УДК 004

Якупова И.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

ПРОБЛЕМЫ БЕЗОПАСНОСТИ IOT-УСТРОЙСТВ И НАПРАВЛЕНИЯ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Развитие технологии IoT сопровождается ростом угроз; недостаточная исходная защищенность, слабые и устаревшие протоколы работы IoT- и IIoT-устройств, размытость зоны контроля киберфизических систем с использованием IoT это факторы риска, которые сложно закрыть при традиционном подходе к управлению безопасностью предприятия или кибер-объекта. В статье выполнен анализ проблем безопасности IoT-устройств и изложены пути и методы снижения рисков ИБ, связанных с IoT-устройствами.

Ключевые слова: IoT, интернет вещей, кибербезопасность.

Применение IoT-устройств стало массовым явлением, образуя киберфизические системы умных городов, транспорта и зданий, медицинского интернета вещей и промышленного (IIoT). Так, «IoT Analytics» [3] оценил количество устройств интернета вещей в мире в 2024 г. в 18,8 млрд, в 2025 г. их ожидается 21,5 млрд, а к 2030 г. прогнозируется от 32,1 млрд [4] до 41,1 млрд [3] устройств IoT. При этом активно развивается интеграция с IoT технологий искусственного интеллекта (например, т.н. периферийного ИИ), создавая новые неочевидные уязвимости и усложняя процессы управлениях безопасностью.

Большинство IoT-устройств штатно слабо защищены или не защищены вовсе, а их широкая распространенность привлекает киберхакеров, которые ищут способы эксплуатировать их уязвимости. Технологические цифровые инновации в производстве сопровождаются развитием промышленного интернета вещей, что делает промышленность основной мишенью для атак вредоносного ПО. В 2022 г. число кибератак на IoT выросло на 400 % по сравнению с предшествующим периодом (согласно отчету исследовательской группы Zscaler ThreatLabz [1]); к середине 2024, по оценке Zscaler ThreatLabz, количество лишь заблокированных атак на IoT увеличилось на 45 % по сравнению с 2023 [5], причем эти атаки шли преимущественно на промышленный IoT (в 3 раза чаще, чем на другие отрасли [1]). Анализ методов атак на IoT устройства свидетельствует о разнообразии эксплуатируемых уязвимостей IoT. Комбинирование традиционных и «инновационных» приемов позволяет хакерам обходить стандартные средства защиты и эксплуатировать вновь возникающие уязвимости на стыке технологий. Хакеры применяют вредоносы, в т. ч. шифровальщики (часто это Mirai и Gafgyt), используя уязвимости прошивок и недостаточную защиту операционных систем мобильных платформ, уязвимые протоколы передачи данных [6] (при этом для интернета вещей характерно большое разнообразие протоколов передачи данных, что усложняет защиту и требует стандартизации в этой сфере). Уязвимостями служат и ошибки в конфигурации систем безопасности (в т. ч. облачных центров хранения и обработки производственных данных), позволяя кибервзломщикам получать с помощью IoT доступ к критическим элементам киберфизической инфраструктуры. Хакеры используют социальную инженерию, ИИ-технологии для поиска уязвимостей, длительные скрытые (APT) кибератаки. Среди угроз IoT – эксплуатация аппаратных уязвимостей и недостатков прошивки, DDoS-атаки, заражение вирусами с последующим отказом в обслуживании и поломке оборудования киберфизических систем. Целью киберпреступников является проникновение в промышленные сети, искажение данных, получением контроля над управляющими командами в исполнительных устройствах, изменение в прошивках и программах промоборудования, и как итог – аварии. Стремительная эволюция методов и числа атак на IoT актуализируют проблематику кибербезопасности интернета вещей и

цифровой инфраструктуры с использованием IoT и ИИ, и важность комплексного подхода к защите информации предприятий и другой критической инфраструктуры, постоянное совершенствование методов и средств защиты, новых стратегий противодействия таким угрозам.

Анализ эксплуатируемых уязвимостей IoT показывает, что основными проблемами являются: уязвимости программного обеспечения, базовые настройки IoT-устройств без учета угроз, отсутствие надежной аутентификации, незащищенный выход в интернет, ошибки в конфигурации систем безопасности, отсутствие (или слабые схемы) шифрования данных, когда это необходимо; неправильная настройка сетевых протоколов упрощает [7] злоумышленникам доступ. В результате IoT-устройства оказываются заражены и используются в качестве входных точек для ботнет-атак на корпоративную инфраструктуру. При этом для IoT-устройств, подключаемых через интернет откуда угодно, нет контролируемой зоны, которую можно было бы изолировать традиционными средствами безопасности, что затрудняет контроль и удаленное управление устройством в случае его некорректной работы. IoT-устройства, как правило, невозможно непосредственно защитить, как компьютер или телефон, наложенными средствами защиты от киберугроз, поскольку операционная система если и есть – то упрощенная и несовместимая с традиционными средствами защиты, а разработчики «умных вещей», как правило, не закладывают в них функций информационной безопасности.

Многообразие угроз, реализуемых через IoT, указывает на важность системного подхода к кибербезопасности в отношении IoT-устройств, однако защита IoT на практике нередко возможна лишь на уровне каналов связи (сети, протоколов и средств коммуникации устройства с хранилищем или платформой, использующей данные IoT). Для управления трафиком от IoT к облаку или платформе применяются IoT-шлюзы, в функционал которых входит фильтрация данных от IoT, перевод протоколов, отправка данных в облако или интрасети, а также отслеживание событий безопасности; некоторые IoT шлюзы (например, продукт Kaspersky IoT Secure Gateway [2] предоставляют дополнительный слой защиты и возможность удаленного администрирования IoT-устройствами. Использование защищенных протоколов передачи данных, мониторинг событий безопасности для выявления аномалий помогают отслеживать и нейтрализовать атаки и повышает уровень защиты IoT-устройств. Стратегия защиты требует реализации принципов «нулевого доверия» при выстраивании системы защиты, продуманного конфигурирования настроек безопасности устройств, а также, когда это возможно для IoT, регулярности обновления ПО, применения антивирусов, усиления аутентификации, применения средств доверенной загрузки, средств анализа аномального поведения IoT-устройств. Угрозы для разных IoT-устройств в цифровой инфраструктуре (например, предприятия) должны быть описаны в модели угроз, а меры

защиты IoT-устройств изложены в политике безопасности, как это делается для «традиционных» компонентов объекта.

Список использованных источников:

1. Gandhi V. 2023 ThreatLabz Report Indicates 400 % Growth in IoT Malware Attacks // info.zscaler.com: [сайт]. URL: https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks.

2. Kaspersky IoT Secure Gateway // kaspersky.ru: [сайт]. URL: https://www.kaspersky.ru/enterprise-security/kaspersky-iot-secure-gateway.

3. State of IoT 2024: Number of connected IoT devices growing 13 % to 18.8 billion globally // iot-analytics.com: [сайт]. URL: https://iot-analytics.com/number-connected-iot-devices.

4. Vailshery L. S. Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033 // statista: [сайт]. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

5. Zscaler ThreatLabz 2024 Mobile, IoT, & OT Threat Report. URL: https://newsletter.radensa.ru/wp-content/uploads/2024/12/threatlabz-mobile-iot-ot-report.pdf.

6. Григорьев А.А., Орлов В.С. Современные методы киберзащиты мобильных и IoT-устройств. Новосибирск: Наука, 2021. 310 с.

7. Соколова Е.В. Критическая инфраструктура и информационная безопасность. М.: Инфра-М, 2022. 280 с.

Yakupova I.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

IOT DEVICE SECURITY PROBLEMS AND WAYS TO PROTECT THE INTERNET OF THINGS

Abstract. The development of Internet of Things technologies against the backdrop of a growing threat; reverse initial security, weak and outdated protocols for the operation of IoT and IIoT devices, and the blurring of the control zone of cyber-physical systems using IoT are risk factors that are difficult to close with the traditional approach to ensuring the security of enterprise or cyber facility management.The article analyzes the security issues of IoT devices and outlines ways and methods for reducing information security risks associated with IoT devices.

Keywords: IoT, Internet of Things, Cybersecurity.