5. EvalPacker Obfuscator [Электронный ресурс]. – Инструмент для обфускации кода с возможностью защиты от копирования. – https://tools.100zona.com/evalpacker.html.

6. JavaScript Obfuscator [Электронный ресурс]. – Обфускатор JavaScript с функциями минификации и защиты кода. – https://beautifytools.com/javascript-obfuscator.php.

7. PHP Obfuscator [Электронный ресурс]. – Онлайн-обфускатор для защиты PHP-кода. – https://php-minify.com/php-obfuscator/.

8. WB PHP Obfuscator [Электронный ресурс]. – Инструмент для обфускации PHP-кода с множеством функций. – http://wb0.ru/phpobf.php.

УДК 004.03.26+004.56

АНАЛИЗ НАПРАВЛЕНИЙ ПРИМЕНЕНИЯ В БЕСПИЛОТНЫХ СИСТЕМАХ МОДЕЛЕЙ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Д.В. САЗОНОВА
Белорусский государственный технологический университет
Минск, Беларусь

Беспилотные системы (БПС) в последние годы прочно вошли в сферу гражданских и военных технологий, охватывая широкий спектр задач – от мониторинга и картографирования до логистики и обеспечения безопасности [1]. Их развитие невозможно без комплексного применения цифровых технологий, специализированного программного обеспечения и искусственного интеллекта (ИИ).

Однако широкое внедрение автономных платформ неизбежно сопровождается ростом киберугроз. БПС постоянно обмениваются данными — как между отдельными устройствами, так и с наземными пунктами управления. Передача телеметрии, видеопотоков и управляющих команд делает беспилотники уязвимыми для перехвата, подмены и атак «человек посередине». В связи с этим одной из актуальных задач становится разработка и внедрение инновационных методов защиты информации.

Одним из перспективных направлений в обеспечении безопасности БПС является использование стеганографических технологий и нейросетевых алгоритмов, изначально созданных для скрытой передачи данных в мультимедиа, но адаптируемых к задачам киберустойчивости беспилотных систем.

Рассмотрим основные модели стеганографических систем на основе нейронных сетей:

1) Нейросетевые архитектуры для скрытой передачи данных

Классические стеганографические системы на основе архитектуры «кодер–декодер» нашли широкое применение в компьютерном зрении для сокрытия изображений внутри других изображений [2]. Перенос этих подходов в сферу БПС позволяет встроить секретные данные (например, ключи аутентификации или управляющие пакеты) внутрь видеопотока с камер дрона.

Достоинства архитектуры:

– высокая скрытность информации;

– возможность передачи по уже существующим каналам;

– устойчивость к шумам и помехам.

При этом важным ограничением остаётся значительная вычислительная нагрузка, что требует оптимизации программного обеспечения для применения на платформах с ограниченными ресурсами.

2) Генеративно-состязательные сети (GAN) и адаптивная маскировка

Генеративно-состязательные сети (GAN) [3] обеспечивают принципиально новый уровень скрытой передачи данных. В их основе лежит взаимодействие генератора и дискриминатора: первый формирует маскированный поток, а второй обучается его распознавать [4].

Для БПС это означает возможность динамической адаптации каналов связи. GAN позволяют:

– маскировать сигналы под легитимные данные;

– обеспечивать устойчивость к анализу со стороны противника;

– имитировать обычный трафик, скрывая управляющие команды.

Таким образом, применение GAN способно значительно повысить защищённость связи при выполнении беспилотниками критически важных миссий.

3) Обратимые нейросети и гарантированное восстановление информации

Особое значение для БПС имеют обратимые нейросети [5], которые позволяют не только встроить информацию, но и полностью восстановить её без потерь. Это критически важно в условиях, когда утрата даже небольшой части управляющих данных может привести к потере контроля над системой.

Алгоритмы этого класса обеспечивают:

– точность передачи критически важных данных;

– устойчивость к шумам и помехам;

– снижение риска разрушения информационного пакета при атаках.

Однако главным недостатком является высокая вычислительная сложность и трудоёмкость обучения моделей.

4) Перенос стилей и интеллектуальная маскировка

Методы переноса стиля [6] в компьютерном зрении позволяют адаптировать визуальные характеристики объектов. В контексте БПС это направление может применяться не только для обработки изображений, но и для камуфляжа беспилотников в визуальном диапазоне.

В частности, дрон может менять стиль отображаемых сигналов или даже внешнего облика (например, в инфракрасном спектре), что позволяет повысить скрытность при выполнении задач разведки и мониторинга.

Использование стеганографических и нейросетевых подходов в БПС позволяет решать следующие задачи:

– защита каналов управления от перехвата и подмены;

– устойчивость к атакам «человек посередине» и стеганоанализу;

– повышение защищённости в условиях активных помех;

– снижение риска компрометации миссий.

При этом необходимо учитывать и потенциальные угрозы:

– возможность использования тех же технологий противником для скрытой передачи вредоносных команд;

– высокая вычислительная нагрузка на бортовое ПО;

– риск ошибок моделей при обучении, ведущих к снижению уровня защиты.

В перспективе интеграция цифровых технологий и ИИ в БПС будет развиваться в направлении:

1. Оптимизации программного обеспечения – разработка лёгких нейросетевых моделей, способных работать на встраиваемых платформах.

2. Адаптивных систем безопасности – использование самообучающихся алгоритмов, реагирующих на новые типы атак.

3. Интеграции с криптографическими методами – объединение стеганографии с шифрованием для создания комплексной защиты.

4. Развития нормативной базы — формирование стандартов кибербезопасности для беспилотных систем.

Цифровые технологии и искусственный интеллект формируют основу для нового уровня безопасности в беспилотных системах. Перенос и адаптация стеганографических методов на основе нейросетей

позволяют создать устойчивые, скрытные и интеллектуальные системы защиты информации. Несмотря на высокую вычислительную сложность и потенциальные риски, такие подходы открывают перспективы формирования по-настоящему киберустойчивых беспилотных платформ, способных эффективно функционировать в условиях современных угроз.

ЛИТЕРАТУРА

1. Islam S., Karam A., Boualem A., Valli Pathan K. 6G-Enabled Network Security in Drone Technology: Revolutionizing Communications and Enhancing Security Applications // Nordic e-Infrastructure Tomorrow. Tallinn, Estonia, May 27–29, 2024 – p. 28-44.
2. Baluja S. Hiding Images in Plain Sight: Deep steganography Advances in Neural Information Processing Systems. In: NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems, Long Beach California, USA, December 4 - 9, 2017. – NY: Red Hook, 2017. – P. 2069–2079.
3. Goodfellow Ian J. et al. Generative adversarial nets Proceedings. In: Neural Information Processing Systems. 2014 – p. 2672–2680.
4. Zhang R., Dong, S. & Liu, J. Invisible steganography via generative adversarial networks. Multimed Tools Appl. 2019 – p. 8559–8575.
5. Guan Z. et al. DeepMIH: Deep Invertible Network for Multiple Image Hiding. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 1 Jan. 2023 – p. 372–390.
6. Bi X. et al. High-capacity image steganography algorithm based on image style transfer. Security and Communication Networks. 2021 – p.1–14.

УДК 003.26;004.056

ОСОБЕННОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ СОКРЫТИЯ ИНФОРМАЦИИ В СЕТЕВОМ ТРАФИКЕ

А. Н. НИКОЛАЙЧУК
Белорусский государственный технологический университет
Минск, Беларусь

Взаимодействие между любыми устройствами в сети подчиняется правилам, которые определены стеком (набором) протоколов TCP/IP. Согласно этим правилам, предмет передачи (текст, изображение и т.д.)