные, фильтровать доступ и поддерживать различные схемы авторизации с помощью списков контроля доступа.

Контейнеризация межсетевого экрана с функцией балансировки нагрузки сети осуществляется с помощью программного обеспечения NGINX, входящего в состав ОССН «Astra Linux». Для этого в конфигурационных файлах нужно указать IP-адреса серверов и доменное имя локального веб-сервера. Гибкая настройка позволяет добавлять вес для распределения нагрузки между серверами, сохранять сессии на сайте и настраивать пассивные проверки работоспособности веб-ресурсов. В рамках исследовательской работы был реализован алгоритм балансировки Round Robin, что обеспечило более эффективное использование ресурсов и повысило отказоустойчивость системы.

Контейнеризация межсетевого экрана с функцией мониторинга сетевой инфраструктуры. Для имитации работы межсетевого экрана с функцией мониторинга событий сетевой инфраструктуры было использовано программное обеспечение Zabbix, входящее в состав ОССН «Astra Linux». Данный docker-контейнер позволяет отслеживать динамику работы серверов и сетевого оборудования. Создан шаблон для проверки целостности конфигурационных файлов и доступности средств сетевой безопасности.

Таким образом, применение технологии контейнеризации функций средств сетевой безопасности позволяет увеличить количество сетевых устройств, обеспечивающих политику информационной безопасности, что в свою очередь и ведет к увеличению количества уровней эшелонированной защиты.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 004.77

Д. В. Большунов, А. С. Марков
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: bolshunov01@mail.ru)

РАЗРАБОТКА ТЕХНИЧЕСКОГО РЕШЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ БЕЗОПАСНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ АСУ ТП В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрен подход к разработке технического решения по развертыванию серверного оборудования и операционной системы для инсталляции специального программного обеспечения с целью моделирования сетевой инфраструктуры АСУ ТП в агропромышленном комплексе.

Ключевые слова: информационная безопасность, автоматизированная система управления технологическим процессом, моделирование, сетевая инфраструктура, сервер.

D. V. Bolshunov, A. S. Markov
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

DEVELOPMENT OF A TECHNICAL SOLUTION FOR MODELING A SECURE NETWORK INFRASTRUCTURE OF AUTOMATED PROCESS CONTROL SYSTEMS IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The article considers an approach to developing a technical solution for deploying server equipment and an operating system for installing special software for the purpose of modeling the network infrastructure of an automated process control system in the agro-industrial complex.

Keywords: information security, automated process control system, modeling, network infrastructure, server.

Большое количество атак приходится на автоматизированные системы управления технологическими процессами (АСУ ТП). Причем, в соответствии с отчетами Positive Technologies, число атак на АСУ ТП на различных предприятиях (в том числе в агропромышленных комплексах) из года в год увеличивается. Поскольку практически каждое производство имеет в своем составе автоматизированные системы управления, решение данной проблемы становится крайне актуальным. Использование систем управления без предъявления требований по защите может привести как к остановке целого производ-

ства, так и к более серьезным последствиям [1] – нанесению недопустимого ущерба экологии и к человеческим жертвам (особенно, если атака была произведена на критически важные и потенциально опасные объекты агропромышленного комплекса (АПК)).

Моделирование и анализ сетевой инфраструктуры позволяет эффективно организовать работу всего предприятия, а также выявить потенциальные уязвимости в системе и определить, какие меры безопасности нужно внедрить, чтобы защитить данные и оборудование. Это особенно важно в условиях роста количества кибератак на предприятия агропромышленного комплекса.

Аппаратное обеспечение технического решения позволяет осуществлять хранение данных, вычислительные операции на своих ресурсах, а также межсетевое взаимодействие с другими узлами (рис. 1).

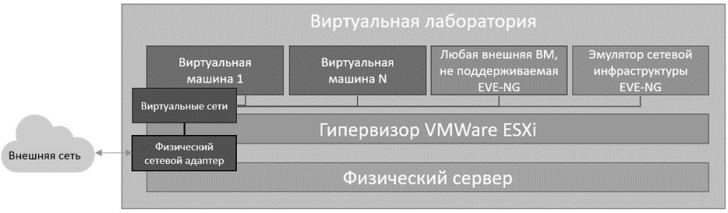


Рис. 1. Схема моделирования технического решения

На физический сервер производится установка платформы виртуализации и эмулятора сетевой инфраструктуры. Для разделения ресурсов сервера на виртуальные машины (ВМ), а также управления ими используется VMware ESXi, располагающийся непосредственно на физическом сервере, обеспечивая взаимодействие с ним операционной системы (ОС) и программного обеспечения (ПО), установленного на ВМ [2]. Именно исходя из ресурсов физического сервера устанавливается максимальное количество ВМ, которое можно развернуть в гипервизоре. ВМ представляет собой наиболее близкий аналог реального пользовательского компьютера, позволяющего использовать различные типы ОС. При этом в рамках одного физического сервера может функционировать несколько ВМ, имеющих различные характеристики.

Одна из виртуальных машин будет представлять собой образ эмулятора EVE-NG. За счет того, что EVE-NG обладает широким инструментарием конфигурирования, моделирования и проверки работоспособности межсетевой инфраструктуры, этот программный продукт является наиболее важным элементом структуры комплекса. Схема взаимодействия пользователей и администратора с моделируемой инфраструктурой представлена на рис. 2.

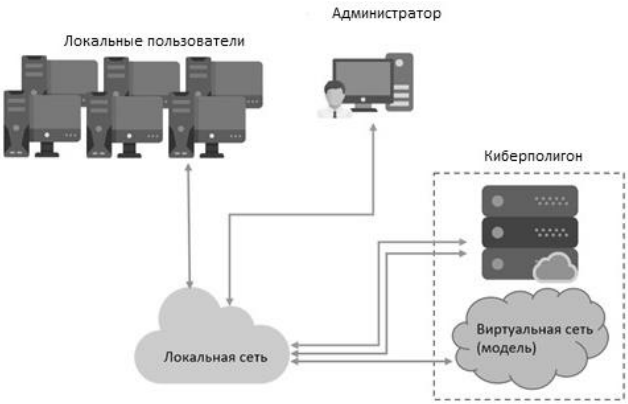


Рис. 2. Схема взаимодействия технического решения

Масштаб модели сетевой инфраструктуры ограничивается только физическими ресурсами сервера, которые, по мере необходимости, можно наращивать без ущерба самому стенду. Таким образом, моделирование сетевой инфраструктуры полезно для планирования, тестирования, оптимизации и защиты сетей, что помогает предприятиям, включая агропромышленные комплексы, повысить эффективность работы, снизить затраты на внедрение новых технологий и защитить критически важные данные и системы.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 681.518

Н. Г. Буранова
(ЧВПОУ «Западно-Казахстанский инновационно-технологический университет»,
г. Уральск, Республика Казахстан,
e-mail: nurslu_1986@mail.ru)

ОБ ОДНОМ ПОДХОДЕ К РАЗРАБОТКЕ АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПЕЛЛЕТНОЙ КОТЕЛЬНОЙ

Аннотация. Рассмотрены особенности и основные этапы разработки алгоритмического обеспечения интеллектуальной системы управления пеллетной котельной.

Ключевые слова: алгоритмическое обеспечение, интеллектуальная система управления, пеллетная котельная.

N. G. Buranova
(West Kazakhstan Innovation and Technology University,
Uralsk city, Republic of Kazakhstan)

ABOUT ONE APPROACH TO THE DEVELOPMENT OF ALGORITHMIC SOFTWARE INTELLIGENT PELLET BOILER CONTROL SYSTEM

Abstract. The features and main stages of the development of algorithmic support for an intelligent control system of a pellet boiler house are considered.

Keywords: algorithmic support, intelligent control system, pellet boiler.

Одной из ключевых тенденций современной теплоэнергетики является переход на возобновляемые источники энергии. В системах теплоснабжения активно развивается направление, связанное с использованием экологически чистого биотоплива в виде топливных пеллет, получаемых из отходов сельскохозяйственного и промышленного производства (древесных опилок, лузги подсолнечника, соломы и т.д.) [1].

Одним из преимуществ пеллетного котла является возможность достичь высокого уровня автоматизации процесса теплоснабжения за счет применения современной системы управления, которая обеспечит непрерывный мониторинг и оптимальное управление котельной.

Многие теплоэнергетические и теплотехнологические объекты, с точки зрения автоматизации, относятся к классу сложных многосвяз-

ных систем. Поэтому разработка алгоритмического обеспечения систем управления такими объектам, во многих случаях представляет собой сложную техническую задачу с элементами научного исследования, поскольку в состав алгоритмического обеспечения системы могут включаться алгоритмы, основанные на совместном применении методов системного анализа; математического, статистического и имитационного моделирования; искусственного интеллекта; теории оптимальных систем и др.

Одним из перспективных подходов к построению систем управления сложными многомерными объектами является подход, рассмотренный в [2]. Рассмотрим основные этапы и особенности разработки алгоритмического обеспечения интеллектуальной системы управления пеллетной котельной.

На первом этапе выполняется формализация и формулировка математических постановок общей и частных задач оптимального управления пеллетной котельной (частные задачи могут формулироваться для оптимального управления отдельными элементами котельной, например, электродвигателями, клапанами, вентиляторами и т.д.).

На втором этапе осуществляется идентификация и оценка адекватности математических моделей динамических и статических режимов работы объектов управления на множестве состояний функционирования. На данном этапе выделяются основные факторы, влияющие на изменение состояний функционирования объектов управления, а также формируются множества наиболее вероятных и критических состояний функционирования. Первое множество включает состояния с нормальной работоспособностью технологического оборудования котельной, а второе – содержит состояния с отказами технических средств. Полученные на данном этапе модели являются основой для разработки цифровых двойников отдельных элементов технологического оборудования и всей котельной в целом.

На третьем этапе проводится анализ задач оптимального управления, результаты которого позволяют определить условия существования решения, а также виды и параметры функций оптимального управления. На данном этапе могут использоваться аналитико-графические методы, основанные на совместном применении принципа максимума Понтрягина, метода синтезирующих переменных и когнитивной графики.

На четвертом этапе формируется база знаний алгоритмов синтеза оптимальных управляющих воздействий для наиболее вероятных состояний функционирования, а также возможные действия для критических состояний. В зависимости от текущего состояния функцио-

нирования объекта управления могут применяться наиболее оптимальные алгоритмы управления (энергосберегающие, помехоустойчивые, робастные, адаптивные, интеллектуальные и др.).

Последующая программная реализация разработанного алгоритмического обеспечения возможна как с использованием специальных проблемно-ориентированных средств, предназначенных для разработки систем автоматизации и управления (например, SCADA-систем), так и с применением CASE- и RAD-технологий. При этом, применительно к рассмотренному подходу к разработке алгоритмического обеспечения, весьма перспективной является концепция построения системы управления на основе теории мультиагентных систем [3].

Список использованных источников

1. Кривокоченко, Л. В. Мировой рынок древесных топливных гранул: современное состояние и перспективы развития / Л. В. Кривокоченко // Российский внешнеэкономический вестник. – 2021. – № 7. – С. 61 – 73.

2. Грибков, А. Н. Информационно-управляющие системы многомерными технологическими объектами: теория и практика: монография / А. Н. Грибков, Д. Ю. Муромцев. – Тамбов : Изд-во ФГБОУ ВО «ТГТУ», 2016. – 164 с.

3. Грибков, А. Н. Концепция построения интеллектуальной системы управления теплоэнергетическими объектами / А. Н. Грибков, Н. Г. Буранова // Радиоэлектроника. Проблемы и перспективы развития : сб. тр. IX Всерос. науч.-практ. конф. с междунар. участием. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2024. – С. 166 – 168.

References

1. Krivokochenko, L. V. Mirovoj ry`nok drevesny`x toplivny`x granul: sovremennoe sostoyanie i perspektivy` razvitiya / L. V. Krivokochenko // Rossijskij vneshnee`konomicheskij vestnik. – 2021. – № 7. – S. 61 – 73.

2. Gribkov, A. N. Informacionno-upravlyayushhie sistemy` mnogomerny`mi texnologicheskimi ob``ektami: teoriya i praktika: monografiya / A. N. Gribkov, D. Yu. Muromcev. – Tambov : Izd-vo FGBOU VO «TGTU», 2016. – 164 s.

3. Gribkov, A. N. Koncepciya postroeniya intellektual`noj sistemy` upravleniya teploe`nergeticheskimi ob``ektami / A. N. Gribkov, N. G. Buranova // Radioe`lektronika. Problemy` i perspektivy` razvitiya : sbornik trudov IX Vserossijskoj nauchno-prakticheskoj konferencii s mezhdunarodny`m uchastiem. – Tambov : Izdatel`skij centr FGBOU VO “TGTU”, 2024. – S. 166 – 168.

УДК 614.849

Р. Н. Бахтиев, Н. В. Гамалеев
(Кафедра «Техносферная безопасность
и транспортно-технологические машины»,
ФГБОУ ВО Вавиловский университет, г. Саратов, Россия,
e-mail: reno201@mail.ru, gamaleev-nikolaj@mail.ru)

АВТОМАТИЗИРОВАНИЕ ПОЖАРОТУШЕНИЯ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ КАК МЕРА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ МАШИН И ОБОРУДОВАНИЯ

Аннотация. Рассмотрен вопрос повышения противопожарной защиты в агропромышленном комплекс, с использованием мобильных пожарных установок.

Ключевые слова: пожарная безопасность, мобильные пожарные установки.

R. N. Bahtiev, N. V. Gamaleev
(Department of Technosphere Safety and Transport
and Technological Machines,
Vavilov University, Saratov, Russia)

AUTOMATION OF FIRE EXTINGUISHING IN THE AGRO-INDUSTRIAL COMPLEX AS A MEASURE TO IMPROVE SAFETY IN THE OPERATION OF MACHINERY AND EQUIPMENT

Abstract. The article deals with the issue of improving fire protection in the agro-industrial complex, using mobile fire installations.

Keywords: fire safety, mobile fire installations.

Обеспечение продовольственной безопасности нашей страны невозможно без выполнения комплексных противопожарных мероприятий на всех объектах сельскохозяйственного сектора; а также на всех стадиях посадки, выращивания, уборки урожая зерновых, кормовых культур, содержания мясомолочных пород скота, пушных зверей. Сельскохозяйственные предприятия разных форм собственности – от небольших частных ферм до крупных агрохолдингов различаются организационно-экономическими возможностями, соответственно, наличием или отсутствием пожарных депо, автоматическими системами противопожарной защиты, автотехники, количеством обученных сотрудников пожарных формирований.

Модернизация системы противопожарной защиты наиболее необходима в тех местах, где существуют серьезные трудности с воз-

можностью осуществлять тушения общепринятыми способами, а также в тех местах, где временной интервал играет ключевую роль.

Кроме этого, территории, относящиеся к лесостепным и степным зонам, на которых ведется интенсивное сельскохозяйственное производство, находятся, как правило, в пограничном состоянии с лесными массивами. В этом случае, пожар дополнительно может перейти в лесной, тем самым нанести двойной удар: по ведению сельскохозяйственного производства и лесного хозяйства.

Из всех видов деятельности, с научной точки зрения, наиболее перспективными являются обоснование использования мобильных средств пожаротушения с автоматической подачей огнетушащего вещества.

Функциональная схема данного решения представлена на рис. 1.

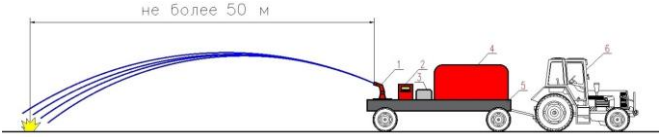


Рис. 1. Принципиальная функциональная схема мобильной пожарной установки

На схеме, изображенной на рис.1, представлена мобильная пожарная установка (МПП).

Данная установка сформирована на базе прицепа *5*, на котором расположен резервуар с огнетушащим составом *4*, мотопомпой и генератором *3*, управляемым лафетным стволом с приводом *1*, шкафом управления лафетным стволом *2*.

В качестве техники, используемой для перемещения МПП, может быть использован трактор *6* или иная машина, с возможностью сцепки через фаркоп.

Принцип работы МПП основан на автоматическом обнаружении пожара и наведении лафетного ствола.

Данное решение позволит ускорить и обезопасить процесс тушения путем:

– мобильности средства пожаротушения;

– автоматического определения возгорания, наведения лафетного ствола и подачи огнетушащего вещества без прямого участия человека;

– сохранить жизнь и здоровье человека, участвующего в тушении, путем исключения его непосредственной деятельности в ликвидации пожара.

Основополагающими достоинствами данного изделия является:

– наличие автоматического обнаружения возгорания;

– система наведения лафетного ствола с использованием программного обеспечения;

– отсутствие постоянного участия человека в процессе тушения;
– дальность подачи огнетушащего состава до 50 м.

В возможности установки входит ее способность управляться автоматизированным способом – где итоговое решение о начале и завершении процесса тушения, выбора приоритетной цели тушения (в случае возникновения более одного очага пожара) остается за оператором.

Оператор отдает команды установке посредством использования пульта дистанционного управления или нажатия кнопок/переключателей, расположенных на системном шкафе.

Переоценить достоинство данного решения сложно, ведь, как известно, определяющим фактором, обеспечивающим безопасность, является время, затраченное на реагирование, выбор дальнейшего алгоритма действий и непосредственно потраченное на решение сложившейся ситуации.

Временной фактор при ликвидации возгорания напрямую отражается на безопасности при эксплуатации машин и сельскохозяйственной техники.

Данное решение позволит значительно сэкономить время на принятие решения о тушении и увеличит скорость локализации и ликвидации пожара.

А это является фундаментом основы спасения, ликвидации и предотвращения чрезвычайной ситуации.

Список использованных источников

1. Технический регламент о требованиях пожарной безопасности : федер. закон № 123-ФЗ.
2. О пожарной безопасности : федер. закон от 21.12.1994 № 69-ФЗ.
3. Об утверждении Правил противопожарного режима в Российской Федерации : постановление Правительства РФ от 16 сентября 2020 г. № 1479.
4. ФГБУ ВНИИПО МЧС России «Пожары и пожарная безопасность в 2023 г. Информационно-аналитический сборник. Статистика пожаров и их последствий». – Балашиха, 2024.

References

1. Technical Regulations on Fire Safety Requirements : Federal Law No. 123-FZ.
2. On Fire Safety : Federal Law dated 12/21/1994 No. 69-FZ.
3. On approval of the Rules of fire protection in the Russian Federation : Decree of the Government of the Russian Federation No. 1479 dated September 16, 2020.
4. Federal State Budgetary Institution VNIIPO of the Ministry of Emergency Situations of Russia “Fires and fire safety in 2023. Information and analytical collection. Statistics of fires and their consequences”. – Balashikha, 2024.

УДК 378.016

А. С. Гордеев, Б. С. Мишин, А. Н. Попов
(Мичуринский государственный аграрный университет,
г. Мичуринск, Россия)

ЦИФРОВОЙ МЕТОД КОНТРОЛЯ ЗРЕЛОСТИ ЯБЛОК

Аннотация. В данной статье яблоко рассматривается как электрическая емкость, характеристики заряда которой зависит от зрелости плода. Заряд плода аппроксимируется экспонентой, по которой и определяется зрелость. За базовый метод определения зрелости взят метод содержания крахмала в плоде при его реакции на раствор йода, имеющий основной недостаток – субъективность выводов. Приведена методика контроля и принципиальная электронная схема измерения заряда ткани плода, а также структура прибора на ее основе.

Ключевые слова: яблоко, зрелость, крахмал, плод.

A. S. Gordeev, B. S. Mishin, A. N. Popov
(Michurinsk State Agrarian University,
Michurinsk, Russia)

DIGITAL METHOD OF APPLE MATURITY CONTROL

Abstract. In this article, an apple is considered as an electric capacity, the charge characteristics of which depend on the maturity of the fruit. The charge of the fetus is approximated by an exponent, which determines maturity. The basic method for determining maturity is the method of starch content in the fruit during its reaction to an iodine solution, which has the main drawback – the subjectivity of conclusions. The method of control and the basic electronic circuit for measuring the charge of fetal tissue, as well as the structure of the device based on it, are given.

Keywords: apple, maturity, starch, fruit.

Уборка плодов, в частности яблок, является важнейшим этапом в их выращивании, хранении и реализации населению. Потери яблок при хранении зависят от зрелости, т.е. от их сроков съема с дерева [1, 2].

Один из классических методов контроля зрелости яблок – по степени разложения в ткани яблока крахмала в сахар (метод йод-крахмальной пробы). Метод основан на способности йода окрашивать крахмал в синий цвет [1, 2].

Определение баллов по данному методу осуществляется человеком, что вносит большой субъективный элемент в результат контроля. Существует автоматический прибор контроля зрелости яблок Amilon

итальянской компании Isocell [3]. Принцип его работы основан на методе ЙКП, а процесс определения балла зрелости осуществляется компьютерным анализом изображения по фото разреза яблока. Недостатки прибора: зависимость от иностранного производителя, большая цена, громоздкая конструкция, невозможность определять зрелость в полевых условиях (в саду) и необходимость в специально обученном персонале.

С целью устранения указанных недостатков нами разрабатывается прибор контроля зрелости яблока на основе изменения электрофизических характеристик яблока в процессе созревания [4].

Методы проведения эксперимента. В основу построения прибора для контроля зрелости яблок положено предположение, что ткань яблока можно рассматривать как совокупность отдельных элементов – биологических клеток с мембранами, находящимися в среде ионов [4].

Структура прибора для контроля зрелости яблок приведена на рис. 1.

Рис. 1. Структура прибора для контроля зрелости яблок

Предварительно компьютер ПК загружает в микропроцессор МК программу работы (алгоритм измерения). После внедрения в ткань яблока электродов e1 и e2 оператор через ПК дает команду на начало измерения. Микропроцессор МК подает на измерительный модуль, а тот в свою очередь на электроды e1 и e2 импульс напряжения U = 5 В. Начался процесс заряда ткани плода, который продолжается в течение всего времени действия этого импульса. По мере заряда ткани измерительный модуль подает электрический потенциал с электро-

да e1 на аналого-цифровой преобразователь (АЦП), который через определенные промежутки времени осуществляет преобразование аналогового сигнала заряда в цифровую форму. Цифровой сигнал записывается в память компьютера. После окончания действия импульса заряд ткани заканчивается. Время измерения можно варьировать программным путем в пределах 0,1…2 с.

Обработка экспериментальных данных осуществлялась в программной среде Matlab. Зрелость Z в эксперименте получали классическим методом йод-крахмальной пробы по 5-балльной шкале. Полученные экспериментальные данные аппроксимировались экспоненциальной зависимостью:

$$Y(x) = a*\exp(b*x) + c*\exp(d*x),$$

где Y – получаемая при аппроксимации теоретическая зависимость сигнала от времени заряда; a, b, c, d – коэффициенты аппроксимации экспоненты.

На рисунке 2 и табл. 1 приведены результаты аппроксимации экспонент заряда ткани на 15 августа и 2 сентября для помологического сорта Лобо. Корреляционный анализ данных, из которых была получена табл. 1, показывает, что корреляция между зрелостью Z и коэффициентами экспоненты находится в пределах –0.7433… 0.7713.

Таким образом, между зрелостью плода и параметрами экспоненты существует несильная статистическая связь. Это может быть следствием использования базового метода определения зрелости по йод-крахмальной пробе. Его погрешность определения зрелости в литературе не упоминается.

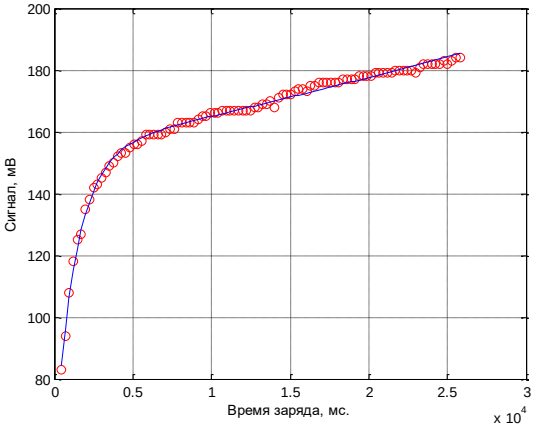


Рис. 2. Заряд ткани плода на 15 августа:
o – экспериментальные данные; —— – теоретическая зависимость

1. Параметры экспоненты *a, b, c, d* помологического сорта Лобо на дату *t*

t (дата)	*q*	*ps*	*z*	*a*	*b*	*c*	*d*
15.08	1.0000	1.0000	1.5000	153.4584	0.0000	–96.1981	–0.0007
19.08	1.0000	1.0000	3.0000	122.7145	0.0000	–61.9856	–0.0007
23.08	1.0000	1.0000	1.5000	124.6307	0.0000	–65.4291	–0.0005
28.08	1.0000	1.0000	2.0000	133.4447	0.0000	–78.2383	–0.0008
2.09	1.0000	1.0000	2.0000	136.6554	0.0000	–77.0371	–0.0008

Выводы и предложения

1. Современные методы и приборы контроля зрелости плодов не предполагают полевого применения, что затрудняет массовое измерение зрелости на практике.

2. Предложен метод определения зрелости яблок по параметрам заряда ткани яблока.

3. Путем лабораторных исследований показано, что заряд ткани яблока во времени происходит по экспоненте и зависит от времени роста (зрелости) плодов.

4. Предложена электронная схема для измерения заряда ткани яблока и на ее основе – структура прибора для контроля зрелости яблок, позволяющая использовать прибор непосредственно в саду при работе в автоматизированных (интеллектуальных) системах управления уборкой, хранением и реализацией плодов в садоводческих предприятиях и хранилищах.

Список использованных источников

1. Гудковский, В. А. Система сокращения потерь и сохранение качества плодов и винограда при хранении : методические рекомендации / В. А. Гудковский. – Мичуринск, 1990. – 119 с.

2. Франчук, Е. П. Товарные качества плодов / Е. П. Франчук. – М. : Агропромиздат, 1986.

3. Официальный сайт Isocel, прибор Amilon. – URL : https://storage.isolcell.com/en/amilon/ (дата обращения: 14.12.2022 г.).

4. Гордеев, А. С. Автоматизированная обработка яблок : дис. … д-ра техн. наук / А. С. Гордеев. – М., 1996.

УДК 681.5

С. В. Дронов, Е. А. Светлишина, А. В. Андрющенко
(ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: sergejdronov2@gmail.com)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ПРОЦЕССА ДИАЗОТИРОВАНИЯ ПРИ ПРОИЗВОДСТВЕ ПИГМЕНТА АЛОГО

Аннотация. Рассмотрен процесс разработки АСУ ТП диазотирования при производстве пигмента алого. Определены основные цели и назначение АСУ ТП.

Ключевые слова: производство пигмента алого, диазотирование, автоматизированная система управления.

S. V. Dronov, E. A. Svetlishina, A. V. Andryushchenko
(TSTU, Tambov, Russia)

MODERN AUTOMATION TECHNOLOGIES THE PROCESS OF DIAZOTIZATION IN THE PRODUCTION OF RED PIGMENT

Abstract. This article discusses the process of developing an automated process control system for diazotization in the production of red pigment. It also defines the main objectives and purposes of this automated process control system.

Keywords: production of red pigment, diazotization, automated control system.

Производство химической продукции – одна из самых важнейших и развивающихся отраслей народного хозяйства в Тамбовской области. Спрос на продукцию, производимую на АО «Пигмент», постоянно растет. Поэтому в химической промышленности важное место отводится решению проблемы автоматизации производственных процессов.

Задача автоматизации состоит в том, чтобы с помощью современной техники обеспечить протекание технологического процесса так, чтобы в результате более гибкого управления процессом поддерживать определенное качество продукта, снизить процент брака, а также затраты на энергоресурсы, что приведет в конечном итоге к снижению себестоимости выпускаемой продукции.

АСУ ТП должна выполнять информационно-вычислительную и управляющую функции. Каждая из этих функций включает ряд задач. В их число входит и комплекс задач осуществления общеси-

стемных функций (организация вызовов задач в заданных последовательности и времени, обслуживание базы данных и обеспечение ее сохранности, организация обмена информацией между задачами).

Целью создания АСУ ТП является повышение эффективности процесса за счет использования современных микропроцессорных средств управления.

Разрабатываемая автоматизированная система управления должна обеспечить:

– более точное поддержание параметров процесса;

– более надежную работу оборудования;

– снижение до минимума количества внештатных ситуаций за счет своевременного информирования персонала о тенденции к их возникновению;

– снижение влияния человеческого фактора.

АСУ ТП должна выполнять все требуемые от нее запросы по автоматизации процесса, сбору данных и предотвращение аварийных ситуаций. Оператор при этом должен применять минимальные действия по отношению к процессу в целом. Система в своем целом должна работать с минимальным вмешательством человека.

АСУ ТП должна иметь иерархическую двухступенчатую архитектуру:

– на нижнем уровне находятся: датчики, измерительные преобразователи, исполнительные механизмы, вторичные приборы;

– на верхнем уровне находятся: программно-логические контроллеры (ПЛК), установленные в щитах контроля и управления (ЩКУ), обеспечивающие прием, первичную обработку информации от датчиков и исполнительных механизмов, а также формирование команд управления в соответствии с заданиями, поступающими от местных пультов, реализованных с помощью сенсорных панелей оператора и реализованного на ПК;

Разработанная АСУ ТП должна реализовывать следующие функции:

– мониторинг технологических параметров, состояния технологического оборудования;

– автоматизированное управление клапанами, регулирующими температуру, управление насосами;

– представление текущей и исторической информации;

– выделение аварийных и предаварийных ситуаций с автоматической генерацией сигналов тревоги;

– возможность выбора режима управления.

Список использованных источников

1. Промышленные вычислительные сети : учебное пособие / И. А. Елизаров, П. М. Оневский, В. А. Погонин, А. А. Третьяков. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2012. – 152 с.
2. Интегрированные системы проектирования и управления. SCADA-системы : учебное пособие / И. А. Елизаров, А. А. Третьяков, А. Н. Пчелинцев и др. – Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2015. – 160 с.

References

1. Promyshlennye vychislitel'nye seti : uchebnoe posobie / I. A. Elizarov, P. M. Onevskij, V. A. Pogonin, A. A. Tret'yakov. – Tambov : Izd-vo FGBOU VPO “TGTU”, 2012. – 152 s.
2. Integrirovannye sistemy proektirovaniya i upravleniya. SCADA-sistemy : uchebnoe posobie / I. A. Elizarov, A. A. Tret'yakov, A. N. Pchelincev i dr. – Tambov : Tambovskij gosudarstvennyj tekhnicheskij universitet, EBS ASV, 2015. – 160 c.

УДК 004.056

А. В. Душкин, Д. Р. Мусин, И. С. Порсев
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, г. Москва, Россия,
e-mail: a_dushkin@mail.ru)

СРАВНЕНИЕ МЕТОДОВ ОБРАБОТКИ СЛАБОСТРУКТУРИРОВАННОЙ ИНФОРМАЦИИ В УСЛОВИЯХ СИЛЬНЫХ ШУМОВ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ СРЕДСТВ ДЛЯ РЕШЕНИЯ ЗАДАЧ БЕЗОПАСНОСТИ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Представлено экспериментальное сравнение методов обработки слабоструктурированной информации на естественном языке в условиях сильных шумов для решения задач безопасности. Показаны преимущества разработанного метода.

Ключевые слова: слабоструктурированная информация, метод, разборчивость, текст, шум, эффективность.

A. V. Dushkin, D. R. Musin, I. S. Porsev
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

COMPARISON OF METHODS FOR PROCESSING WEAKLY STRUCTURED INFORMATION IN CONDITIONS OF STRONG NOISE USING DIGITAL TOOLS FOR SOLVING SECURITY PROBLEMS IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The paper presents an experimental comparison of methods for processing weakly structured information in natural language under strong noise conditions for solving security problems. The advantages of the developed method are shown.

Keywords: semi-structured information, method, legibility, text, noise, efficiency.

Защита акустической речевой информации от ее утечки по техническим каналам является одной из важнейших задач обеспечения конфиденциальности переговоров, ведущихся в выделенных помещениях. В качестве показателя оценки эффективности ее защиты используется словесная разборчивость речи, под которой понимается относительное

количество правильно понятых слов из перехваченного средством акустической разведки разговора. Для оценки эффективности защиты акустической речевой информации от утечки по техническим каналам используется методика, в основу которой положен форматный метод оценки разборчивости речи [1]. Ее основным недостатком является то, что при расчете разборчивости речи учитывается только тот случай, когда оператор услышит звуки речи во всех семи октавных полосах. При низких отношениях сигнал/шум слышимость звуков речи в октавных полосах носит вероятностный характер, при прослушивании речи могут возникнуть различные комбинации октавных полос, в которых оператор может услышать звуки речи. С целью оценки вклада различных комбинаций (сочетаний) октавных полос в словесную разборчивость речи проведены экспериментальные исследования, где в качестве исходных тестовых речевых сигналов использовались по две артикуляционные таблицы слов для каждого диктора из ГОСТ 16600–72 «Требования к разборчивости речи и методы артикуляционных измерений». Расчетное количество комбинаций октавных полос составило 128. Однако в ходе экспериментов было выявлено, что 1-я и 7-я октавные полосы мало влияют на разборчивость речи. Их учет приводит к увеличению показателя разборчивости речи не более, чем на 0,1% независимо от используемой комбинации, что подтверждено в рекомендациях Международного союза электросвязи, согласно которым измерение эффективного спектра речи производится в диапазоне частот от 300 до 3400 Гц. Поэтому при экспериментальных исследованиях исследовались только комбинации октавных полос со 2-й по 6-ю. В результате расчетов количество комбинаций составило 32.

На основе проведенных экспериментальных исследований авторами предложен метод (способ) вероятностной оценки (измерения) разборчивости [2]. С целью проверки достоверности расчетов по методике, в основу которой положен вероятностный метод, проведены экспериментальные исследования словесной разборчивости речи методом артикуляционных испытаний.

Результаты словесной разборчивости речи, рассчитанные по методикам, в основу которых положены вероятностный и формантный методы, а также полученные в ходе экспериментальных исследований приведены на рис. 1.

Анализ полученных графиков (рис. 1) показывает высокую сходимость результатов расчетов по методике, в основу которой положен вероятностный метод, с экспериментальными данными. Разница

между рассчитанными и экспериментальными значениями возможно объясняется тем, что при проведении испытаний некоторые слова, включенные в артикуляционные таблицы, были труднораспознаваемыми, даже при высоких отношениях сигнал/шум, что повлияло на результаты испытаний. Словесная разборчивость речи, рассчитанная по методике, в основу которой положен формантный метод, существенно ниже, чем полученная по результатам экспериментальных исследований и методике, в основу которой положен вероятностный метод.

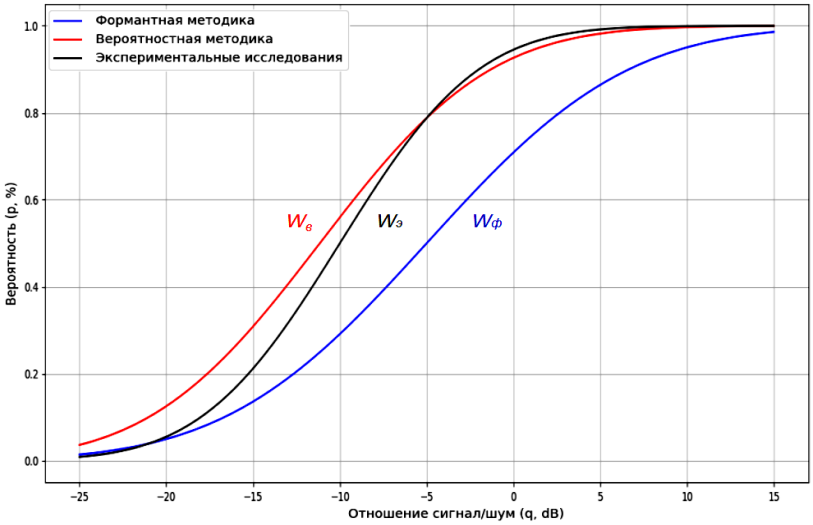


Рис. 1. Графики зависимости словесной разборчивости речи (W) от отношения сигнал/шум (q), полученные: $W_в$ – по результатам расчетов (вероятностный метод); $W_ф$ – по результатами расчетов (формантный метод); $W_э$ – по результатам артикуляционных испытаний

Занижение возможностей средств акустической разведки противника может привести к утечке речевой информации. Разработанная методика может быть использована для оценки эффективности защиты акустической речевой информации от ее утечки по техническим каналам, так как дает более высокие значения разборчивости речи, по сравнению с используемой в настоящее время методикой, на основе формантного метода. Материалы подготовлены в рамках гранта РНФ № 24-11-00340.

Список использованных источников

1. Хорев, А. А. Методика вероятностной оценки разборчивости речи / А. А. Хорев, И. С. Порсев // Защита информации. Инсайд. – СПб., 2020. – № 2. – С. 44 – 52.

2. Porsev, I. S. Analysis and Control of the Effectiveness of Information Protection Against Leakage Through Technical Channels Based on Probabilistic Assessment / I. S. Porsev, M. A. Melshiyan, A. V. Dushkin // 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – 2022. – P. 398 – 401.

References

1. Khorev, A. A. Metodika veroyatnostnoi otsenki razborchivosti rechi / A. A. Khorev, I. S. Porsev // Zashchita informatsii. Insaid. – SPb., 2020. – № 2. – S. 44 – 52.

2. Porsev, I. S. Analysis and Control of the Effectiveness of Information Protection Against Leakage Through Technical Channels Based on Probabilistic Assessment / I. S. Porsev, M. A. Melshiyan, A. V. Dushkin // 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). – 2022. – P. 398 – 401.

УДК 681.5

М. И. Елизарова
(Институт компьютерных наук и кибербезопасности,
ФГАОУ ВО «Санкт-Петербургский политехнический
университет Петра Великого», г. Санкт-Петербург, Россия,
e-mail: elizarova2002@ yandex.ru)

К ВОПРОСУ ВЫБОРА ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ НА ОБЪЕКТАХ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Предложена классификация объектов агропромышленного комплекса с точки зрения площади и возможности организации стационарного питания средств автоматизации. Для каждого класса приведены рекомендации по использованию беспроводных технологий передачи данных для построения систем управления.

Ключевые слова: беспроводные технологии передачи данных, LoRaWAN, ZigBee, Wi-Fi, сотовая связь.

M. I. Elizarova
(Institute of Computer Science and Cybersecurity
St. Petersburg Polytechnic University Peter the Great,
St. Petersburg, Russia)

ON THE ISSUE OF CHOOSING THE TECHNOLOGY OF DATA TRANSMISSION AT THE FACILITIES OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. The classification of objects of the agro-industrial complex is proposed in terms of area and the possibility of organizing stationary catering of automation equipment. Recommendations on the use of wireless data transmission technologies for building control systems are provided for each class.

Keywords: Wireless data transmission technologies, LoRaWAN, ZigBee, Wi-Fi, cellular communication,

Агропромышленный комплекс (АПК) включает в себя все отрасли хозяйства, направленные на производство, переработку и доставку до потребителя сельскохозяйственной продукции. Это предприятия растениеводства и животноводства, хранения и переработки сельскохозяйственной продукции. В зависимости от отрасли отличаются условия размещения оборудования и требования, предъявляемые к системе управления. По обслуживаемой площади и возможности использовать стационарные источники питания для устройств можно разделить предприятия АПК на три группы.

Первая группа объединяет предприятия растениеводства, занимающие большую открытую площадь (сотни гектар, например, промышленные сады или поля) и крупные тепличные комплексы (десяткисотни гектар). Использование кабельных линий связи для передачи данных на контроллер и управляющих сигналов к оконечным устройствам в этом случае экономически не рационально ввиду больших затрат на кабельную продукцию. Кроме того, важным становится вопрос энергоэффективности и времени автономной работы оконечного устройства, потому что часто отсутствует возможность организовать питание от стационарного источника. Возможна передача данных посредством сетей сотовой связи и технологий CSD, SMS или GPRS (например, с использованием устройств серии MOXA OnCell). Технология CSD обеспечивает скоростной канал передачи данных, что удобно при наладке удаленного оборудования. Тарификация производится на временной основе, а для передачи данных требуется предварительная установка соединения, следовательно, необходимо применение оборудования с поддержкой функции работы с модемами. Технология SMS подходит для отправки коротких сообщений, не превышающих 140 байт [1]. При большем объеме передаваемой информации посылка будет разбита на два сообщения. Используя функцию SMS Tunnel можно указать номера для входящих и исходящих сообщений, чтобы устройство принимало сигналы только с авторизованных пользователей. При использовании технологии GPRS информация передается посредством неиспользуемых в данный момент голосовых каналов связи, а тарификация происходит по объему переданных данных. При использовании технологий SMS и GPRS возникает задержка несколько секунд, что не критично при медленно протекающем процессе роста растений и подходит, например, для периодического опроса датчиков. Таким образом, использование передачи данных посредством сетей сотовой связи целесообразно в случае близкого расположения предприятия АПК к вышкам сотовой связи и высоком качестве сигнала. Кроме того, присутствует зависимость от оператора сотовой связи и необходимость внесения абонентской платы.

Альтернативным вариантом организации беспроводного канала связи является использование сети LoRaWAN. Она позволяет обеспечить передачу сигнала на расстояние до 15 км в зоне прямой видимости при высокой помехозащищенности и низкое энергопотребление, которое особенно важно при большом количестве распределенных по территории комплекса автономных оконечных устройств [2]. Кроме того, сеть можно масштабировать в процессе эксплуатации. Важно помнить, что эта технология не позволяет организовать обмен боль-

шими пакетами данных, но подходит, например, для периодического опроса датчиков температуры и влажности почвы.

Вторая группа предприятий АПК объединяет крытые предприятия, занимающие площадь единицы-десятки гектар, например, тепличные комплексы, животноводческие хозяйства. В этом случае применение проводной технологии передачи данных также не рационально ввиду большого расстояния до оконечных устройств, но возможна организация питания от стационарного источника. В этом случае возможно применение технологии LoRaWAN, несмотря на то, что покрытие избыточно для небольших комплексов. Также возможно использование технологии Wi-Fi с применением повторителей и направленных антенн.

Третья группа объединяет предприятия перерабатывающей промышленности, например, спиртовые и сахарные заводы. Эта группа характеризуется относительно небольшой площадью цехов, большим количеством технологического оборудования (следовательно, большим количеством технических средств автоматизации) и более быстро протекающими технологическими процессами, требующими постоянного мониторинга. Таким образом, для опроса оконечных устройств и передачи сигналов управления необходим канал связи с высокой пропускной способностью. Наиболее предпочтительным в данном случае является использование проводных технологий передачи, например, посредством промышленных сетей на базе интерфейса RS-485 или Ethernet. При сложности прокладки проводной сети возможно использование беспроводных технологий.

Одной из таких технологий является технология Zigbee. Ее отличительная особенность – возможность создания ячеистой топологии, что повышает надежность системы за счет создания самовосстанавливающейся сети [3]. К недостаткам можно отнести меньшее, чем, например, у LoRaWAN покрытие и большее энергопотребление модулей. Сеть Zigbee может быть применена для организации сети опроса датчиков и управления исполнительными механизмами, создания системы промышленного интернета вещей (IIoT) на предприятии.

Для организации высокоскоростного обмена данными посредством беспроводных технологий между контроллерами, удаленными модулями ввода-вывода, автоматизированными рабочими местами операторов рационально использование сети Wi-Fi.

Список использованных источников

1. Масленкова, И. GSM/GPRS технологии в системах промышленной автоматики [Электронный ресурс] / И. Масленкова, А. Команцев // Control Engineering Россия. – URL : https://controlengrussia.com/bezopasnost/gsmgprs-tekhnologii-v-sistemakh-promyshlennoi-promyshlennoi/ (дата обращения: 18.09.2024).

2. Выбор беспроводной технологии передачи данных для построения системы мониторинга в интенсивном садоводстве / И. А. Елизаров, А. А. Третьяков, В. Н. Назаров, М. И. Елизарова // Цифровизация агропромышленного комплекса : сб. науч. ст. III Междунар. науч.-практ. конф., Тамбов, 25 – 27 октября 2022 года. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – Т. 1. – С. 65 – 67.

3. Еркин, А. Особенности проектирования беспроводных ZigBee-сетей на базе микроконтроллеров фирмы Jennic [Электронный ресурс] / А. Еркин // Беспроводные технологии – URL : https://wireless-e.ru/wpan/zigbee/jennic/ (дата обращения: 18.09.2024).

References

1. Maslenkova, I. GSM/GPRS technologies in industrial automation systems [Electronic resource] / I. Maslenkova, A. Komantsev // Control Engineering Russia. – URL : https://controlengrussia.com/bezopasnost/gsmgprs-tekhnologii-v-sistemakh-promyshlennoi-promyshlennoi / (accessed: 18.09.2024).

2. The choice of wireless data transmission technology for building a monitoring system in intensive horticulture / I. A. Elizarov, A. A. Tretyakov, V. N. Nazarov, M. I. Elizarova // Digitalization of the agro-industrial complex : Collection of scientific articles of the III International scientific and practical conference, Tambov, October 25 – 27, 2022. – Tambov Publishing Center of Tambov State Technical University, 2022. – V. 1. – P. 65 – 67.

3. Yerkin, A. Features of designing wireless ZigBee networks based on Jennic microcontrollers [Electronic resource] / A. Yerkin // Wireless technologies. – URL : https://wireless-e.ru/wpan/zigbee/jennic / (date of notification: 09/18/2024).

УДК 681.5

М. И. Елизарова
(Институт компьютерных наук и кибербезопасности,
ФГАОУ ВО «Санкт-Петербургский политехнический
университет Петра Великого», г. Санкт-Петербург, Россия,
e-mail: elizarova2002@ yandex.ru)

МАКЕТ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОПЫЛЕНИЕМ В ТЕПЛИЧНОМ КОМПЛЕКСЕ

Аннотация. Предложен подход к созданию распределенной системы управления опылением для тепличного комплекса с использованием беспроводного канала связи. Описаны программные и аппаратные решения для увеличения энергоэффективности оконечных устройств. Приведено описание функционирования автоматизированного рабочего места оператора.

Ключевые слова: тепличный комплекс, бомбидарий, распределенная система управления, SCADA-система.

M. I. Elizarova
(Institute of Computer Science and Cybersecurity
St. Petersburg Polytechnic University Peter the Great,
St. Petersburg, Russia)

LAYOUT OF A DISTRIBUTED CONTROL SYSTEM FOR POLLINATION IN A GREENHOUSE COMPLEX

Abstract. An approach to the creation of a distributed pollination management system for a greenhouse complex using a wireless communication channel is proposed. Software and hardware solutions for increasing the energy efficiency of terminal devices are described. The description of the functioning of the operator's automated workplace is given.

Keywords: Greenhouse complex, bombedarium, distributed control system, SCADA system.

При выращивании пасленовых, например, томатов или баклажанов, а также некоторых ягод (земляники, голубики) в качестве насекомых-опылителей используют шмелей. Это позволяет увеличить урожай с участка и улучшить качество плодов. Однако, внутри тепличного комплекса насекомые подвержены действию таких опасных факторов как полив, внесение удобрений и гербицидов, ночная досветка. Все это может привести к гибели шмелиной семьи, а, следовательно, снижению эффективности опыления и недополученной прибыли для тепличного комплекса. Чтобы избежать этого, можно использовать

бомбидарии с автоматизированным летком, т.е. оснащенным поворотной заслонкой, закрывающей выходное отверстие.

Для построения распределенной системы управления комплексом бомбдариев предлагается использовать модульный принцип [1], согласно которому она состоит из автоматизированного рабочего места оператора (далее АРМ), модуля контроллера узла сети и модулей оконечных устройств (рис. 1). Учитывая большую площадь помещений, а также периодическое перемещение бомбидариев внутри тепличного комплекса, рационально использовать беспроводной канал для связи с контроллерами оконечных устройств [2].

Рис. 1. Структура системы

Для проектирования макета и отладки алгоритма управления была выбрана программно-аппаратная платформа Arduino. При выборе аппаратных компонентов для оконечного устройства главным критерием было низкое энергопотребление. По результатам тестов выбраны плата Arduino Pro mini и сервопривод SG90. Помимо аппаратных средств увеличения энергоэффективности использовались и программные. Например, управление оконечным устройством по следующему алгоритму: выход контроллера из режима сна; подача питания на приемник, если сигнал передатчика есть, то происходит считывание поступивших данных; если требуется изменение положения заслонки, то происходит подача питания на обмотку реле и выдается команда управления на поворот вала сервопривода; отключение питания приемника и сервопривода, вход в режим сна. Использованием совокупности программных и аппаратных средств удалось добиться

следующих результатов: потребление в режиме сна контроллера 0.06 мА, во время приема сообщения – 0.12 мА, а режиме позиционирования сервопривода – 300 мА.

Для максимизации времени автономной работы можно использовать питание от аккумулятора и модуль подзарядки от солнечной батареи, который включает в себя солнечную батарею, повышающий преобразователь напряжения со встроенным стабилизатором, контроллер заряда аккумулятора.

Поскольку устройство узла сети подключено к стационарному источнику питания, снижение энергопотребления для него не является актуальным. Связь с устройством узла сети осуществляется через последовательный порт (USB-UART) с использованием протокола Modbus RTU. АРМ оператора реализован в SCADA-системе MasterSCADA 4D. MasterSCADA 4D поддерживает большое количество коммуникационных протоколов, в том числе Modbus RTU/TCP, OPC DA, OPC UA. В проекте используется передача данных по Modbus RTU, опробована возможность передачи посредством OPC DA. Внешний вид АРМ оператора показан на рис. 2.

Рис. 2. Вид АРМ оператора

Для удобства оператора предусмотрена возможность как ручного управления каждым летком, так и одновременного открытия/закрытия всех, а также автоматическое управление согласно расписанию.

При необходимости функционал АРМа оператора может быть расширен. Для этого предлагается построить его по модульному принципу (рис. 3). Модуль прогнозирования оставшейся времени автоном-

ной работы включает в себя математические модели, связывающие напряжение на аккумуляторе с оставшимся зарядом. Модуль контроля работоспособности приводов заслонок обеспечивает контроль поворота заслонки, формирует оповещение в случае, если текущее положение заслонки по истечении контрольного времени не соответствует заданному. Модуль формирования рекомендаций по проведению регламентных работ формирует напоминание о скорой замене батарей. Модуль формирования сигналов оповещения персонала позволяет отправить уведомление о внештатных ситуациях, о проведении регламентных работ и т.д. посредством SMS или социальных сетей. Модуль обеспечения удаленного web-доступа позволяет получить доступ к системе посредством браузера, при этом установка MasterSCADA на устройство не требуется [3].

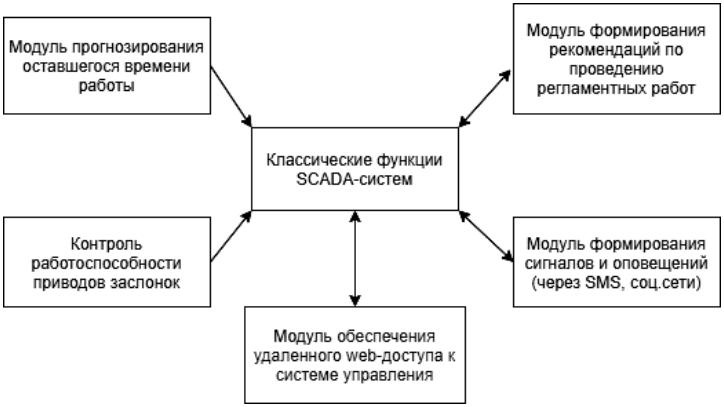


Рис. 3. Структура АРМ оператора

Список использованных источников

1. Касьянов, Я. В. Групповое использование дронов для наблюдения и разведки / Я. В. Касьянов, Е. С. Гебель // Молодой инженер – основа научно-технического прогресса : сб. науч. тр. Междунар. науч.-техн. конф., Курск, 09–10 октября 2015 года. – Курск : ИП Пучков Игорь Иванович, 2015. – С. 169 – 173.

2. Гуровский, А. Модуль расширения системы управления мобильного робота IE-ROBO-CIRCLE / А. Гуровский, Е. С. Гебель, Е. В. Солонин // Автоматизация, мехатроника, информационные технологии. Automation, Mechatronics, Information Technologies : материалы IV Междунар. науч.-техн. интернет-конф. молодых ученых, Омск, 14–15 мая 2014 года. – Омск : ФГБОУ ВО «Омский государственный технический университет», 2014. – С. 214 – 217.

3. Елизарова, М. И. Интеллектуальная распределенная система управления бомбидариями в тепличнвых комплексах / М. И. Елизарова, Е. С. Гебель // Неделя науки ИКНК : материалы докл. науч.-практ. конф., 15 апреля – 17 мая 2024 г. – СПб. : ПОЛИТЕХ-ПРЕСС, 2024. – С. 260 – 262.

References

1. Kasyanov, Ya. V. Group use of drones for surveillance and reconnaissance / Ya. V. Kasyanov, E. S. Gebel // Young engineer – the basis of scientific and technological progress : Collection of scientific papers of the International Scientific and Technical Conference, Kursk, October 09–10, 2015. – Kursk : IP Puchkov Igor Ivanovich, 2015. – P. 169 – 173.

2. Gurovsky, A. Module for expanding the control system of the IE-ROBO-CIRCLE mobile robot / A. Gurovsky, E. S. Gebel, E. V. Solonin // Automation, mechatronics, information technologies Automation, Mechatronics, Information Technologies : materials of the IV International Scientific and Technical Internet Conference of Young Scientists, Omsk, May 14–15, 2014. – Omsk : Omsk State Technical University, 2014. – P. 214 – 217.

3. Elizarova, M. I. Intelligent distributed bomb control system in greenhouse complexes / M. I. Elizarova, E. S. Gebel // ICNK Science Week : materials of reports of the scientific and practical conference, April 15 – May 17, 2024. – St. Petersburg : POLYTECHNIC PRESS, 2024. – P. 260 – 262.

УДК 004

Р. О. Китаев, А. Г. Морозов, Ю. В. Минин
(Кафедра «Информационные системы и защита информации»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: sky.sand18@gmail.com)

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ЗАПАСАМИ ЗАПАСНЫХ ЧАСТЕЙ ДЛЯ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ТЕХНИКИ

Аннотация. Представлен подход к определению объема запасных частей у организации для сельскохозяйственной техники, для чего разработана соответствующая математическая модель.

Ключевые слова: управление запасами, модель, сельскохозяйственная техника, информационная система.

R. O. Kitaev, A. G. Morozov, Yu. V. Minin
(Department of Information Systems and Information Security,
TSTU, Tambov, Russia)

MATHEMATICAL SUPPORT FOR THE INVENTORY MANAGEMENT SYSTEM OF SPARE PARTS FOR AGRICULTURAL MACHINERY

Abstract. The paper presents an approach to determining the volume of spare parts an organization has for agricultural machinery, for which a corresponding mathematical model has been developed.

Keywords: inventory management, model, agricultural machinery, information system.

Автоматизация управления запасами, а также поиск оптимальных управленческих решений в данной области, является актуальной и важной проблематикой [1 – 3]. В рамках данной статьи рассмотрим один из элементов математического обеспечения информационной системы управления запасами запасных частей для сельскохозяйственной техники, а именно, модель для расчета запланированных заказов запасных частей в условиях, когда происходит размещение заказов на пополнение в головной офис компании.

Предположим, что имеется $i \in \{1, ..., i\}$ видов запасных частей и $j \in \{1, ..., j\}$ пунктов продажи. Таким образом, каждая единица складского учета соответствует кортежу $(i, j) \in \{1, ..., i\} \times \{1, ..., j\}$. Обозначим S как конкретное подмножество всех единиц складского учета, т.е. $S \subseteq \{1, ..., i\} \times \{1, ..., j\}$.

Спрос на продукт i в пункте j в момент времени $t \in T = \{1, ..., t\}$ обозначается как $X_{ij}(t)$. Этот спрос может быть удовлетворен за счет уровня запасов $B_{ij}(t)$ и поставок $D_{ij}(t)$.

Таким образом, динамика уровня запасов $B_{ij}(t)$ со временем описывается следующим образом: где $B_{ij}(1) = b_{ij}^0$ – некоторый фиксированный начальный запас

$$B_{ij}(t+1) = \max\left\{0,\ B_{ij}(t) + D_{ij}(t) - X_{ij}(t)\right\},\ t \in T. \qquad (1)$$

Предположим, что пункт j может размещать заказы на продукт i в заранее определенные дни $O_{ij} \subset T$. Количество заказа, размещенного в момент $t \in T$, обозначается как $Q_{ij}(t)$ и оно равно нулю, если момент t не является одним из дат заказа. Размеры упаковок $c_{ij} \in N$ могут варьироваться, и, следовательно, количество заказа удовлетворяет условию $Q_{ij}(t) \in \{k \cdot c_{ij} \mid k \in N\}$. Время выполнения заказа на продукт i в пункте j составляет $l_{ij}(t) \in N$ при заказе в день $t \in O_{ij}$.

Поставки продукта i в пункт j в момент $t \in T$ задаются следующим образом:

$$D_{ij}(t) = \sum_{\substack{t' \in O_{ij} \\ t' + l_{ij}(t') = t}} Q_{ij}(t'). \qquad (2)$$

Решение о количестве заказа $Q_{ij}(t)$ зависит от уровня запасов на момент времени t и от поставок и прогнозируемого спроса за период пересмотра и выполнения заказа (ПиВЗ), который определяется как

$$\tau_{ij}(t) = \left\{t, ..., t' + l_{ij}(t') - 1\right\},\ \text{где}\ t' = \min\left\{t'' \in O_{ij} \mid t'' > t\right\}. \qquad (3)$$

Учитывая минимальное требование к запасам $m_{ij} \geq 0$, прогнозируемый спрос определяется следующим образом

$$Q_{ij}(t) = \min_{k \in N}\left\{ kc_{ij} \,\middle|\, B_{ij}(t) + \sum_{\hat{\imath} \in \tau_{ij(t)}} D_{ij}(\hat{t}) - \sum_{\hat{\imath} \in \tau_{ij}(t)} \hat{X}_{ij}(\hat{t}) + kc_{ij} \geq m_{ij} \right\}, \qquad (4)$$

где $\tau_{ij}(t)$ задается выражением (3), а $\hat{X}_{ij}(t)$ представляет собой точечный прогноз спроса. Это означает, что заказ размещается только в том случае, если прогнозируемый спрос достаточно велик, чтобы снизить уровень запасов ниже минимального требования к запасам в течение периода ПиВЗ. При применении уравнения (1) ненаблюдаемые требования $X_{ij}(t)$ оцениваются с помощью точечных прогнозов $\hat{X}_{ij}(t)$, кото-

рые представляют собой средние оценки, основанные на исторических данных о продажах. Исходя из прогнозируемого уровня запасов на первую дату заказа, количество заказа определяется из уравнения (4). Затем уровни запасов итеративно рассчитываются до второй даты заказа, и расчет заказа повторяется. Эта процедура продолжается до тех пор, пока все даты заказа в $O_{ij} \subset T$ не будут обработаны.

Список использованных источников

1. Управление запасами в цепях поставок : учебник и практикум для вузов / В. С. Лукинский и др. – М. : Юрайт, 2024. – 625 с.
2. Григорьев, М. Н. Логистика : учебник / М. Н. Григорьев. – М. : Юрайт, 2019. – 836 с.
3. Дроздов, П. А. Логистика запасов / П. А. Дроздов. – М. : Литрес, 2018. – 270 с.

References

1. Inventory management in supply chains: textbook and workshop for universities / V. S. Lukinsky, et al. – M. : Yurayt Publishing House, 2024. – 625 p.
2. Grigoriev, M. N. Logistics : textbook / M. N. Grigoriev. – M. : Yurayt, 2019. – 836 p.
3. Drozdov, P. A. Inventory logistics / P. A. Drozdov. – M. : Litres, 2018. – 270 p.

УДК 681.5

И. Г. Благовещенский, М. М. Клягин, В. А. Холопов
(Кафедра «Промышленная информатика»,
РТУ МИРЭА, г. Москва, Россия,
e-mail: mmklyagin@gmail.com)

ПЕРЕХОД ОТ СЕРИЙНОГО ПРОИЗВОДСТВА К МНОГОНОМЕНКЛАТУРНОМУ МЕЛКОСЕРИЙНОМУ ПРОИЗВОДСТВУ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрены ключевые особенности перехода от серийного производства к многономенклатурному мелкосерийному производству. Определены основные требования к мелкосерийному многономенклатурному производству. Приведена стратегия переналадки мелкосерийного многономенклатурного производства с использованием автоматизированного рабочего места.

Ключевые слова: многономенклатурное мелкосерийное производство, автоматизированное рабочее место, интерактивное сопровождение сборочных операций, машинное зрение.

I. G. Blagoveshchenskiy, M. M. Klyagin, V. A. Kholopov
(Department of Industrial Informatics,
RTU MIREA, Moscow, Russia

TRANSITION FROM MASS PRODUCTION TO MULTI-NOMENCLATURE SMALL-BATCH PRODUCTION IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The key features of the transition from mass production to multi-nomenclature small-batch production are considered. The basic requirements for small-batch multi- nomenclature production are defined. The strategy of readjustment of small-batch multi-nomenclature production using an automated workplace is presented.

Keywords: multi-nomenclature small-batch production, automated workplace, interactive support of assembly operations, machine vision.

Одним из ключевых направлений для повышения гибкости производственных систем в агропромышленном комплексе является внедрение автоматизированных сборочных рабочих мест с интерактивным сопровождением операций. Такие технологии позволяют оперативно переналаживать производственные процессы под выпуск новых видов продукции, ускоряя подготовку персонала, минимизируя ошибки при сборке и упаковке готовых продуктов.

Серийное производство ориентировано на выпуск большого количества однотипных изделий. Производственные линии настраи-

ваются на выполнение одних и тех же операций в течение длительного времени, что позволяет сократить затраты на переналадку оборудования и оптимизировать технологические процессы.

Переход к многономенклатурному мелкосерийному производству требует пересмотра и адаптации традиционных производственных процессов. В отличие от массового серийного производства, многономенклатурное мелкосерийное производство должно обеспечивать выпуск продукции небольшими партиями при постоянном изменении ассортимента. Для этого необходимы гибкие системы управления, адаптивные процессы и особый подход к организации труда и логистики.

Для успешного многономенклатурного производства необходима организация труда, способная поддерживать частую смену номенклатуры и адаптироваться к изменяющимся условиям производства. Производственные процессы требует регулярного повышения квалификации сотрудников. Необходимы программы обучения по внедрению новых технологий, оборудования и методов управления производственными процессами.

Для обеспечения стабильного качества продукции при частых изменениях в производстве необходимы эффективные системы контроля качества и стандартизации процессов. Использование систем машинного зрения, автоматизированного контроля и измерительного оборудования позволяет выявлять отклонения и дефекты на ранних этапах производства.

Переход к многономенклатурному мелкосерийному производству требует внедрения современных технологий и методов управления производством. Одним из ключевых направлений для успешной трансформации производственной системы является использование автоматизированных сборочных рабочих мест с интерактивным сопровождением операций. Это позволяет достичь высокой гибкости, оптимизировать сборочные процессы и повысить качество выпускаемой продукции.

Внедрение автоматизированных сборочных рабочих мест с интерактивным сопровождением операций решает проблему быстрой переналадки производственных процессов, позволяя гибко и эффективно организовать работу персонала. Современные автоматизированные рабочие места позволяют выполнять переналадку оборудования без участия оператора. В системе задаются параметры нового изделия, и оборудование автоматически перенастраивается для выполнения новых операций. Это значительно сокращает время простоя и повышает производительность в условиях частой смены продукции.

Автоматизированные сборочные рабочие места оснащены интерактивными системами обучения, которые позволяют быстро вводить новых сотрудников в производственный процесс и переобучать их при смене номенклатуры. Интегрированные в рабочее место системы интерактивного обучения показывают рабочим, как выполнять операции в режиме реального времени. Текстовые инструкции, анимации и графические схемы позволяют сотрудникам быстро освоить сборку новой продукции. Такой подход сокращает время на подготовку новых операторов и снижает зависимость от их опыта и квалификации. Когнитивные искажения сотрудников могут приводить к ошибкам в процессе сборки. Использование интерактивного сопровождения и систем контроля позволяет минимизировать влияние человеческого фактора. Интегрированная система машинного зрения осуществляет контроль каждого этапа сборки, сравнивая с эталонными образцами. Если система обнаруживает отклонение от нормы, она мгновенно сигнализирует оператору и фиксирует ошибку в системе. Таким образом, ошибки устраняются в режиме реального времени, а качество продукции поддерживается на высоком уровне.

Сбор и анализ данных с автоматизированных рабочих мест позволяют оптимизировать производственные процессы и выявлять узкие места в сборочном процессе. Автоматизированные рабочие места передают данные о производительности, времени выполнения операций, количестве обнаруженных ошибок и состоянии оборудования в систему управления производством.

Переход от серийного производства к многономенклатурному мелкосерийному производству является актуальной и сложной задачей для современных предприятий. Рассмотренные в данной статье методы и технологии, такие как автоматизированные сборочные рабочие места с интерактивным сопровождением, системы цифровизации и автоматизации, обеспечивают успешное выполнение этих задач.

Список использованных источников

1. Благовещенский, В. Г. Обучение работников ручной сборке изделий с использованием интерактивного сопровождения и машинного зрения / В. Г. Благовещенский, М. М. Клягин, В. А. Серебрянкин // Автоматизация. Современные технологии. – 2024. – Т. 78, № 4. – С. 188 – 192.

References

1. Blagoveshchenskiy, V. G. Training of workers in manual assembly of products using interactive support and machine vision / V. G. Blagoveshchenskiy, M. M. Klyagin, V. A. Serebryankin // Avtomatizaciya. Sovremennye tekhnologii. – 2024. – V. 78, No. 4. – P. 188 – 192.

УДК 621.311.1

С. В. Кочергин[1], С. В. Артемова[1], В. Ф. Калинин[2]
(1Кафедра КБ-1 «Защита информации»,
РТУ МИРЭА, Москва, Россия,
e-mail: kochergin_s@mirea.ru;
[2]Кафедра «Электроэнергетика», ФГБОУ ВО «ТГТУ»,
г. Тамбов, Россия)

МОДЕЛИРОВАНИЕ КИБЕРАТАК НА СИСТЕМУ ЭЛЕКТРОСНАБЖЕНИЯ АПК: АНАЛИЗ УЯЗВИМОСТЕЙ И ОЦЕНКА РИСКОВ

Аннотация. Представлена модель классификации кибератак по типу угрозы, уровню риска и последствиям. Использован комплексный подход с матрицами угроз, деревьями атак и моделированием перехода системы электроснабжения в неустойчивое состояние при кибератаке.

Ключевые слова: кибератака, комплексный подход, матрицы угроз, деревья атак, моделирование, система электроснабжения, неустойчивое состояние.

S. V. Kochergin[1], S. V. Artemova[1], V. F. Kalinin[2]
([1]Department of KB-1 “Information Security”,
RTU MIREA, Moscow, Russia;
[2]Department of “Electric Power Engineering”,
TSTU, Tambov, Russia)

SIMULATION OF CYBER ATTACKS ON THE AGRICULTURAL POWER SUPPLY SYSTEM: VULNERABILITY ANALYSIS AND RISK ASSESSMENT

Abstract. The article presents a model for classifying cyber attacks by threat type, risk level and consequences. An integrated approach is used with threat matrices, attack trees and modeling of the transition of the power supply system to an unstable state during a cyber attack.

Keywords: cyberattack, integrated approach, threat matrices, attack trees, modeling, power supply system, unstable state.

Современные агропромышленные комплексы все активнее интегрируются с компьютерными сетями, что делает их уязвимыми от кибератак [1]. Приведем общую концепцию использования комплексного подхода, включающего использование матриц угроз и деревьев атак, а также моделирование перехода системы электроснабжения АПК в неустойчивое состояние при кибератаке.

Система электроснабжения может быть описана как совокупность множества элементов оборудования: $E = \{e_1, e_2, \ldots, e_n\}$, каждый из которых может находиться в одном из множества возможных состояний $S_i = \{s_{i1}, s_{i2}, \ldots, s_{im}\}$. Состояния оборудования делятся на стабильные $S_{i,\text{ стаб}}$ и неустойчивые $S_{i,\text{ неуст}}$.

Общее состояние системы в определенный момент времени t является комбинацией состояний всех ее элементов:

$$S(t) = (s_1(t), s_2(t), \ldots, s_n(t)), \quad (1)$$

где $s_i(t) \in S_i$. В стабильном состоянии система находится в точке $s(0) \in S_{\text{стаб}}$, что соответствует нормальной работе оборудования и обеспечению стабильного энергоснабжения. Однако под воздействием угроз система может перейти в неустойчивое состояние, что может привести к аварии.

Рассмотрим использование матрицы угроз. Для каждого элемента оборудования e_i, находящегося в стабильном состоянии $s_i(t) \in S_{i,\text{ стаб}}$, можно определить вероятность как кибератак (внешняя угроза), так и отказов оборудования (внутренняя угроза). Вероятность возникновения инцидентов зависит от характеристик элементов. Например, элемент e_k, который связан с сетевыми интерфейсами, может иметь повышенную уязвимость к кибератакам, что делает его критическим с точки зрения безопасности системы.

Для оценки степени влияния угроз используется модель каскадного изменения состояний. Если состояние элемента e_k переходит в неустойчивое состояние, это может вызвать каскадное изменение состояний других элементов системы. Вероятность такого каскадного перехода можно выразить как:

$$P(e)_k = \sum_{i=1}^{n} P(s_i(t_i) = f_i(s_{i-1}(t_{i-1}))), \quad (2)$$

здесь $P(e_k)$ – вероятность того, что нарушение состояния элемента e_k вызовет изменения в других элементах системы, вплоть до полного перехода системы в неустойчивое состояние.

Проведем анализ с использованием деревьев атак. На каждом шаге дерева атак оценивается вероятность дальнейшего распространения угрозы.

1. **Входная точка атаки**: На момент времени t_1 элемент e_k подвергается атаке (например, вирусной). Это приводит к его переходу в неустойчивое состояние:

$$s_k(t_1) \in S_{k,\text{неус}}. \quad (3)$$

2. **Промежуточные шаги**: Переход элемента e_k в неустойчивое состояние может повлечь за собой каскадное изменение состояний других элементов системы. Это изменение описывается функцией перехода:

$$s_i(t_{i+1}) = f_i(s_{i-1}(t_i)), \quad (4)$$

где t_i – момент времени изменения состояния элемента e_i.

3. **Целевая точка атаки**: Целью атакующих является перевод всей системы в неустойчивое состояние:

$$s(t_{kp}) \in S_{\text{неус}}. \quad (5)$$

Это состояние может привести к аварии или полному отказу системы.

Каждое звено дерева атак оценивается с точки зрения вероятности реализации угрозы и ее потенциальных последствий для системы. Это позволяет классифицировать инциденты по уровню риска и степени серьезности.

Для систематизации угроз и анализа уязвимых зон системы электроснабжения, входящей в состав АСУ ТП, целесообразно использовать комбинацию матриц угроз и деревьев атак:

1. Начальная оценка уязвимостей: На первом этапе, с использованием матриц угроз, проводится оценка вероятности атак и их влияния на каждый элемент системы. Это позволяет определить, какие элементы наиболее уязвимы.

2. Построение дерева атак: На основе матриц угроз строится дерево атак, моделирующее возможные пути распространения угрозы от начальной точки до полной дестабилизации системы.

3. Классификация инцидента: После построения дерева атак инциденты классифицируются по типу угрозы (кибератака или отказ оборудования), степени риска (низкий, средний, высокий) и масштабу последствий (локальные или каскадные изменения).

Описания модели неустойчивого состояния включает такие элементы: инициация угрозы, каскадное изменение, неустойчивое состояние системы.

Представленная модель помогает классифицировать инциденты по типу угрозы, уровню риска и возможным последствиям, что способствует разработке более эффективных методов предотвращения аварийных ситуаций и повышения безопасности систем.

Список использованных источников

1. Хамракулов, А. Г. Современные киберугрозы в АСУ ТП / А. Г. Хамракулов, Е. М. Самойлова // Технологии и техника: пути инновационного развития : сб. науч. ст. Междунар. науч.-техн. конф., Воронеж, 09 июня 2023 года. – Воронеж: Воронежский государственный технический университет, 2023. – С. 527 – 530.

References

1. Khamrakulov, A. G. Modern cyber threats in automated control systems / A. G. Khamrakulov, E. M. Samoilova // Technologies and equipment: ways of innovative development : collection of scientific articles of the International Scientific and Technical Conference, Voronezh, June 09, 2023. – Voronezh : Voronezh State Technical University, 2023. – P. 527 – 530.

УДК 004.021

С. Л. Сахаров, А. С. Кравченко
(Кафедра «Вычислительная техника и информационные системы»,
ФГБОУ ВО «ВГЛТУ», г. Воронеж, Россия,
e-mail: a27380@mail.ru, kr_and@inbox.ru)

ОБНАРУЖЕНИЯ ПРИЗНАКОВ СТЕГАНОГРАФИЧЕСКИХ ВЛОЖЕНИЙ В АУДИОФАЙЛАХ НА ОСНОВЕ АНАЛИЗА РАСПРЕДЕЛЕНИЯ МЛАДШИХ БИТ

Аннотация. Рассмотрен вариант обнаружения стеганографического вложения в условиях отсутствия исходного файла (пустого контейнера) с использованием для сравнения распределения первых (соседних с нулевыми) разрядов байт данных.

Ключевые слова: стеганография, наименьшие значащие биты, бинарная последовательность, параметры распределения.

S. L. Saharov, A. S. Kravchenko
(Department of Computer Technology and Information Systems,
VSUFT, Voronezh, Russia)

DETECTION OF SIGNS OF STEGANOGRAPHIC ATTACHMENTS IN AUDIO FILES BASED ON THE ANALYSIS OF THE DISTRIBUTION OF THE LOWEST BITS

Abstract. A variant of detecting a steganographic attachment in the absence of a source file (empty container) using the distribution of the first (adjacent to zero) bits of data bytes for comparison is considered.

Keywords: steganography, least significant bits, binary sequence, distribution parameters.

Повсеместное внедрение компьютерной техники не только упрощает обработку постоянно увеличивающихся объемов информации, но и возлагает на пользователей широкий круг обязанностей по защите обрабатываемых данных. Среди многочисленных методов, используемых злоумышленниками, следует обратить внимание на возможности активно развивающейся цифровой стеганографии. Доставка вредоносных кодов или утечка данных с компьютера жертвы могут быть реализованы с помощью основного стенографического принципа – маскировка нелегального контента путем встраивания в структуру контейнеров.

Простой и эффективный способ реализации скрытых вложений – метод наименьших значащих бит, который заключается в замене

младших двоичных разрядов данных на биты скрываемого вложения. Для вложений используются хранящиеся на дисках компьютера многочисленные и не вызывающие подозрений изображения, аудио- или видеозаписи. Для файлов с записью оцифрованных данных без сжатия алгоритм вложения прост и легко реализуем программно. Примером является бесплатная программа FoxSecret с русским интерфейсом и хорошим справочным материалом как по алгоритму работы, так и по основным принципам стеганографии.

Для оценки возможности выявления скрытого вложения в качестве пустого контейнера был использован файл формата «.wav» (1,5 Мбайт), содержащий запись прямой речи (чтение текста). В этот файл методом наименьших значащих бит был размещен текстовый файл размером 100 Кбайт. В соответствии с алгоритмом FoxSecret, внедряемый текстовый файл предварительно архивировался и шифровался с помощью алгоритма Blowfish, где в качестве ключа использовались параметры файла контейнера. Сравнение пустого и заполненного контейнера показало, что изменениям подвергались около 347 000 первых байт.

Архивация и шифрование позволяют предположить, что последовательность бит скрываемого вложения будет иметь статистические характеристики свойственные случайной бинарной последовательности и эти характеристики будут отличаться от параметров распределения младших бит пустого контейнера.

Для проверки этого предположения использован набор тестов NIST, предназначенный для тестирования на случайность бинарных последовательностей [1]. Показанные далее результаты по выявлению признаков скрытого вложения получены на основе частотного побитового теста, который оценивает количество бинарных символов (в случайной последовательности соотношение должно быть примерно одинаковым).

Тест проводится в три этапа. Сначала двоичные нули заменяются на –1. На втором этапе определяется взвешенная сумма по формуле:

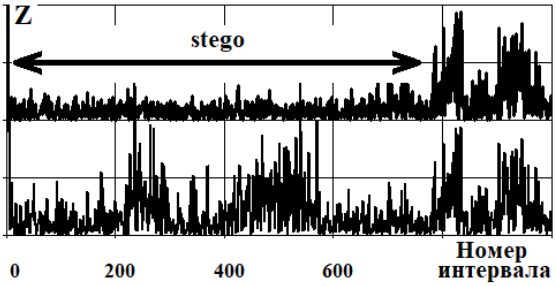
$$Z = \frac{\left|\sum_n x_n\right|}{\sqrt{n}},$$

где n – количество элементов исследуемой последовательности, x_n – элемент бинарной последовательности, в которой 0 заменены на –1.

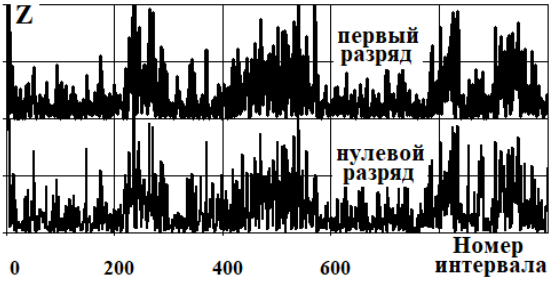
На третьем этапе полученный результат подставляется в формулу дополнительной функции ошибок для формирования численной оценки соответствия последовательности параметрам случайного распределения.

Результаты исследования последовательности младших бит пустого и заполненного контейнеров показаны на рис. 1, *а*, где приведены значения взвешенных сумм для интервалов по 500 бит (для удобства сравнения графики смещены по вертикальной оси).

Очевидно, что характер распределения полученных результатов позволяет не только подтвердить изменения, внесенные скрытым вложением в младшие разряды контейнера, но и определить примерный размер вложения. Расчеты по формуле дополнительной функции ошибок существенных результатов не дали, поэтому на графиках не приведены.



а)



б)

Рис. 1. Значения взвешенных сумм для интервалов

Следует учитывать, что файл для сравнения может отсутствовать. Тогда для поиска вложений необходимо использовать параметры единственного исследуемого файла, которые позволят принять решение: является ли этот файл заполненным контейнером. Для этого может быть использована связь в распределениях двух младших двоичных разрядов [2]. Оценка взвешенных сумм на интервалах по 500 бит нулевого и первого разрядов пустого контейнера показана

на рис. 1, *б*. Распределения достаточно точно повторяют друг друга, поэтому изменение статистики распределения, при внесении изменений в младшие биты, можно оценивать на основе сравнения с параметрами первого разряда.

Таким образом, простой тест на соотношение элементов в бинарной последовательности может быть использован для определения параметров файла, характерных для контейнеров, заполненных стеганографическими вложениями.

Список использованных источников

1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22 Revision 1a. / National Institute of Standards and Technology (NIST). April 2010.
2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002.

References

1. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22 Revision 1a. / National Institute of Standards and Technology (NIST). April 2010.
2. Gribunin, V. G. Digital steganography / V. G. Gribunin, I. N. Okov, I. V. Turincev – M. : SOLON-Press, 2002.

УДК 681.5

Д. С. Лавринов
(Кафедра «Информационные процессы и управление»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: texlavrds@gmail.com)

МЕТОДИКИ АВТОМАТИЗАЦИИ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ И РЕМОНТА (ТОиР) НА ПРОИЗВОДСТВЕННЫХ ПРЕДПРИЯТИЯХ АГРОПРОМЫШЛЕННОГО СЕКТОРА

Аннотация. Описаны преимущества автоматизации систем технического обслуживания и ремонта. Рассмотрены основные методики автоматизации управления ТОиР. Приведены примеры успешной автоматизации ТОиР в агропромышленном секторе.

Ключевые слова: техническое обслуживание и ремонт, ТОиР, АПК, CMMS-системы, предиктивная аналитика, Web SCADA, IoT.

D. S. Lavrinov
(Department of Information Processes and Control,
TSTU, Tambov, Russia)

METHODS OF AUTOMATION OF TECHNICAL MAINTENANCE AND REPAIR (MRO) AT PRODUCTION ENTERPRISES IN THE AGRO-INDUSTRIAL SECTOR

Abstract. Describes the advantages of automating maintenance and repair systems. The main methods of automation of MRO management are considered. Examples of successful automation of MRO in the agro-industrial sector are provided.

Keywords: maintenance and repair, MRO, agro-industrial complex, CMMS systems. predictive analytics, Web SCADA, IoT.

Автоматизация технического обслуживания и ремонта (ТОиР) в агропромышленном комплексе (АПК) направлена на повышение производительности и снижение затрат. Это позволяет избежать простоев, минимизировать аварийные ситуации и поддерживать оборудование в рабочем состоянии. Автоматизация процессов ТОиР внедряется с помощью специализированных решений, которые включают в себя системы мониторинга, планирования и анализа работы оборудования.

Преимущества автоматизации ТОиР. Предиктивная аналитика – внедрение систем, основанных на искусственном интеллекте и анализе

данных с датчиков, помогает предсказать возможные поломки оборудования, уведомлять обслуживающий персонал заранее и предотвращать аварии.

Снижение затрат – автоматизация позволяет продлить срок службы оборудования, сократить внеплановые ремонты и оптимизировать использование ресурсов.

Повышение безопасности – датчики для контроля критических параметров (температура, вибрация, давление) позволяют оперативно реагировать на аномалии, снижая вероятность аварийных ситуаций.

Эффективное планирование – автоматизация помогает точно планировать графики обслуживания, избегая простоев в периоды интенсивной работы оборудования.

Основные методики автоматизации. (Computerized Maintenance Management Systems) – это программные решения CMMS-системы для управления ТОиР, позволяющие вести учет, планировать обслуживание и отслеживать состояние оборудования. Они также обеспечивают анализ эффективности процессов ТОиР. [1]

Мониторинг состояния оборудования – используется для сбора данных о работе техники в реальном времени с помощью датчиков. Эти данные анализируются с применением машинного обучения, что позволяет предсказывать неисправности.

Интернет вещей (IoT) – позволяет соединить оборудование с датчиками в единую сеть, передавая данные в систему управления ТОиР в реальном времени, что улучшает точность прогнозирования и минимизирует риски поломок. [2]

Web-ориентированные SCADA-системы – благодаря развитию веб-ориентированных SCADA-систем с клиент-серверной архитектурой, обеспечилась возможность организации на их базе систем автоматизации ТОиР, обеспечивающих бесшовный контакт с оборудованием, простоту реализации и доступность из удаленных точек контроля. Серверная часть этих систем строится на современных веб-платформах, а клиентская часть может использовать любые браузеры. Благодаря HTML5, встроенному в современные браузеры, человеко-машинные интерфейсы могут отображаться не только на стационарных компьютерах, но и на портативных устройствах, что в свою очередь обеспечивает кроссплатформенность исполнительных систем.

Виртуальные и дополненные реальности (VR и AR) в ТОиР – инновационные технологии VR и AR находят применение и в области технического обслуживания. С помощью дополненной реальности технические специалисты могут получать подсказки и инструкции прямо в поле зрения во время работы с оборудованием. Виртуальная

реальность используется для обучения персонала, что повышает их квалификацию и позволяет избежать ошибок при проведении ремонта.

Примеры успешной автоматизации ТОиР в агропромышленном секторе. Некоторые агропромышленные предприятия уже внедрили автоматизированные системы для управления техобслуживанием и достигли значительных результатов. Примером может служить компания «Агропромхолдинг», которая внедрила CMMS-систему для управления своим парком сельскохозяйственной техники. Это позволило компании сократить затраты на ремонт на 15% и увеличить время безотказной работы техники на 20%.

Заключение. Автоматизация технического обслуживания и ремонта на предприятиях агропромышленного сектора открывает новые возможности для повышения эффективности производства, сокращения затрат и улучшения качества продукции. Внедрение современных технологий и методик, таких как предиктивная аналитика, IoT, Web SCADA, VR и AR, позволяет не только минимизировать риски поломок, но и строить более безопасное и устойчивое производство. В будущем такие технологии станут неотъемлемой частью каждого агропромышленного предприятия, стремящегося к успеху в условиях быстро меняющегося рынка.

Список использованных источников

1. BPM Team. Обзор методов автоматизации ТОиР, с описанием классификаций технического обслуживания и восстановления работоспособности оборудования [Электронный ресурс]. – URL : https://bpmteam.ru (дата обращения: 19.09.2024).

2. ООО «Портал «Управление Производством». Применение дополненной реальности (AR) и промышленного интернета вещей (IIoT) для оптимизации ТОиР [Электронный ресурс]. – URL : https://up-pro.ru (дата обращения: 19.09.2024).

References

1. BPM Team. Overview of methods for automating maintenance and repair processes, with descriptions of classifications of technical maintenance and equipment restoration. Online. – URL : https://bpmteam.ru (Accessed: September 19, 2024).

2. LLC “Production Management Portal”. Application of augmented reality (AR) and industrial Internet of Things (IIoT) for optimizing maintenance and repair processes. Online. – URL : https://up-pro.ru (Accessed: September 19, 2024).

УДК 681.518

Д. С. Луцков, А. Н. Грибков
(Кафедра «Энергообеспечение предприятий и теплотехника»
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: teplotehnika@mail.tstu.ru)

УСТАНОВКА ГИДРОТЕРМАЛЬНОЙ КАРБОНИЗАЦИИ БИООТХОДОВ КАК ОБЪЕКТ АВТОМАТИЗАЦИИ

Аннотация. Рассмотрены ключевые элементы установки для гидротермальной карбонизации биоотходов с точки зрения автоматизации и построения информационно-управляющей системы.

Ключевые слова: гидротермальная карбонизация, биоотходы, автоматизация, информационно-управляющая система.

D. S. Lutskov, A. N. Gribkov
(Department of Enterprise Energy Supply and Heat Engineering,
TSTU, Tambov, Russia)

INSTALLATION OF HYDROTHERMAL CARBONATION OF BIOWASTE AS AN OBJECT OF AUTOMATION

Abstract. The key elements of the installation for hydrothermal carbonation of biowaste are considered from the point of view of automation and the construction of an information and control system.

Keywords: hydrothermal carbonation, biowaste, automation, information and control system.

Переработка больших объемов биоотходов сельского хозяйства с использованием технологии гидротермальной карбонизации во вторичное сырье с высокой добавленной стоимостью позволяет решить проблему их утилизации, защитить окружающую среду и создать востребованный на рынке продукт [1].

Установка гидротермальной карбонизации биоотходов (ГТКБ) состоит из 9 основных элементов. Графовая модель установки показана на рис. 1.

С точки зрения автоматизации и управления установка ГТКБ представляет собой сложный многомерный объект, имеющий множество взаимосвязанных входных и выходных переменных [2]. Для разработки информационно-управляющей системы процессом ГТКБ, необходимо провести анализ ключевых элементов установки с точки зрения их автоматизации и определить основные контролируемые и регулируемые параметры, влияющие на процесс карбонизации.

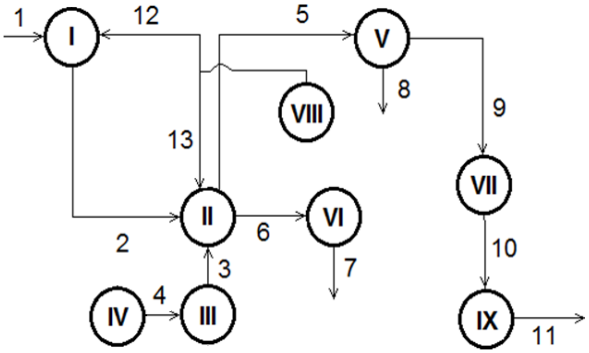


Рис. 1. Графовая модель установки ГТКБ:
I – бункер исходного материала; II – реактор гидротермальной карбонизации;
III – пароперегреватель; IV – электрогенератор; V – циклон;
VI – бункер биоугля; VII – теплообменник; VIII – баллон с азотом;
IX – емкость сбора конденсата; *1, 2, 6, 7* – потоки биоугля;
3, 4, 5, 9 – потоки пара; *8* – поток мелких частиц угля; *10* – поток конденсата;
11 – поток несконденсированных газов; *12, 13* – потоки азота

Ключевыми элементами установки являются: бункер исходного материала I; реактор II; бункер угля VI; циклон V.

Бункер исходного материала представляет собой закрытый контейнер или резервуар, предназначенный для хранения и подачи биоотходов в процесс карбонизации. Бункер обычно изготавливается из прочных материалов, таких как нержавеющая сталь или специальные полимерные покрытия, чтобы обеспечить устойчивость к высоким температурам и давлению, которые могут возникнуть во время процесса.

Размер и конструкция бункера могут различаться в зависимости от масштаба установки и объема биоотходов, которые необходимо обработать. Бункер может быть оснащен механизмом загрузки, например конвейерной лентой или воронкой для удобства подачи материала. В бункере контролируется и регулируется температура и количество исходного материала, который поступает в процесс.

Реактор представляет собой закрытую систему, в которой происходит процесс преобразования биоотходов в углеродный материал при высоких температурах и давлениях. Ключевыми параметрами являются температура, давление и скорость перемешивания исходного материала. Информационно-управляющая система позволит осуществлять сбор, обработку и анализ данных с целью оптимизации работы реактора и улучшения теплотехнологического процесса ГТКБ.

Бункер угля представляет собой контейнер, в котором происходит процесс карбонизации, т.е. превращение биомассы в угольный материал. В бункере контролируется и измеряется несколько параметров, включая температуру, давление и влажность.

Циклон – это устройство, представляющее собой цилиндрическую камеру с коническим дном, в которой происходит разделение частиц воздуха и твердых отходов. Принцип работы циклона основан на центробежной силе. Газовая смесь, содержащая в себе твердые отходы, поступает в циклон со стороны верхней части. Первоначально газовая смесь вращается вокруг вертикальной оси циклона, создавая центробежную силу. Это позволяет отделить твердые отходы от газовой фазы. Благодаря форме конического дна циклона, твердые частицы, подвергнутые действию центробежной силы, перемещаются вниз и собираются на дне камеры. После этого они могут быть отброшены в специальный сборный резервуар или далее направлены для дополнительной обработки и использования.

В циклоне контролируется разделение и удаление твердых частиц и материалов, которые не сгорели или не растворились в процессе карбонизации. Параметры, которые контролируются и регулируются в циклоне, включают давление и температуру.

Разработка и практическое применение информационно-управляющей системы установкой ГТКБ позволит осуществлять непрерывный мониторинг и управление теплотехнологическим процессом, что обеспечит оптимизацию режимов работы установки и получение конечного продукта требуемого качества.

Список использованных источников

1. Муратова, Н. С. Гидротермальная карбонизация биоотходов в кипящем слое в среде перегретого водяного пара : дис. … канд. техн. наук : 05.17.08 / Н. С. Муратова. – Тамбов, 2021. – 209 с.

2. Грибков, А. Н. Информационно-управляющие системы многомерными технологическими объектами: теория и практика : монография / А. Н. Грибков, Д. Ю. Муромцев. – Тамбов : Изд-во ФГБОУ ВО «ТГТУ», 2016. – 164 с.

References

1. Muratova, N. S. Gidrotermal`naya karbonizaciya biootxodov v kipyashhem sloe v srede peregretogo vodyanogo para : dis. … kand. texn. nauk: 05.17.08 / N. S. Muratova. – Tambov, 2021. – 209 s.

2. Gribkov, A. N. Informacionno-upravlyayushhie sistemy` mnogomerny`mi texnologicheskimi ob``ektami: teoriya i praktika: monografiya / A. N. Gribkov, D. Yu. Muromcev. – Tambov : Izd-vo FGBOU VO “TGTU”, 2016. – 164 s.

УДК 004

А. С. Мещеряков, В. К. Зольников, А. В. Шпинев
(ВГЛТУ им. Г. Ф. Морозова, г. Воронеж, Россия,
e-mail: asm13052004@mail.ru, wkz@rambler.ru, andr0ne0@yandex.ru)

МЕТОДЫ ИЗМЕРЕНИЯ ПОГЛОЩЕННОЙ ДОЗЫ ИОНИЗИРУЮЩЕГО ИЗЛУЧЕНИЯ ДЛЯ КОНТРОЛЯ РАДИАЦИОННОЙ ОБСТАНОВКИ СЕЛЬСКОХОЗЯЙСТВЕННЫХ ЗЕМЕЛЬ

Аннотация. Рассмотрено краткое описание методов и средств измерения поглощенной дозы ионизирующего излучения. Воздействие радиации зависит от мощности излучения и продолжительности воздействия, которые характеризуются поглощенной дозой. Для измерения дозы излучения используется дозиметр, который основан на различных методах измерения.

Ключевые слова: детектор, дозиметр, радиация, ионизирующие излучения, метод измерения.

A. S. Meshcheriakov, V. K. Zolnikov, A. V. Spinev
(VSUFT named after G. F. Morozov, Voronezh, Russia)

METHODS FOR MEASURING THE ABSORBED DOSE OF IONIZING RADIATION FOR MONITORING THE RADIATION SITUATION OF AGRICULTURAL LANDS

Abstract. This article provides a brief description of the methods and means of measuring the absorbed dose of ionizing radiation. The effect of radiation depends on the radiation power and duration of exposure, which are characterized by the absorbed dose. A dosimeter is used to measure the radiation dose, which is based on various measurement methods.

Keywords: detector, dosimeter, radiation, ionizing radiation, measurement method.

Ионизирующее излучение – неотъемлемая часть нашего мира. Оно присутствует в окружающей среде, в медицине и промышленности. В малых дозах оно может быть полезным, например, при лечении онкологических заболеваний. В больших дозах оно представляет серьезную опасность для здоровья человека и окружающей среды, и для этого проводятся исследования и используются различные средства защиты [1]. Поэтому измерение поглощенной дозы ионизирующего излучения является важным фактором для обеспечения безопасности человека.

Основные методы регистрации ионизирующего излучения. Фотографический метод является первым методом, который позволил А. Беккерелю открыть явление радиоактивности. Основывается дан-

ный принцип на воздействии радиоактивного излучения на фоточувствительные материалы.

В состав светочувствительной эмульсии входит бромистое серебро или хлористое серебро. После нанесения эмульсии на регистрирующий материал образуется фотопленка (фотопластинка и фотобумага). При облучении светочувствительного слоя гамма-излучением воздействие оказывают электроны, образующиеся при поглощении излучения в среде. В итоге, химически обработанная пленка имеет прозрачные и почерневшие участки на регистрирующем материале. Если использовать этот эффект в дозиметрии, можно определить связь между степенью почернения регистрирующего материала и экспозиционной дозой.

Ионизационный метод является самым распространенным при регистрации ионизирующего излучения. Данный метод основан на ионизации атомов и молекул. В результате электропроводимость среды увеличивается. Это может быть зафиксировано специализированными электронно-техническими устройствами.

В качестве детектора чаще всего применяются ионизационные камеры. Они состоят из двух электродов, между которыми находится газовая среда. При подключении к источнику питания создается электрическое поле. При отсутствии ионизирующих излучений ток в электрической цепи камеры не протекает, так как отсутствуют свободные электроны.

Сцинтилляционный метод. Принцип действия заключается в следующем. Излучение вступает в реакцию со сцинтиллятором, который производит серию вспышек различной интенсивности. Интенсивность вспышек пропорциональна энергии излучения.

При взаимодействии гамма-излучения с веществом сцинтиллятора в нем образуются электроны, которые, поглощаясь в сцинтилляторе, создают вспышки света. Сцинтилляция – это кратковременная световая вспышка, которая возникает в веществах под действием ионизирующих излучений. Свет через световод направляется на фотокатод фотоэлектронного умножителя. Из материала фотокатода выбиваются фотоэлектроны, которые разгоняются электрическим полем и умножаются за счет выбивания вторичных электронов на динодах. Количество пришедших на анод электронов определяется коэффициентом умножения фотоэлектронного умножителя.

Полупроводниковый метод. Метод основан на деградации электропараметров полупроводниковых устройств, таких как транзисторы. Ионизирующее излучение создает дефекты в кристаллической решетке полупроводника, изменяя его проводимость.

Основные виды деградации электропараметров:

1. Изменение порогового напряжения: Доза излучения приводит к увеличению или уменьшению порогового напряжения, влияя на проводимость транзистора.

2. Увеличение тока утечки: Радиация может создавать новые пути для утечки тока, повышая ток утечки транзистора.

Радиационная стойкость транзисторов является важным фактором при разработке электронных устройств, которые будут работать в условиях воздействия ионизирующего излучения. Для повышения радиационной стойкости выбираются наиболее чувствительные и стабильные полупроводниковые материалы.

Важно отметить, что такой метод измерения поглощенной дозы подходит для определения воздействия излучения на полупроводниковые устройства, но не является универсальным методом для всех типов излучения и материалов.

Приборы используемы для контроля ионизирующего излучения.

Радиометр – прибор, который измеряет число актов радиоактивного распада в единицу времени. При измерении мощности экспозиционной дозы фотонного излучения функции радиометра и дозиметра совпадают.

Дозиметр – устройство для измерения дозы радиоактивного излучения или величин, связанных с дозами (мощность экспозиционной дозы, мощность поглощенной дозы).

Спектрометр – устройство, которое позволяет измерять распределение радиоактивного излучения по энергии, массе и заряду.

Список использованных источников

1. Особенности проектирования микросхем, выполненных по глубокосубмикронным технологиям / А. В. Ачкасов, М. В. Солодилов, Н. Н. Литвинов и др. // Моделирование систем и процессов. – 2022. – Т. 15, № 4. – С. 7 – 17.

2. Полуэктов, А. В. Моделирование ослабления ионизирующего излучения за счет защитного корпуса микросхем / А. В. Полуэктов, Р. Ю. Медведев, А. И. Заревич // Моделирование систем и процессов. – 2024. – Т. 17, № 2. – С. 93 – 100.

References

1. Features of the design of microcircuits made using deep submicron technologies / A. V. Achkasov, M. V. Solodilov, N. N. Litvinov et al. // Modeling of systems and processes. – 2022. – V. 15, No. 4. – P. 7 – 17.

2. Poluektov, A. V. Modeling of attenuation of ionizing radiation due to the protective housing of microcircuits / A. V. Poluektov, R. Yu. Medvedev, A. I. Zarevich // Modeling of systems and processes. – 2024. – V. 17, No. 2. – P. 93 – 100.

УДК 004.056

Д. Р. Мусин, А. В. Душкин
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: musindamirrin@yandex.ru)

ПРИМЕНЕНИЕ СКАНЕРОВ УЯЗВИМОСТЕЙ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА С ЦЕЛЬЮ ПОВЫШЕНИЯ ЕГО ЗАЩИЩЕННОСТИ

Аннотация. Сканеры уязвимостей являются ключевыми инструментами для выявления и оперативного устранения недостатков в системе информационной безопасности. Их использование является необходимым для обеспечения безопасности информационной инфраструктуры крупных производств, в том числе в сфере агропромышленности.

Ключевые слова: информационная безопасность, сканер уязвимостей, MaxPatrol 8, RedCheck, агропромышленный комплекс.

D. R. Musin, A. V. Dushkin
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

APPLICATION OF VULNERABILITY SCANNERS IN THE INFORMATION INFRASTRUCTURE OF THE AGRO-INDUSTRIAL COMPLEX IN ORDER TO INCREASE ITS SECURITY

Abstract. Vulnerability scanners are key tools for identifying and promptly eliminating flaws in the information security system. Their use is necessary to ensure the security of the information infrastructure of large-scale production facilities, including in the agricultural industry.

Keywords: information security, vulnerability scanner, MaxPatrol 8, RedCheck, agro-industrial complex.

В соответствии с отчетами министерства сельского хозяйства уже более 30% агропромышленных предприятий Российской Федерации прошли «цифровую трансформацию». Информационные технологии используются для управления производственными процессами, для хранения данных, для автоматизации трудоемких задач. Подобный подход значительно повышает эффективность агропромышленного комплекса (АПК). Исходя из исследований студентов Уральского государственного университета эффективность агропромышленных производств, прошедших этап цифровизации, значительно выше – в среднем, более чем в 5 раз.

Однако повсеместное внедрение цифровых технологий делает информационную инфраструктуру агропромышленного комплекса более уязвимой к угрозам информационной безопасности. Отказ в обслуживании, нарушение работоспособности автоматизированных систем управления, утечки конфиденциальной информации – все это может привести к нарушению производственных процессов, к серьезным финансовым потерям, а также может представлять собой угрозу безопасности как сотрудников предприятия, так и конечных потребителей (рис. 1).

Рис. 1. Риски, сопряженные с получением неправомерного доступа к подсистемам агропромышленного комплекса

Чтобы уменьшить поверхность проведения кибератак, недостаточно единоразово провести ряд организационных и технических действий. Даже настроенная по Best Practices система, работающая со стандартными средствами защиты не может быть абсолютно безопасной.

В последние годы наблюдается тренд по увеличению количества найденных Zero-day уязвимостей (это четко прослеживается в отчетах MITRE ATT&CK по найденным за последние 25 лет CVE). Таким образом, каждая система, по умолчанию, является потенциально уязвимой. Одна из основных задач специалиста по информационной

безопасности заключается в том, чтобы вовремя узнать о том, что система уязвима, и предпринять действия по устранению данной уязвимости. Главным инструментом для достижения данной цели являются сканеры уязвимостей (Vulnerability scanners).

Сканеры уязвимостей – это программные инструменты, автоматизирующие процесс поиска уязвимостей в информационных системах. После сканирования сетей и конечных устройств сканеры составляют отчеты по проведенной работе, указывая на потенциальные дыры в системе безопасности.

В данный момент в реалиях импортозамещения наиболее целесообразными отечественными решениями для информационной инфраструктуры агропромышленного комплекса в области сканеров безопасности являются MaxPatrol 8 от Positive Technologies и RedCheck Enterprise от Алтекс Софт. Функционал, предоставляемый сканерами крайне обширен. Помимо стандартного анализа существующих хостов и открытых портов в сети, сканеры уязвимостей позволяют производить проверку версий установленного ПО, анализировать безопасность веб-приложений, проверять настройки конечных устройств на соответствие стандартам безопасности и т.п.

В целом, использование сканеров уязвимостей должно быть неотъемлемой частью обеспечения безопасности на крупных производствах, в частности на предприятиях агропромышленного комплекса.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina, i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 004.056

Д. Р. Мусин, В. А. Щербаков
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: musindamirrin@yandex.ru)

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SECURITY AS A SERVICE В СФЕРЕ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Security as a Service (SECaaS) – набирающая популярность бизнес-модель, которая предлагает комплексные услуги в области информационной безопасности. В данной работе проводятся исследование потенциала SECaaS и анализ перспектив его применения в сфере агропромышленного комплекса.

Ключевые слова: Security as a Service, информационная безопасность, безопасность агропромышленного комплекса, облачные вычисления, аутсорсинг.

D. R. Musin, V. A. Shcherbakov
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

PROSPECTS FOR THE IMPLEMENTATION OF THE SECURITY AS A SERVICE INFORMATION SECURITY MODEL IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. Security as a Service (SECaaS) is a growing business model that offers comprehensive information security services. This paper examines the potential of SECaaS and analyzes the prospects for its application in the agro-industrial complex.

Keywords: Security as a Service, information security, agro-industrial complex security, cloud computing, outsourcing.

Вопрос обеспечения безопасности на крупных производствах в последнее время стал особенно актуальным [1]. В соответствии с отчетами Positive Technologies число компьютерных атак на предприятия стран СНГ растет с каждым годом [2]. Так, во II квартале 2024 года было зафиксировано в 2,5 раза больше кибератак, чем в аналогичный период 2023 года. Причем 73% всех атак, направленных против организаций СНГ, приходится на долю Российской Федерации.

Агропромышленный комплекс (АПК) является критически важной отраслью для любого государства. В современных условиях, когда киберугрозы становятся все более изощренными, обеспечение информационной безопасности (ИБ) в АПК так же обретает особую актуальность. Традиционные подходы к обеспечению ИБ часто оказываются крайне затратными и недостаточно гибкими и для крупных промышленных предприятий.

Бизнес-модель Security as a Service (SECaaS) предлагает новые возможности для эффективного решения проблем кибербезопасности. SECaaS позволяет предприятиям АПК оптимизировать затраты на ИБ, избавляя их от необходимости инвестировать в дорогостоящее оборудование, программное обеспечение и штат специалистов. Более того, данная модель позволяет предприятиям выбирать только те сервисы, которые им необходимы, и легко масштабировать их в зависимости от потребностей (рис. 1). Помимо этого, SECaaS предоставляет доступ к экспертизе ведущих специалистов в области ИБ, которые постоянно следят за изменениями в ландшафте угроз.

Таким образом, Security as a Service обеспечивает более высокий уровень защиты за счет использования современных технологий и инструментов ИБ, которые постоянно обновляются. При этом сам процесс управления информационной безопасностью значительно упрощается, так как часть задач по обеспечению ИБ делегируется на поставщика услуг (рис. 2).

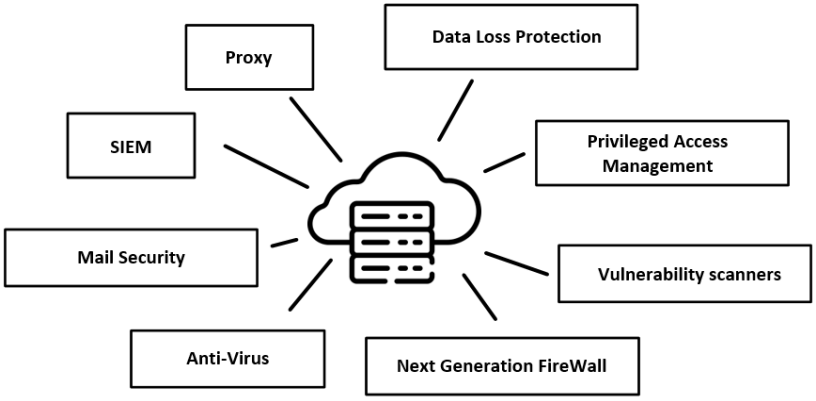


Рис. 1. Услуги информационной безопасности, предоставляемые в качестве сервисов в рамках модели SECaaS

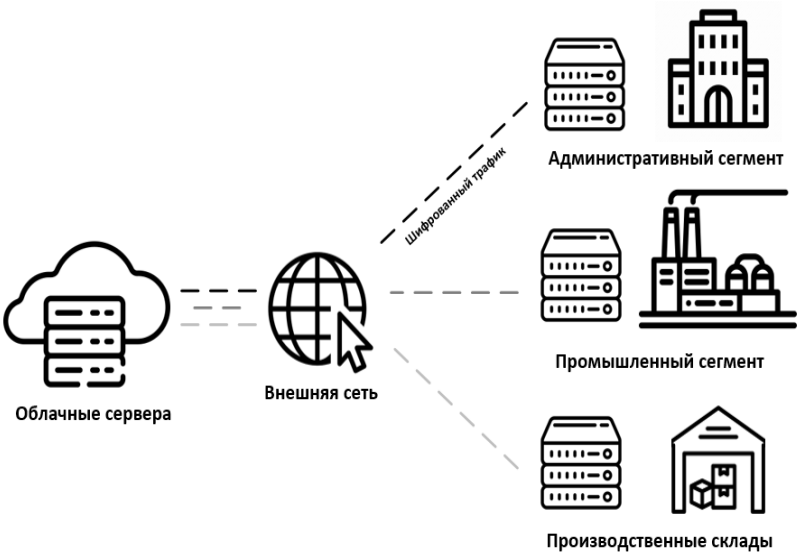


Рис. 2. Схема подключения сегментов агропромышленного комплекса к ресурсам поставщика услуг

Однако несмотря на множество преимуществ, использование SECaaS в АПК также сопряжено с некоторыми вызовами и рисками. В первую очередь, важно выбирать надежного поставщика услуг с проверенной репутацией и сильными гарантиями безопасности. Во-вторых, SECaaS-решения должны быть совместимы с существующими системами АПК, чтобы обеспечить бесперебойную работу. В-третьих, данные услуги требуют стабильного соединения с внешней сетью. В-четвертых, необходимо учитывать законодательные ограничения в области хранения, передачи и обработки информации.

В целом, SECaaS – это перспективная модель для обеспечения информационной безопасности в агропромышленных комплексах. Она предлагает множество преимуществ, таких как доступность, масштабируемость, высокий уровень экспертности поставщика и снижение затрат на ИБ в организации. Однако, при выборе решения Security as a Service необходимо учитывать законодательные ограничения, а также вызовы и риски, связанные с совместимостью систем и выбором надежного поставщика. В будущем SECaaS может стать ключевым фактором повышения эффективности и безопасности агропромышленных комплексов.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.
2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.
2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina, i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 004.056

К. А. Перфильева, Ю. В. Савченко
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: a_dushkin1@mail.ru)

ВНЕДРЕНИЕ DCAP-СИСТЕМЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Аннотация. Описывается процесс внедрения системы Data-Centric Audit and Protection (DCAP) на примере предприятия агропромышленного комплекса.

Ключевые слова: DCAP, информация, защита, целостность, конфиденциальность.

X. A. Perfilieva, Yu. V. Savchenko
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

IMPLEMENTATION OF A DCAP SYSTEM FOR INFORMATION PROTECTION AT THE ENTERPRISE

Abstract. The process of implementing the Data-Centric Audit and Protection (DCAP) system is described using the example of an agro-industrial complex enterprise.

Keywords: DCAP, information, security, integrity, confidentiality.

В настоящее время защита неструктурированных данных, особенно в крупных компаниях, которыми являются предприятия агропромышленного комплекса, становится все большей проблемой с каждым днем [1, 2].

Целью данной статьи является использование разработанной методики внедрения DCAP (Data-Centric Audit and Protection), которая состоит из четырех основных фаз: формулирование основных фаз подготовки к внедрению DCAP-системы, планирование процесса внедрения DCAP-системы, реализация и тестирование внедренной DCAP-системы, оценка эффективности внедренной DCAP-системы для решения проблемы обработки информации ограниченного доступа, например, персональных данных или конфиденциальной информации.

DCAP-система является современной системой, предназначенной для нормативизации процессов обработки информации ограниченного доступа. Ее основной задачей является обеспечение контроля над целостностью и конфиденциальностью информации, а также управление доступом к ней в организации.

Формулирование основных фаз подготовки к внедрению DCAP-системы.

1. Формирование команды проекта. В нее должны войти представители различных подразделений компании»: ИТ, юридический отдел, отдел безопасности и т.д. Команда проекта должна отвечать за планирование, координацию и контроль всего процесса внедрения DCAP-системы.

2. Определение процессов обработки информации ограниченного доступа. В этой фазе необходимо проанализировать и определить все процессы обработки информации ограниченного доступа в компании. Это необходимо для настройки DCAP-системы в соответствии с потребностями организации.

3. Выбор конкретной DCAP-системы, соответствующей требованиям компании с учетом таких факторов, как функциональность, стоимость, масштабируемость, совместимость с существующей инфраструктурой и другие (дальнейшее рассмотрение будем проводить на примере Zecurion DCAP).

4. Оценка существующей инфраструктуры и ее готовности к внедрению. Это включает в себя оценку аппаратного и программного обеспечения, сетевых ресурсов, а также наличия необходимых навыков и знаний у персонала.

5. Разработка плана внедрения DCAP-системы, включая определение времени, бюджета, а также задач, ответственных лиц и сроков выполнения.

6. Проверка готовности инфраструктуры и персонала к внедрению. Перед запуском проекта проводится проверка аппаратного и программного обеспечения, сетевых ресурсов, а также проведение обучения персонала работе с DCAP-системой.

7. Запуск проекта внедрения DCAP-системы с соответствующим контролем и тестированием выполненных работ.

Планирование процесса внедрения.

1. Построение концептуальной модели внедрения DCAP-системы в организацию, включающей архитектуру системы, процессы и workflows, а также требования к безопасности и отчетности.

2. Разработка сценариев тестирования DCAP-системы, проводимого на разных этапах внедрения и после него. Это помогает выявить и устранить ошибки и недостатки системы.

3. Обучение сотрудников работе с DCAP-системой, включающее в себя проведение обучающих семинаров, создание руководств и других ресурсов, которые способствуют в освоении сотрудниками функционала системы.

4. Начало внедрения DCAP-системы в деятельность компании и ее поддержка в процессе эксплуатации.

Реализация и тестирование внедренной DCAP-системы.

1. Выбор инструментов и технологий для реализации DCAP-системы (на примере Zecurion DCAP).

Исходя из потребностей компании, целесообразно выбрать следующие инструменты и технологии для реализации DCAP-системы: система управления базами данных (DBMS) – PostgreSQL; система управления удостоверениями и доступом (IAM) – Microsoft Active Directory; инструменты шифрования данных – McAfee Database Encryption; системы аудита и мониторинга – Splunk; инструменты анализа данных – Apache Spark; инструменты управления конфигурацией и автоматизации процессов – Ansible; инструменты тестирования и отладки – LoadRunner; инструменты визуализации данных – Power BI.

2. Реализация выбранных инструментов. Создается база данных, которая используется для хранения информации о доступе к ресурсам в компании. Перед внедрением DCAP-системы в производственную среду проводится тестирование работы системы на тестовых ресурсах, что способствует исправлению ошибок.

Следующим шагом является окончательное внедрение DCAP-системы.

Таким образом, в данной работе рассмотрена методика внедрения DCAP-системы на примере ее использования для предприятия агропромышленного комплекса.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina, i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 004.056

Е. М. Портнов, С. Г. Свиридов, А. В. Бобровских
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: a_dushkin1@mail.ru)

МЕТОДИКА ПРОВЕДЕНИЯ АУДИТА УГРОЗ СЕТЕВОЙ БЕЗОПАСНОСТИ IT-ИНФРАСТРУКТУРЫ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Рассмотрена методика проведения аудита угроз сетевой безопасности, а также рассмотрен процесс анализа защищенности IT-инфраструктуры агропромышленного комплекса.

Ключевые слова: IT-инфраструктура, аудит, анализ, сетевая безопасность, методика.

E. M. Portnov, S. G. Sviridov, A. V. Bobrovskikh
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

METHODOLOGY FOR CONDUCTING AN AUDIT OF NETWORK SECURITY THREATS TO THE IT INFRASTRUCTURE OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. The methodology for conducting an audit of network security threats is considered, and the process of analyzing the security of the IT infrastructure of the agro-industrial complex is also considered.

Keywords: IT infrastructure, audit, analysis, network security, methodology.

Согласно аналитическому отчету компании «Код Безопасности», в 2023 году продолжает фиксироваться повышенное количество целевых кибератак на объекты инфраструктуры, в том числе критическую информационную инфраструктуру, объекты промышленного производства, агропромышленного комплекса и другие государственные объекты. Для повышения уровня собственной информационной безопасности организации необходимо самостоятельно или с привлечением внешних специалистов находить слабые места в своей IT-инфраструктуре и своевременно их устранять.

Целью работы является разработка методики аудита ресурсов автоматизированных систем компаний, с помощью которой возможно своевременное обнаружение слабых мест в IT-инфраструктуре,

а в дальнейшем устранение недочетов системы безопасности и закрытие уязвимостей.

Разрабатываемая методика разделяется на два раздела – разведка по открытым источникам и исследование IT-инфраструктуры.

Описание этапов методики:

1. Разведка по открытым источникам – сбор и анализ информации, полученной из разных общедоступных информационных каналов.

- Сбор информации о компании.
  – Финансовая отчетность.
  – Клиенты и партнеры.
  – Организационная структура и вакансии.
- Сбор информации о сотрудниках.
  – Социальные сети, личная информация. Источниками информации могут выступать: Telegram, VK, OK, Linkedin и др.
  – Почтовые адреса. Утилита theHarvester – инструмент для сбора адресов электронной почты, имен сотрудников из разных открытых источников (поисковики, сервера ключей pgp).
  – Телефоны.
  – Упоминания в СМИ.
- Сетевая инфраструктура.
  – IP-адреса. Сервис WHOIS позволяет по доменному имени определить публичный IP-адрес, а также подробную информацию о владельцах домена.
  – Домены. Для поиска доменов и поддоменов, определения масштаба и детализации сетевой структуры компании можно воспользоваться онлайн-инструментом DNSdumpster.
  – Территориальная принадлежность. Инструмент DNSdumpster, помимо определения поддоменов организации, строит карту сети и карту территориального расположения серверов.
- Техническая информация. Поиск осуществляется с использованием Google Dork-техники для обнаружения скрытой информации и уязвимостей на общедоступных серверах.
  – Конфигурационные файлы.
  – Административные лог-файлы и журналы.
  – Служебные учетные записи.

2. Исследование IT-инфраструктуры.

- Исследование серверов. Получение подробной технической информации о физических или виртуальных серверах, расположенных в инфраструктуре.
  – Определение открытых портов. Для полноценного сканирования портов можно использовать инструмент nmap.

– Исследование активных сервисов и служб.

– Определение версий запущенного ПО.

– Поиск уязвимостей. Ресурсом для поиска может являться National Vulnerability Database – национальная база данных уязвимостей.

– Поиск эксплоитов. Поиск механизма эксплуатации осуществляется на ресурсе Github.

- Исследование веб-приложений на наличие угроз безопасности.

– Обнаружение URL-адресов. Для исследования структуры сайта используется специальный инструмент, который предназначен для автоматического обнаружения новых URL-адресов на проверяемом сайте.

– Использование сканера уязвимостей поможет выявить слабые места и устранить их прежде, чем они будут проэксплуатированы злоумышленником.

– Тестирование на SQL-инъекции. Для проверки наличия возможности эксплуатации инъекций можно использовать инструмент SQLMap.

Таким образом, в работе показана методика проведения аудита угроз сетевой безопасности компании. Использование данной методики на постоянной основе может обеспечить своевременное обнаружение слабых мест в IT-инфраструктуре и уязвимостей программных компонентов, которые в дальнейшем могут быть устранены.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina, i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 621.396.43

В. С. Румянцев, Р. М. Башкиров
(Межвидовой центр подготовки и боевого применения войск радиоэлектронной борьбы (учебный и испытательный),
Россия, г. Тамбов,
e-mail: nauchnajarota@yandex.ru)

КОНЦЕПЦИЯ МАСШТАБИРУЕМОЙ ТРАНКОВОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ БПЛА-РЕТРАНСЛЯТОРОВ С ТЕХНОЛОГИЕЙ РОЕВОГО ИНТЕЛЛЕКТА В СЕЛЬСКОМ ХОЗЯЙСТВЕ

Аннотация. Представлена концепция транковой сети, основанной на беспилотных летательных аппаратах (БПЛА). Также рассмотрены преимущества ее применения для обеспечения связи в удаленных регионах как для частных, так и для государственных нужд.

Ключевые слова: БПЛА, транковая сеть, роевой интеллект, спутниковая связь, сельское хозяйство.

V. S. Rumyantsev, R. M. Bashkirov
(Interspecific Center for Training and Combat use of Electronic Warfare troops (Training and Testing),
Russia, Tambov)

THE CONCEPT OF A SCALABLE TRUNK NETWORK USING UAV REPEATERS WITH SWARM INTELLIGENCE TECHNOLOGY IN AGRICULTURE

Abstract. This article presents the concept of a trunk network based on unmanned aerial vehicles (UAVs). The advantages of its application for providing communications in remote regions for both private and public needs are also considered.

Keywords: UAV, trunk network, swarm intelligence, satellite communications, agriculture.

В современном мире надежная и качественная связь является одним из ключевых факторов эффективного функционирования государственных и коммерческих структур, а также служб экстренного реагирования.

Обеспечение связи в удаленных регионах сталкивается с множеством проблем, таких как сложная логистика при создании инфраструктуры и ее высокая стоимость на фоне небольшой плотности населения. Наземные базовые станции часто требуют соблюдения ряда специфических условий для их установки и обслуживания, что затрудняет их эксплуатацию.

Использование БПЛА в качестве ретрансляторов предлагает целый ряд преимуществ:

– возможность поднятия антенны на значительную высоту;

– способность перемещаться за пользователем;

– формирование мобильной, адаптируемой и самоорганизующейся сети с участием БПЛА, управляемых технологией роевого интеллекта;

– применение в труднодоступных районах, где наземные телекоммуникационные системы недоступны.

Высота подъема антенны. Согласно нормативным требованиям (СанПиН 2.1.8/2.2.4.1190-03 и СанПиН 2.1.8/2.2.4.1383-03), сотовым операторам рекомендуется устанавливать антенны на вышках высотой 29 м. БПЛА, однако, способны достигать намного большей высоты.

Например, квадрокоптеры на электрической тяге могут подниматься на высоту до 500 м, а дроны самолетного типа – до 6000 м. Это позволяет значительно увеличить радиус охвата связи.

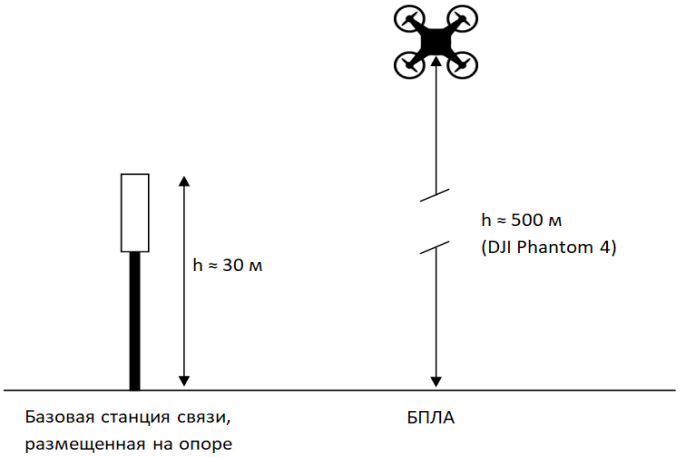


Рис. 1. Соотношение средних значений высоты размещения антенны базовой станции и высоты полета БПЛА квадрокоптерного типа

В соответствии с публикацией Пескова С. Н. [3], качество связи напрямую зависит от высоты расположения антенны, что делает БПЛА эффективным решением для удаленных регионов.

Возможность следовать за пользователем. Для обеспечения качественной и стабильной связи в движении, дрон может следовать за пользователем, используя технологию отслеживания через GPS или беспроводную связь с пультом управления. Дрон может быть оснащен

антенной для приема и передачи сигнала, обеспечивая пользователя мобильной «радиовышкой». Такой подход позволяет разворачивать сеть оперативно, не привязывая ее к конкретной точке на местности, что особенно полезно в условиях транковой сети, где каждый пользователь может иметь свой собственный дрон-ретранслятор, поддерживающий постоянную связь (рис. 2).

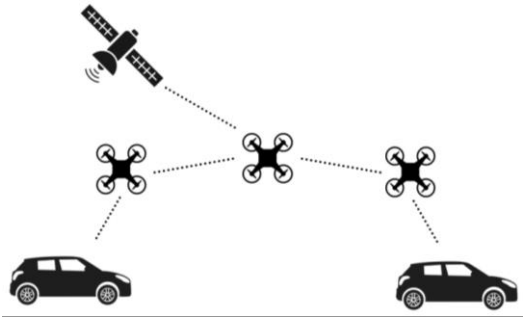


Рис. 2. БПЛА-ретранслятор в движении

Использование в труднодоступных регионах вне зоны действия наземных телекоммуникационных сетей. В регионах, где нет наземной телекоммуникационной инфраструктуры, может быть развернута транковая сеть на основе БПЛА. Главный дрон в такой сети будет ретранслировать сигнал со спутника конечным пользователям, что позволяет избежать необходимости дорогостоящих спутниковых терминалов для каждого абонента. Этот метод предоставляет стабильную связь с геостационарным спутником через дрон-ретранслятор и дает возможность быстро развернуть сеть в любом регионе.

Сеть, основанная на БПЛА с технологией роевого интеллекта, обладает рядом преимуществ. Она обеспечивает большую дальность связи благодаря высоте полета дронов, а также отличается мобильностью и гибкостью, поскольку сеть может быть расширена за счет добавления новых дронов, что делает ее легко масштабируемой.

Список использованных источников

1. Гигиенические требования к размещению и эксплуатации средств сухопутной подвижной радиосвязи (СанПиН 2.1.8/2.2.4.1190-03).

2. Гигиенические требования к размещению и эксплуатации передающих радиотехнических объектов (СанПиН 2.1.8/2.2.4.1383-03).

3. Песков, С. Н. Аналитические методы расчета напряженности поля, создаваемой передатчиком / С. Н. Песков // Теле-Спутник. – 2008. – № 10.

УДК 681.5.08

К. В. Скоморохов, З. М. Селиванова
(Кафедра «Конструирование радиоэлектронных
и микропроцессорных систем»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: kirillv6812@gmail.com, selivanova_zm@mail.ru)

ЦИФРОВАЯ ИЗМЕРИТЕЛЬНАЯ СИСТЕМА КОНТРОЛЯ КЛИМАТИЧЕСКИХ ПАРАМЕТРОВ ОБЪЕКТОВ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА НА БАЗЕ МИКРОКОНТРОЛЛЕРА И ТЕХНОЛОГИИ NB-iot

Аннотация. Предложен модульный принцип проектирования архитектуры цифровой измерительной системы для мониторинга нормируемых параметров в различных отраслях агропромышленного комплекса на базе микроконтроллера и технологии NB-iot.

Ключевые слова: климатические параметры, технологии NB-iot, цифровая измерительная система.

K. V. Skomorokhov, Z. M. Selivanova
(Department of “Design of Radioelectronic and Microprocessor Systems”,
TSTU, Tambov, Russia)

DIGITAL MEASURING SYSTEM FOR MONITORING CLIMATE PARAMETERS OF AGRICULTURAL FACILITIES BASED ON A MICROCONTROLLER AND NB-IOT TECHNOLOGY

Abstract. A modular principle for designing the architecture of a digital measuring system for monitoring standardized parameters in various sectors of the agro-industrial complex based on a microcontroller and NB-iot technology is proposed.

Keywords: climate parameters, NB-iot technologies, digital measuring system.

Направления деятельности и решаемые задачи в агропромышленном комплексе (АПК) связаны с проектом «Цифровое сельское хозяйство», в рамках которого предполагается создание цифровой среды принятия цифровых агрорешений.

Разработана цифровая измерительная система (ЦИС) контроля климатических параметров объектов АПК на базе микроконтроллера (МК) и технологии NB-iot, реализующая методы контроля нормирующих параметров (температуры, влажности, теплопроводности и др.) как в процессе производства продукции отраслей сельского хозяйства (растениеводство, животноводство), так и на стадиях технологических

процессов перерабатывающих отраслей АПК (масложировое производство) [1].

ЦИС контроля климатических параметров на основе технологии NB-iot (Narrowband internet of things) позволяет вести мониторинг в различных условиях, отправляя данные на сервер для анализа и хранения (рис. 1).

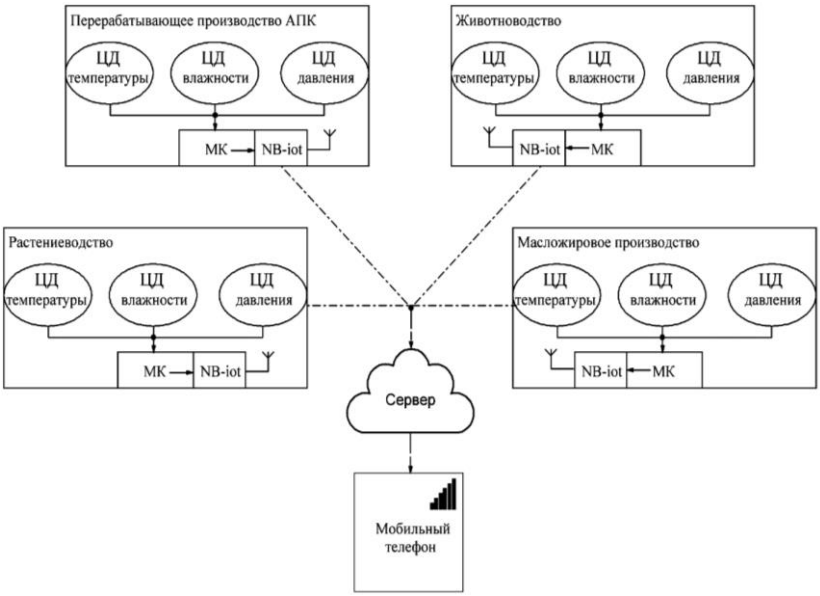


Рис. 1. Цифровая измерительная система климатических параметров объектов агропромышленного комплекса на базе микроконтроллера и NB-iot

Контроль параметров осуществляют цифровые датчики (ЦД), которые обеспечивают высокую точность и стабильность: цифровой датчик температуры DS18B20, влажности HTU21D, барометрический датчик BMP280. В ЦИС используется микроконтроллер со встроенными Wi-Fi и Bluetooth, что делает его соответствующим для IoT-проектов, который управляет процессом передачи и обработки информации от цифровых датчиков. NB-iot является модулем связи, который использует технологию NB-iot для передачи данных на облачный сервер для их хранения и анализа.

Архитектура ЦИС отличается модульным принципом построения, что позволяет адаптировать систему под различные объекты АПК.

В качестве примера приведено применение ЦИС на сыродельном заводе Тамбовской области для контроля климатических параметров на технологической линии производства сыра (рис. 2) [2].

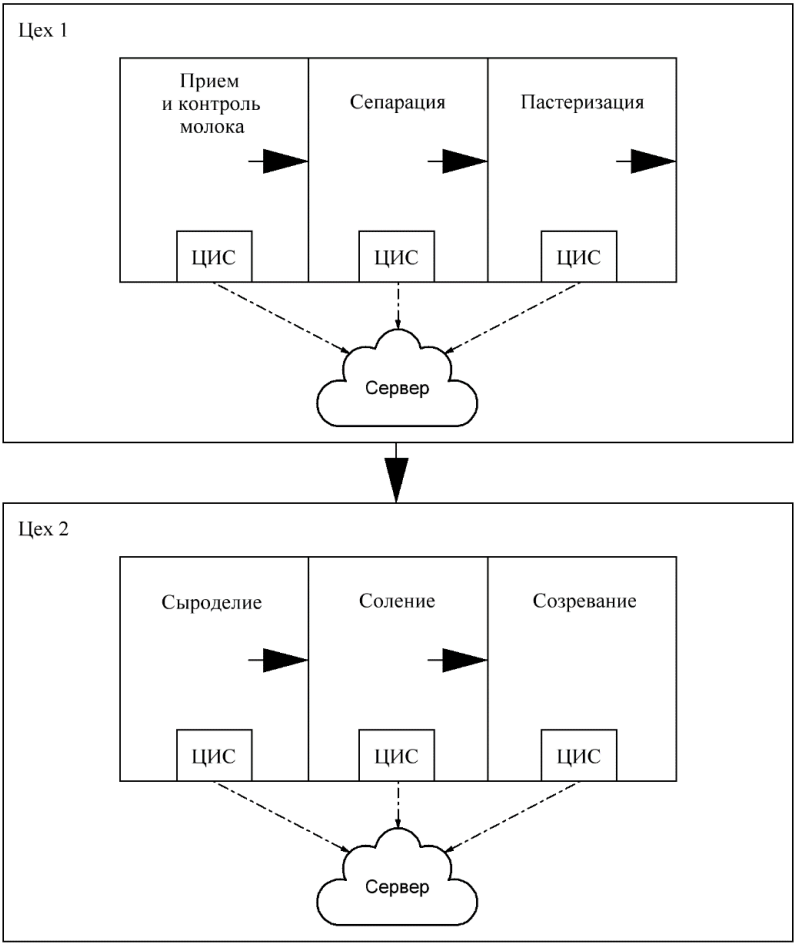


Рис. 2. Реализация ЦИС климатических параметров в сыродельном производстве

На каждом этапе производственного процесса сыродельного завода применяется цифровая измерительная система, которая позволяет контролировать нормирующие параметры. Выполняется контроль температуры молока для обработки при высокой температуре для уни-

чтожения патогенных микроорганизмов при его приемке. ЦИС применяется для поддержания необходимого температурного режима с целью предотвращения роста бактерий и оптимизации процесса созревания сыра, а также осуществляет контроль влажности для формирования правильного процесса созревания. ЦИС используется в процессе пастеризации и других этапах производства сыра, где необходимо контролировать давление для предотвращения аварий и обеспечения безопасной работы оборудования.

Применение ЦИС и технологии NB-iot позволяет повысить точность и надежность сбора измерительных данных в процессе функционирования объектов АПК для повышения эффективности их функционирования.

Список использованных источников

1. Громова, И. С. Применение IoT в агрономии / И. С. Громова. – Новосибирск : Сибагропроект, 2022. – 160 с.

2. Михайлова, Е. А. Современные технологии производства сыра / Е. А. Михайлова. – Нижний Новгород : Волжское издательство, 2023. – 250 с.

References

1. Gromova, I. S. Application of IoT in agronomy / I. S. Gromova. – Novosibirsk : Sibagroproekt, 2022. – 160 p.

2. Mikhailova, E. A. Modern technologies of cheese production / E. A. Mikhailova, . – Nizhny Novgorod : Volzhskoe Publishing House, 2023. – 250 p.

УДК 004.056

М. М. Смотряев, А. В. Облиенко
(Кафедра «Информационная безопасность»,
НИУ МИЭТ, г. Зеленоград, Москва, Россия,
e-mail: cookielover340@yandex.ru)

ПРИНЦИПЫ БЕЗОПАСНОСТИ ПОСТРОЕНИЯ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ УСТРОЙСТВ С ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID, ИСПОЛЬЗУЕМЫХ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ

Аннотация. Рассмотрен подход к обеспечению безопасности прикладного программного обеспечения для операционной системы Android с учетом особенностей применения устройств с данной операционной системой в агропромышленном комплексе.

Ключевые слова: Android, приложение, программное обеспечение, целостность, доступность, конфиденциальность.

M. M. Smotryaev, A. V. Oblienko
(Department of Information Security,
MIET, Zelenograd, Moscow, Russia)

SECURITY PRINCIPLES FOR BUILDING APPLICATION SOFTWARE FOR DEVICES WITH THE ANDROID OPERATING SYSTEM USED IN THE AGRO-INDUSTRIAL COMPLEX

Abstract. The article examines an approach to ensuring the security of application software for the Android operating system, taking into account the specific features of using devices with this operating system in the agro-industrial complex.

Keywords: Android, application, software, integrity, availability, privacy.

По состоянию на 2024 г. Android OS является самой популярной мобильной операционной системой в мире. Она сочетает в себе такие качества, как нетребовательность к аппаратным ресурсам, а также простоту разработки приложений к данной системе. Благодаря этой особенности устройства на операционной системе Android могут использоваться в агропромышленном комплексе. Для агропромышленного комплекса приоритет дается доступности и целостности обрабатываемой информации, так как получение некорректных данных или команд может привести к катастрофическим последствиям. Например, нару-

шение целостности передаваемой команды или несвоевременность ее получения может дать непредвиденный результат. Таким образом, очень важна реализация криптографической защиты путем добавления имитовставки в передаваемое сообщение [1].

Структура безопасности приложений для Android должна включать в себя как минимум:

- контроль целостности;
- обфускацию программного кода приложения;
- защиту пользовательских данных;
- аутентификацию пользователей на устройстве.

Контроль целостности данных приложения обеспечивается путем сверки хешей файлов и данных приложения с эталонными, сгенерированными либо при написании приложения, либо при окончании сессии с приложением, если речь о конфигурационных файлах или иных ячейках памяти, которые в ходе работы приложения вынуждены меняться [2]. Это позволяет обеспечить неизменность данных программы в тот момент, пока она не используется. Компанией Google создана процедура Android Verified Boot, осуществляющая контроль целостности системных разделов при запуске устройства. Для обеспечения безопасности непосредственно приложений на устройстве, аналог Android Verified Boot должен иметься в самом прикладном программном обеспечении.

Обфускация исходного кода приложения обеспечивает защиту от реверс-инжиниринга и модификации алгоритма работы программы. Она состоит в приведении исходного кода в нечитаемый и непонятный для человека вид, сохраняя исходный функционал программного обеспечения. Благодаря данной процедуре значительно усложняется анализ уже скомпилированного приложения внешним наблюдателем, получившим дистрибутив. Это позволяет скрыть алгоритм работы программы.

Защита пользовательских данных и их шифрование особенно актуально в случае, когда устройством пользуются несколько человек. Вместе с этим должна быть реализована аутентификация пользователей на устройстве. Для этого могут использоваться разные идентификаторы: от пароля и графического ключа, вплоть до биометрии, включая отпечаток пальца или скан сетчатки глаза.

Аутентификация пользователей также позволяет обеспечить неотказуемость в сети и на устройстве, так как по журналам на устройстве будет видно, какой пользователь совершил то или иное действие. Разграничение доступа позволяет предоставлять более высокие пол-

номочия на устройстве. Так, одному пользователю на устройстве в приложении может быть доступен интерфейс камеры или микрофона, в то время как другому человеку на том же самом устройстве с использованием того же самого приложения – нет. При этом, доступ к API Android будет одинаковый, но возможности будут ограничены на уровне приложения.

Разрабатываемые мобильные приложения, используемые в различных сферах, включая агропромышленность, должны использовать комплексный подход в обеспечении конфиденциальности, доступности и целостности передаваемой информации, и той, что хранится на устройстве. Рассмотренные выше принципы безопасности позволяют сделать надежным информационный обмен между узлами сети агропромышленного комплекса и ускорить информатизацию данной области.

Список использованных источников

1. Исследование эффективности мер защиты при выявлении признаков наличия активности вредоносного программного обеспечения / А. С. Смирнов, Н. Р. Пандыклы, А. В. Душкин, Н. И. Гончаров // Промышленные АСУ и контроллеры. – 2019. – № 1. – С. 40 – 52.

2. Применение технологии нейронных сетей в подсистеме безопасности информационных систем / А. В. Душкин, Т. И. Касаткина, Л. В. Россихина и др. // Приборы и системы. Управление, контроль, диагностика. – 2019. – № 6. – С. 31 – 38.

References

1. Issledovanie effektivnosti mer zashchity pri vyyavlenii priznakov nalichiya aktivnosti vredonosnogo programmnogo obespecheniya / A. S. Smirnov, N. R. Pandykly, A. V. Dushkin, N. I. Goncharov // Promyshlennye ASU i kontrollery. – 2019. – № 1. – S. 40 – 52.

2. Primenenie tekhnologii neironnykh setei v podsisteme bezopasnosti informatsionnykh sistem / A. V. Dushkin, T. I. Kasatkina, L. V. Rossikhina, i dr. // Pribory i sistemy. Upravlenie, kontrol', diagnostika. – 2019. – № 6. – S. 31 – 38.

УДК 004.9

П. М. Трефилов
(Лаборатория «Киберфизические системы»,
ИПУ РАН, Москва, Россия
e-mail: petertrfi@ipu.ru)

АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НАВИГАЦИОННОГО КОМПЛЕКСА МАЛОГО БПЛА ДЛЯ ЗАДАЧ МОНИТОРИНГА СЕЛЬСКОХОЗЯЙСТВЕННЫХ УГОДИЙ

Аннотация. Рассмотрена разработка алгоритмического обеспечения для навигационного комплекса беспилотных летательных аппаратов, предназначенных для мониторинга сельскохозяйственных угодий. Особое внимание уделено повышению точности определения навигационных параметров в условиях ограниченной видимости спутниковых сигналов и подверженности внешним возмущающим факторам. В работе предложены методы комплексной обработки информации от инерциальной и спутниковой навигационных систем, а также алгоритм выбора приоритетного режима работы навигационного комплекса в зависимости от внешних условий. Проведены имитационные и натурные эксперименты, подтвердившие эффективность предложенных решений.

Ключевые слова: БПЛА, навигационный комплекс, алгоритмы обработки информации, инерциальная навигационная система, спутниковая навигационная система, фильтр Калмана, мониторинг сельскохозяйственных угодий, точность навигации, выбор приоритетного режима работы.

P. M. Trefilov
(Cyberphysical systems laboratory,
ICS RAS, Moscow, Russia)

ALGORITHMIC SUPPORT OF NAVIGATION COMPLEX OF SMALL UAV FOR AGRICULTURAL LAND MONITORING TASKS

Abstract. The paper deals with the development of algorithmic software for the navigation system of unmanned aerial vehicles designed for monitoring agricultural land. Particular attention is paid to improving the accuracy of navigation parameters determination in conditions of limited visibility of satellite signals and exposure to external disturbing factors. Methods of complex processing of information from inertial and satellite navigation systems, as well as an algorithm for selecting the priority mode of operation of the navigation complex depending on external conditions are proposed. Simulation and field experiments have been carried out, which confirmed the effectiveness of the proposed solutions.

Keywords: UAV, navigation complex, information processing algorithms, inertial navigation system, satellite navigation system, Kalman filter, agricultural land monitoring, navigation accuracy, priority mode selection.

В современных условиях развития цифровых технологий, робототехники и систем автоматизированного управления беспилотные летательные аппараты (БПЛА) находят широкое применение в различных сферах, включая сельское хозяйство. Использование малых БПЛА для мониторинга сельскохозяйственных угодий позволяет оперативно и с высокой точностью получать данные о состоянии посевов, уровне увлажненности почвы и наличии вредителей, что, в свою очередь, способствует повышению эффективности управления аграрными процессами. Однако высокая точность выполнения задач мониторинга требует навигационного обеспечения, способного функционировать в условиях ограниченного приема спутниковых сигналов и повышенной подверженности внешним возмущающим факторам. Основной проблемой является накопление погрешностей в инерциальных навигационных системах (ИНС) при отсутствии корректирующих сигналов спутниковых навигационных систем (СНС). В данной работе предложено алгоритмическое решение, направленное на повышение точности и надежности навигации малых БПЛА.

Выявлено, что стандартные схемы объединения измерительной информации не обеспечивают достаточную точность при выполнении задач мониторинга в условиях ограниченной видимости спутниковых сигналов. Для решения этой проблемы предложен новый метод комплексной обработки навигационной информации на основе фильтра Калмана, который учитывает динамические изменения внешних условий и состояния самого БПЛА. Для этого разработан алгоритм выбора приоритетного режима работы навигационного комплекса в зависимости от текущих условий эксплуатации. В основу предложенного алгоритма положен принцип адаптации параметров фильтрации и коррекции навигационных данных на основе анализа качества поступающих сигналов и условий полета.

Разработан математический аппарат для моделирования погрешностей ИНС и СНС, а также создана модель их комплексного объединения [1]. В алгоритме предусмотрена возможность перехода между режимами работы навигационного комплекса, что позволяет минимизировать ошибки навигации в условиях отсутствия спутниковых сигналов или их зашумленности. Проведенные имитационные исследования показали, что применение предложенного алгоритма позволяет сократить среднюю ошибку определения координат и ориентации БПЛА на 10…15% по сравнению с традиционными методами, использующими фиксированные схемы интеграции данных. Натурные экспе-

рименты, проведенные с использованием малого БПЛА, подтвердили полученные результаты.

Полученные результаты подтверждают целесообразность внедрения предложенных решений в существующие системы навигации малых БПЛА, что позволит значительно расширить их функциональные возможности и повысить точность выполнения полетных заданий. Дальнейшие исследования будут направлены на оптимизацию предложенного алгоритма для работы в более сложных условиях эксплуатации и интеграцию с другими сенсорными системами для повышения автономности и точности навигации.

Список использованных источников

1. Trefilov, P. M. Synthesis of Algorithms for Complex Information Processing of Inertial Navigation System for UV Control in Smart City Model / P. M. Trefilov // Proceedings 2022 International Russian Automation Conference (RusAutoCon). – Сочи : IEEE, 2022. – С. 542 – 547.

УДК 004

А. С. Кравченко, А. М. Тюнина
(Кафедра «Вычислительная техника и информационные системы»,
ФГБОУ ВГЛТУ имени Г. Ф. Морозова, г. Воронеж,
e-mail: kr_and@inbox.ru, dif.me@bk.ru)

ЦИФРОВИЗАЦИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. Рассмотрено влияние, оказанное цифровизацией на агропромышленный комплекс. Подробнее рассказано о том, на какие именно сферы повлияла цифровизация и каким образом.

Ключевые слова: цирфовизация, сельскохозяйственная промышленность, агропромышленный комплекс, автоматизация.

A. S. Kravchenko, A. M. Tyunina
(Department of Computer Engineering and Information Systems,
G. F. Morozov Moscow State Technical University, Voronezh, Russia)

DIGITALIZATION OF THE AGRO-INDUSTRIAL COMPLEX

Abstract. this article examines the impact of digitalization on the agro-industrial complex. It tells in more detail about which areas have been affected by digitalization and how.

Keywords: digitalization, agricultural industry, agro-industrial complex, automation.

Совсем недавно автоматизация сельского хозяйства ограничивалась только использованием самых простых программ для учета финансов, работы с клиентами и проведения инвентаризации. Но что цифровизация может предложить нам сейчас? Фермы и агропромышленные комплексы все чаще внедряют технологии в самых разных направлениях ведения хозяйства. Это может быть и круглосуточный мониторинг посева, состояния скота или любых других процессов, также связанных и с бизнесом в сфере АПК (агропромышленный комплекс).

Данная инфраструктура все больше привлекает внимание компаний, разрабатывающих системы для управления процессами, так как только в 2024 году на развитие агропромышленного комплекса в Российской Федерации выделено 559 млрд рублей. А если мы посмотрим на темпы технического роста, то заметим, что производство сельскохозяйственной техники увеличилось на 8%, а на 40% увеличился выпуск машин из отрасли пищевой промышленности. В свою

очередь, данная техника работает с помощью программ, которые необходимо обновлять, поддерживать, а иногда и полностью заменять более продвинутым. ЭВМ с помощью программы обрабатывает поступающую в нее информацию с самых разных датчиков и приборов, например, уровень влажности воздуха, температура, индекс ультрафиолета, параметры почвы и т.д. На выходе можно получить как простое представление всех данных, так и какое-либо заключение на их основе. Таким образом, цифровизация значительно упрощает и ускоряет работу со сбором, хранением, обработкой и представлением данных, важных для ведения сельского хозяйства в АПК [3].

Более подробно поговорим о том, какие именно процессы можно будет автоматизировать при помощи программ. Это может быть объединение различных машин и агрегатов, датчиков и приборов, используемых в работе для повышения эффективности и сбора более точных данных. Так же появляется возможность использования Интернета вещей и подключения к облачным базам данных, что позволит обмениваться разной информацией в более упрощенном формате. Однако, одним из наиболее перспективных направлений остается робототехника. С помощью автоматизации процессов, которые физически остаются сложными для человека, повышается эффективность работы и уменьшается риск ошибки из-за человеческого фактора. Благодаря возможности технической поддержки на каждом этапе ведения с/х работ появляется возможность создания цифровой модели жизненного цикла производства, что, с свою очередь, может помочь с решением вопроса оптимизации самого этого цикла [1].

Новейшие системы технической поддержки позволят максимально быстро реагировать на ЧП, принимать меры по их ликвидации, просчитывать пути предотвращения большого количества потерь при различных угрозах, а также планировать графики деятельности для наибольшей урожайности, и просчитывать потенциальную себестоимость всего производства, прибыли и затрат. В дальнейшем это поможет любому производству повысить эффективность и выстроить стратегии для решения кризисных ситуаций, таких как непредсказуемые природные факторы и нестабильные ситуации на рынке.

Все вышеперечисленное помогает агропромышленному комплексу значительно повысить прибыль, так как с помощью прогнозов, созданных на основе собранных данных, можно свести к минимуму потери при возведении с/х культур, их сборе и хранении, т.е. максимально сохранить урожай, а также улучшить качество посева и посевного материала. С помощью передовых систем видеонаблюдения

появляется возможность организовать мониторинг большого количества посевных площадей и хранилищ, тем самым снизить риски хищения и нецелевого использования материала [2].

Цифровизация способствует упрощению взаимоотношений производителей с государством с помощью автоматизации таких процессов, как документооборот, кредитование, доступ к государственным цифровым платформам, сертификация продукции и контроль экологии. Помимо прочего, внедрение мобильных технологий и различных интернет-сервисов способствуют образованию и поддержке связей отдельных фермеров со всеми цепочками товарооборота, что, в свою очередь, позволяет фермерам получать доступ к лучшим посадочным материалам и удобрениям. Как следствие, увеличивается объем производства и качество товара, появляется возможность продажи без посредников.

Цифровизация, бесспорно, полезна для агропромышленного комплекса, так как она позволяет повысить эффективность, снизить затраты, улучшить качество продукции и обеспечить устойчивое развитие сельского хозяйства.

Список использованных источников

1. Минаков, И. А. Экономика агропромышленного комплекса / И. А. Минаков, Б. И. Смагин. – Лань, 2024. – 320 с.

2. Носов, А. М. Циклическое развитие региональных систем сельского хозяйства / А. М. Носов, А. А. Ямашкин: ЭТАП: экономическая теория, анализ, практика. – 2011. – С. 67 – 82.

3. Халтурина, Д. А. Системный мониторинг глобальных и региональных рисков / Д. А. Халтурина, А. В. Коротаев. – М. : Книжный дом «ЛИБРОКОМ», 2010. – 416 с.

Referenses

1. Minakov, I. A. Economics of the agro-industrial complex / I. A. Minakov, B. I. Smagin. – Lan, 2024. – 320 p.

2. Nosov, A. M. Cyclic development of regional agricultural systems / A. M. Nosov, A. A. Yamashkin: STAGE: economic theory, analysis, practice. – 2011. – P. 67 – 82.

3. Khalturina, D. A. System monitoring of global and regional risks / D. A. Khalturina, A. V. Korotaev. – M. : Book house “LIBROCOM”, 2010. – 416 p.

УДК 681.5

К. Б. Фам, В. В. Кушнаренко, В. Н. Богатиков
(Кафедра «Информационные системы»,
ФГБОУ ВО «ТвГТУ», г. Тверь, Россия,
e-mail: vnbgtk@mail.ru)

УПРАВЛЕНИЕ СЕЛЬСКОХОЗЯЙСТВЕННОЙ СУШИЛКОЙ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО КОНТРОЛЛЕРА

Аннотация. Рассмотрены вопросы разработки и моделирования интеллектуального контроллера на основе применения контроллера нечеткой логики.
Ключевые слова: процесс сушки, математическая модель, управление.

K. B. Fam, V. V. Kushnarenko, V. N. Bogatikov
(Department of Information Systems,
TvSTU, Tver, Russia)

CONTROL OF AN AGRICULTURAL DRYER BASED ON AN INTELLIGENT CONTROLLER

Abstract. The issues of development and modeling of an intelligent controller based on the use of a fuzzy logic controller are considered.
Keywords: drying process, mathematical model, control.

Введение. Управление температурой в сельскохозяйственных сушилках играет ключевую роль в процессе обработки и хранения урожая. Известным методом управления, который стал классическим методом регулирования температуры процесса сушки, а также многих других промышленных устройств, является ПИД (пропорциональная, интегральная, производная). Однако проектирование ПИД-регулятора включает в себя математические уравнения, кинематику, передаточные функции, а выбор коэффициентов K_p, K_i и K_d должен пройти множество этапов расчета. При управлении оборудованием оператор в основном полагается на эти параметры для настройки выходного отклика управляемого объекта так, чтобы он был стабильным. Этот метод применим только к системам управления простыми объектами. Кроме того, найденные параметры K_p, K_i и K_d не являются оптимальными. Между тем, управление Fuzzy Logic считается одним из интеллектуальных методов управления благодаря тому преимуществу, что при проектировании не обязательно заранее знать математическую модель, а необходимо лишь понимание того, как работает объект с символами.

Математическая модель термической печи. Математическая модель термической печи определяется экспериментальным методом, для печи задается максимальная температура (мощность p = 100%), температура печи постепенно увеличивается и через определенный промежуток времени достигает необходимого значения. Передаточная функция термической печи определяется выражением:

$$G(s) = \frac{200}{(60s+1)(720s+1)}.$$

Предлагаемые решения. Модель системы управления температурной стабильностью сушильной печи с интеллектуальным контроллером PID-Fuzzy разработана на основе принципа, показанного на рис. 1.

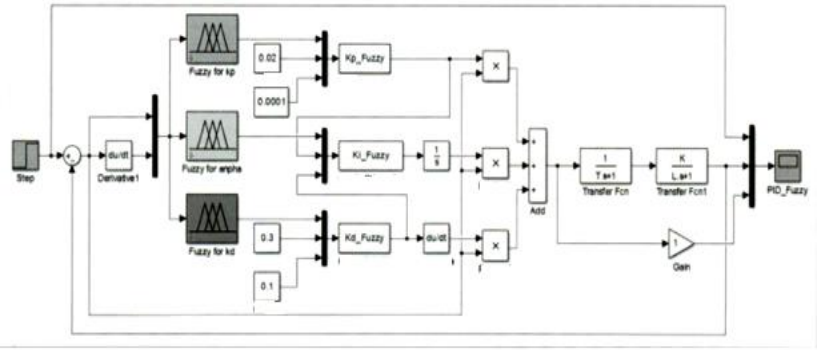


Рис. 1. Схема регулирования температуры сушильной печи с помощью интеллектуального контроллера

Определение входных/выходных переменных наборов:

– входные данные:

+ Отклонение: ET = (заданная температура) – (измеренная температура);

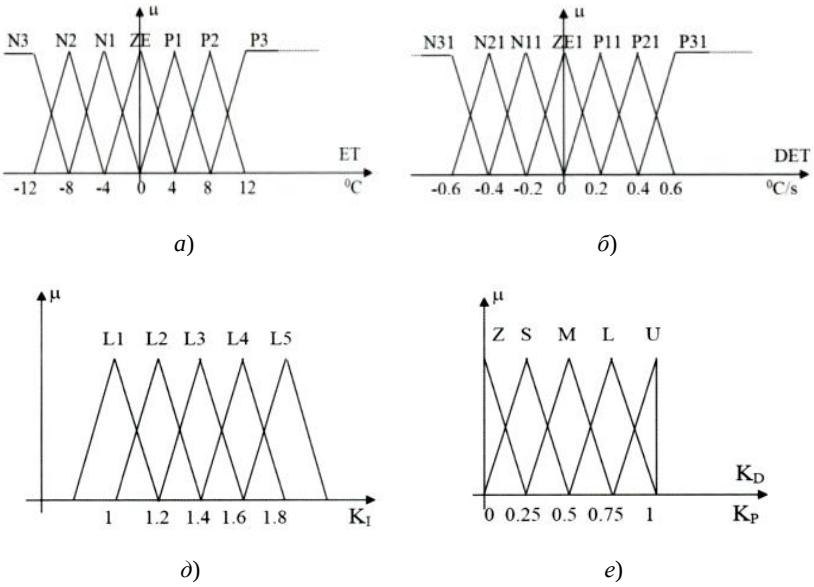
+ Производное отклонение: $DET = \frac{ET(i+1) - ET(i)}{T}$;

– выход: имеются 3 переменные из 3-х нечетких множеств, соответственно K_p, K_i и K_D.

Определение нечеткого множества для входных и выходных:

– диапазон значений входных переменных: $ET \in [-12\ 12]$ и $DET \in [-0{,}6\ 0{,}6]$;

– диапазон выходных значений: $K_p \in [0\ 1]$, $K_j \in [0\ 2]$ и $K_p \in [0\ 1]$.



а) *б*)

д) *е*)

Рис. 2. Нечеткий набор переменных:
а – ошибка *ET*; *б* – производная ошибки; *д* – K_I; *е* – K_P, K_D

Представляется функция принадлежности нечетких входных и выходных переменных, показанных на рис. 2.

Правила управления.

1. Правила K_P

K_P		DET						
		N3	N2	N1	ZE	P1	P2	P3
ET	N3	U	U	U	U	U	U	U
	N2	L	L	L	L	L	L	L
	N1	M	M	M	M	M	M	M
	ZE	Z	Z	Z	Z	Z	Z	Z
	P1	M	M	M	M	M	M	M
	P2	L	L	L	L	L	L	L
	P3	U	U	U	U	U	U	U

2. Правила K_I

K_I		DET						
		N3	N2	N1	ZE	P1	P2	P3
ET	N3	L1	L1	L1	L1	L1	L1	L1
	N2	L3	L2	L2	L1	L2	L2	L3
	N1	L4	L3	L2	L1	L2	L3	L4
	ZE	L5	L4	L3	L2	L3	L4	L5
	P1	L4	L3	L2	L1	L2	L3	L4
	P2	L3	L2	L2	L1	L2	L2	L3
	P3	L1	L1	L1	L1	L1	L1	L1

3. Правила K_D

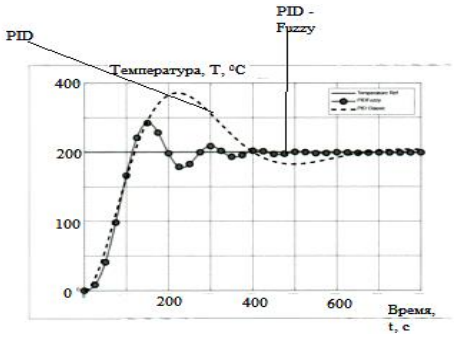
K_D		DET						
		N3	N2	N1	ZE	P1	P2	P3
ET	N3	U	U	U	U	U	U	U
	N2	L	L	M	M	M	L	L
	N1	M	M	M	M	M	M	M
	ZE	Z	Z	Z	Z	Z	Z	Z
	P1	M	M	M	M	M	M	M
	P2	L	L	M	M	M	L	L
	P3	U	U	U	U	U	U	U

Результат. В этом разделе автор выполняет моделирование в Matlab, чтобы оценить качество интеллектуального регулятора по сравнению с классическим ПИД-регулятором.

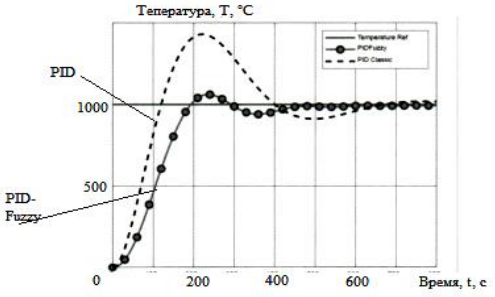
Результаты моделирования с заданной температурой 200 °C представлены на рис. 3, *а*. Легко видеть, что оба контроллера обеспечивают хорошее качество управления. Однако интеллектуальные контроллеры имеют меньшее время перерегулирования и стабилизации, чем ПИД-регуляторы. Это доказывает, что интеллектуальный регулятор лучше классического ПИД-регулятора.

Результаты моделирования с заданной температурой 1000 °C представлены на рис. 3, *б*. Легко заметить, что интеллектуальные контроллеры лучше ПИД-регуляторов. В частности, перерегулирование

интеллектуального контроллера не превышает 10%, а для ПИД-регулятора перерегулирование доходит до 40%. С другой стороны, время настройки ПИД-регулятора составляет более 800 с по сравнению с 500 с для интеллектуального контроллера.



а)



б)

Рис. 3. Результаты контроля при заданной температуре:
а – 200 °С; *б* – 1000 °С

Заключение. В этой статье исследованы и предложены решения для улучшения качества классических ПИД-регуляторов с помощью интеллектуальных контроллеров. Основным моментом исследования является успешная разработка и моделирование интеллектуального контроллера на основе применения контроллера нечеткой логики. Результаты исследований показывают, что интеллектуальный контроллер может стабильно контролировать температуру сушильной печи с практически нулевой погрешностью настройки. Кроме того, интеллектуальный контроллер значительно сокращает время перерегулирования и время настройки по сравнению с обычным ПИД-регулятором.

УДК 631.3

Р. Ю. Курносов, А. И. Иванин
(Кафедра «Конструирование радиоэлектронных
и микропроцессорных систем»
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: romankurnosov@yandex.ru, ivanin-3@yandex.ru)

ПРИМЕНЕНИЕ ОДНОПЛАТНЫХ КОМПЬЮТЕРОВ ДЛЯ СИСТЕМ СТАЦИОНАРНЫХ ЛОКАЛЬНЫХ МЕТЕОКОМПЛЕКСОВ

Аннотация. На основе проведенного анализа преимуществ одноплатных систем, рассмотрено применение Arduino Uno для построения стационарных локальных метеокомплексов, а также разработана обобщенная структурная схема такой станции и принцип подключения ее датчиков к центральному устройству.

Ключевые слова: одноплатный компьютер, Arduino Uno, датчики, метеорологические данные.

R. Y. Kurnosov, A. I. Ivanin
(Department of “Design of Radioelectronic
and Microprocessor Systems”,
TSTU, Tambov, Russia)

THE USE OF SINGLE-BOARD COMPUTERS FOR SYSTEMS OF STATIONARY LOCAL METEOROLOGICAL COMPLEXES

Abstract. the article, based on the analysis of the advantages of single-board systems, examines the use of Arduino Uno for building stationary local meteorological complexes, and also develops a generalized block diagram of such a station and the principle of its connection of sensors to a central device.

Keywords: single-board computer, Arduino Uno, sensors, meteorological data

В настоящее время наблюдается растущий интерес к метеорологическим измерениям и системам мониторинга окружающей среды. Одним из современных решений для реализации метеосистем являются одноплатные компьютеры (ОПК), к которым относятся Raspberry Pi, Arduino, Firefly, NanoPi, Radxa Rock и другие. Одноплатный компьютер представляет собой компактное устройство, в основу которого входит процессор, оперативная память и различные интерфейсы для подключения периферийных устройств [1]. Такие компьютеры обеспечивают высокую производительность и предоставляют широкие

возможности интеграции, за счет масштабируемости и гибкости подключений [4]. Применение ОПК дает возможность в разработке стационарных локальных метеокомплексов, которые представляют собой системы, предназначенные для постоянного мониторинга атмосферных явлений и метеорологических параметров. В статье рассмотрено применение одноплатного компьютера – ArduinoUno на базе микроконтроллера Atmega328 для систем стационарных локальных метеокомплексов, обобщенная структурная схема которого представлена на рис. 1.

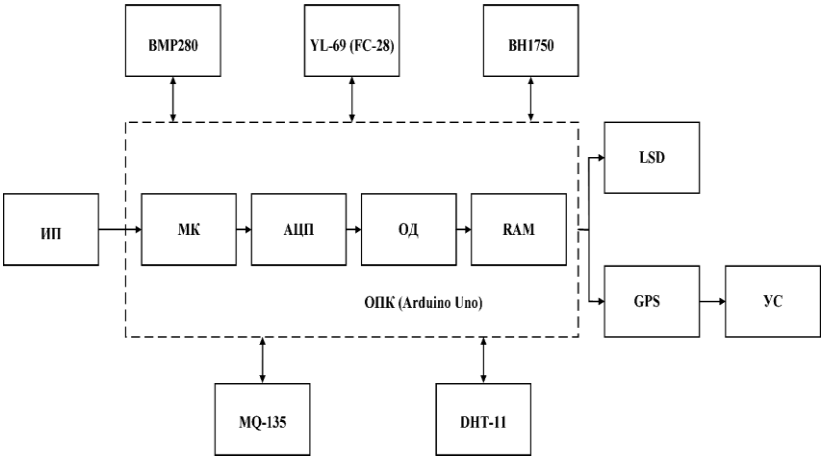


Рис. 1. Обобщенная структурная схема стационарной локальной метеостанции на базе ОПК:
ИП – источник питания, МК – микроконтроллера Atmega 328;
АЦП – аналого-цифровой преобразователь; ОД – обработка данных;
RAM – память; BMP280 – датчик атмосферного давления;
YL-69 (FC-28) – датчик влажности почвы; BH1750 – датчик освещенности цифровой; MQ-135 – модуль датчика угарного и углекислого газа;
DHT-11 – датчик температуры и влажности; LSD – цветной дисплей, 1,8-дюймовый ЖК-модуль TFT LCD ЖК – экран; GPS (ATGM336H) – навигационный модуль, позволяющий определить свои координаты по широте, долготе и высоте ; УС – устройство считывания

В основу стационарного локального метеокомплекса входит одноплатный компьютер ArduinoUno, который является центральным контроллером для считывания, обработки данных с датчиков и принятия решений в зависимости от запрограммированных условий [2, 3]. Программное обеспечение позволяет реализовывать различные алго-

ритмы, такие как усреднение данных за определенный промежуток времени. Рассматриваемый вариант метеостанции оснащен датчиками измерения температуры, влажности воздуха, атмосферного давления, освещенности, интенсивности ультрафиолетового света, угарного газа и влажности почвы. Каждый датчик подключается к Arduino Uno через аналоговые и(или) цифровые порты. После обработки данные передаются для хранения или отображения на интерфейс. Передача может осуществляться через различные интерфейсы – последовательный, I2C или SPI. Для отображения текущих значений метеорологических параметров в статье предложен LCD-дисплей. Схема подключения локальных датчиков к центральному устройству представлена на рис. 2.

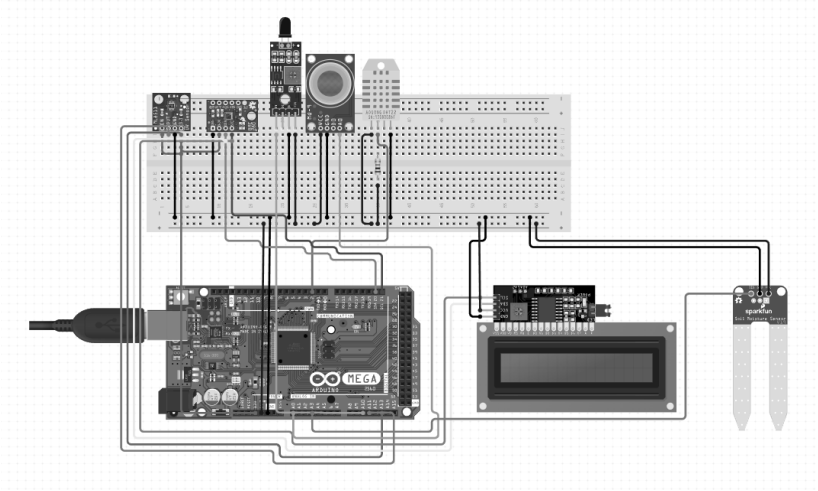


Рис. 2. Схема подключения локальных датчиков к центральному устройству

Разработка стационарной локальной метеостанции на основе одноплатного компьютера представляет собой эффективное решение для мониторинга внешних метеорологических условий, благодаря модульной конструкции, а также возможности быстрого вывода информации с последующей ее обработкой с помощью персонального компьютера.

Список использованных источников

1. Фрейман, В. И. Цифровая обработка сигналов : учебное пособие / В. И. Фрейман // Лань : электронно-библиотечная система. – Пермь : ПНИПУ, 2021. – 114 с. – URL : https://e.lanbook.com/book/239828

2. Мальцева, Н. С. Цифровая обработка сигналов : учебное пособие / Н. С. Мальцева // Лань: электронно-библиотечная система. – Астрахань : АГТУ, 2021. – 92 с. – URL : https://e.lanbook.com/book/261188

3. Воскресенский, Д. И. Устройства СВЧ и антенны. Проектирование фазированных антенных решеток / Д. И. Воскресенский. – М. : Радиотехника, 2012. – 744 с.

4. Чернышова, Т. И. Метрологический анализ измерительной процедуры цифровых средств измерений / Т. И. Чернышова, Р. Ю. Курносов // Вестник Тамбовского государственного технического университета. – 2023. – Т. 29, № 3. – С. 375 – 382.

References

1. Freiman, V. I. Digital signal processing : a textbook / V. I. Freiman // Lan: electronic library system. – Perm : PNRPU, 2021. – 114 p. – URL : https://e.lanbook.com/book/239828

2. Maltseva, N. S. Digital signal processing: a textbook / N. S. Maltseva // Lan: electronic library system. – Astrakhan : AGTU, 2021. – 92 p. – URL : https://e.lanbook.com/book/261188

3. Voskresensky, D. I. Microwave devices and antennas. Design of phased antenna arrays / D. I. Voskresensky. – M. : Radio Engineering, 2012. – 744 p.

4. Chernyshova, T. I. Metrological analysis of the measuring procedure of digital measuring instruments / T. I. Chernyshova, R. Y. Kurnosov // Bulletin of the Tambov State Technical University. – 2023. – V. 29, No. 3. – P. 375 – 382.

УДК 681.2

А. А. Третьяков[1], Ан. А. Третьяков[2],
И. А. Елизаров[1], В. Н. Назаров[1]
([1]ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
[2]ФГАОУ ВО «Национальный исследовательский технологический университет «МИСиС», Москва, Россия,
e-mail: tsasha74@mail.ru)

РАЗРАБОТКА ПРОГРАММНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ СБОРА ДАННЫХ И УПРАВЛЕНИЯ ПРОЦЕССОМ ТОЧНОГО ВЫСЕВА МНОГОФУНКЦИОНАЛЬНЫМИ ПОСЕВНЫМИ КОМПЛЕКСАМИ ТИПА ЕМС

Аннотация. Предложен подход к построению системы сбора данных тест-стенда для проведения контрольных испытаний, тестирования и отладки сеялок точного высева.

Ключевые слова: сеялки точного высева, датчик пролета семян, программируемый логический контроллер, SCADA.

A.A. Tret'yakov, An. A. Tret'yakov,
I. A. Elizarov, V. N. Nazarov
(TSTU, Tambov, Russia;
National University of Science and Technology MISIS, Moscow, Russia)

DEVELOPMENT OF SOFTWARE AND HARDWARE FOR A DATA COLLECTION SYSTEM AND CONTROL OF THE PRECISION SEEDING PROCESS USING MULTIFUNCTIONAL SEEDING COMPLEXES OF THE EMS TYPE

Abstract. An approach to constructing a test stand data collection system for conducting control tests, testing and debugging of precision seeders is proposed.

Keywordz: precision seeders, seed flight sensor, programmable logic controller, SCADA.

Обеспечение отечественной сельскохозяйственной продукцией населения нашей страны является одним из основных аспектов продовольственной безопасности Российской Федерации. Для повышения урожайности используются сеялки точного высева [1].

Основной задачей настоящей работы является разработка системы сбора данных тест-стенда для проведения контрольных испытаний, тестирования и отладки сеялок точного высева.

Система сбора данных должна обеспечивать:

– получение данных от штатных средств контроля высева, представляющих собой оптические датчики пролета семян. В проекте требуется получить информацию от фотодатчиков системы контроля высева «СКИФ-Т04» производства «Завод Радиан»;

– получение данных от тензометрических датчиков для измерения массы высеянных семян;

– получение данных от модуля измерения скоростных характеристик системы точного высева, построенного на базе бесконтактных индуктивных датчиков.

Система СКИФ Т04 предназначена для контроля технологических параметров сеялки точного высева как отечественного, так и зарубежного производителя с количеством рядков от 6 до 12 шт.

Система СКИФ Т04 контролирует [2]:

– факт пролета семян через сошник;

– исправность датчиков и целостность цепи их подключения;

– факт вращения дозаторов высевных агрегатов.

Предоставляемая информация по сеялке:

– засеянная площадь (га);

– количество высеянных семян (шт);

– эталонная и фактическая норма высева (шт/м).

Предоставляемая информация по каждому сошнику:

– относительное количество двойников и пропусков (%);

– отклонения фактической нормы высева от эталонной нормы (%).

В состав системы входит:

– блок сбора данных, предназначенный для сбора первичной информации от всех датчиков системы, обработки ее и передачи в монитор;

– датчик пролета семян ДТФ, предназначенный для установки в высевающий аппарат или на семяпровод сеялки точного высева;

– датчик пути ДМ, предназначенный для определения скорости сеялки и пройденного ею расстояния;

– втулка 60КВ 16-6 – втулка с магнитами, необходимая для работы датчика ДМ;

– комплект соединительных кабелей.

Ключевым элементом получения данных от системы контроля высева является оптический датчик пролета семян, выходной каскад которого представляет собой npn- или pnp-транзистор (схема подключения – открытый коллектор).

Для подключения подобных датчиков к дискретным входам серийно изготавливаемым промышленным контроллерам необходимо согласовать уровни сигналов. Это согласование возможно реализовать за счет использования оптрона или транзистора, включенного в ключевом режиме.

Измерение веса с использованием тензодатчиков является типовой задачей при построении систем контроля в промышленности.

Измерение скорости движения посевных агрегатов осуществляется с использованием бесконтактных индуктивных датчиков с дискретным выходным сигналом.

Структурная схема комплекса технических средств представлена на рис. 1 и на чертеже ТГТУ.2021/2.АТХ.С1.

При построении автоматизированной системы контроля и управления используется иерархическая информационная структура с применением на разных уровнях вычислительных средств различной мощности.

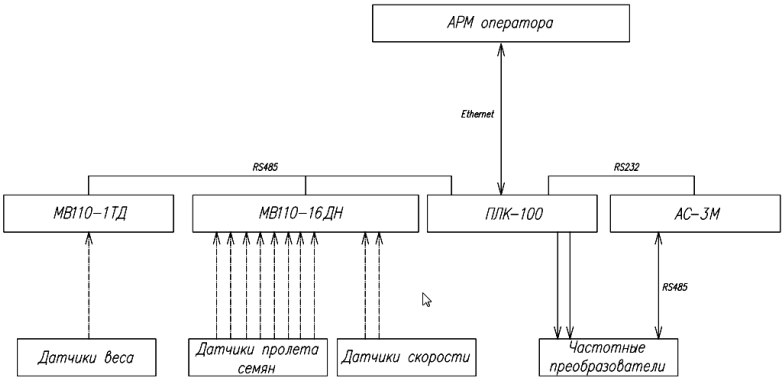


Рис. 1. Структура комплекса технических средств

Первый (нижний, полевой) уровень представлен датчиками и частотными преобразователями приводов колес.

В состав датчиков нижнего (полевого) уровня входят датчики пролета семян, датчик веса и датчики скорости колес сеялки. Информация от дискретных датчиков пролета семян и скорости колес сеялки

поступает на модуль дискретного ввода МВ110-16ДН, а сигнал от датчика веса – на модуль аналогового ввода МВ110-1ТД. Информация от этих модулей в цифровом виде поступает по сети RS-485 и протоколу Modbus RTU в программируемый логический контроллер ПЛК-100.

Взаимодействие с частотными преобразователями приводов колес и программируемого логического контроллера ПЛК-100 также осуществляется в цифровом виде по сети RS-485 и протоколу Modbus RTU через преобразователь интерфейсов АС-3М.

Второй (средний) уровень комплекса технических средств представлен щитом контроля и управления, в котором расположен управляющий контроллер ОВЕН ПЛК-100, модули аналогового и дискретного ввода и преобразователь интерфейсов.

Третий (верхний) уровень комплекса технических средств представлен автоматизированным рабочим местом (АРМ) оператора, разработанным с помощью SCADA-системы MasterSCADA [3].

Список использованных источников

1. Якушев, В. П. На пути к точному земледелию / В. П. Якушев // ПИЯФ РАН. – СПб, 2002. – 17 с.

2. Система контроля высева СКИФ-Т04 [Электронный ресурс]. – URL : https://radianzavod.ru/ru/product/skif_t04.html

3. Интегрированные системы проектирования и управления: SCADA-системы : учебное пособие / А. Н. Пчелинцев и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2015. – 160 с.

References

1. Yakushev, V. P. Na puti k tochnomu zemledeliyu / V. P. Yakushev // PIYAF RAN. – SPb, 2002. – 17 c.

2. Sistema kontrolya vyseva SKIF-T04 [Elektronnyy resurs]. – URL : https://radianzavod.ru/ru/product/skif_t04.html

3. Integrirovannyye sistemy proyektirovaniya i upravleniya: SCADA-sistemy : uchebnoye posobiye / A. N. Pchelintsev i dr. – Tambov : Izd-vo FGBOU VPO “TGTU”, 2015. – 160 s.

УДК 681.2

И. А. Фирсов[1], Ан. А. Третьяков[2], А. А. Третьяков[1]
([1]ФГБОУ ВО «ТГТУ», г. Тамбов, Россия;
[2]ФГАОУ ВО «Национальный исследовательский технологический университет «МИСиС», Москва, Россия,
e-mail: tsasha74@mail.ru)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА ПАСТЕРИЗАЦИИ МОЛОКА

Аннотация. Рассмотрено математическое моделирование технологического процесса пастеризации молока в пластинчатой пастеризационно-охладительной установке.

Ключевые слова: молоко, пастеризация, математическая модель.

I. A. Firsov[1], An. A. Tret'yakov[2], A. A. Tret'yakov[1]
([1]TSTU, Tambov, Russia;
[2]National University of Science and Technology MISIS, Moscow, Russia)

MATHEMATICAL MODELING OF THE MILK PASTEURIZATION PROCESS

Abstract. The article discusses mathematical modeling of the technological process of milk pasteurization in a plate pasteurization and cooling unit.

Keywords: milk, pasteurization, mathematical model.

Современное развитие промышленного производства молочных продуктов сопровождается все более широким применением автоматизированных систем управления технологическими процессами (АСУТП) [1].

Одной из основных стадий производства молока является стадия пастеризации, которая проводится на пластинчатых пастеризационно-охладительных установках (ППОУ), где осуществляется подогрев, очистка (сепарирование), пастеризация и охлаждение молока.

Для выбора структуры системы управления технологическим процессом производства молока на стадии пастеризации необходимо провести исследование влияния входных параметров процесса на выходные.

Математическое моделирование является одним из методов научного исследования, позволяющих установить в моделируемом процессе основные, присущие ему закономерности [2].

В общем случае ППОУ состоит из 3-х секций (рис. 1):

– секция регенерации (рекуперации), где уже нагретое молоко предварительно нагревает поступающее сырое;

– секция пастеризации – молоко нагревается до заданной температуры горячей водой;

– секция охлаждения – молоко охлаждается ледяной водой.

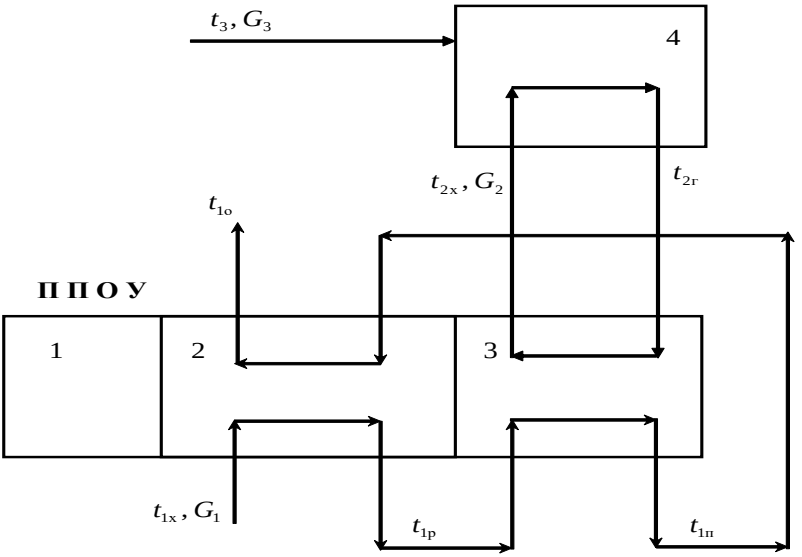


Рис. 1 Структурная схема ППОУ:
1 – секция охлаждения; *2* – секция регенерации; *3* – секция пастеризации; *4* – теплообменник для нагрева воды; *t* – температура; *G* – массовый расход; индексы: *1* – молоко; *2* – вода; *3* – греющий пар

Задачей управления является поддержание на заданном уровне температуры пастеризации $t_{1п}$ на выходе из секции пастеризации.

При разработке математической модели принимаются следующие допущения:

– теплоемкость и плотность молока можно считать в заданном технологией температурном диапазоне величинами постоянными;

– теплоемкость и плотность воды также можно считать величинами постоянными;

– греющий пар подается в инжектор при температуре парообразования;

– секции пастеризации и регенерации рассматриваются как одноемкостные объекты с сосредоточенными параметрами;

– потери в окружающую среду отсутствуют.

На основании закона сохранения вещества и энергии запишем дифференциальные уравнения для каждого из потоков процесса пастеризации.

Для пароводяного нагревателя:

$$(V_{4с}\rho_2 c_2 + m_{4с}c_4)\frac{dt_{2г}(\tau)}{d\tau} = r_3 G_3 + G_2 c_2 (t_{2х} - t_{2г}),$$

$$t_{2г}(0) = t_{2г}^0.$$

Для секции пастеризации по каналу продукта:

$$(V_{1п}\rho_1 c_1 + m_{4п}c_4)\frac{dt_{1п}(\tau)}{d\tau} = k_п F_п\left(\frac{t_{2г} + t_{2х}}{2} - \frac{t_{1п} + t_{1р}}{2}\right) - G_1 c_1 (t_{1п} - t_{1р}),$$

$$t_{1п}(0) = t_{1п}^0.$$

Для секции пастеризации по каналу греющей воды:

$$(V_{2п}\rho_2 c_2 + m_{4п}c_4)\frac{dt_{2х}(\tau)}{d\tau} = G_2 c_2 (t_{2г} - t_{2х}) - k_п F_п\left(\frac{t_{2г} + t_{2х}}{2} - \frac{t_{1п} + t_{1р}}{2}\right),$$

$$t_{2х}(0) = t_{2х}^0.$$

Для секции регенерации по каналу холодного молока:

$$(V_{1р}\rho_1 c_1 + m_{4р}c_4)\frac{dt_{1р}(\tau)}{d\tau} = k_р F_р\left(\frac{t_{1п} + t_{1о}}{2} - \frac{t_{1р} + t_{1х}}{2}\right) - G_1 c_1 (t_{1р} - t_{1х}),$$

$$t_{1р}(0) = t_{1р}^0.$$

Для секции регенерации по каналу горячего молока:

$$(V_{1р}\rho_1 c_1 + m_{4р}c_4)\frac{dt_{1о}(\tau)}{d\tau} = G_1 c_1 (t_{1п} - t_{1о}) - k_р F_р\left(\frac{t_{1п} + t_{1о}}{2} - \frac{t_{1р} + t_{1х}}{2}\right),$$

$$t_{1о}(0) = t_{1о}^0.$$

Здесь V – вместимость секции установки, м^3; ρ – плотность, кг/м^3; m – масса, кг; t – температура, °С; τ – время, с; r – теплосодержание пара, Дж/кг; G – массовый расход, кг/с; k – коэффициент теплопереда-

чи, Дж/(м^2·°С·с); F – площадь поверхности теплообмена, м^2; 1 – продукт (молоко); 2 – вода; 3 – пар; 4 – металл; г – горячий; х – холодный; п – пастеризатор; р – рекуператор; с – смеситель; о – охлаждение.

Разработанная математическая модель может быть так же использована при решении задачи оптимизации процесса пастеризации молока.

Список использованных источников

1. Хромова, Л. Г. Технология молока и молочных продуктов : учебное пособие / Л. Г. Хромова. – Воронеж : ВГАУ, 2019. – 259 с.

2. Моделирование систем : учебное пособие для вузов / И. А. Елизаров, Ю. Ф. Мартемьянов, А. Г. Схиртладзе, А. А. Третьяков. – Тамбов : ФГБОУ ВПО «ТГТУ», 2011. – 96 с.

References

1. Khromova, L. G. Tekhnologiya moloka i molochnykh produktov : uchebnoye posobiye / L. G. Khromova. – Voronezh : VGAU, 2019. – 259 s.

2. Modelirovaniye sistem: uchebnoye posobiye dlya vuzov / I. A. Yelizarov, Yu. F. Martem'yanov, A. G. Skhirtladze, A. A. Tret'yakov. – Tambov : FGBOU VPO “TGTU”, 2011. – 96 s.

УДК 349.42

У. Т. Андашев[1], Р. В. Косов[2]
([1]Кафедра «Гражданское и трудовое право»,
КНУ им. Ж. Баласагына, г. Бишкек, Кыргызстан,
e-mail: aulanand2006@mail.ru;
[2]Кафедра «Теория и история государства и права»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: 15641564a@mail.ru)

ФОРМИРОВАНИЕ «ПРАВОВОГО ФУНДАМЕНТА» ЦИФРОВИЗАЦИИ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА С УЧЕТОМ РЕАЛИЗАЦИИ ЗАДАЧ ЕВРАЗИЙСКОЙ ИНТЕГРАЦИИ

Аннотация. Рост сельскохозяйственного производства и увеличение экспортного потенциала отечественного АПК невозможны без повышения эффективности управления и производительности труда. «Правовой фундамент» цифровизации агропромышленного комплекса образуют принятые на национальном уровне концепции и стратегии развития сельского хозяйства. Логика развития интеграционных процессов и необходимость повышения эффективности АПК требуют принятия соответствующего нормативного документа на уровне ЕАЭС. Таким актом может быть Решение Евразийской экономической комиссией «Стратегии правового регулирования цифровизации агропромышленного комплекса государств-членов ЕАЭС».

Ключевые слова: цифровизация, ЕАЭС, агропромышленный комплекс, гармонизация законодательства, правовое регулирование.

U. T. Andashev[2], R. V. Kosov[2]
([1]Department of Civil and Labor Law,
KNU named after J. Balasagyn, Bishkek, Kyrgyzstan;
[2]Department of Theory and History of State and Law,
TSTU, Tambov, Russia)

FORMATION OF THE “LEGAL FOUNDATION” FOR DIGITALIZATION OF THE AGRO-INDUSTRIAL COMPLEX, TAKING INTO ACCOUNT THE IMPLEMENTATION OF THE TASKS OF EURASIAN INTEGRATION

Abstract. The growth of agricultural production and the increase in the export potential of the domestic agro-industrial complex are impossible without improving management efficiency and labor productivity. The “legal foundation” of digitalization of the agro-industrial complex is formed by nationally accepted concepts and strategies for the development of agriculture. The logic of the development of integration processes and the need to improve the efficiency of the

agro-industrial complex require the adoption of an appropriate regulatory document at the EAEU level. Such an act may be the Decision of the Eurasian Economic Commission on the “Strategy for legal regulation of digitalization of the agro-industrial complex of the EAEU Member States”.

Keywords: digitalization, the EAEU, the agro-industrial complex, harmonization of legislation, legal regulation.

Эффективность национальных и международных механизмов правового регулирования все больше зависит от комплекса взаимосвязанных внутренних и внешних факторов, влияющих на объем и содержание создаваемых норм права. Одним из них является процесс правовой интеграции, выражающийся в сближении нескольких национальных правовых систем, относящихся к определенным региональным или глобальным международным объединениям нескольких стран. Практическое выражение сближения права непосредственно зависит от успешности гармонизации правового регулирования отдельных общественных отношений в рамках более масштабных интеграционных процессов. Наиболее яркими примерами таких объединений являются Европейский союз (ЕС) и Евразийский экономический союз (ЕАЭС), которые уже вполне состоялись как самодостаточные транснациональные континентальные образования с разной степенью правовой, экономической и политической интеграции. В основе указанных интеграционных объединений лежит стремление входивших в них государств решить конкретные, прежде всего социально-экономические, проблемы. Европейский союз возник как экономическое объединение «угля и стали», в которое первоначально входили шесть государств. Евразийский экономический союз возник как инструмент интенсификации торговли и упрощения таможенных процедур.

Нормы союзного законодательства и политические установки наднациональных органов управления постепенно становятся заметными факторами эффективности правового регулирования на национальном уровне. Это наиболее выражено в таких сугубо отраслевых, специфических сферах, как, например, сельское хозяйство, где координация усилий государств-участников интеграционных объединений по вопросам объемов и технологий производства определяет большинство экономических показателей отрасли на региональном и глобальном уровнях.

Межнациональный, транснациональный, и глобальный характер цифровизации неизбежно приводит к пониманию необходимости гармонизации правового регулирования соответсвующей сферы социально-экономических отношений в рамках интеграционного объединения.

Сельское хозяйство является одним из наиболее ярких примеров такой сферы современной экономики, так как «ликвидность» качественных продовольственных товаров по мере нарастания кризисных явлений будет только увеличиваться. В 2023 году российский экспорт сельхозпродукции вырос на 12%, до более $ 45 млрд, сообщил замруководителя центра «Агроэкспорт» при Минсельхозе Андрей Кучеров на пленарной сессии в рамках выставки «Продэкспо – 2024» [1].

Очевидно, что дальнейший рост сельскохозяйственного производства и увеличение экспортного потенциала отечественного АПК, его поступательное развитие в рамках союзной экономики ЕАЭС, невозможны без повышения производительности труда. В свою очередь, реализация такой задачи непосредственно связана с увеличением темпов цифровизации сельского хозяйства и развитием механизмов внутренней кооперации между странами ЕАЭС на основе гармонизации механизмов правового регулирования и сближения законодательства в этой сфере.

«Правовой фундамент» цифровизации агропромышленного комплекса на национальном уровне образуют три группы программных нормативных документов, в которых закрепляются основные цели и задачи развития отечественного АПК. К первой группе, например, относится Указ Президента Российской Федерации от 21.07.2016 № 350 «О мерах по реализации государственной научно-технической политики в интересах развития сельского хозяйства». Другим примером является Распоряжение Правительства РФ от 04.07.2023 № 1788-р «Об утверждении Стратегии развития производства органической продукции в Российской Федерации до 2030 года».

Вторую группу образуют подзаконные нормативные акты, расширяющие положения нормативных актов первой группы. Например, принятые во исполнение Указа Президента РФ № 350: Постановление Правительства РФ от 14.07.2012 № 717 «О государственной программе развития сельского хозяйства и регулирования рынков продукции, сырья и продовольствия»; Приказ Минсельхоза России от 28.08.2020 № 517 «Об утверждении методик расчета значений отдельных показателей Государственной программы развития сельского хозяйства и регулирования рынков сельскохозяйственной продукции, сырья и продовольствия» и т.д.

К третьей группе относятся нормативные акты, конкретизирующие правовое регулирование цифровизации АПК на уровне функционирования отдельных федеральных информационных систем. В качестве примера можно привести Постановление Правительства РФ от 16.05.2023 № 762 «Об утверждении Положения о государственной

информационной системе «Информационно-аналитическая система оперативного мониторинга и оценки состояния и рисков научно-технического обеспечения развития сельского хозяйства»; Постановление Правительства РФ от 09.10.2021 № 1722 «О Федеральной государственной информационной системе прослеживаемости зерна и продуктов переработки зерна».

В странах ЕАЭС к нормативным актам первой группы относятся концепции и стратегии, закрепляющие национальные цели и задачи по развитию и функционированию национальных агропромышленных комплексов. Например, в Кыргызстане принята Концепция аграрного развития Кыргызской Республики на 2021 – 2025 годы. Концепция разработана в соответствии с Указом Президента КР от 09.02.2021 № 25 и является основой для формирования секторальных программ в агропромышленном комплексе Кыргызской Республики на основе принципов кластерного развития.

В Концепции аграрного развития Кыргызской Республики закреплены национальные задачи цифровизации АПК до 2025 года:

– разработать информационную систему, позволяющую прослеживать товары пищевой промышленности от производителя до потребителя;

– интегрировать национальную систему идентификации и отслеживания животных (СИОЖ) с системой ЕАЭС;

– обеспечить точный геоинформационный мониторинг и анализ агроресурсов страны;

– создать и обеспечивать работу агроаукциона государственных земель;

– решить проблемы фермеров с получением информации по сбыту, финансам и новым технологиям;

– создать единую электронную торговую площадку для позиционирования экспортной продукции.

В результате анализа нормативных актов первого уровня стран-участниц ЕАЭС установлена определенная схожесть основных задач по цифровизации АПК. Главными среди них являются: создание и развитие цифровых систем прослеживаемости товаров сельскохозяйственных товаропроизводителей, внедрение цифровых технологий поддержки экспорта (в этом смысле практически везде говорится об интеграции с системами ЕАЭС), а также стимулирование развития цифровых институциональных сервисов, основным назначением которых является модернизация инфраструктуры сельского хозяйства.

Решение этих задач требует гармонизации правового регулирования цифровизации АПК в рамках ЕАЭС. Пока эта цель может быть

поставлена лишь на перспективу по причине слишком большой разницы в степени развития национального законодательства в этой сфере общественных отношений. На наш взгляд, первый шаг к ее достижению должен быть сделан на уровне ЕАЭС в форме принятия Решения Евразийской экономической комиссией «Стратегии правового регулирования цифровизации агропромышленного комплекса государств-членов ЕАЭС». Принятие такой стратегии позволит сделать процесс правового регулирования цифровизации АПК более синхронным (гармоничным), что существенно повысит эффективность цифровизации на национальном уровне, а в конечном итоге – сделать сельское хозяйство стран-участниц ЕАЭС более конкурентоспособным на внешних рынках.

Список использованных источников

1. Россия в 2023 году увеличила экспорт продукции АПК [Электронный ресурс]. – URL : https://www.interfax.ru/business/944602 (дата обращения: 20.09.2024).

References

1. Russia increased exports of agricultural products in 2023 [Electronic resource]. – URL : https://www.interfax.ru/business/944602 (accessed: 09/20/2024).

УДК 621.868.277.7

Д. В. Лапин, Д. А. Полубояринов,
Т. В. Кожарина, М. В. Соколов
(Кафедра «Компьютерно-интегрированные системы в машиностроении»,
ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: ldv17112000@gmail.com)

ИННОВАЦИОННЫЕ ПОДХОДЫ К СОЗДАНИЮ МОДУЛЬНОЙ ОСНАСТКИ ДЛЯ ПОГРУЗЧИКОВ: ГИБКОСТЬ, ЭФФЕКТИВНОСТЬ И БЕЗОПАСНОСТЬ

Аннотация. В условиях динамично развивающегося рынка логистики и складской техники, традиционные подходы к оснастке погрузчиков уже не могут удовлетворить все возрастающие потребности предприятий. Ограниченная функциональность, высокие затраты на хранение и обслуживание, а также риски, связанные с неправильным использованием, вынуждают искать новые решения. Именно в этом контексте на передний план выходят инновационные подходы к созданию модульной оснастки для погрузчиков, предлагающие гибкость, повышение эффективности и безопасности. В данной статье рассматриваются преимущества модульной оснастки, а также инновационные подходы к ее созданию, включая использование композитных материалов, индивидуальное проектирование и унификацию.

Ключевые слова: модульная оснастка, погрузчики, гибкость, эффективность, безопасность, индивидуальное проектирование, унификация и стандартизация, инновационные подходы.

D. V. Lapin, D. A. Poluboyarinova,
T. V. Kazarina, M. V. Sokolov
(Department of Computer Integrated Systems in Mechanical Engineering,
TSTU, Tambov, Russia)

INNOVATIVE APPROACHES TO THE CREATION OF MODULAR EQUIPMENT FOR LOADERS

Abstract. In the context of a dynamically developing logistics and ware-house equipment market, traditional approaches to equipping loaders can no longer meet the ever-increasing needs of enterprises. Limited functionality, high storage and maintenance costs, as well as the risks associated with improper use, force us to look for new solutions. It is in this context that innovative approaches to the creation of modular equipment for loaders come to the fore, offering flexi-bility, increased efficiency and safety. This article discusses the advantages of modular tooling, as well as innovative approaches to its creation, including the use of composite materials, individual design and unification.

Keywords: modular tooling, loaders, flexibility, efficiency, safety, customized design, unification and standardization, innovative approaches.

Введение. Погрузчики являются неотъемлемой частью современных логистических и складских операций. Однако, традиционные подходы к оснастке погрузчиков, основанные на использовании специализированных приспособлений, не всегда способны удовлетворить требованиям динамично меняющегося рынка. Высокие затраты на хранение и обслуживание, а также риски, связанные с неправильным использованием, вынуждают предприятия искать новые решения, которые позволят повысить гибкость, эффективность и безопасность работы погрузчиков.

Модульная оснастка: преимущества и возможности. Модульная оснастка представляет собой систему, состоящую из взаимозаменяемых элементов, которые можно комбинировать различными способами для выполнения широкого спектра задач. Вместо того, чтобы покупать отдельные приспособления для каждой операции, предприятия могут инвестировать в универсальную систему, которую можно легко адаптировать к меняющимся требованиям.

Преимущества модульной оснастки:

- **Гибкость:** Модульная система позволяет быстро и легко изменять конфигурацию оснастки в зависимости от типа груза, задач и условий работы. Это позволяет оптимизировать использование погрузчиков и сократить время простоя.
- **Экономичность:** Инвестиции в модульную оснастку окупаются за счет снижения затрат на хранение, обслуживание и замену отдельных приспособлений. Кроме того, универсальность системы позволяет использовать ее для выполнения различных задач, что повышает эффективность использования оборудования.
- **Безопасность:** Модульная оснастка, как правило, разработана с учетом современных стандартов безопасности. Использование качественных материалов и инновационных технологий обеспечивает надежную фиксацию груза и снижает риски травм.
- **Простота использования:** Модульная система проста в установке и использовании, что снижает риск ошибок и повышает производительность операторов.

Инновационные подходы к созданию модульной оснастки:

1. Использование композитных материалов. Композитные материалы, такие как углепластик, обладают высокой прочностью, легкостью и устойчивостью к коррозии. Их использование позволяет создавать легкие и прочные конструкции, которые могут выдерживать большие нагрузки. Композитные материалы также обладают высокой стойкостью к воздействию окружающей среды, что увеличивает срок службы оснастки.

2. Индивидуальное проектирование. Современные технологии позволяют создавать оснастку, которая идеально подходит для конкретных задач и условий работы. Индивидуальное проектирование позволяет оптимизировать производительность и снизить риски. Например, для работы с хрупкими грузами можно разработать специальные захваты с мягкими прокладками, а для работы в условиях низких температур – оснастку с подогревом.

3. Унификация и стандартизация. Разработка унифицированных и стандартизированных компонентов позволяет сократить время и затраты на разработку и производство оснастки. Кроме того, это облегчает обслуживание и ремонт оборудования. Унификация и стандартизация также способствуют повышению безопасности, так как позволяют использовать проверенные и сертифицированные компоненты.

Заключение. Инновационные подходы к созданию модульной оснастки для погрузчиков открывают новые возможности для предприятий, стремящихся повысить эффективность, гибкость и безопасность своей работы. Инвестиции в современные технологии и материалы позволяют создавать оснастку, которая будет соответствовать самым высоким стандартам качества и надежности. Модульная оснастка, разработанная с учетом инновационных подходов, станет надежным инструментом для оптимизации логистических и складских операций в условиях современного рынка.

Список использованных источников

1. Карпенко, М. М. Перспектива использования гидравлического энергосберегающего привода / М. М. Карпенко, Л. Е. Пелевин // Технико-технологические проблемы сервиса. – 2017. – № 3. – С. 7 – 11.

2. Филонов, И. П. Инновации в технологии машиностроения / И. П. Филонов. – 1. – Минск : Вышэйшая школа, 2009. – 111 с.

References

1. Karpenko, M. M. The prospect of using a hydraulic energy-saving drive / M. M. Karpenko, L. E. Pelevin // Technical and technological problems of the service. – 2017. – No. 3. – P. 7 – 11.

2. Filonov, I. P. Innovations in mechanical engineering technology / I. P. Filonov. – 1. – Minsk : Higher School, 2009. – 111 p.

УДК 531

А. А. Китаева
(Факультет автоматизированных информационных технологий,
Пензенский государственный технологический университет,
г. Пенза, Россия,
e-mail: kitalina24@mail.ru)

ТРЕХМЕРНЫЕ ОБЪЕКТЫ И ПЕРСПЕКТИВНЫЕ ИСКАЖЕНИЯ

Аннотация. Определены ключевые элементы современных трехмерных моделей и объектов, рассмотрены виды и основные перспективные искажения, которые послужат художникам и дизайнерам примером для создания более убедительных и динамичных изображений, как в художественных произведениях искусства, так и в новейших технических моделях.

Ключевые слова: модели, искажения, объекты трехмерного моделирования.

A. A. Kitaeva
(Faculty of Automated Information Technologies,
Penza State Technological University,
Penza, Russia)

THREE-DIMENSIONAL OBJECTS AND PERSPECTIVE DISTORTIONS

Abstract. The article identifies the key elements of modern three-dimensional models and objects, examines the types and main perspective distortions that will serve as an example for artists and designers to create more convincing and dynamic images, both in works of art and in the latest technical models.

Keywords: models, distortions, objects of three-dimensional modeling.

Введение. Трехмерные объекты – это объекты, имеющие длину, ширину и высоту. Они занимают объем в пространстве и могут быть представлены с помощью точек, линий и поверхностей. Когда трехмерный объект проектируется на двухмерную поверхность, такую как фотография или рисунок, он претерпевает перспективные искажения. Это происходит потому, что проекционные линии от трехмерного объекта сходятся в точке схода. Точка схода – это точка на горизонте, в которой сходятся параллельные линии, идущие от трехмерного объекта. Горизонт – это воображаемая линия, отделяющая небо от земли [1].

В характеристики трехмерных объектов входят различные формы, такие как сферы, кубы, цилиндры и конусы. Они бывают любых размеров – от маленьких до больших. А также располагаться в любом месте пространства и могут быть ориентированы в любом направлении.

Существует различные объекты и фигуры. К естественным объектам относятся люди, животные, растения и различные формы рельефа. Искусственные объекты определяют здания, машины, мебель и электроника. К геометрическим фигурам относят сферы, кубы, конусы и остальные объекты. В свою очередь абстрактные объекты – это скульптуры, картины, инсталляции и остальное. Трехмерные объекты представляют в качестве двумерных чертежей, которые показывают форму, размер и расположение. Также изображения, запечатлевающие внешний вид трехмерного объекта. Модели, которые представляют форму и структуру трехмерного объекта. И компьютерная графика для создания трехмерных сцен на компьютере [2].

Трехмерные объекты являются основой скульптуры, живописи и архитектуры, также им есть место в проектирования продуктов, зданий и окружающей среды и в анализе механических конструкций. А науке также используются трехмерные объекты для изучения структуры молекул, клеток и других объектов. И, наконец, они используются для создания видеоигр, фильмов и анимации [3].

Перспективный вид объекта показывает, как он выглядит с определенной точки зрения. Важные характеристики перспективного вида включают:

Точки схода. Ими называют точки на линии горизонта, в которой сходятся параллельные в реальности линии.

Ракурс. Угол, под которым объект виден с точки зрения наблюдателя. Он влияет на то, как объект выглядит в перспективном виде.

Масштаб. Относительный размер объекта по сравнению с другими объектами в сцене. Он влияет на то, насколько большим или маленьким объект выглядит в перспективном виде.

Линейная перспектива. Параллельные линии, идущие от трехмерного объекта, сходятся в точке схода. Это наиболее распространенная форма перспективных искажений. Линейная перспектива – это система рисования или черчения трехмерных объектов на двухмерной поверхности таким образом, чтобы создать иллюзию глубины и пространства. Она основана на принципе, что параллельные линии, идущие от трехмерного объекта, сходятся в точке схода на горизонте.

Атмосферная перспектива. Объекты, находящиеся дальше от наблюдателя, имеют более низкую контрастность и насыщенность цвета по сравнению с объектами, находящимися ближе.

Коррекция перспективных искажений. Перспективные искажения можно скорректировать с помощью графического программного обеспечения или с помощью специальных линз для фотокамер [4].

Коррекция может использоваться для:

Во-первых, это корректировка относительных размеров объектов. Во-вторых, это исправление искажений, вызванных объективами фотокамеры [5].

Перспективные искажения можно использовать для создания глубины и реалистичности в рисунках, картинах и фотографиях. А также в оптических иллюзиях используют перспективные искажения, чтобы создать ощущение глубины, тени или движения. Кроме того, такие искажения могут направлять взгляд зрителя на определенные области композиции. А некоторые художники используют перспективные искажения как стилистический прием для создания драматизма или абстракции, а архитекторы для создания чертежей и визуализаций зданий, которые показывают, как они будут выглядеть в реальной жизни. Фотографы, в свою очередь, используют их для создания эффектов глубины и композиции. Например, благодаря объективу с широким углом для создания ощущение простора. Художники пользуются ими для получения трехмерных сцен и иллюзий. Например, они могут использовать линейную перспективу, чтобы создать ощущение глубины в пейзаже или атмосферную перспективу, чтобы показать расстояние между объектами [6].

Заключение. Таким образом, перспективные искажения являются неотъемлемой частью трехмерных объектов. Они могут создавать глубину, реализм и художественный эффект в рисунках, картинах и фотографиях. Понимая и используя перспективные искажения, художники и дизайнеры могут создавать более убедительные и динамичные изображения.

Список использованных источников

1. Власов, С. П. Компьютерная графика и трехмерные объекты / С. П. Власов. – Екатеринбур : Урал. ун-т, 2021.

2. Особенности синтеза визуально наблюдаемой во время полета 3d-модели внешней среды для авиационного тренажера / В. Р. Роганов, М. Ю. Михеев, М. В. Четвергова, Б. С. Долговесов // Приборы и системы. Управление, контроль, диагностика. – 2023. – № 10. – С. 14 – 24.

3. Четвергова, М. В. Использование оптико-аппаратно-программных комплексов для обучения управления подвижными объектами / М. В. Четвергова, В. Р. Роганов, А. В. Семочкин // Современные проблемы науки и образования. – 2014. – № 6. – С. 174.

4. Пермяков, Р. В. Фотограмметрическая обработка и применение разновременных стереопар космических снимков / Р. В. Пермяков. – 2021. – С. 32 – 34.

5. Свешникова, Н. В. Восстановление трехмерных сцен: первичная модель и способы ее последующего уточнения / Н. В. Свешникова, Д. В. Юрин // Математические методы распознавания образов – Т. 13. – № 1. – С. 378 – 381.

6. Паньшева, А. А. Ликвидация перспективных искажений / А. А. Паньшева, В. П. Миронов, А. В. Фирсов // Студенческий. – 2018. – № 11-2 (31). – С. 42 – 44.

УДК 681.327.12

С. С. Горшкова
(Факультет автоматизированных информационных технологий,
Пензенский государственный технологический университет,
г. Пенза, Россия,
e-mail: sonj@mail.ru)

СОВРЕМЕННЫЕ МЕТОДЫ АНАЛИЗА ТЕКСТУР В КОМПЬЮТЕРНОМ ЗРЕНИИ: ПОДХОДЫ, ПРИМЕНЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. Рассмотрена актуальность анализа текстур в компьютерном зрении, предложены основные методы и области применения. Особое внимание уделено существующим подходам к анализу текстур, таким как гистограммы направленных градиентов (HOG), фильтры Габора и локальные бинарные паттерны (LBP). Описаны сферы применения анализа текстур в медицине, сельском хозяйстве, промышленности и дистанционном зондировании Земли. Обсуждаются перспективы улучшения существующих методов, включая использование гибридных моделей глубокого обучения и многомасштабных подходов.

Ключевые слова: текстурный анализ, гистограммы направленных градиентов (HOG), фильтры Габора, локальные бинарные паттерны (LBP), компьютерное зрение, распознавание текстур.

S. S. Gorshkova,
(Faculty of Automated Information Technologies,
Penza State Technological University, Penza, Russia)

MODERN METHODS OF TEXTURE ANALYSIS IN COMPUTER VISION: APPROACHES, APPLICATIONS AND DEVELOPMENT PROSPECTS

Abstract. The article discusses the relevance of texture analysis in computer vision, proposes the main methods and areas of application. Particular attention is paid to existing approaches to texture analysis, such as histograms of directional gradients (HOG), Gabor filters and local binary patterns (LBP). The areas of application of texture analysis in medicine, agriculture, industry and remote sensing of the Earth are described. Prospects for improving existing methods are discussed, including the use of hybrid deep learning models and multi-scale approaches. Keywords: Texture analysis, histograms of directional gradients (HOG), Gabor filters, local binary patterns (LBP), computer vision, texture recognition.

Keywords: texture analysis, histograms of directional gradients (HOG), Gabor filters, local binary patterns (LBP), computer vision, texture recognition.

Введение. Анализ текстур представляет собой одну из ключевых задач в компьютерном зрении и машинном обучении, особенно в контексте распознавания и идентификации объектов на изображениях [1].

С увеличением объемов обработки визуальных данных и ростом запросов на автоматизацию анализа изображений, требования к методам анализа текстур значительно возросли [2]. Текстурные признаки обладают высокой информативностью, так как они помогают выделять объекты, которые сложно сегментировать или классифицировать по цвету или форме. Это делает анализ текстур важным направлением исследований, особенно в задачах медицинской визуализации, распознавания материалов и анализа спутниковых изображений.

Современные методы анализа текстур можно разделить на три основные категории: статистические [3], структурные [4] и спектральные [5]. Одним из наиболее популярных статистических методов является использование гистограмм направленных градиентов (HOG), которые позволяют выделять текстурные особенности объектов через анализ локальных изменений интенсивности пикселей изображения [6]. Другой широко используемый метод — это фильтры Габора, которые предназначены для анализа частотных и ориентационных свойств текстур [7]. Эти фильтры позволяют идентифицировать специфические текстурные паттерны в изображениях на различных масштабах и углах наклона. Важно также отметить метод анализа текстур на основе локальных бинарных паттернов (LBP), который отличается высокой вычислительной эффективностью и используется для анализа микротекстур [8]. Он оценивает соотношение интенсивности пикселей относительно их соседей, что позволяет детектировать локальные структурные особенности изображения. Эти методы часто комбинируются с алгоритмами машинного обучения, такими как сверточные нейронные сети (CNN), которые позволяют улучшить качество классификации и сегментации объектов, опираясь на текстурные признаки [9].

Методы анализа текстур находят широкое применение в различных сферах. В медицине они используются для анализа изображений, полученных с помощью КТ, МРТ и УЗИ, для диагностики заболеваний и оценки состояния тканей [10]. В сельском хозяйстве анализ текстур помогает в мониторинге состояния растений, выявлении болезней и оценке зрелости урожая [11]. В промышленности эти методы применяются для контроля качества продукции и обнаружения дефектов в материалах [12]. В области дистанционного зондирования Земли текстурный анализ используется для классификации земных покровов и идентификации изменений ландшафта на спутниковых изображениях [13].

Для повышения точности и эффективности анализа текстур можно предложить несколько направлений улучшений. Одним из них является разработка методов глубокого обучения, более адаптивных

к изменению условий освещения, перспективы и шума на изображениях. Это можно достичь за счет внедрения гибридных моделей, объединяющих традиционные методы фильтрации (например, фильтры Габора) с глубокими сверхточными нейронными сетями. Еще одним перспективным направлением является использование многомасштабных подходов, где анализ текстуры проводится на нескольких уровнях детализации, что позволит более точно распознавать сложные объекты. Также стоит отметить развитие методов обработки гиперспектральных данных, что расширит возможности анализа текстур на основе более широкого диапазона длин волн.

Анализ текстур остается важным направлением в области компьютерного зрения и машинного обучения благодаря своей высокой информативности и широкому спектру применения. Современные методы, такие как HOG, фильтры Габора и LBP уже зарекомендовали себя как эффективные инструменты для распознавания объектов и анализа их текстурных особенностей. Однако дальнейшие исследования должны быть направлены на улучшение адаптивности и устойчивости этих методов к различным условиям, включая изменение освещенности, наличие шума и сложность текстур. Комбинация традиционных подходов с методами глубокого обучения, а также использование гиперспектральных данных представляют собой перспективные направления для дальнейшего развития области анализа текстур.

Выводы.

– анализ методов обработки текстур показал:

– увеличение производительности программно-технических систем привело к использованию текстур в разных отраслях народного хозяйства.

– в настоящее время нет универсального метода оценки текстур. Все известные методы привязаны к необходимости решать задачи в конкретных отраслях народного хозяйства

Список использованных источников

1. Analysis of directions for improvement of flight simulators : in E3S Web of Conferences / V. Roganov, B. Dolgovesov, E. Asmolova, M. Chetvergova. – 2023. – P. 04037.

2. Кувшинова, О. А. Распределение информационных ресурсов компьютерного генератора изображения по всей площади модели участка местности / О. А. Кувшинова, В. Р. Роганов // Надежность и качество : тр. междунар. симпозиума. – 2024. – Т. 1. – С. 353 – 358.

3. Хасан, А. А. А. Алгоритм сравнения изображений на основе анализа статистических характеристик текстуры / А. А. А. Хасан, В. С. Панищев, М. И. Труфанов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2017. – Т. 7, № 4(25). – С. 34 – 40.

4. Методы интеллектуального структурного анализа текстурных изображений / А. В. Куприянов, Д. Г. Асатрян, М. Е. Арутюнян и др. // Информационные технологии и нанотехнологии (ИТНТ-2021) : сб. тр. по материалам VII Междунар. конф. и молодежной школы, Самара, 20 – 24 сентября 2021 года. – Самара : Самарский национальный исследовательский университет имени академика С. П. Королева, 2021. – Т. 3. – С. 34813.

5. Определение параметров искажений изображений спектральным способом в задаче обработки снимков поверхности Земли, полученных со спутников и самолетов / С. Сизиков, А. В. Степанов, А. В. Меженин и др. // Оптический журнал. – 2018. – Т. 85, № 4. – С. 19 – 27.

6. Клюев, В. В. Обнаружение объектов на изображениях с помощью гистограммы направленных градиентов / В. В. Клюев // Аллея науки. – 2019. – Т. 2, № 2(29). – С. 913 – 917.

7. Xie, Z. Распознавание лиц по совместным изображениям инфракрасного и видимого диапазонов на основе расширенных разреженных представлений и локальных бинарных паттернов / Z. Xie, S. Zhang, X. Yu, G. Liu // Оптический журнал. – 2019. – Т. 86, № 7. – С. 19 – 26.

8. Ковалев, В. А. Анализ текстуры трехмерных медицинских изображений : монография / В. А. Ковалев. – Минск : Белорусская наука, 2008. – 263 с.

9. Дадонова, М. М. Выявление временных изменений текстур различных типов растений на изображениях, полученных с БПЛА / М. М. Дадонова, М. Ю. Катаев, М. О. Крылов // Электронные средства и системы управления : материалы докл. Междунар. науч.-практ. конф. – 2019. – № 1-2. – С. 80 – 84.

10. Федянина, Н. И. Методы определения цветовых характеристик растительного сырья. Обзор / Н. И. Федянина, О. В. Карастоянова, Н. В. Коровкина // Пищевые системы. – 2021. – Т. 4, № 4. – С. 230 – 238.

11. Изучение особенностей эволюции текстуры и структуры при горячей прокатке в непрерывной группе клетей алюминиевого сплава 6016 / Е. В. Арышенский, В. Ю. Арышенский, Е. С. Каурова, А. В. Трибунский // Цветные металлы. – 2021. – № 7. – С. 84 – 91.

12. Картушинский, А. В. Изучение градиентных полей поверхности Земли по спутниковым данным / А. В. Картушинский, Н. А. Кукоба // Вестник Сибирского государственного аэрокосмического университета им. академика М. Ф. Решетнева. – 2015. – Т. 16, № 3. – С. 587 – 596.

УДК 634.11:581.821:628.9:577.152

С. А. Родиков, Д. О. Болдырев
(Кафедра «Агроинженерия и электроэнергетика»,
ФГБОУ ВО «МичГАУ»,
Научно-консультационный центр по хранению плодов, ягод
и винограда ФНЦ им. И. В. Мичурина, г. Мичуринск, Россия,
e-mail: rsa_rih@mail.ru)

УСТРОЙСТВО ИЗМЕРЕНИЯ МЕДЛЕННОЙ ИНДУКЦИИ ФЛУОРЕСЦЕНЦИИ ХЛОРОФИЛЛА КОЖИЦЫ ЯБЛОК

Аннотация. Рассмотрено устройство измерения медленной индукции флуоресценции хлорофилла кожицы яблок. Даны спектральные характеристики применяемых оптических приборов и светофильтров, указаны длины волн возбуждения и излучения флуоресценции. Приведено описание устройства крепления яблока.

Ключевые слова: яблоки, хлорофилл, медленная индукция флуоресценции хлорофилла.

S. A. Rodikov, D. O. Boldyrev
(Department of Agroengineering and Electric Power Engineering,
Michurinsk State Agrarian University,
Scientific and Consulting Center for Storage of Fruits, Berries
and Grapes, I. V. Michurin Federal Scientific Center,
Michurinsk, Russia)

DEVICE FOR MEASURING SLOW INDUCTION OF CHLOROPHYLL FLUORESCENCE IN APPLE SKIN

Abstract. The article discusses a device for measuring slow induction of chlorophyll fluorescence in apple skin. The spectral characteristics of the optical devices and filters used are given, the wavelengths of excitation and emission of fluorescence are indicated. A description of the device for fixing the apple is given.

Keywords: apples, chlorophyll, slow induction of chlorophyll fluorescence.

Флуоресценция хлорофилла является одним из немногих показателей, который позволяет исследовать в живых объектах протекание фотохимических реакций [1]. Для проведения измерений медленной индукции флуоресценции хлорофилла разработано устройство, включающее в себя рабочий столик со светодиодом и фотодиодом, на которое помещается яблоко, измерительный блок, сопряженный с компьютером. Для исследования разработаны несколько режимов измерения флуоресценции.

При подаче напряжения на устройстве загорается зеленый индикатор «СЕТЬ» и красный индикатор «ИЗМЕРЕНИЕ», также на рабочем столе объекта измерения загорается синий светодиод.

На жидкокристаллическом индикаторе в верхней строке отображается информация о номере выбранного режима измерения R и количестве циклов *C*. В нижней строке индикатора отображается значение тока синего светодиода в миллиамперах. В данном режиме возможна установка тока синего светодиода вращением ручки переменного резистора «Ток светодиода mA».

Устройство крепления яблока состоит из цилиндра небольшой высоты, с одной высоты которого имеется сферическое углубление, в которое помещается яблоко одной стороной, которая обучается светом. Для облучения поверхности яблока предусмотрено в центре сферического углубления отверстие. Облучение поверхности яблока осуществляется светодиодом с длиной волны излучения в максимуме 470 нм (рис. 1). Под углом к оси цилиндра просверлено отверстие, в котором находится фотодиод, на который падает отраженное от поверхности яблока излучение флуоресценции. Максимум излучения флуоресценции находится на длине волны 685 нм. На рисунке 2 показаны спектры фотодиода, синего светодиода, красного фильтра и спектр флуоресценции кожицы яблока.

Для проверки влияния постороннего света на интенсивность флуоресценции засветку проводили от лампы излучения на длине волны 470 нм (рис. 3). Флуоресценция измерялась на длине волны 685 нм. Для достоверного измерения интенсивности флуоресценции достаточно выдерживать яблоки в темноте в течение 25 минут.

В результате проведенных работ показана возможность разработки автономного прибора и методики для измерения индукции флуоресценции хлорофилла кожицы яблок.

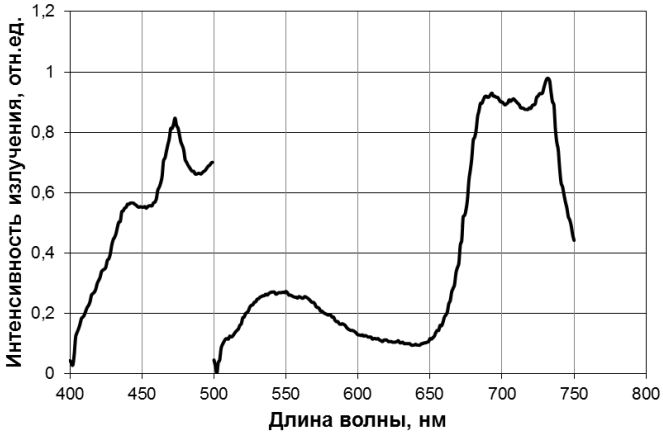


Рис. 1. Спектры возбуждения (слева) и излучения флуоресценции поверхности яблок

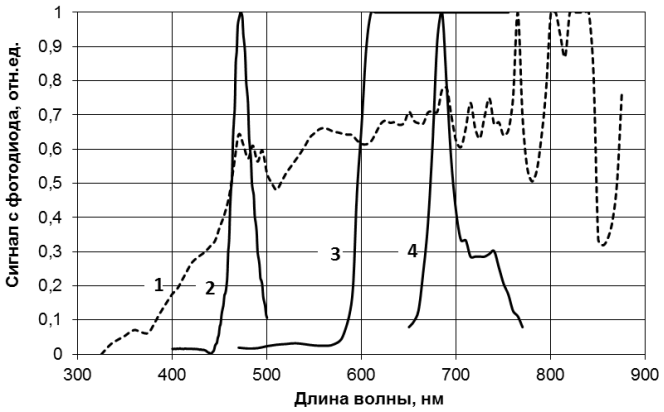


Рис. 2
1 – спектр фотодиода, *2* – спектр синего светодиода,
3 – спектр красного фильтра, *4* – спектр флуоресценции кожицы яблока

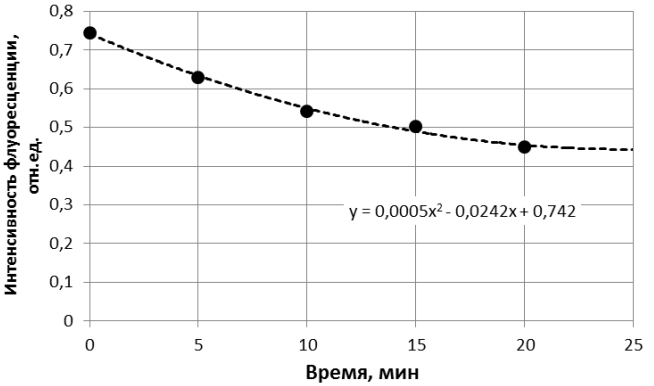


Рис. 3. Зависимость интенсивности флуоресценции поверхности яблок от времени их засветки

Список использованных источников

1. Корнеев, Д. Ю. Информационные возможности метода индукции флуоресценции хлорофилла / Д. Ю. Корнеев. – К. : Альтерпрес, 2002. – 188 с.

References

1. Korneev, D. Yu. Information capabilities of the chlorophyll fluorescence induction method / D. Yu. Korneev. – K. : Alterpres, 2002. – 188 p.

УДК 621.3.011.6

Е. И. Алгазин, К. А. Лайко, Ю. О. Филимонова, А. С. Разумихин
(Кафедры «Электроника и Электротехника», «Конструирование
и технология радиоэлектронных средств»,
ФГБОУ ВО «НГТУ», г. Новосибирск, Россия,
e-mail: evgeniialgazin@gmail.com, obd@mail.ru, play-byte@mail.ru,
yu.filimonova@corp.nstu.ru, at-te1@mail.ru)

ОБ ОДНОМ МЕТОДЕ ОЦЕНКИ ВРЕМЕНИ ДИССИПАЦИИ ЭНЕРГИИ В ЦЕПИ С РЕАКТИВНЫМ ЭЛЕМЕНТОМ СИСТЕМЫ АВТОМАТИКИ СЕЛЬСКОХОЗЯЙСТВЕННОГО ОБОРУДОВАНИЯ

Аннотация. Проведены исследования, имеющие своей целью определение времени диссипации энергии до определенного уровня в цепи системы автоматики сельскохозяйственного оборудования, содержащей емкость. При этом емкость описана линейным законом при наличии постоянной составляющей. В литературе достаточно полно освещены исследования емкости с нелинейным законом вольт-кулонной характеристики и линейным законом без постоянной составляющей.

Ключевые слова: диссипация энергии в цепи, емкость, электрическая цепь, время диссипации энергии до заданного уровня.

E. I. Algazin, K. A. Laiko, Yu. O. Filimonova, A. S. Razumikhin
(Departments of “Electronics and Electrical Engineering”,
“Design and Technology of Radioelectronic Devices”,
NSTU, Novosibirsk, Russia)

ON ONE METHOD FOR ESTIMATING THE TIME OF ENERGY DISSIPATION IN A CIRCUIT WITH A REACTIVE ELEMENT OF AN AUTOMATION SYSTEM OF AGRICULTURAL EQUIPMENT

Abstract. In this paper, studies have been carried out with the aim of determining the time of energy dissipation to a certain level in the circuit of the automation system of agricultural equipment containing a container. In this case, the capacity is described by a linear law in the presence of a constant component. In the literature, studies of capacitance with a nonlinear law of the volt-coulomb characteristic and a linear law without a constant component are sufficiently fully covered.

Keywords: energy dissipation in a circuit, capacitance, electric circuit, time of energy dissipation to a given level.

Введение. Один из методов нахождения времени диссипации энергии до заданного уровня в электрических цепях предложен авторами настоящей работы. Суть этого метода заключается в решении уравнения баланса энергии цепи относительно переменной времени диссипации энергии.

В настоящей работе рассматривается цепь с емкостью. В работе использован математический аппарат дифференциального исчисления и теории электрических цепей [1 – 3].

1. Постановка задачи. Дана электрическая цепь в виде последовательно соединенных: резистора, обладающего сопротивлением R, конденсатора, заряда, на обкладках которого нужно описать. Емкость предварительно заряжена до напряжения U_0; схема такой цепи изображена на рис. 1.

В работе приняты следующие допущения:

1. Элементы цепи сосредоточены.

Необходимо: для данной электрической цепи найти время диссипации энергии до заданного уровня.

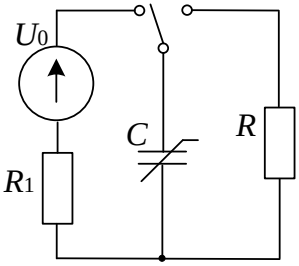


Рис. 1. Электрическая цепь

2. Пути решения

Рассмотрим цепь, изображенную на рис. 1, после коммутации ключа. Она представлена на рис. 2.

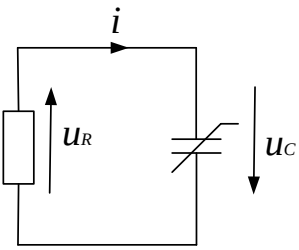


Рис. 2. Схема цепи после коммутации

Система уравнений такой цепи имеет вид:

$$q(u_C) \text{ – заданная функция,} \tag{1}$$

$$i(t) = \frac{dq(t)}{dt}, \tag{2}$$

$$u_R(t) = Ri(t), \tag{3}$$

$$u_R(t) + u_C(t) = 0. \tag{4}$$

Подставляя выражение (1) в уравнение (2), получим:

$$i(t) = \frac{dq(u_C)}{du_C}\frac{du_C(t)}{dt} = C_D\frac{du_C(t)}{dt}, \tag{5}$$

где $C_D = \frac{dq(u_C)}{du_C}$ – дифференциальная емкость.

Подставим формулу (5) в уравнение (3) и с учетом (4) получим:

$$RC_D(u_C(t))\frac{du_C(t)}{dt} + u_C(t) = 0. \tag{6}$$

Подставим выражение $u_C(t) = U_0 e^{-\frac{t}{RC_D}}$ в уравнение (6).

Пусть функция $q(u_C)$ имеет вид

$$q(u_C) = q_0 + C_0 u_C,$$

где q_0 и C_0 – коэффициенты.

При $q_0 = 0$ получен обычный линейный конденсатор с емкостью C_0.

Поскольку мы имеем дело с обычной цепью первого порядка, то следует функцию первого порядка $q(u_C) = q_0 + C_0 u_C$ подставить в уравнение (6) для проверки правильности решения.

$$RC_D(u_C(t))\frac{du_C(t)}{dt} + u_C(t) = 0,$$

$$R\frac{dq(u_C)}{du_C}\frac{du_C(t)}{dt} + u_C(t) = 0,$$

$$R\frac{d}{du_C}\left[q_0 + C_0\ u_C\right]\frac{du_C(t)}{dt} + u_C(t) = 0,$$

$$RC_0\frac{du_C(t)}{dt} + u_C(t) = 0.$$

Перейдем к характеристическому уравнению:

$$RC_0\ p\ u_C(t)+u_C(t)=0\,,$$

$$RC_0\ p\ +1=0\,,$$

$$p=-\frac{1}{RC_0}\,.$$

Следовательно, решение дифференциального уравнения (6) будем искать в виде $u_C(t)=Ae^{pt}$.

Проверим правильность решения с учетом $p=-\frac{1}{RC_0}$.

$$RC_0\ \left(-\frac{1}{RC_0}\right)Ae^{pt}+Ae^{pt}=0\,,$$

$$-Ae^{pt}+Ae^{pt}=0\,,$$

$A=U_0$ – определяется с учетом $t(0)=0$.

$$u_C(t)=U_0\ e^{-\frac{1}{RC_0}t}\,.$$

Чтобы определить энергию, запасенную в нелинейной емкости, воспользуемся аналитическим выражением тока в цепи:

$$i(t)=\frac{dq(u_C)}{du_C}\frac{du_C(t)}{dt}=C_0\frac{du_C(t)}{dt}=C_0\frac{d}{dt}\left(U_0\ e^{-\frac{1}{RC_0}t}\right)=$$

$$=C_0\left[-\frac{1}{RC_0}\right]U_0e^{-\frac{t}{RC_0}}=-\frac{U_0}{R}e^{-\frac{t}{RC_0}}\,.$$

Если за время заряда конденсатора напряжение u_C нарастает от нуля до U_0 в его электрическом поле запасается энергия

$$W_0=\int_0^{U_0}C_Du_C\,du_C\,,$$

где $C_D=\frac{dq}{du_C}=\frac{d}{du_C}(q_0+C_0u_C)=C_0$,

$$W_0=\int_0^{U_0}C_Du_C\,du_C=C_0u_C\,du_C=\frac{C_0{U_0}^2}{2}\quad[1].$$

Конечное аналитическое выражение закона сохранения энергии будет иметь вид:

$$W_0 + R\int_0^{T_{\text{дис}}} i^2(t)dt = W_0 + R\int_0^{T_{\text{дис}}} \left[\frac{U_0}{R} e^{-\frac{t}{RC_0}}\right]^2 dt =$$

$$= W_0 + \frac{{U_0}^2}{R}\int_0^{T_{\text{дис}}} e^{-\frac{2t}{RC_0}} dt = W_0 - \frac{{U_0}^2}{2}\frac{RC_0}{2}\int_0^{T_{\text{дис}}} e^{-\frac{2t}{RC_0}} d(-\frac{2t}{RC_0}) =$$

$$= W_0 - W_0 e^{-\frac{2t}{RC_0}}\Big|_0^{T_{\text{дис}}} = W_0 + \left[W_0 e^{-\frac{2t}{RC_0}} - \frac{{U_0}^2 C}{2}\right] =$$

$$= W_0 + \left[W_0(e^{-\frac{2t}{RC_0}} - 1)\right] = \varepsilon,$$

где ε – заданный уровень диссипации энергии.

Преобразуем полученное выражение к виду:

$$-W_0 + \varepsilon = W_0\left[e^{-\frac{2T_{\text{дис}}}{RC_0}} - 1\right],$$

откуда

$$\frac{1}{W_0}(-W_0 + \varepsilon) = e^{-\frac{2T_{\text{дис}}}{RC_0}} - 1,$$

$$-\frac{2T_{\text{дис}}}{RC_0} = \ln\left[\frac{1}{W_0}(-W_0 + \varepsilon) + 1\right],$$

$$T_{\text{дис}} = -\frac{RC_0}{2}\ln\left[\frac{1}{W_0}(-W_0 + \varepsilon) + 1\right],$$

$$T_{\text{дис}} = \frac{RC_0}{2}\ln\left[\frac{1}{\frac{1}{W_0}(-W_0 + \varepsilon) + 1}\right] =$$

$$= \frac{RC_0}{2}\ln\left[\frac{1}{-1 + \frac{\varepsilon}{W_0} + 1}\right] = \frac{RC_0}{2}\ln\frac{W_0}{\varepsilon}.$$

К примеру, если относительный уровень остаточной энергии соответствует времени диссипации $\frac{\varepsilon}{W_0}$, составляющего 10%, следовательно $\frac{\varepsilon}{W_0} = 0{,}1$,

$$T_{\text{дис}} = \frac{RC_0}{2} \ln 10 \approx 1{,}15RC_0 .$$

Если $\frac{\varepsilon}{W_0} \doteqdot 1\%$, то $\frac{\varepsilon}{W_0} = 0{,}01$,

$$T_{\text{дис}} = \frac{RC_0}{2} \ln 100 \approx 2{,}3RC_0 .$$

3. **Результаты.** В результате проведенных исследований получено аналитическое выражение, позволяющее определить время диссипации энергии до заданного уровня в рассматриваемой цепи.

Полученные аналитические выражения указывают на зависимость такого времени от параметров элементов цепи, что позволяет изменять значение времени диссипации как в большую, так и в меньшую сторону.

Выводы. Предложенный авторами метод оценки времени диссипации энергии в электрических цепях с емкостью возможно использовать в качестве дополнительного к классическим методам такой оценки.

Список использованных источников

1. Зернов, Н. В. Теория радиотехнических цепей / Н. В. Зернов, В. Г. Карпов. – 2-е изд., перераб. и доп. – Ленинград : Энергия, Ленинградское отделение, 1972. – 816 с.

2. Краткий физико-технический справочник / под общ. ред. К. П. Яковлева. – Т. 1. Математика. Физика. – М. : Государственное издательство физико-математической литературы, 1960. – 446 с.

3. Краткий физико-технический справочник / под общ. ред. К. П. Яковлева. – Т. 2. Общая механика. – М. : Государственное издательство физико-математической литературы, 1960. – 411 с.

References

1. Zernov, N. V. Theory of radio engineering circuits / N. V. Zernov, V. G. Karpov. – Second edition, revised. and additional. – Leningrad : Energiya, Leningrad branch, 1972. – 816 p.

2. Brief physical and technical reference book / under the general editorship of K. P. Yakovlev. – V. 1. Mathematics. Physics. – M. : State Publishing House of Physical and Mathematical Literature, 1960. – 446 p.

3. Brief physical and technical reference book / under the general editorship of K. P. Yakovlev. – V. 2. General mechanics. – M. : State Publishing House of Physical and Mathematical Literature, 1960. – 411 p.

УДК 681.5

Н. В. Саяпин[1], А. Н. Пахомов[2]
([1]ООО «БиС-Агро», г. Тамбов, Россия;
([2]Кафедра «Технологические процессы, аппараты и техносферная безопасность», ФГБОУ ВО «ТГТУ», г. Тамбов, Россия,
e-mail: info@bis-agro.ru, panpost@yandex.ru)

ОПЫТ ПРИМЕНЕНИЯ СИСТЕМ ТОЧНОГО ЗЕМЛЕДЕЛИЯ И РЕШЕНИЙ ДЛЯ УВЕЛИЧЕНИЯ МОЩНОСТИ ДВИГАТЕЛЯ В СЕЛЬСКОХОЗЯЙСТВЕННЫХ ПРЕДПРИЯТИЯХ

Аннотация. Развитие цифровых средств и систем управления в агропромышленном комплексе подразумевает применение современных решений, таких как системы точного земледелия и разработки для увеличения мощности двигателей. Линейка систем точного земледелия, включающая в себя электрическое подруливающее устройство, гидравлический автопилот, систему корректирующих сигналов и решения для увеличения мощности двигателя позволяет экономить средства до 10% от общих вложений в урожай.

Ключевые слова: подруливающее устройство, автопилот, корректирующие сигналы, урожайность, мощность, расход.

N. V. Sayapin[1], A. N. Pakhomov[2]
([1]BiS-Agro LLC, Tambov, Russia;
([2]Department of Technological Processes, Devices and Technosphere Safety, TSTU, Tambov, Russia)

EXPERIENCE IN THE APPLICATION OF PRECISION FARMING SYSTEMS AND SOLUTIONS TO INCREASE ENGINE POWER IN AGRICULTURAL ENTERPRISES

Annotation. The development of digital tools and control systems in the agro-industrial complex implies the use of modern solutions, such as precision farming systems and developments to increase engine power. The range of precision farming systems, which includes an electric thruster, a hydraulic autopilot, a system of corrective signals and solutions for increasing engine power, allows you to save up to 10% of the total investment in the crop.

Keywords: thruster, autopilot, corrective signals, productivity, power, consumption.

Фирма «БиС-Агро», в рамках развития цифровых средств и систем управления в агропромышленном комплексе, разрабатывает и продвигает на отечественном рынке два направления – это системы точного земледелия и разработки для увеличения мощности двигателей.

Линейка систем точного земледелия предназначена для реализации концепции рационального использования ресурсов сельскохозяйственного предприятия в области обработки почвы, связанной с такими процес-

сами как вспашка, внесение удобрений, полив, обработка, сбор урожая [1]. То есть это качественно новый подход к управлению всем хозяйством.

Представляемая линейка включает в себя:

1) электрическое подруливающее устройство;

2) гидравлический автопилот;

3) виды корректирующих сигналов (спутниковый, радиопоправка и gsm-поправка).

Как показывает практика эксплуатации подобных устройств, экономия средств от точного земледелия достигает 10% от общих вложений в урожай.

При возделывании сельскохозяйственных культур и обслуживании предприятий животноводства самые значительные расходы приходятся на функционирование машинно-тракторного парка [2]. При этом остро стоит задача повышения мощности двигателей имеющихся машин.

Модули мощности STEINBAUER предоставляют оптимизацию почти для всех систем впрыска. Эти модули можно использовать не только в тракторах, но также в комбайнах. Для комбайнов оптимизация мощности всего на 1 кВт уже означает значительную экономию времени. Эта оптимизация может быть применима для всех транспортных средств сельскохозяйственной отрасли.

Решения для увеличения мощности двигателя с электронным впрыском топлива от компании STEINBAUER включают в себя работу с прошивкой электронного блока управления двигателем. В результате увеличивается крутящий момент и мощность двигателя на всем диапазоне оборотов, максимально сглаживается турбояма на двигателях с наддувом, улучшается работа на холодном двигателе, холостом ходу и при включенном кондиционере.

Результаты эксплуатации наших систем показали:

1) повышение мощности и крутящего момента до +25%;

2) снижение расхода топлива от 10 до 15%.

Как показал наш опыт, применение подобных устройств на сельскохозяйственных машинах в настоящий момент является экономически выгодным.

Список использованных источников

1. Лопачев, Н. А. Основы построения прецизионных систем земледелия / Н. А. Лопачев, Е. В. Ковалева. – М. ; Лань, 2021. – 120 с.

2. Григулецкий, В. Г. Цифровые технологии в АПК. Цифровые модели роста и продуктивности сельскохозяйственных растений / В. Г. Григулецкий. – М. : Лань, 2024. – 316 с.

References

1. Lopachev, N. A. Fundamentals of building precision farming systems / N. A. Lopachev, E. V. Kovaleva. – M. : Lan, 2021. – 120 p.

2. Griguletsky, V. G. Digital technologies in agriculture. Digital models of growth and productivity of agricultural plants / V. G. Griguletsky. – M. : Lan, 2024. – 316 p.

Научное электронное издание

IV Международная научно-практическая конференция

«ЦИФРОВИЗАЦИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА»

В 3-х томах

Том I

Сборник научных статей

Редактирование И. В. Калистратовой, Е. С. Мордасовой,
Л. В. Комбаровой
Компьютерное макетирование Т. Ю. Зотовой

ISBN 978-5-8265-2817-4

Подписано к использованию 16.10.2024.
Тираж 100 шт. Заказ № 107

Издательский центр ФГБОУ ВО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14.
Телефон (4752) 63-81-08.
E-mail: izdatelstvo@tstu.ru