DOI 10.36622/VSTU.2023.26.1.002
УДК 004.735

ОЦЕНКА И РЕГУЛИРОВАНИЕ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ АТАКАХ, ИСПОЛЬЗУЮЩИХ УЯЗВИМОСТИ ПРОТОКОЛОВ ПРИКЛАДНОГО УРОВНЯ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Котышенко, А.А. Болгов, Ю.Г. Пастернак, А.Г. Краснобородкин

Предложено методическое обеспечение количественной оценки рисков, а также алгоритмическое обеспечение регулирования рисков нарушения конфиденциальности информации при атаках, использующих уязвимости протоколов прикладного уровня в телекоммуникационных системах Интернета вещей. Разработана модель системы, учитывающая архитектуру и топологию телекоммуникационной системы «умный дом», а также модель угроз, включающая в себя набор уязвимостей и атак для каждого устройства и описание возможностей злоумышленника. Алгоритмическое обеспечение регулирования рисков основано на модели системы «умный дом», построенной по полносвязной топологии, и предназначено для выявления в ней наиболее уязвимых компонентов и формирования набора мер для увеличения защищенности. Полученные результаты в виде численной оценки и алгоритмического обеспечения позволяют адекватно оценить состояние защищенности телекоммуникационной системы «умный дом» и сформировать набор мер по её повышению.

Ключевые слова: умный дом, риск, конфиденциальность, телекоммуникационная система, полносвязная топология.

Введение

Устройства Интернета вещей становятся все более популярными в повседневной жизни. Их можно найти в самых разных отраслях, от заводов до здравоохранения. Широкое распространение технологий и устройств Интернета вещей способствовало появлению нового объекта, который получил название «умный дом», под которым принято понимать комплекс технологий, позволяющих автоматизировать процессы с помощью интеграции систем домашних устройств, выполняющих действия и решающих определенные базовые задачи без человеческого вмешательства [1].

Технология Интернета вещей в системе «умный дом» объединяет различные устройства в единую компьютерную сеть. Эти устройства собирают данные при помощи датчиков, а затем происходит передача данных на другие устройства или в облачную инфраструктуру, доступ к которой пользователи получают различными способами, включая Wi-Fi, спутниковую или сотовую связь, Bluetooth и другие виды связи. Пользователь может удаленно взаимодействовать с устройствами, отправляя команды на выполнение определенных действий, просматривая данные, полученные с датчиков, а также создавая автоматизированные сценарии.

Согласно обновленной оценке исследовательской компании IDC, в 2025 году по всему миру будет насчитываться около 41.6 миллиарда IoT-устройств [2]. При этом по данным «Лаборатории Касперского», с января по июнь 2022 года количество атакованных в России IoT-устройств выросло на 40%. В январе на них было зафиксировано 9 миллионов атак с 12 тысяч уникальных IP-адресов, а уже в июне — почти 13 миллионов атак с 29 тысяч уникальных IP-адресов [3]. Согласно отчету SAM Seamless Network, атаки на маршрутизаторы составляют 46% от всех атак. Также в список наиболее атакуемых устройств вошли VoIP камеры (29%), радионяня (19%), расширители Wi-Fi (2%). Наибольший процент (51%) от общего количества составляют атаки, использующие уязвимости протокола Telnet. Также злоумышленники используют протокол SSH. Процент атак, использующих уязвимости данного протокола, составляет 11% [4].

Ключевое противоречие в проблеме обеспечения безопасности сетей технологии Интернета вещей сосредоточено между несоответствием темпов развития систем Интернета вещей и консервативностью классических методов оценки величины риска, принципы которых сформировались еще до появления этой технологии. Этот факт становится главным драйвером для поиска способов адаптации имеющихся или формирования новых подходов к анализу и управлению рисками в сетях, построенных в соответствии с концепцией Интернета вещей [5].

В связи с этим требуется все больше различного рода оценок и показателей для того, чтобы будущий пользователь данной технологии имел представление об этой сети в целом [6].

Существующие решения по информационной безопасности построенных телекоммуникационных систем не внедрены в достаточном количестве, в то же время статистика компьютерных атак, совершенных в отношении телекоммуникационных систем Интернета вещей, также активно растёт [7].

Большое количество уязвимостей в IoT-устройствах обусловлено несколькими факторами, а именно: отсутствием у производителей устройств достаточного опыта по обеспечению надёжной защиты своей продукции, сложный процесс обновления прошивок и программного обеспечения, большим разнообразием систем, построенных с использованием устройств разных типов, а также отсутствие пользовательского внимания к угрозам, провоцируемым IoT-устройствами [8].

Таким образом, актуальность обусловлена следующими факторами:

– стремительным развитием Интернета вещей и увеличением количества IoT-устройств;

– необходимостью количественной оценки рисков успешной реализации атак, использующих уязвимости протоколов прикладного уровня, на устройства системы «умный дом», построенной по полносвязной топологии;

– необходимостью увеличения защищенности телекоммуникационной системы «умный дом» в условиях повышенных рисков нарушения конфиденциальности информации;

– потребностью в программно-техническом комплексе для автоматизированной оценки и регулирования рисков, включая выявление наиболее уязвимых устройств и формирование рекомендаций по повышению защищенности для системы «умный дом».

Обзор методик по оценке рисков нарушения конфиденциальности информации системы «умный дом»

В своём исследовании Джон Солдатос, Стефанос Астарас и другие [9] описали модель телекоммуникационной системы «умный дом». В нем определены типы устройств и информации, которой они обмениваются. Наряду с этим, проведена оценка наиболее ценных информационных активов, которые включают информацию или устройства, входящие в исследуемую систему. Также был проведен анализ потенциальных угроз для каждого актива и вероятность успешной реализации выявленных уязвимостей. Риск в их модели рассчитывается с учетом возможности проведения атаки, привлекательности устройства для компрометации и потенциального ущерба при успешной атаке. В данном исследовании была описана схема взаимодействия между устройствами и определены ограничения. Все уязвимости, описанные в работе, были направлены на несанкционированный доступ к информации посредством компрометации центрального контроллера, прослушивания и анализа трафика, идущего от датчиков. В исследовании не была описана и проанализирована возможность атаки умного устройства, доступ к которому можно получить за пределами локальной сети. При заражении устройств такого типа злоумышленник получал точку входа в локальную сеть системы «умный дом». Зараженное устройство может прослушивать трафик с ближайших устройств и нарушать конфиденциальность информации, которая находится в системе.

Джозеф Бугея и другие [10] в своем исследовании проводят анализ рисков в системе «умный дом», построенной на

топологии «звезда». В исследовании они описывают риски, связанные с человеческим фактором. В работе рассматриваются риски, связанные с атакой злоумышленника на систему аутентификации и авторизации и риски, связанные с модификацией пользователем программного обеспечения устройств, входящих в систему. В ходе исследования был сделан вывод о том, что риски, связанные с человеческим фактором, представляют наибольшую опасность. В работе рассматривались только риски, связанные с неправильной настройкой устройств пользователем, но не учитывались уязвимости в устройствах и протоколов передачи данных. В работе рассматривалась риски нарушения конфиденциальности и целостности информации только для конечных устройств, имеющих возможность удаленного управления.

В исследовании Н'Гессан Ив-Ролан Доуха и других [11] описывается методика оценки рисков с использованием EBIOS Risk Manager для телекоммуникационной системы «умный дом». В исследовании проводится анализ активов для исследуемой сети, определение источников риска и оценку уровня угроз. Так как в исследование определена топология, модели устройств и протоколы взаимодействия, то методика оценки рисков будет справедлива для других систем соответствующей конфигурации. При разработке методики рисков использовались конкретные устройства, а не их типы. Это ограничивает применение данной методики при оценке рисков для других видов системы «умный дом», построенных на базе устройств других моделей. Также в работе приняты ограничения на технологию беспроводного подключения. Данная методика количественной оценки рисков нарушения доступности информации будет справедлива только для систем «умный дом», построенных с использованием проводного подключения.

Модель телекоммуникационной системы «умный дом», построенной по полносвязной топологии

Необходимость описания модели телекоммуникационной системы «умный дом» заключатся в том, что на текущий момент не существует количественной и качественной оценки рисков, которые могут применяться для всех моделей систем. Следовательно, была разработана методика, позволяющая произвести оценку рисков нарушения конфиденциальности информации при атаках, использующих уязвимости протоколов прикладного уровня для системы «умный дом», построенной по полносвязной топологии.

Для этого определена архитектура, топология по которой построена система, типы устройств, входящих в систему и протоколы связи между ними.

При создании и описании модели системы учитывались только устройства, имеющие доступ к конфиденциальной информации. В модели системы «умный дом» представлены следующие устройства:

− центральный контроллер, в котором выполняется сбор конфиденциальной информации от датчиков и отправка данных в облако;

− смарт-динамик или умная колонка в которой находится постоянно включенный микрофон;

− устройство робот-пылесос, в котором находится камера;

− устройство радионяня в которой находится постоянно включенная камера и микрофон;

− IP-камеры в которых находится постоянно включенная камера и микрофон;

− концентратор, который объединяет разнородные устройства и позволяют пользователю удаленно взаимодействовать с ними.

Также при разработке моделей описаны технологии подключения устройств и технологий защиты в них. Так как система «умный дом» представляет собой большое количество устройств с разными функциями и технологиями подключения, то система является разнородной. Для выбора версий или протоколов необходима качественная или количественная оценка уровня защищенности.

Для расчета количественной оценки защищенности технологий необходимы входные значения защищенности для каждого вида подключения. Так как на данный момент времени нет статистических данных для различных технологий

подключения, то исходными данными могут быть только оценки, полученные экспертным методом. Качественна экспертная оценка для работы взята из исследования Янга и других [12]. В исследовании экспертным методом была получена качественная оценка защищенности для таких технологий, как: Wi-Fi, Bluetooth, ZigBee, Thread.

Модель угроз нарушения конфиденциальности информации в телекоммуникационной системе «умный дом», построенной по полносвязной топологии

При построении модели угроз для системы, описанной выше, выделены типы атак, направленных на нарушение конфиденциальности информации. Соответствующие данные получены на основе ранее проведенных исследований в области обеспечения конфиденциальности информации для устройств системы «умный дом» [10]. Все атаки разделены по объектам и типам.

На основе описанной ранее модели системы, а также определенными источниками угроз и видов атак, элементы системы описаны кортежем $e = <V, R, A>$, где e – элемент системы, V – множество уязвимостей для данного элемента, R – возможность эксплуатации уязвимости, A – воздействие атаки на конфиденциальность информации. Система «умный дом» описывается как множество элементов $E = \{e_1, \ldots, e_i, \ldots, e_n\}$, где $i \in N = \{1, \ldots, n\}$.

Метрики для оценки рисков нарушения конфиденциальности информации для модели системы «умный дом», построенной по полносвязной топологии

Метрики, представленные ниже, помогают получить меру риска нарушения конфиденциальности информации для субъекта данных. Для количественной оценки рассмотрены три метрики, характеризующие возможность эксплуатации, потенциальный ущерб при атаке и степень влияния на конфиденциальность информации в телекоммуникационной системе «умный дом»:

− базовая оценка CVE (v^b);

− оценка возможности успешной реализации уязвимости и актуальность угрозы (v^e);

− потенциал нарушителя (v^c);

− ущерб от атаки (a_i).

Для вычисления количественной оценки получена информация об уязвимости каждого устройства из базы данных CVE.

Одной из метрик количественной оценки взята базовая оценка CVE, так как она содержит минимум три оценки:

− оценку возможности эксплуатации уязвимости нарушителем;

− оценку влияния на конфиденциальность информации;

− интегральную оценку критичности CVE.

На основе построенной ранее модели оценки риска нарушения конфиденциальности информации PRASH [10] можно выделить метрики, которые позволяют просчитать вероятность успешной реализации атаки, направленной на нарушение конфиденциальности информации. Данными метриками являются:

− вероятность обнаружения уязвимости злоумышленником (D);

− вероятность проведения атаки (R);

− вероятность эксплуатации уязвимости (E).

Вероятность успешной атаки определяется по формуле:

$$p_{усп} = p(D) \times p(R) \times p(E),$$

где $p(D)$ – вероятность обнаружения уязвимости злоумышленником;

$p(R)$ – вероятность воспроизведения атаки;

$p(E)$ – вероятность эксплуатации уязвимости, которая определяется нормированной метрикой v^c.

При определении ущерба определен уровень идентификации и чувствительность контекста информации. Матрица решений для исследуемой системы основана на матрице, описанной в модели DREAD [13].

Для подсчета ущерба используется формула:

$$U = \vec{\alpha}_l \times \vec{D}m,$$

где $\vec{\alpha}_l$ – нормированная оценка степени идентификации пользователя при атаке;

$\vec{Dm}$ – нормированная оценка степени негативного воздействия, которая определяется метрикой v^b.

Расчёт вероятности успешной реализации атак для нескольких элементов при получении контроля над исходным узлом системы определяется по правилу агрегации с логическим условием «И» и представляет собой произведение вероятностей при условии возможности их реализации для исследуемых устройств. Данный параметр вычисляется по следующей формуле:

$$p_s = \prod_{i=1}^{n} p_{e.i},$$

где p_e – вероятность получения контроля над одним устройством системы;

n – количество уязвимостей устройств системы.

После этого была разработана количественная оценка рисков нарушения конфиденциальности информации для системы «умный дом», построенной по полносвязной топологи. Данная оценка вычисляется по формуле:

$$P_{res} = p_{усп} \times p_s \times U,$$

где $p_{усп}$ – вероятность реализации актуальных угроз для устройства;

p_s – вероятность получения контроля над соседним устройством системы при компрометации или захвате исходного;

U – ущерб от атаки.

Алгоритмическое обеспечение регулирования рисков нарушения конфиденциальности информации в телекоммуникационной системе «умный дом», построенной по полносвязной топологии

Для разработки алгоритмического обеспечения регулирования рисков нарушения конфиденциальности информации все компоненты системы «умный дом», построенной по полносвязной топологии, рассмотрены по отдельности, так как с большинством устройств, находящихся в системе можно взаимодействовать удаленно и, соответственно, каждое устройство может являться точкой входа в систему.

Для каждого устройства, имеющего уровень риска в не приемлемых зонах, предложены методы снижения рисков нарушения конфиденциальности информации. Для создания алгоритмического обеспечения были определены меры защиты. Меры разделены по группам. Для защиты от атак, направленных на получения контроля над устройством выделены следующие меры:

− блокировка учетной записи после нескольких неудачных попыток входа;

− блокировка аккаунта используя pam_faillock;

− запрет входа для пользователя root напрямую;

− использование SSH Rate Control;

− включение аутентификации по ключам SSH.

Для защиты от атак, направленных на канал связи выделены следующие меры:

− использование хэширования SHA-256;

− включение сквозного шифрования на устройстве;

− отключение ретрансляции для устройства.

Общими мерами для всех устройств являются:

− изменение порта SSHD и Telnet;

− включение SSHv2;

− использование port knocking при включении запрета удаленного входа для пользователя;

− использование Fail2Ban.

Для каждого устройства была проведена количественная оценка рисков. Далее применялись одиночные меры и производилась переоценка рисков. При несущественном влиянии конкретных мер осуществляется поиск комплекса мер.

Изначально набор состоит из одной меры, направленной на защиту аутентификации, так как большая часть устройств имеет как минимум одну уязвимость механизма аутентификации.

Далее для устройства исследуются уязвимости канала передачи информации между устройствами. Если вероятность успешной реализации данной атаки больше 0.7, то для данного устройства выбирается одна мера из группы мер, направленных на защиту данных при передаче информации между устройствами. После применения

меры проводится переоценка возможности успешной реализации уязвимости. При снижении вероятности до диапазона 0.3-0.7 подбор комбинации мер из данного набора прекращается, в противном случае определяется оптимальный набор из данной подгруппы.

Общие меры помогают увеличить защищенность только от атак, связанных с использованием ботнетов по типу Zerobot или Mirai. Данные ботнеты сканируют активность определенных портов на атакуемых устройствах. Следовательно, изменив порт соединения можно устранить угрозу данного типа.

Алгоритм получения меры риска нарушения конфиденциальности информации для каждого компонента телекоммуникационной системы «умный дом» представлен на рис. 1

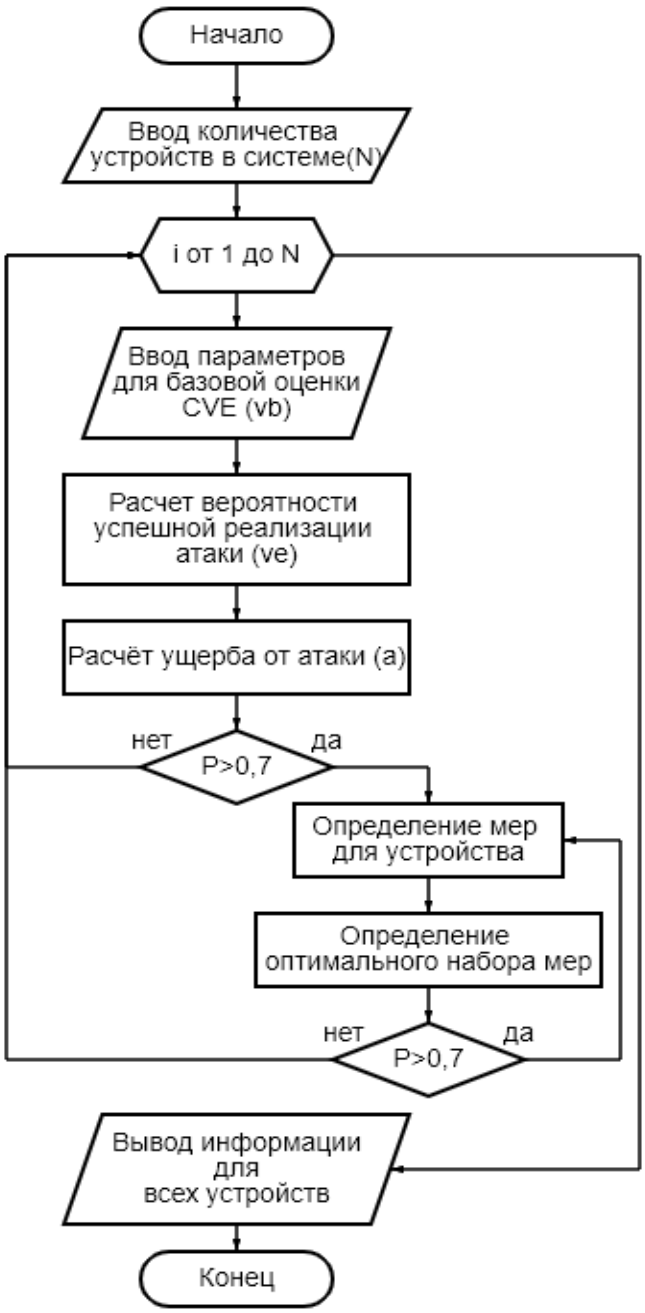

Рис. 1. Алгоритм расчета меры риска нарушения конфиденциальности информации

Заключение

Предложенное методическое обеспечение для риск-анализа нарушения конфиденциальности информации в телекоммуникационной системе «умный дом», построенной по полносвязной топологии, позволит адекватно оценить состояние защищенности телекоммуникационной системы «умный дом» для выработки дальнейших мер по регулированию рисков.

Разработанное алгоритмическое обеспечение регулирования рисков нарушения конфиденциальности информации в телекоммуникационной системе «умный дом» имеет перспективу практической программной реализации процедур для автоматизированного формирования комплекса мер защиты. При применении пользователем системы «умный дом», построенной на полносвязной топологии, разработанного алгоритма регулирования рисков повышается степень защищенности устройств.

Список литературы

1. Домашняя автоматизация. URL: https://ru.wikipedia.org/wiki/Домашняя_автоматизация (дата обращения 14.01.23).

2. Internet of Things and data placement. URL: https://infohub.delltechnologies.com/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement (дата обращения 14.01.23).

3. Пресс-релиз «Лаборатории Касперского». URL: https://www.kaspersky.ru/about/press-releases/2022_kolichestvo-atak-na-iot-ustrojstva-v-rossii-vyroslo-na-40-za-pervoe-polugodie-2022-goda (дата обращения 14.01.23).

4. 2022 IoT Security Landscape. URL: https://securingsam.com/2021-iot-security-landscape/ (дата обращения 14.01.23).

5. А.А. Болгов. Оценка риска безопасности в сетях Интернета вещей / А.А. Болгов, С.А. Ермаков, Л.В. Паринова, Н.И. Баранников // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 561-566.

6. С.А. Ермаков. Оценка эффективности защищенности Iot-сети на примере реализации технологии умный дом / С.А. Ермаков, А.А. Болгов. // Информация и безопасность. 2019. Т. 22. Вып. 1. С. 130-133.

7. В.Е. Кунавин. Оценка и регулирование рисков реализации угроз несанкционированного доступа к данным автоматизированной информационной системы «умный дом»: методическое обеспечение / В.Е. Кунавин, С.А. Ермаков, А.А. Болгов // Информация и безопасность. 2020. Т. 24. Вып. 4. С. 511-520.

8. Investigating threats of information security in IoT apps and methods of protection against these threats, 2021. 187 p.

9. Security risk management for the internet of things URL: https://library.oapen.org/bitstream/handle/20.500.12657/47872/1/9781680836837.pdf / editor John Soldatos. USA, Hanover: now Publisher Inc. 2020. 288 p. P. 119-125 (дата обращения 14.01.23).

10. PRASH: A Framework for Privacy Risk Analysis of Smart Homes. URL: https://www.mdpi.com/1424-8220/21/19/6399 / J. Bugeja, A. Jacobsson, P. Davidsson, 2021 (дата обращения 14.01.23).

11. Threat Level Assessment of Smart-Home Stakeholders Using EBIOS Risk Manager / N'guessan Yves-Roland Douha, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi; The Fifteenth International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2021): IARIA XPS Press. 2021/ 11. P. 31-40.

12. Smart home system network architecture. URL: https://researchprofiles.herts.ac.uk/en/publications/smart-home-system-network-architecture / C. Yang, E. Mistretta, S. Chaychian, J. Siau. // 1st International Conference on Smart Grid Inspired Future Technologies, SmartGIFT 2016 - Liverpool, United Kingdom Duration: Springer Verlag. 19 May 2016 - 20 May 2016. P. 174-183.

13. DREAD. URL: https://www.delphiplus.org/zashchishchennyi-kod/dread--metodika-otsenki-riska.html (дата обращения 14.01.23).

Концерн «Созвездие»
Concern «Sozvezdie»

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 26.01.2023

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, АО «Концерн «Созвездие», e-mail: mnac@comch.ru
Котышенко Андрей Александрович – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Пастернак Юрий Геннадьевич – д-р техн. наук, Воронежский государственный технический университет, e-mail: mnac@comch.ru
Краснобородкин Александр Геннадьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ASSESSMENT AND REGULATION OF RISKS OF VIOLATION OF CONFIDENTIALITY OF INFORMATION IN ATTACKS USING VULNERABILITIES OF APPLICATION LAYER PROTOCOLS IN TELECOMMUNICATION SYSTEMS OF THE INTERNET OF THINGS

S.A. Ermakov, A.A. Kotyshenko, A.A. Bolgov, Yu.G. Pasternak, A.G. Krasnoborodkin

A methodical tooling for quantitative risk assessment is proposed, as well as algorithmic tooling for regulating the risks of information confidentiality violation during attacks that use vulnerabilities in application-level protocols in telecommunication systems of the Internet of things. A system model has been developed that takes into account the architecture and topology of the "smart home" telecommunications system, as well as a threat model that includes a set of vulnerabilities and attacks for each device and a description of the attacker's capabilities. Algorithmic provision of risk management is based on the model of the "smart home" system, built on a full-mesh topology, and is intended to identify the most vulnerable components in it and form a set of measures to increase security. The obtained results in the form of a numerical assessment and algorithmic support make it possible to adequately assess the state of security of the "smart home" telecommunication system and form a set of measures to improve the security of the system.

Key words: smart home, risk, privacy, telecommunication system, full-mesh topology.

Submitted 26.01.2023

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Concern "Sozvezdie", e-mail: mnac@comch.ru
Andrey A. Kotyshenko – student, Voronezh State Technical University, e-mail: mnac@comch.ru
Andrey A. Bolgov – graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru
Yurii G. Pasternak – Dr. Sc. (Technical), Voronezh State Technical University, e-mail: mnac@comch.ru
Alexander G. Krasnoborodkin – student, Voronezh State Technical University, e-mail: mnac@comch.ru