**УДК 004.042**

# Исследование и разработка метода безопасного мониторинга для Internet of Things

**Казакова Е.С.**
Санкт-Петербург, Университет ИТМО
**Научный руководитель – доцент, Донецкая Ю.В.**
Санкт-Петербург, Университет ИТМО

**Аннотация.**
Системы мониторинга предназначены для сбора и обработки больших данных и являются основной частью интеллектуальной среды. В данной работе предлагается метод для повышения безопасности Internet of Things (IoT) при мониторинге данных путем внедрения политики безопасности, протокола MQTT и безопасной архитектуры Fog/Edge.

## Введение.

Несмотря на достижения в области безопасности IoT, большинство распространённых на рынке систем не лишено множества уязвимостей. Один из основных таких классов уязвимостей можно обнаружить при мониторинге информации. Системы мониторинга предназначены для сбора и обработки больших данных о и являются основной частью интеллектуальной среды. В процессе работы используются программные агенты, выполняющие сбор данных, очистку, кластеризацию, сравнение временных рядов, извлечение данных для визуализации, подготовку диаграмм и отчетов, выполнение пространственного анализа и др. Собираются большие сенсорные данные и другая разнородная информация из других источников (метеостанции, системы видеонаблюдения, оборудование мобильной связи, встроенное автомобильное навигационное оборудование и т.д.). Из-за этого мультиагентный подход целесообразно использовать для сбора больших объемов данных и интеллектуального анализа данных и вообщем для реализации процедур мониторинга в целом. Мониторинг это регулярное наблюдение и регистрация мероприятий, проводимых в рамках проекта или программы. Но из-за постоянного взаимодействия агентов с серверными компонентами системы мониторинга, происходит понижение конфиденциальности и целостности системы.

## Основная часть.

В данной работе предлагается внедрение решений для повышения безопасности IoT при мониторинге данных путем внедрения политики безопасности, протокола MQTT и других шагов для реализации централизованного регулятора для мониторинга действий между устройствами IoT и выявления подозрительной вредоносной активности для дальнейшего расследования. Применение данных решений приводит к меньшим рискам возникновения ошибок безопасности, при этом существенная часть системного и прикладного программного обеспечения реализована с сокращением задержки передачи и объема передаваемых данных. Обеспечение контроля доступа к памяти за счет облачной архитектуры и инструментов сетевого мониторинга позволяет минимизировать количество ошибок, возникающих на уровне мониторинга из-за некорректного использования средств управления памятью. В рамках данной работы рассматриваются протоколы для IoT, а также предлагается метод, совместно использующий реализованные в них концепции систем

IDS/IPS, регулярного мониторинга сетевых ресурсов и их распределения и безопасной архитектуры Fog/Edge.

**Выводы.**

Внедрение решений, основанных на новых технологиях, таких как Fog/Edge и IoT, требует изучения аспектов кибербезопасности для оценки соответствующих мер по обеспечению безопасности инфраструктуры. В данной работе представлена и проанализирована реализация инфраструктуры IoT и облака для мониторинга данных интеллектуальной среды с точки зрения кибербезопасности. Предлагаемое решение основано на широко используемых инструментах, таких как протоколы OpenHAB, Mosquitto и MQTT/MQTTS. Здесь они объединены в новую безопасную и экономичную платформу, основанную на частном облаке и одноплатных компьютерах для мониторинга и управления интеллектуальной системой. Связь осуществляется с помощью протокола MQTT. Меры кибербезопасности, необходимые для защиты обмена сообщениями, были проанализированы и оценены с точки зрения затрат на производительность и с учетом ошибок безопасности, возникающих во время мониторинга. Предлагаемое решение позволяет реализовать экономически эффективную платформу для конкретного варианта использования с защищенными компонентами и коммуникациями, сокращая используемые ресурсы, но способную гарантировать требования кибербезопасности и ограничения по времени связи в случае использования. Этот анализ направлен на решение проблемы безопасности по принципу проектирования, когда меры кибербезопасности должны быть рассмотрены и реализованы, начиная с первых этапов развития инфраструктуры.

Казакова Е.С. (автор) _____

Донецкая Ю.В. (научный руководитель) _____