АЛГОРИТМ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ

Дорогина А.С., студент гр. 940401, Земсков Г.А., студент гр. 940401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Половеня С.И. – канд. техн. наук, доцент

Аннотация. В тезисе рассматривается алгоритм обеспечения кибербезопасности сети интернета вещей.

Интернет вещей (далее ИВ) – это сеть устройств, которые обмениваются данными и информацией между собой без участия человека, используя различные технологии связи, такие как Wi-Fi, Bluetooth, NFC и др. ИВ могут быть оснащены разнообразными устройствами, такими как датчики и исполнительные устройства, для сбора, передачи и анализа данных, а также управления другими устройствами. ИВ применяется во многих областях, включая умный дом, здравоохранение, медицина, транспорт и промышленность, и является важным элементом концепции "Умного города".

Кибербезопасность ИВ является критически важной задачей, так как устройства ИВ могут быть подвержены различным видам кибератак. Например, злоумышленники могут захватывать ИВ-устройства для использования их в качестве ботнетов для DDoS-атак, украсть личные данные пользователей, перехватить данные, передаваемые между устройствами ИВ, и многое другое. Поэтому важно разработать алгоритмы обеспечения кибербезопасности ИВ, которые будут гарантировать безопасность и конфиденциальность передаваемых данных, защищать устройства от несанкционированного доступа и обеспечивать целостность системы в целом.

Общая структурная схема обнаружения уязвимости сети ИВ [2] приведена на рисунке 1.

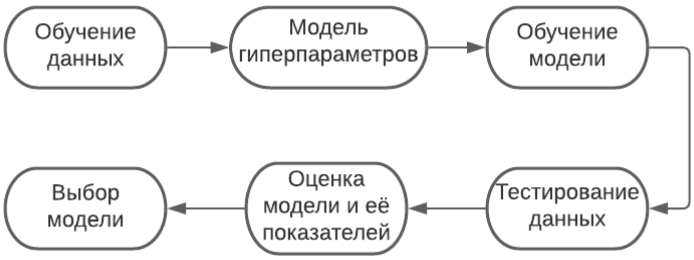

Рисунок 1 – Структурная схема обнаружения уязвимости сети ИВ

Обучение данных: в этом шаге мы собираем данные из устройств ИВ и подготавливаем их для обучения модели (предобработка данных, т.е. очистка, преобразование и масштабирование).

Модель гиперпараметров: здесь мы выбираем модель машинного обучения и определяем ее гиперпараметры.

Обучение модели: в этом шаге мы обучаем модель на подготовленных данных (использование методов обучения, таких как классификация, регрессия или кластеризация).

Тестирование данных: после обучения модели мы тестируем ее на независимых данных, чтобы оценить ее производительность и обнаружить возможные проблемы.

Оценка модели и ее показателей: в этом шаге мы оцениваем производительность модели, используя различные метрики, такие как точность, полноту и другие.

Выбор модели: на основе результатов оценки мы выбираем модель, которая дает наилучшую производительность на тестовых данных, и применяем ее для обнаружения уязвимостей в сети ИВ.

Кибератаки могут представлять серьезную угрозу для безопасности сетей ИВ. Для предотвращения таких атак существуют различные методы защиты. Однако, поскольку существует множество типов кибератак, необходимо использовать различные меры защиты в зависимости от типа атаки.

Алгоритм обеспечения кибербезопасности сети ИВ изображен на рисунке 2. Алгоритм описывает процесс обеспечения кибербезопасности сети ИВ, начиная с настройки системы обнаружения вторжений и добавления устройств. Затем происходит определение уязвимости для каждого устройства по его IP-адресу. Если обнаруживается кибератака, система определяет тип атаки и пытается устранить ее. В остальных случаях система продолжает работать в нормальном режиме, обеспечивая безопасность сети.

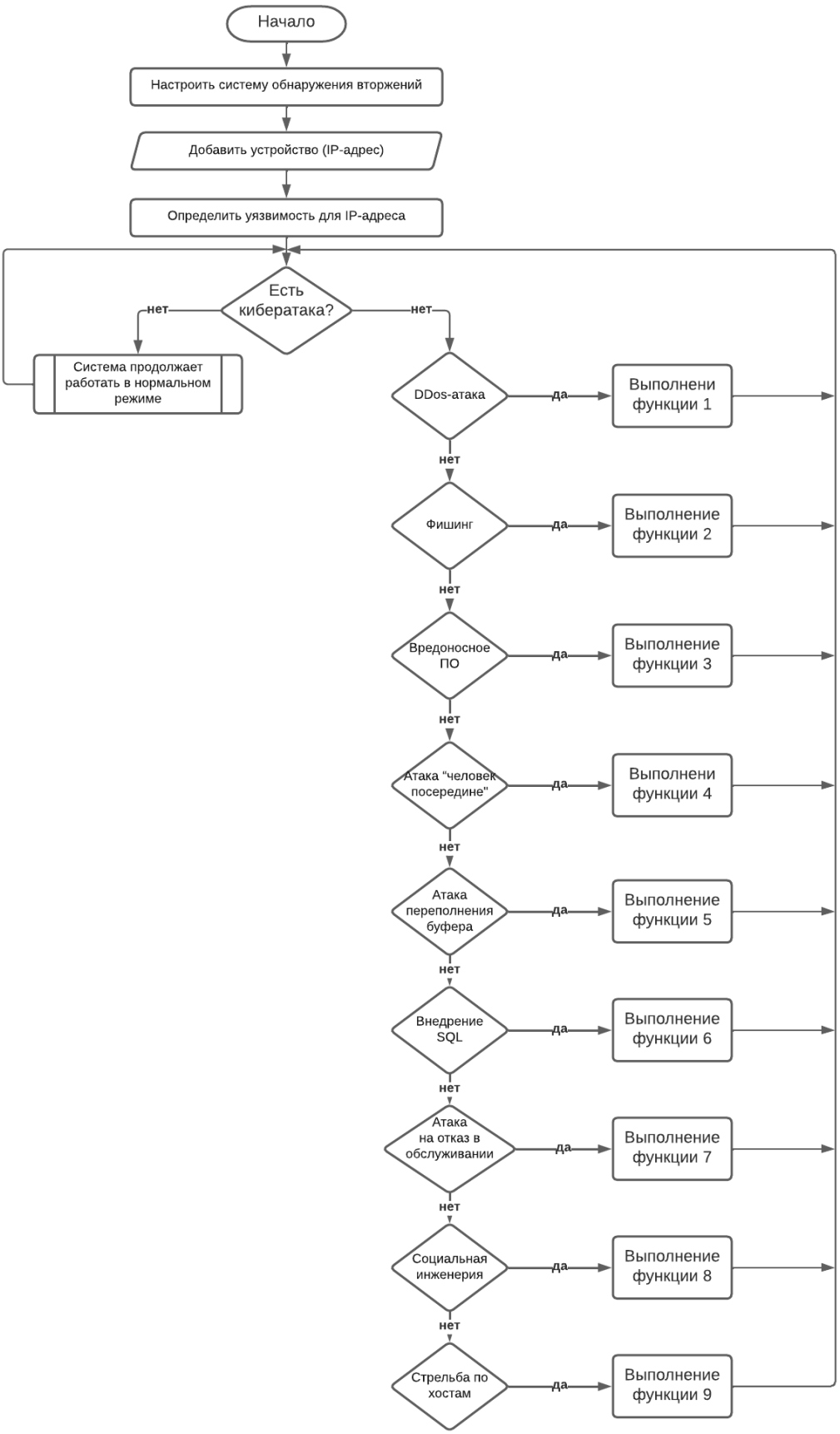

Рисунок 1 – Алгоритм обеспечения кибербезопасности сети ИВ

Борьба с различными типами кибератак может варьироваться в зависимости от конкретного типа атаки и используемых средств защиты.

Например, для борьбы с фишингом необходимо обучать пользователей распознавать подозрительные письма и ссылки, а также использовать проверенные источники для ввода своих личных данных. Для борьбы с вредоносным ПО, следует использовать антивирусное ПО и избегать загрузки программ из ненадежных источников. Для защиты от DDoS-атак, необходимо использовать специальное ПО, которое блокирует потоки нежелательного трафика. Для борьбы с SQL-инъекциями, следует использовать проверку вводимых пользователем данных и форматирование SQL-запросов. Для защиты от кражи учетных данных, следует использовать сложные пароли и двухфакторную аутентификацию.

Результаты исследования алгоритма кибербезопасности сети интернета вещей могут привести к повышению безопасности сети Интернета вещей в целом. Благодаря исследованию можно выявить уязвимости в существующих алгоритмах и предложить улучшения и дополнения, которые помогут защитить сеть от кибератак. Кроме того, результаты исследования могут использоваться для обучения персонала, занимающегося кибербезопасностью, а также для разработки новых продуктов и услуг, связанных с Интернетом вещей.

Список использованных источников:

1. *Ли П. Архитектура интернета вещей/ пер. с анг. М.А. Райтмана. – М.: ДМК Пресс. – 2019. – 454 с.*
2. *Кибербезопасность ИВ с помощью машинного обучения [Электронный ресурс]. – Режим доступа https://github.com/harshilpatel1799/Iot-Cyber-Security-with-Machine-Learning-Research-Project/blob/master/Project_Part_1.pdf. – Дата доступа: 11.04.2023*