DOI 10.36622/VSTU.2023.4.26.006
УДК 004.735

МОДЕЛЬ ПЕРЕХВАТА И ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, П.А. Анцупов, А.Г. Чурсин

Беспроводные сети широко используются во всех сферах нашей жизни обеспечивая доступ к интернету и другим сетевым ресурсам. На базе беспроводных сетей строятся сети интернета вещей, а в связи с экспоненциальным распространением включения в Интернет различных вещей, устройств и датчиков возникают различные риски безопасности систем, в том числе связанные с перехватом информации в беспроводных сетях. Цель работы – защита информации беспроводных IoT устройств от атак, направленных на выведение из строя и до ведения до отказа вещей в сети предприятия. В статье предложена модель перехвата информации, состоящая из беспроводной распределенной компьютерной сети предприятия, имеющей IoT устройства, в которые после успешной атаки загружается вредоносная программа Mirai. В процессе исследования предложена модель защиты информации с применением системы обнаружения вторжения.

Ключевые слова: беспроводные сети, Интернет Вещей, перехват и защита информации, Wi-Fi 6, распределенные сети, DDoS, системы обнаружения вторжений, IDS.

Введение

Беспроводные сети широко используются во всех сферах нашей жизни обеспечивая доступ к интернету и других сетевым ресурсам. Беспроводные сети, одна из самых актуальных новинок IT-технологий [1]. В данной работе рассматриваются сети промышленного интернета вещей (Industrial Internet of Things, IIoT), построенных с использованием сети Wi-Fi, а конкретно последний стандарт беспроводной связи Wi-Fi 6, так же известный как 802.11ax. Разработчики из Cisco, ведущего разработчика сетевых технологий пишут о том, как Wi-Fi 6 делает беспроводные сети быстрее, умнее и эффективнее [2], что в свою очередь влияет и на производительность IIoT устройств.

Преимущества Wi-Fi 6 [3]:

1. Более высокая скорость передачи данных: Wi-Fi 6 обеспечивает более высокую скорость передачи данных по сравнению с предыдущими версиями. Это особенно полезно для работы с большим объемом данных, что несомненно полезно при построении сети промышленного интернета вещей, где используется огромное количество датчиков и сенсорных устройств.

2. Более высокая емкость сети: Wi-Fi 6 имеет возможность подключать устройств к сети без ухудшения производительности. Это особенно важно в современных сетях с большим количеством подключенных устройств.

3. Улучшенная производительность в условиях загруженной сети: Wi-Fi 6 использует технологии, такие как OFDMA (ортогональное разделение частотного разделения множества доступа), чтобы эффективно использовать доступную пропускную способность и улучшить производительность сети в условиях высоких нагрузок.

4. Эффективность энергопотребления: Wi-Fi 6 включает в себя функцию Target Wake Time, которая позволяет устройствам "спать" и "просыпаться" для проверки сигнала, что снижает энергопотребление и увеличивает время работы от батареи.

Недостатки Wi-Fi 6:

1. Ограниченная совместимость: устройства, не поддерживающие Wi-Fi 6, не получат преимущества этой технологии. Большинство старых устройств поддерживают только предыдущие стандарты Wi-Fi, поэтому

владельцы этих устройств не смогут в полной мере использовать Wi-Fi 6.

2. Более высокая стоимость: оборудование поддержки Wi-Fi 6 может быть более дорогим по сравнению с предыдущими версиями Wi-Fi. Это может ограничить доступность и принятие новой технологии.

3. Влияние окружающей среды: Wi-Fi 6 работает на более высоких частотах, что означает, что его сигнал может быть менее устойчивым и меньше проникать сквозь стены и препятствия, по сравнению с низкочастотными сетями. Это может ухудшить качество сигнала и производительность в некоторых условиях, особенно в больших зданиях или на больших расстояниях от маршрутизатора.

Изучив все преимущества сетей Wi-Fi 6 можно сделать вывод об актуальности их использования для сетей IIoT, а высокая цена оборудования по мере распространения технологии будет снижаться, так как повсеместный переход на новую технологию неизбежен из-за высокой загрузки современных беспроводных сетей, стандарт 802.11ax решает эту проблему. Wi-Fi 6, хотя и предлагает улучшенные функции безопасности, стандарт также сталкивается с проблемами информационной безопасности такими как уязвимости в протоколе безопасности WPA3, который включен в Wi-Fi 6 [4], DDoS-атаки, атаки на устаревшие устройства, не обновленные до новейших стандартов безопасности и т.д.

Исходя из представленного выше в работе предлагается рассмотреть модель перехвата информации для сетей промышленного интернета вещей, построенных на базе сети IEEE 802.11ax, и разработать модель защиты от перехвата информации.

Уязвимости беспроводных сетей.

Важнейшей задачей в области информационной безопасности является обнаружение и устранение уязвимостей. Наличие слабых мест или незащищенности в системе на программном или аппаратном уровне будет использоваться злоумышленниками для нарушения безопасности или выполнения несанкционированных действий. Уязвимости возникают из-за ошибок в коде, при неправильном конфигурировании или проектировании. Беспроводным сетям стандарта IEEE 802.11 присуще уязвимости, связанные с недостатками процесса функционирования, свойствами архитектуры сети, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратной платформой [1].

Беспроводные сети стандарта IEEE 802.11ax подвержены таким уязвимостям как:

1) уязвимости среды передачи,
2) уязвимости систем аутентификации,
3) уязвимости криптографических протоколов,
4) уязвимости используемого программного обеспечения,
5) уязвимости, связанные с человеческим фактором.

Исходя из перечисленных уязвимостей образуются различные модели и виды атак на беспроводные сети.

Угрозы Индустриального Интернета Вещей, реализованного с использованием беспроводных сетей.

Сети IIoT построенные с использованием беспроводных технологий подвергнуты угрозам, описанным ниже.

Угрозы, связанные с отказом или выходом системы из строя:

а) отказ системы умного города может вызвать проблемы с управлением транспортной инфраструктурой и общественными службами, такими как управление светофорами, обработка отходов, контроль загрязнения воздуха и другие аспекты, влияющие на повседневную жизнь горожан.

б) выход из строя системы умного хозяйства в промышленных предприятиях может привести к простоям в производстве и убыткам для компаний, так как многие процессы могут быть автоматизированы и контролируемы с использованием IoT.выход из строя системы умного производства может повлиять на процессы производства и предоставление услуг в различных отраслях, таких как автомобильная, аэрокосмическая, машиностроительная и другие.

в) отказ системы умной энергетики может привести к потере управления и контроля над энергосистемой, что может негативно сказаться на энергоэффективности, безопасности и доставке энергетических услуг.

г) отказ системы умной логистики может затруднить отслеживание грузов и управление поставками, что может привести к задержкам в доставке товаров и потере доверия партнеров и клиентов.

Угрозы, связанные с умышленным действием:

а) кибератаки: Хакеры могут проникнуть в систему умного устройства и осуществить кибератаки на другие устройства, сети или даже государственные системы.

б) кража личной информации: Умные устройства собирают и обрабатывают большое количество личных данных, которые могут стать целью для хакеров и злоумышленников в целях вымогательства, мошенничества или идентификационной кражи.

в) физические повреждения: Атаки на умные устройства могут привести к физическим повреждениям системы, которые могут вызвать аварию или пожар.

г) нарушение конфиденциальности: Злоумышленники могут перехватывать и регистрировать передачу данных от умного устройства, нарушая приватность и конфиденциальность пользователей.

д) спам и мошенничество: Хакеры могут использовать умные устройства для массовой отправки спама или для проведения мошеннических операций, таких как фишинг или фальшивые транзакции.

е) отключение устройств: Атаки на центральные серверы или инфраструктуру IoT могут привести к временному или постоянному отключению устройств, что может создать серьезные проблемы для пользователей.

ж)вмешательство в работу системы: Хакеры могут изменять настройки или контролировать работу умного устройства, влияя на его функциональность и возможности.

з) злоупотребление ресурсами: Хакеры могут использовать умные устройства для массовых атак или для майнинга криптовалюты, что может привести к перегрузке серверов и повышению энергопотребления.

Угрозы, связанные с подслушиванием, перехватом, кражей информации:

а) распространение вредоносных программ и вирусов: Индустриальные устройства интернета вещей могут быть подвержены атакам злоумышленников, которые могут распространять вредоносные программы и вирусы, позволяющие им подслушивать или перехватывать информацию.

б) взлом устройств: Злоумышленники могут взломать IoT-устройства и получить доступ к ним, чтобы перехватывать и красть информацию. Некоторые устройства, такие как умные замки или системы безопасности, могут быть использованы для несанкционированного доступа к помещениям или сетям.

в) необходимость установки обновлений программного обеспечения: Множество IoT-устройств требует обновлений программного обеспечения для исправления уязвимостей и обеспечения безопасности данных. Однако, если эти обновления не устанавливаются правильно или не делаются вовремя, это может привести к возникновению уязвимостей и возможности кражи информации.

г) слабые или неправильные настройки безопасности: Некоторые устройства IoT имеют слабые или недостаточно настраиваемые параметры безопасности по умолчанию. Злоумышленники могут использовать эти уязвимости, чтобы получить доступ к информации и перехватить данные.

д) нехватка шифрования данных: Если данные, передаваемые через IoT-устройства, не зашифрованы должным образом, они могут быть подвержены перехвату и краже. Это особенно критично для данных о персональной жизни, таких как медицинские записи или финансовая информация.

е) сетевые атаки: Многие устройства IoT подключены к сетям и могут быть атакованы через них. Злоумышленники могут использовать различные виды атак, таких как отказ в обслуживании (DDoS) или атаки

маршрутизации, чтобы перехватывать информацию и краденые данные.

Существующие меры защиты от сетевых атак типа отказ от обслуживания (DDoS)

В данной статье были исследованы меры защиты от DDoS атак, которые представляют собой рекомендации, следование которым снижает риск атак. Рассмотрим основные рекомендации.

Для защиты от атак типа отказ от обслуживания CVSS рекомендует:

1. Устанавливать системы обнаружения (IDS) и системы предотвращения (IPS) атак, функция данных систем — это способность к обнаружению подозрительного трафика и его блокированию.
2. Периодическое обновление программного обеспечения (ПО) для устранения известных уязвимостей.
3. Использование брандмауэров для защиты сетевых устройств.
4. Расчет количества запросов/соединений, обрабатываемых сервером для балансировки нагрузки и предотвращения перегрузки системы.
5. Ограничение количества запросов для одного источника, для предотвращения перегрузки системы из-за одного злоумышленника.
6. Постоянный мониторинг трафика с использованием системы журналирования и обнаружения аномалий, для нахождения подозрительной активности и принятия советующих мер.
7. Отключение открытых портов и неиспользуемых сервисов, чтобы уменьшить поверхность атаки.
8. Резервирование данных и составление плана восстановления после атаки для минимизации возможного ущерба от DDoS атаки.

Меры и рекомендации Федеральной службы технического и экспортного контроля (ФСТЭК):

1. Разработка и применение политики безопасности.
2. Использование ПО и аппаратных средств, для обнаружения и отражения атак.
3. Регулярный анализ и мониторинг трафика для выявления аномального поведения и потенциальных атак.
4. Обеспечение высокой пропускной способности, что в свою очередь позволяет справиться с высоким уровнем трафика во время атаки.
5. Обучение персонала и сотрудников основам информационной безопасности и мерам предотвращения атак.
6. Резервное копирование данных.
7. Незамедлительное реагирование в случае детектирования DDoS атаки: блокировка IP-адресов и перераспределение нагрузки.

Рекомендации национального института стандартов и технологий (NIST) включают в себя:

1. Разработку и реализацию стратегии защиты от атак.
2. Изучение сети и выявление слабых мест для разработки архитектуры сети, на которую атаки типа DDoS будут иметь меньшее воздействие.
3. Установку систем мониторинга и IDS.
4. Реализацию механизма фильтрации, блокирующего пакеты от потенциально вредоносных источников.
5. Использование услуг Content Delivery Network (CDN) для смягчения эффекта атаки.
6. Распределение сети на разных физически и географически разделенных серверах.
7. Разработку политик безопасности, определяющих допустимое поведение пользователей в сети.
8. Обучение персонала.Резервное копирование.
9. Сотрудничество с провайдерами для обмена информации с области сетевой безопасности.

Рекомендации, описанные выше, имеют сходства и различия, описные в табл. 1

Таблица 1

Рекомендации для защиты от атак типа отказ в обслуживании

Рекомендация/ источник	CVSS	ФСТЭК	NIST
Разработка политики безопасности	Отсутствует	Имеется	Имеется
Установка систем обнаружения и предотвращения атак	Имеется	Имеется	Имеется
Обновление программного обеспечения	Имеется	Отсутствует	Отсутствует
Использование брандмауэров	Имеется	Отсутствует	Отсутствует
Расчет количества запросов/соединений, обрабатываемых сервером	Имеется	Отсутствует	Отсутствует
Ограничение количества запросов для одного источника	Имеется	Отсутствует	Отсутствует
Постоянный мониторинг трафика	Имеется	Имеется	Имеется
Отключение открытых портов и неиспользуемых сервисов	Имеется	Отсутствует	Имеется
Резервирование данных	Имеется	Имеется	Имеется
Разработка и применение политики безопасности.	Отсутствует	Имеется	Имеется
Использование ПО и аппаратных средств	Имеется	Имеется	Имеется
Обеспечение высокой пропускной способности	Отсутствует	Имеется	Имеется
Обучение персонала и сотрудников основам информационной безопасности	Отсутствует	Имеется	Имеется
Незамедлительное реагирование в случае детектирования DDoS атаки	Отсутствует	Имеется	Отсутствует
Распределение сети на разных физически и географически разделенных серверах	Отсутствует	Отсутствует	Имеется
Разработку политик безопасности, определяющих допустимое поведение пользователей	Отсутствует	Отсутствует	Имеется

Представленные рекомендации снижают риск DDoS атаки с высокого уровня до среднего, но не могут полностью защитить сеть промышленного интернета вещей от атак направленных на использование уязвимостей протокола через SYN-флуд.

Модель перехвата информации в беспроводных сетях IIoT.

Предлагаемая модель перехвата информации представляет из себя сеть Промышленного Интернета Вещей, на которую производится DDoS-атака с целью перегрузки сети предприятия, для скрытой загрузки вредоносного программного обеспечения на IoT устройства. Сеть предприятия представлена на рис. 1. В ее состав входит. IoT устройства, беспроводная точка доступа WI-FI 6, маршрутизатор, база данных и администратор сети, также имеется выход в сеть Интернет.

После успешной DDoS-атаки устройства IoT заражаются и объединяются в ботнет, который в последствии используется для хакерских DDoS-атак, перегружая серверы других предприятий для нарушения их работы или затруднения доступа к этим ресурсам [5].

Вредоносной программой служит Mirai – троянская программа, маскирующаяся под легитимное программное обеспечение, направленная для захвата устройств Интернета Вещей, так как это недорогие устройства, со слабой защитой и неизменяемыми заводскими настройками.

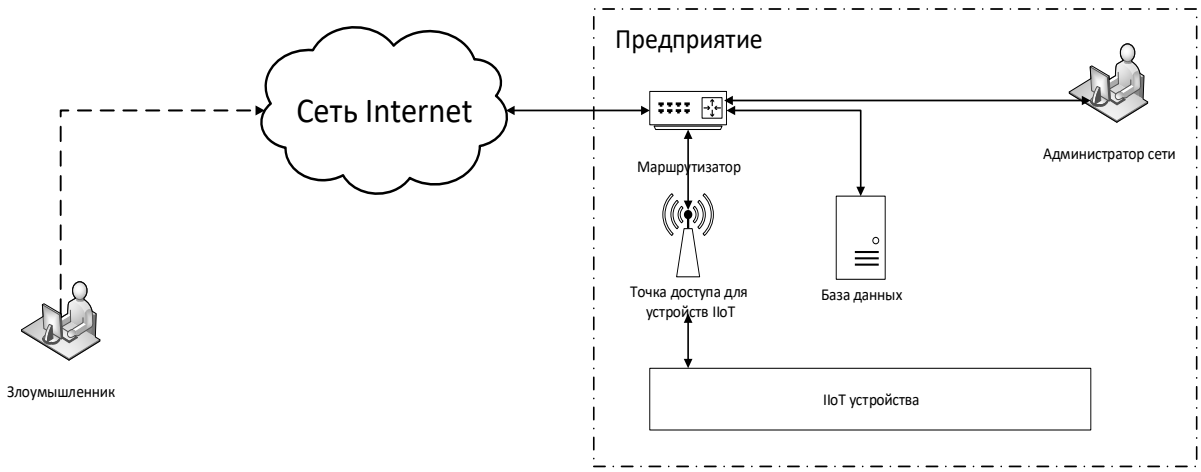

Рис. 1 Модель заражения сети предприятия, заражаемого ботнетом Mirai

Модель защиты информации в беспроводных сетях IIoT.

В связи с увеличением количества IoT-устройств, подключенных к сети, и передаваемых данных, которая может содержать конфиденциальную информацию, возникает риск утечки безопасности. Злоумышленники могут попытаться проникнуть в сеть и получить несанкционированный доступ к конфиденциальным данным или даже нанести ущерб системе.

Для предотвращения таких инцидентов важно использовать эффективную модель защиты информации. Одной из таких моделей является применение системы обнаружения вторжений. IDS — это программное или аппаратное оборудование, которое анализирует сетевой трафик и обнаруживает попытки несанкционированного доступа или аномалии в сети.

IDS в беспроводных сетях IIoT способна обнаружить различные виды атак, включая отказ в обслуживании (DoS), подмену данных, перехват трафика и другие. Она работает на основе заранее настроенных правил и алгоритмов, которые позволяют ей анализировать сетевой трафик и определять необычные или подозрительные активности.

Помимо обнаружения атак, IDS также может предоставить ценную информацию о событиях в сети, которая может быть использована для улучшения безопасности и принятия решений. Она может помочь идентифицировать уязвимые места в сети и предложить рекомендации по улучшению безопасности.

Основными компонентами модели защиты информации с применением IDS являются:

1. Сенсоры IDS: устройства, которые устанавливаются в беспроводных сетях IIoT и собирают информацию о сетевом трафике. Сенсоры мониторят и анализируют пакеты данных, чтобы обнаружить потенциальные атаки или аномалии.

2. Центр управления IDS: центральный узел, который получает данные от сенсоров IDS и анализирует их. Центр управления может выполнять различные функции, включая обнаружение атак, генерацию предупреждений или автоматическое реагирование на инциденты.

3. База данных IDS: здесь хранится информация о предыдущих атаках, аномалиях и обнаруженных уязвимостях. База данных позволяет IDS проводить сравнение текущего сетевого трафика с предыдущими событиями и определять потенциальные угрозы.

4. Анализаторы IDS: программное обеспечение, которое проводит анализ данных, собранных сенсорами IDS. Анализаторы применяют различные алгоритмы и правила для определения атак и аномалий в сетевом трафике.

Преимущества модели защиты информации в беспроводных сетях IIoT с применением IDS включают:

1. Обнаружение атак: IDS позволяет обнаружить различные виды атак, включая

известные и новые угрозы. Это позволяет оперативно реагировать на инциденты и предотвращать потенциальный ущерб для системы.

2. Анализ сетевого трафика: IDS анализирует сетевой трафик и может предоставить ценную информацию о событиях в сети. Это помогает идентифицировать уязвимые места и предлагает рекомендации по улучшению безопасности.

3. Проактивная защита: IDS может предупредить о потенциальных угрозах до их реализации. Это позволяет принимать меры по предотвращению атак и снижению рисков.

4. Централизованное управление: Модель защиты информации с применением IDS предоставляет централизованное управление безопасностью в беспроводных сетях IIoT. Это облегчает мониторинг и управление безопасностью системы.

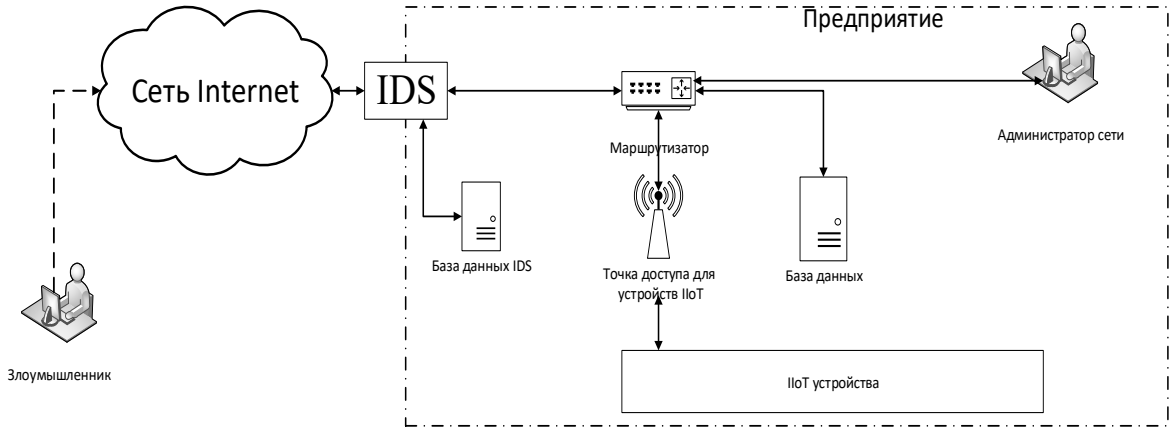

Рис. 2. Модель защиты сети предприятия с применением системы обнаружения вторжений для защиты от вредоносного трафика

Заключение

В данной статье рассмотрены вопросы повышения защищенности информации в беспроводных распределенных сетях промышленного интернета вещей. Был проведен анализ уязвимостей беспроводных сетей, на примере атак с использованием DDoS и ботнета Mirai. Необходимо выделить, что недостаточность мер защиты несет за собой материальный, репутационный ущерб, а также технические сбои работы в беспроводных распределенных компьютерных сетях. По результатам анализа принципов работы системы противодействия вторжений отмечена необходимость использования IDS для повышения мер защиты компьютерной сети и конфиденциальных данных. Также была выработана модель обеспечения защиты беспроводной РКС на примере предприятия, использующего IoT-устройства.

Список литературы

1. Щербаков В.Б. Безопасность беспроводных сетей: стандарт IEEE 802.11 / В.Б. Щербаков, С.А. Ермаков; под ред. В.И. Борисова. М.: РадиоСофт, 2010. 256 с.

2. The wireless future - «smater, better, and faster» URL: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2021/m02/the-wireless-future-smarte r-better-and-faster-.html (дата обращения 5.11.2023).

3. A tutorial on IEEE 802.11 ax High Effiency WLANSs. URL: https://www.researchgate.net/publication/327785405_A_Tutorial_on_IEEE_80211ax_High_Efficiency_WLANs (дата обращения 5.11.2023).

4. Vanhoef M. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd / M. Vanhoef, E. Ronen. // In 2020 IEEE Symposium on Security and Privacy (SP). 2020. P. 517-533.

5. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures / ENISA. Hague: European Union Agency For Network And Information Security, 2017. 103 p.

6. Ferrag M.A. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. / M.A. Ferrag,

L. Maglaras, S. Moschoyiannis, H. Janicke // Journal of Information Security and Applications. 2020. 50, 10241.

Концерн «Созвездие», г. Воронеж
Concern «Sozvezdie», Voronezh

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 15.11.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», г. Воронеж, e-mail: alexanderostapenkoias@gmail.com

Анцупов Павел Андреевич – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Чурсин Андрей Германович – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

A MODEL OF INTERCEPTION AND PROTECTION OF INFORMATION IN DISTRIBUTED COMPUTER NETWORKS OF THE INDUSTRIAL INTERNET OF THINGS

S.A. Ermakov, P.A. Antsupov, A. G. Chursin

Wireless networks are widely used in all spheres of our life providing access to the Internet and other network resources. The Internet of Things networks are being built on the basis of wireless networks, and due to the exponential spread of the inclusion of various things, devices and sensors on the Internet, various security risks of systems arise, including those associated with the interception of information in wireless networks. The purpose of the work is to protect the information of wireless IoT devices from attacks aimed at disabling and failing things in the enterprise network. The article proposes a model of information interception consisting of a wireless distributed computer network of an enterprise having IoT devices into which, after a successful attack, the Mirai malware is loaded. In the course of the research, a model of information protection using an intrusion detection system is proposed.

Keywords: wireless networks, Internet of Things, interception and protection of information, Wi-Fi 6, distributed networks, DDoS, intrusion detection systems, IDS.

Submitted 15.11.2023

Information about the authors

Sergey A. Ermakov – Cand. Sc (Technical), Head of Department, Concern “Sozvezdie”, Voronezh, email: alexanderostapenkoias@gmail.com.

Pavel A. Antsupov – Graduate Student, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com.

Andrey G. Chursin – Graduate Student, Voronezh State Technical University, email: alexanderostapenkoias@gmail.com.