цифровых водяных знаков. В этом случае в изображение внедряются метки, которые должны сохраняться даже после редактирования. Устойчивость водяных знаков к модификациям критически важна для обеспечения подлинности фотографии. Однако результаты исследований показали, что водяные знаки неустойчивы к различным шумовым воздействиям и геометрической трансформации [3].

В предлагаемой работе для защиты изображения предлагается использовать спектральный подход и трактовать изображение как 2D-сигнал. Анализ частотной области выявил, что ИИ-инструменты генерации изображений сильнее всего искажают средние и высокие частоты. На основе этого был разработан нелинейный метод искажения частот исходного изображения. Предложенный алгоритм имеет простую реализацию и устойчив к jpeg-сжатию, а также к «print/scan» атаке. Метод был протестирован на модели Nano Banana.

Список использованных источников

1. Huang Y. et al. Diffusion model-based image editing: A survey/ IEEE Transactions on Pattern Analysis and Machine Intelligence. 2025.

2. Salman H. et al. Raising the cost of malicious ai-powered image editing /arXiv preprint arXiv:2302.06588. 2023.

3. Cao J. et al. Secure and Robust Watermarking for AI-generated Images: A Comprehensive Survey /arXiv preprint arXiv:2510.02384. 2025.

Никитенкова Светлана Павловна, к.т.н., доцент, доцент каф. БИС, nikitenkova@rf.unn.ru.
Пряничникова Алина Сергеевна, студ., pryanichnikova04@mail.ru.

УДК 004.056

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

П.А. Летюк, Р.М. Яппаров
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, АСУ ТП, модель угроз, защита информации.

Современный этап развития информационных технологий характеризуется широким внедрением автоматизированных систем управления технологическими процессами в различных отраслях экономики. Такие системы применяются в энергетике, промышленности, коммунальном хозяйстве и других сферах, обеспечивающих жизнедеятельность общества. Их функционирование непосредственно

влияет на устойчивость производственных процессов и надежность функционирования инфраструктуры [5].

Нарушение работы подобных систем вследствие реализации угроз информационной безопасности может привести к серьезным экономическим потерям, технологическим сбоям и негативным социальным последствиям. В связи с этим особое значение приобретает защита информационных систем, относящихся к объектам критической информационной инфраструктуры.

В Российской Федерации вопросы обеспечения безопасности таких систем регулируются Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]. В соответствии с данным законом автоматизированные системы управления технологическими процессами (АСУ ТП) относятся к ключевым объектам критической инфраструктуры и требуют реализации комплекса организационных и технических мер защиты [2].

Одним из важнейших этапов обеспечения информационной безопасности АСУ ТП является разработка модели угроз [3]. Модель угроз позволяет выявить потенциальные источники атак, определить возможные уязвимости информационной системы и сформировать обоснованный перечень мер защиты.

Анализ угроз информационной безопасности является важным этапом проектирования системы защиты информации [7]. Его целью является выявление потенциальных источников угроз, определение уязвимостей системы и оценка возможных последствий реализации компьютерных атак [4].

Известно, что основными источниками угроз для АСУ ТП могут выступать:

– внешние нарушители;
– внутренние пользователи;
– вредоносное программное обеспечение;
– технические сбои оборудования.

При этом наиболее распространенными являются:

– несанкционированный доступ к информационным ресурсам;
– внедрение вредоносного программного обеспечения;
– подмена технологических данных;
– нарушение целостности конфигурации системы;
– отказ в обслуживании [5].

Для систем промышленной автоматизации особенно опасны угрозы, способные привести к нарушению технологических процессов и повреждению оборудования [6].

Пример обобщенной модели угроз представлен в таблице 1:

Таблица 1–Модель угроз информационной безопасности АСУ ТП

Источник угрозы	Угроза	Уязвимость	Возможные последствия
Внешний нарушитель	Несанкционированный доступ	Недостаточная защита сетевой инфраструктуры	Нарушение работы системы
Вредоносное ПО	Внедрение вредоносного программного обеспечения	Отсутствие контроля программного обеспечения	Нарушение целостности данных
Внутренний пользователь	Несанкционированные действия персонала	Недостаточный контроль доступа	Искажение технологических параметров
Сетевые атаки	Перехват и подмена данных	Использование незащищенных протоколов	Нарушение технологического процесса
Технические сбои	Отказ оборудования	Износ аппаратных средств	Прекращение функционирования системы

Для повышения уровня информационной безопасности объектов критической инфраструктуры, в том числе АСУ ТП, необходимо применение комплексного подхода, включающего:

- сегментацию технологической сети;
- использование межсетевых экранов;
- внедрение систем обнаружения вторжений;
- контроль действий пользователей;
- регулярное обновление программного обеспечения;
- проведение аудита информационной безопасности.

Комплексное применение указанных мер позволит существенно снизить вероятность реализации угроз и повысить устойчивость функционирования АСУ ТП.

Список использованных источников

1.Федеральный закон от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в ред. от 07.04.2025 №58-ФЗ) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 11.03.2026).

2.Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (в ред. от 07.11.2025 № 1762) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_290595/1b445ea2ca2e30b9350044e3133a1aced3b23a6c/ (дата обращения 11.03.2026).

3.Распоряжение Правительства Российской Федерации от 26.02.2026 № 360-р «Об утверждении перечня типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_527541/ (дата обращения 11.03.2026).

4.Методика моделирования угроз безопасности информации ФСТЭК России. — М., 2021.

5.Малюк А.А. Информационная безопасность: теория и практика. — М.: Горячая линия – Телеком, 2020.

6.Гафнер В.В. Защита информации в автоматизированных системах управления. — М.: Академия, 2019.

7.Исмагилова, А. С. Теоретико-графовая интерпретация системы защиты информации / А. С. Исмагилова, И. А. Шагапов, И. В. Салов // Инженерный вестник Дона. – 2024. – № 9(117). – С. 171-179. – EDN LWCKXX.

Летюк Полина Александровна, студ. ИИГУ, polinaletom@gmail.com
Яппаров Рауф Мидхатович, к.ю.н., доцент, доцент каф. УИБ, bist2002@yandex.ru

УДК 519.87 + 004.056

ОПТИМИЗАЦИЯ МАРШРУТОВ РОЯ БПЛА

В.И. Петренко, М.П. Сутормин
Северо-Кавказский федеральный университет, г. Ставрополь

Ключевые слова: рой БПЛА, многокритериальная маршрутизация, кибербезопасность, GPS-спуфинг, MAVLink, метод анализа иерархий, фронт Парето.

Точное земледелие всё активнее переходит к роевым системам БПЛА с централизованным планированием маршрутов. Такой подход сокращает время обработки угодий и повышает отказоустойчивость, однако существенно расширяет поверхность кибератак: GPS-спуфинг, перехват телеметрии по протоколу MAVLink и DoS-воздействие на ретрансляторы способны нарушить выполнение агротехнологического задания [1]. Классические алгоритмы маршрутизации оптимизируют лишь один критерий — время или энергию — и не учитывают пространственно распределённых киберрисков отдельных сегментов траектории. Настоящая работа предлагает многокритериальный подход, в котором риск формализован как самостоятельный критерий, равноправный с временем полёта.

Пространство угроз задаётся вектором $T = \{t_1, \ldots, t_k\}$, где каждый элемент $t_i = \langle \tau_i, p_i, d_i \rangle$ — тип атаки, вероятность её реализации на данном сегменте и нормированный коэффициент ущерба. Выделяются три класса: GPS-спуфинг (вероятность p_1 растёт с удалением от базовой станции), перехват MAVLink (p_2 обратно пропорциональна ширине спектра канала) и