Программные системы и вычислительные методы
Правильная ссылка на статью:
Князев М.А., Шаброва А.С., Крючков А.А. Подход к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с двумя критериями // Программные системы и вычислительные методы. 2024. № 4. DOI: 10.7256/2454-0714.2024.4.72839 EDN: ZOSMZM URL: https://nbpublish.com/library_read_article.php?id=72839

Подход к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с двумя критериями

Князев Максим Андреевич

ORCID: 0009-0007-3931-7442

аспирант; кафедра информационной безопасности ; ФГБОУ ВО «МИРЭА – Российский технологический университет», Институт Искусственного Интеллекта

119454, Россия, г. Москва, пр-т Вернадского, 78

maxiknyaz@mail.ru

Шаброва Анна Сергеевна

ORCID: 0009-0009-1675-1558

студент; кафедра Информационная безопасность; МГТУ им. Н.Э. Баумана

105005, Россия, г. Москва, ул. 2-я Бауманская, 5, стр. 4

shabrova.anna.2410@list.ru

Крючков Андрей Андреевич

ORCID: 0009-0002-4750-6204

старший преподаватель; кафедра информационной безопасности; ФГБОУ ВО «МИРЭА – Российский технологический университет»

119454, Россия, г. Москва, пр-т Вернадского, 78

kryuchkov_a@mirea.ru

Статья из рубрики "Кодирование и защита информации"

DOI:

10.7256/2454-0714.2024.4.72839

EDN:

ZOSMZM

Дата направления статьи в редакцию:

19-12-2024

Дата публикации:

26-12-2024

Аннотация: Существующие методы защиты устройств персонального Интернета вещей (PIoT) требуют постоянной и непрерывной модернизации с учетом возможного возникновения новых угроз и уязвимостей. Важной и актуальной задачей при этом является разработка универсального и эффективного подхода к обеспечению безопасности таких устройств, учитывающего ограниченность ресурсов производителей потребительской электроники сегмента IoT. В данном исследовании предлагается использование математической модели с критериями сложности реализации и универсальности механизмов защиты для выполнения ранжирования механизмов защиты с целью повышения защищённости портативных умных устройств при их оптимальной реализации, с учётом затрат разработчика и в соответствии с требованиями действующего законодательства в области информационной безопасности. Объектом исследования данной работы является процесс обеспечения информационной безопасности устройств персонального Интернета вещей, учитывающий существующие нормативные и технические требования, а также ограниченность ресурсов производителей и разработчиков. Предметом исследования выступает совокупность механизмов защиты PIoT-устройств, отобранных и ранжируемых на основе разработанной математической модели с двумя критериями. Предложен подход к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с критериями сложности реализации и универсальности механизмов защиты. В рамках представленного исследования был проведен подробный анализ рекомендаций и требований к обеспечению безопасности устройств персонального Интернета вещей в международных и отечественных стандартах и исследованы возможности их реализации при эффективном распределении ресурсов производителя посредством математической модели с двумя критериями. Научная новизна данной исследовательской работы заключается в том, что был предложен оригинальный подход к выбору механизмов защиты PIoT-устройств на основе математической модели с двумя критериями, позволяющий при минимизации затрат на разработку и эксплуатацию эффективно учитывать актуальные угрозы и нормативные требования. В результате проведенного исследования были сделаны выводы о том, что внедрение подхода к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с критериями сложности и универсальности является перспективным и потенциально наиболее эффективным средством решения существующих проблем выбора механизмов обеспечения безопасности устройств персонального Интернета вещей в условиях ограниченности ресурсов производителя.

Ключевые слова:

безопасность IoT, персональный Интернет вещей, методика обеспечения безопасности, PIoT, PIoT устройства, защита умных устройств, интернет, защита устройств, портативные умные устройства, математическая модель

ВВЕДЕНИЕ

В современном мире одной из наиболее динамично развивающихся сфер является

Интернет вещей (IoT, Internet of Things)[1]. Большинство среднестатистических пользователей регулярно взаимодействует с портативными умными устройствами, начиная от фитнес-трекеров и заканчивая наушниками с беспроводной передачей данных. Подобные устройства относятся к классу персонального Интернета Вещей (PIoT, Personal Internet of Things)[2]. Количество брендов, под которыми они разрабатываются и распространяются, стремительно растет. Несмотря на имеющиеся преимущества [3], IoT- и PIoT-устройства сохраняют ряд уязвимостей, тем самым создавая возможности для проведения различных видов атак, что подчеркивает потребность в разработке эффективных методов обеспечения безопасности.

Предлагаемый в данной статье подход к выбору механизмов защиты устройств персонального Интернета вещей может быть полезен для проведения дальнейших исследований в области защиты подобного рода устройств, а также для пересмотра и модернизации существующих подходов к обеспечению защищенности данных, обрабатываемых в рамках систем PIoT.

Целью исследования является разработка методики обеспечения безопасности портативных устройств, в частности, и устройств Интернета вещей в целом.

ТЕКУЩЕЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕГМЕНТА УСТРОЙСТВ ПЕРСОНАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

Актуальность текущего исследования обусловлена стремительным ростом количества PIoT-устройств, что способствует увеличению числа потенциальных угроз утечек персональных данных пользователей и расширению множества методов и технологий, используемых для совершения атак на подобные классы и системы устройств [4]. В современных реалиях существует необходимость непрерывного обновления и усиления мер безопасности портативных умных устройств с целью защиты потребителей от уже имеющихся и вновь выявляемых угроз [5].

Исследование IoT Analytics, проведенное в 2023 году, продемонстрировало увеличение расходов компаний-производителей пользовательской электроники сегмента Интернета вещей на 21.5% по сравнению с предыдущим годом, что также сопровождалось и ростом инцидентов с участием PIoT-устройств[1]. Согласно прогнозам Statista, к 2030 году количество умных устройств превысит 29 миллиардов[2]. По данным исследования Omdia от февраля 2024 года число IoT-устройств с технологией eSIM уже превысило 1 миллиард, причем большая часть из них относится к сегменту персонального Интернета вещей. Ожидается, что к 2030 году их количество увеличится более чем в 3.5 раза, достигнув примерно 13% от общего числа устройств Интернета вещей[3]. Потребительский спрос на умные устройства ежегодно растет на 18%[4].

Исследования в области безопасности IoT и PIoT подтверждают необходимость разработки новых комплексных подходов к обеспечению безопасности и создания правовой базы для регулирования данного сегмента. Эксперты компании HP, проводившие исследование в направлении защищенности устройств Интернета вещей в 2014 году, пришли к выводам о том, что не существует полностью безопасных систем IoT, а сами устройства уязвимы для целевых атак[5]. В октябре 2017 года Еврокомиссия предложила обязательную сертификацию для устройств Интернета вещей, чтобы усложнить хакерам создание ботнетов на их основе[6]. Аналитики Kaspersky Digital Footprint Intelligence в 2023 году зафиксировали более 700 предложений в даркнете по

проведению DDoS-атак с использованием IoT-ботнетов, а также услуги по взлому PIoT-устройств и продаже вредоносного программного обеспечения[7].

В январе 2020 года правительство Великобритании опубликовало законопроект, направленный на защиту IoT-устройств[8]. Министр цифровых технологий Мэтт Уормен отметил, что данный акт обязывает производителей учитывать действия злоумышленников для защиты конфиденциальности и безопасности пользователей. В 2022 году Великобритания стала первой страной, принявшей закон[9] о безопасности потребительских IoT-устройств. Аналогичные законопроекты рассматриваются в России, Китае и США. В Евросоюзе комплексные работы по модернизации действующих законодательных актов, регулирующих IoT и PIoT, запланированы на 2024 год[10].

Обозначенные выше исследования и законопроекты свидетельствуют о повышенном интересе к проблематике IoT как со стороны экспертов в области информационной безопасности, так и с позиции государственных органов в контексте правового регулирования данной сферы [6].

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ УСТРОЙСТВ ПЕРСОНАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

В современных реалиях рынка основной упор в разработке потребительской электроники, в том числе и умных устройств, осуществляется коммерческими предприятиями, главной целью которых является финансовая выгода и приращение прибыли. В данных условиях немаловажной потребностью для компаний-производителей выступает оптимальное управление собственными ресурсами, что также необходимо учитывать при обеспечении безопасности IoT- и PIoT-устройств.

Авторы статьи убеждены в том, что помимо очевидной потребности в правовом регулировании сегмента IoT посредством формирования грамотной законодательной базы, невозможно исключать и наиболее эффективное распределение существующих ресурсов организации на реализацию механизмов защиты производимых устройств. Подразумевается, что должно быть обеспечено выполнение требований законодательства при разработке перечня доступных и универсальных механизмов защиты с целью оптимизации выделяемых на их обеспечение и интеграцию временных, финансовых и интеллектуальных затрат.

Исходя из данного фактора, авторами были решены следующие задачи формируемого в рамках исследования подхода к обеспечению безопасности PIoT-устройств:

- определены критерии оценки механизмов защиты;

- проведен анализ и сбор данных по разрабатываемому устройству;

- сформирована модель угроз и нарушителя;

- определены механизмы защиты;

- проведено ранжирование механизмов защиты в соответствии с введенными критериями;

- реализованы наиболее приоритетные механизмы защиты.

Указанные задачи включают в себя обеспечение безопасности со стороны действующего законодательства и оптимизацию процесса выбора механизмов защиты для PIoT-устройств посредством разработки математической модели определения механизмов

защиты с критериями сложности реализации и универсальности механизмов защиты [7]. В рассматриваемом контексте использование этих двух критериев [8] обусловлено наиболее точным и широким охватом, а также определением оптимальных и эффективных механизмов защиты в том случае, когда можно утверждать о корректности и полноте заданных разработчиком параметров в ходе построения математической модели. Рассмотрим каждую задачу более подробно.

КРИТЕРИИ ДЛЯ ВЫБОРА МЕХАНИЗМОВ ЗАЩИТЫ

Основными критериями приоритета механизмов защиты можно определить:

- универсальность механизма защиты;

- сложность реализации механизма.

Универсальность механизма защиты отражает его способность одновременно удовлетворять требованиям бóльшего числа мер защиты. Сложность реализации каждого механизма оценивается в сравнении с ранее определёнными механизмами, поскольку этот показатель является исключительно субъективной величиной.

В целях дальнейшего ранжирования механизмов предлагается использовать диалоговый метод при подборе комбинации механизмов для обеспечения безопасности в рамках ограничения параметров защиты со стороны затрат и ресурсов организации-разработчика устройств персонального Интернета вещей.

АНАЛИЗ УСТРОЙСТВА И МОДЕЛИРОВАНИЕ УГРОЗ И НАРУШИТЕЛЯ

Следующей решаемой задачей обеспечения безопасности PIoT- и IoT-устройств является проведение предварительного анализа исследуемого устройства. В рамках этого анализа необходимо учитывать такие тактико-технические характеристики PIoT-устройств, как семейство микроконтроллеров, выполняющих роль основного управляющего элемента системы, вспомогательные модули и платы расширений, являющиеся наиболее уязвимыми компонентами IoT-устройств, а также программные компоненты и библиотеки, исследование которых может предоставить важную информацию о возможных уязвимостях программного обеспечения устройства.

Одними из наиболее распространенных семейств микроконтроллеров, выбираемых разработчиками IoT-решений, являются STM32 и ARM Cortex-M0. Обладание информацией об архитектуре управляющих элементов системы может предоставить сведения о потенциальных аппаратных уязвимостях и способах их эксплуатации. Например, в микроконтроллерах STM32 известны уязвимости, связанные с отладочными интерфейсами и механизмами защиты памяти [9].

Дополнительные модули устройства, такие как приёмо-передающие устройства Bluetooth, Wi-Fi, NFC и другие, могут служить точками входа для злоумышленников в систему. На текущий момент известны уязвимости технологии Bluetooth Low Energy, позволяющие осуществлять перехват данных с последующим несанкционированным доступом [10].

Программное обеспечение, версии прошивок и используемые библиотеки являются одними из наиболее информативных источников сведений об имеющихся недостатках механизмов обеспечения безопасности PIoT-устройства. Использование устаревших или уязвимых версий библиотек может привести к эксплуатации Heartbleed в OpenSSL и других известных уязвимостей [11].

Следующей задачей является формирование модели угроз и нарушителя. Опираясь на методический документ[11], модель угроз должна включать:

- Описание системы;

- Идентификацию потенциальных угроз;

- Классификацию нарушителя;

- Выявление потенциальных уязвимостей;

- Способы реализации угроз;

- Оценку последствий от нарушения свойств безопасности информации;

- Оценку последствий от нарушения штатного режима функционирования.

Большая часть информации, собранной на первом этапе реализации предлагаемого подхода, необходима для формирования модели угроз, что официально регламентируется регулирующим органом в сфере информационной безопасности, ФСТЭК[12], с целью дальнейшего описания угроз для каждого отдельного уровня системы.

На основе угроз и классификации злоумышленника, определенных в модели угроз и нарушителя, необходимо сформировать механизмы защиты. Стоит уточнить, что механизмы защиты не являются мерами защиты, существующими в рамках Приказа ФСТЭК России №21от 18.02.2013 года[13]. Меры защиты информации определяют тип и метод защиты, в то время как механизм защиты подразумевает конкретизацию в подходе к обеспечению безопасности.

Таким образом, на основе определенного мерой защиты метода обеспечения безопасности должен быть предложен механизм, способный в полном объеме выполнить ее требования в зависимости от функциональных возможностей и концепции разрабатываемого устройства Интернета вещей.

Предлагаемый авторами подход к обеспечению безопасности подразумевает определение механизмов защиты непосредственно экспертами организации, разрабатывающей устройства Интернета вещей. Это обусловлено тем, что невозможно предложить универсальные конкретизированные механизмы, так как их определение напрямую зависит от функциональных и иных особенностей производимого продукта, а также от сведений, содержащихся в модели угроз и нарушителя. При этом важно понимать, что данный процесс может иметь положительное влияние на универсальность защиты, так как один и тот же механизм может перекрывать одновременно более одной меры. Также открывается возможность для определения нескольких механизмов на реализацию одной меры с дальнейшим выбором наиболее эффективного из них посредством математической модели.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПРЕДЕЛЕНИЯ МЕХАНИЗМОВ ЗАЩИТЫ

Следующей задачей является разработка математической модели оценки механизмов защиты, основанной на системе из двух критериев, что снижает фактор субъективности при принятии решений и обеспечивает рациональное распределение ресурсов производителя. Модель учитывает эффективность механизмов защиты в противодействии угрозам и сложность их реализации.

Предлагается ввести следующие множества:

1 . $A = \{a_1, a_2, \ldots, a_n, \ldots, a_N\}$ – множество механизмов защиты, которые могут быть сопоставлены с мерами защиты из модели угроз для обеспечения безопасности устройства. Элементы этого множества необходимы для последующего определения сложности реализации механизмов защиты и оценки вероятности предотвращения потенциальной атаки на устройство;

2. $U = \{u_1, u_2, \ldots, u_m, \ldots, u_M\}$ – множество угроз безопасности, обозначенных в модели угроз. На основе элементов этого множества производится оценка ущерба для пользователя устройства;

3 . $R = \{r_1, r_2, \ldots, r_l, \ldots, r_L\}$ – множество ресурсов разработчика, которое необходимо для определения оценки возможностей для обеспечения безопасности устройства;

4. $Tr = \{tr_1, tr_2, \ldots, tr_q, \ldots, tr_Q\}$ – множество факторов, представляющих из себя необходимость реализации определенных механизмов защиты.

Для множеств вводятся следующие параметры:

1 . $w_m \geq 0,\ m = 1, \ldots, M$ – оценка ущерба для пользователя устройства IoT в случае успешной реализации *m*-ой угрозы.

2 . $p_j^{(a)} \forall\ j = 1, \ldots, M$ – вероятность (или возможность) появления *j*-ой атаки (реализация угрозы) на устройство IoT.

3 . $p_{nj} \in [0, 1], \forall\, n = 1, \ldots, N,\ j = 1, \ldots, M$ – вероятность (или возможность с точки зрения нечетких множеств) предотвращения *j*-ой атаки (реализации угрозы) при использовании *n*-ого механизма.

4. $c_n \geq 0,\ \forall\, n = 1, \ldots, N$ – числовая оценка сложности реализации *n*-ого механизма.

5 . $v_{ln} \geq 0, \forall\, l = 1, \ldots, L,\ n = 1, \ldots, N$ – числовая оценка возможностей для реализации *n*-ого механизма.

6 . $V_l \geq 0,\ \forall\, l = 1, \ldots, L$ – максимальный «объем» *l*-ых ресурсов (финансовых, технических, кадровых, профессиональных, временных, интеллектуальных), который разработчик готов выделить на обеспечение безопасности устройства IoT.

7 . $B_{<n \times q>} = \|b_{nk}\|,\ n = 1, \ldots, N,\ k = 1, \ldots, Q$ – булева матрица, задающая факторы необходимости реализации определенного механизма для выполнения меры защиты из модели угроз и нарушителя: $b_{nk} = 1$, если *n*-ый механизм обеспечивает выполнение *k*-ого фактора необходимости реализации, $b_{nk} = 0$ – в противном случае.

Сложность реализации каждого механизма защиты c_n оценивается на основе экспертной оценки команды разработчиков. Оценка возможностей для реализации механизмов защиты v_{ln} проводится по каждому ресурсу r_l из множества ресурсов разработчика R. Максимальный объём ресурсов V_l устанавливается разработчиком и отражает предельное количество каждого ресурса r_l, которое организация готова выделить на обеспечение безопасности устройства.

Введем логическую переменную $x_n \in \{0, 1\}, \forall\, n \in N$, такую, что $x_n = 1$, если n-ый механизм используется для защиты, $x_n = 0$ – в противном случае. В результате образуется вектор $\mathbf{X}$.

Предлагается ввести следующие условия, задаваемые для введенных критериев:

1 . Оценка универсальности – это измерение способности механизма защиты одновременно удовлетворять множеству мер защиты:

$$W(\mathbf{X}) - \sum_{j \in M} w_m \, p_j^{(a)} \max_{n \in N} \{p_{nj} x_n\} \quad (1)$$

Данный критерий необходимо максимизировать.

2. Сложность реализации используемых механизмов защиты:

$$C(\mathbf{X}) = \sum_{n \in N} c_n x_n. \quad (2)$$

Данный критерий необходимо минимизировать.

При этом вводятся ограничения:

- на использование ресурсов:

$$\sum_{n \in N} v_{ln} \, x_n \leq V_l, \forall \, l = 1, \ldots, L; \quad (3)$$

- на факторы необходимости реализации механизма (выполнение меры защиты из модели угроз и нарушителя):

$$\sum_{n \in N} b_{nk} x_n \geq 1, \forall \, k = 1, \ldots, Q. \quad (4)$$

Ограничение на использование ресурсов (3) существует по той причине, что v_{ln} представляет собой оценку объёма ресурса r_l, необходимого для реализации механизма a_n, а V_l — максимальное количество данного ресурса, которое доступно разработчику. Этим условием обеспечивается то, что совокупные затраты на выбранные механизмы защиты не будут превышать доступные ресурсы.

Ограничение на выполнение факторов необходимости реализации механизма (4) подразумевает, что для каждого фактора из множества Q, представляющего собой требование к механизму защиты, должен быть задействован хотя бы один механизм a_n, обеспечивающий выполнение этого фактора $b_{nk} = 1$. Это условие необходимо для гарантии того, что все меры защиты, определённые в модели угроз и нарушителя, будут выполнены.

Таким образом, решается задача булевого программирования с двумя показателями качества, где первый показатель является нелинейным, второй определен как линейный, а ограничения линейные. Сформируем систему критериев для дальнейшей оптимизации:

$$\begin{cases} W(\mathbf{X}) = \sum_{j \in M} w_j \, p_j^{(a)} \max_{n \in N} \{p_{nj} x_n\} \rightarrow \max \\ C(\mathbf{X}) = \sum_{n \in N} c_n x_n \rightarrow \min \end{cases}. \quad (5)$$

Полученная система представляется решением процесса ранжирования механизмов защиты посредством их приоритезации.

РАСЧЕТ ПОКАЗАТЕЛЕЙ ПРИОРИТЕТА МЕХАНИЗМОВ ЗАЩИТЫ

Для дальнейшего ранжирования механизмов защиты с учетом сформированной системы критериев (5) необходимо определить их «вес». С целью расчета этого параметра предлагается нормировать веса критериев так, чтобы их сумма равнялась единице. Это

необходимо для обеспечения равномерного и сопоставимого влияния каждого критерия выбор механизмов защиты.

Первым шагом в определении численных значений критериев является фиксация количества мер защиты из модели угроз и нарушителя, выполняемых каждым из предложенных механизмов. Примеры сопоставления мер из модели угроз с механизмами защиты показаны в табл. 1. Обозначения, используемые для идентификации мер защиты, соответствуют требованиям, определённым в Приказе ФСТЭК РФ от 18.02.2013 № 21[14]:

- УПД.6: Ограничение числа неуспешных попыток доступа в информационную систему. Мера направлена на предотвращение перебора паролей и несанкционированного доступа;

- УПД.8: Оповещение пользователя при успешном входе о предыдущем доступе в информационную систему. Мера направлена на информирование пользователя о фактах входа в систему;

- АУД.4: Регистрация событий безопасности. Мера предусматривает фиксацию событий, связанных с безопасностью, для последующего реагирования и анализа;

- АУД.7:Мониторинг безопасности Мера включает в себя постоянное отслеживание состояния безопасности информационной системы для своевременного обнаружения и предотвращения инцидентов.

Рассматриваемые меры используются для оценки универсальности механизмов защиты – их способности одновременно удовлетворять требованиям нескольких мер защиты.

Таблица 1. Количество выполняемых мер защиты отдельными механизмами

Механизм защиты	Реализуемая мера защиты из модели угроз и нарушителя	Количество выполняемых мер защиты посредством реализации механизма
Введение блокировки учетной записи после нескольких неуспешных попыток входа с дальнейшим оповещением пользователя	УПД.6	1
Уведомление по электронной почте или SMS	УПД.8	1
Фиксирование данных о попытках входа с различных IP-адресов за короткий промежуток времени	АУД.4, АУД.7	2

После определения количественного показателя универсальности необходимо оценить сложность реализации каждого механизма защиты. Данный параметр является исключительно субъективным и должен предусматривать индивидуальные возможности команды разработчиков и имеющиеся ресурсы. При определении оценки рекомендуется использование 10-балльной шкалы для наибольшей наглядности показателя, что

позволяет достаточно точно оценить сложность в контексте индивидуальных особенностей организации. Максимальный балл присваивается в наивысшей степени комплексному и объемному с точки зрения реализации механизму защиты в формируемом перечне. Пример оценок сложности механизмов защиты представлен в табл. 2.

Таблица 2. Сопоставление оценки сложности с механизмом по 10 балльной шкале

Механизм защиты	Оценка сложности реализации механизма защиты по 10 балльной шкале
Введение блокировки учетной записи после нескольких неуспешных попыток входа с дальнейшим оповещением пользователя	4
Уведомление по электронной почте или SMS	4
Фиксирование данных о попытках входа с различных IP-адресов за короткий промежуток времени	3

РАНЖИРОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ

Завершающим этапом является ранжирование механизмов защиты в соответствии с ранее определёнными параметрами критериев приоритетности с помощью сформированной математической модели. Для этого производится нормировка «весов» показателей по сложности реализации и универсальности механизмов защиты: суммируются все веса, после чего каждое значение критерия делится на полученную сумму. Пример формирования значений критериев представлен в табл. 3.

Таблица 3. Значения критериев механизмов защиты

№	Цель	Критерии	
		Реализация мер из модели угроз	Сложность реализации
	Вес критериев	0.5	0.5
	Механизмы защиты	Оценка универсальности	Оценка сложности
1	Введение блокировки учетной записи после нескольких неуспешных попыток входа с дальнейшим оповещением пользователя	0.25	0.36
2	Уведомление по электронной почте или SMS	0.25	0.36
3	Фиксирование данных о попытках входа с различных IP-адресов за короткий промежуток времени	0.50	0.28

Значения вычислены таким образом, чтобы в сумме вес всех определенных в модели критериев, а также общая оценка доступных механизмов защиты по каждому отдельному

критерию по модулю были равны единице. В данном случае рассматриваются два критерия с одинаковыми весами 0.5.

После проведенных расчетов можно определить приоритет каждого механизма защиты для их последующего ранжирования по следующей формуле:

$$F_n = \alpha\left(w_j\, p_j^{(a)} \max_{n \in N}\{p_{nj} x_n\}\right) - \beta(c_n x_n). \quad (6)$$

где α – вес критерия универсальности механизма защиты, β – вес критерия сложности реализации механизма защиты, $w_j\, p_j^{(a)} \max_{n \in N}\{p_{nj} x_n\}$ – значение оценки универсальности механизма, $c_n x_n$ – значение оценки сложности реализации механизма.

Расчет приоритетов для механизмов защиты в рассматриваемом примере дает следующие значения:

$$F_1 = 0.5 \times 0.25 \quad 0.5 \times (0.36) = \quad 0.055,$$

$$F_2 = 0.5 \times 0.25 \quad 0.5 \times (0.36) = \quad 0.055,$$

$$F_3 = 0.5 \times 0.5 \quad 0.5 \times (0.28) = 0.11.$$

Таблица иерархии механизмов на основе их приоритета для приведенного в статье примера выглядит следующим образом (табл. 4).

Таблица 4. Перечень механизмов защиты в соответствии с показателями приоритета

Механизм защиты	Показатель приоритета
Фиксирование данных о попытках входа с различных IP-адресов за короткий промежуток времени	0.11
Введение блокировки учетной записи после нескольких неуспешных попыток входа с дальнейшим оповещением пользователя	-0.055
Уведомление по электронной почте или SMS	-0.055

Данные, полученные в результате такого расчета, являются уникальными для каждого продукта и организации, так как напрямую зависят от модели угроз и нарушителя, а также от объема имеющихся в компании-разработчике ресурсов.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ И ИХ ОБСУЖДЕНИЕ

В результате проведённого исследования разработан подход к обеспечению безопасности устройств персонального Интернета вещей на основе математической модели с двумя критериями: универсальность механизма защиты и сложность реализации. Применение данного подхода позволяет определить и ранжировать механизмы защиты, оптимизируя их выбор с учётом ограничений ресурсов и специфики разрабатываемого устройства.

Анализ результатов показал, что предложенный подход достаточно эффективно решает задачу оптимизации выбора механизмов защиты. Использование математической модели дает возможность оценить каждый механизм по заданным критериям, снижая фактор

субъективности в процессе принятия решений [12]. Ранжирование механизмов защиты обеспечивает взвешенное распределение ресурсов, что особенно актуально для коммерческих организаций.

Однако следует учитывать, что точность и эффективность модели зависят от корректности исходных данных и адекватности выбранных критериев. В перспективах дальнейшего исследования целесообразно расширить набор критериев и разработать стандартизированные методы оценки, что позволит повысить точность модели и адаптировать её к различным типам устройств и условиям эксплуатации. Особое внимание следует уделить внедрению механизмов защиты, основанных на алгоритмах машинного обучения. В условиях растущей сложности сетевых угроз и увеличения объёма данных, обрабатываемых в системах PIoT, существует необходимость разработки адаптивных и гибких методов детектирования аномального поведения при проведении различных атак [13]. Также, учитывая, что протокол Bluetooth Low Energy (BLE) является одним из наиболее популярных для портативных устройств [14], важно детально проработать перечень механизмов защиты именно для этой беспроводной технологии [15].

Предлагаемый подход к выбору механизмов защиты устройств персонального Интернета вещейможет способствовать повышению защищённости пользовательских умных устройств, обеспечивая рациональное распределение ресурсов и минимизируя риски компрометации информационных систем.

БЛАГОДАРНОСТИ / GRATITUDE

Авторы выражают искреннюю благодарность канд. техн. наук, А.В. Королькову за критический подход и оперативную вовлеченность в процесс редактирования полученных результатов исследования / The authors express their sincere gratitude to Ph.D. in Technical Sciences A.V. Korolkov for his critical approach and prompt involvement in the process of editing the research results.

[1] State of IoT – Spring 2023. https://iot-analytics.com/product/state-of-iot-spring-2023/

[2] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[3] Omdia: New Omdia research shows eSIM installed base in IoT to top 3.6 billion by 2030. https://omdia.tech.informa.com/pr/2024/feb/new-omdia-research-shows-esim-installed-base-in-iot-to-top-3-point-6-billion-by-2030

[4] Интернет вещей, IoT, M2M мировой рынок. https://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT,_M2M_(мировой_рынок)

[5] HP Discovers Common Vulnerabilities in 10 IoT Devices. https://www.eweek.com/security/hp-discovers-common-vulnerabilities-in-10-iot-devices/

[6] Improving Internet of Things Device Certification with Policy-based Management. https://publications.jrc.ec.europa.eu/repository/handle/JRC106530

[7] DDos, программы-вымогатели, майнеры: «Лаборатория Касперского» проанализировала ландшафт киберугроз для интернета вещей.

https://www.kaspersky.ru/about/press-releases/2023_ddos-programmy-vymogateli-majnery-laboratoriya-kasperskogo-proanalizirovala-landshaft-kiberugroz-dlya-interneta-veshej

[8] Government to strengthen security of Internet-connected products. https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products

[9] Product Security and Telecommunications Infrastructure Act 2022. https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted

[10] IoT Cybersecurity: regulating the Internet of Things. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

[11] «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

[12] Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

[13] Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

[14] Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

Библиография

1. Львович И.Я., Преображенский А.П., Преображенский Ю.П., Чопоров О.Н., Проблемы использования технологии интернет вещей. *Вестник Воронежского института высоких технологий*. 2019;13(1):73-75.
2. Biswa Mohan Sahoo, Mohanty SP, Deepak Puthal, Pillai P. Personal Internet of Things (PIoT): What Is It Exactly? *Cyber Security for Next-Generation Computing Technologies*. 2021 Nov 1;10(6):58–60. DOI:10.1201/9781003404361-14
3. Fariha Eusufzai, Aldrin Nippon Bobby, Farzana Shabnam, Saifur Rahman Sabuj. Personal internet of things networks: An overview of 3GPP architecture, applications, key technologies, and future trends. *International journal of intelligent networks*. 2024 Feb 1; 5(6):77-91; DOI:10.1016/j.ijin.2024.02.001
4. Информационная безопасность в системе "Интернет вещей" / А.Г. Коробейников, А.Ю. Гришенцев, Д.И. Дикий [и др.]. *Вестник Чувашского университета*. 2018. № 1. С. 117-128.
5. Dean A, Agyeman M.O. A Study of the Advances in IoT Security. *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control - ISCSIC* '18. 2018;1-

5; DOI:10.1145/3284557.3284560
6. Каженова Ж.С. Безопасность в протоколах и технологиях IoT: обзор / Ж.С. Каженова, Ж.Е. Кенжебаева. *International Journal of Open Information Technologies*. 2022. № 3. С. 10-15. – ISSN 2307-8162
7. Керимов Вагиф Асад Оглы. Алгоритм принятия решения для одной многокритериальной задачи с матричной моделью / Вагиф Асад Оглы Керимов, Фаик Гасан Оглы Гаджиев. *Universum: технические науки*. 2023. № 2. С. 62-65.
8. Юрлов Ф.Ф. Методика комплексного применения набора принципов оптимальности при выборе эффективных решений при наличии неопределенности внешней среды и многокритериальности / Ф.Ф. Юрлов, С.Н. Яшин, А.Ф. Плеханова. *Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Социальные науки*. 2022. № 1. С. 49-55.
9. Басс А.В. Особенности работы с микроконтроллером stm32. *Известия Тульского государственного университета. Технические науки*. 2019. № 1. С. 35-40.
10. Саенко М.А. Анализ уязвимостей беспроводных каналов передачи информации / М.А. Саенко, Д.А. Мельников, М.А. Данилов. *Образовательные ресурсы и технологии*. 2023. № 1. С. 82-90.
11. Chimtchik N.V. Vulnerabilities detection via static taint analysis / N.V. Chimtchik, V.N. Ignatiev. *Труды Института системного программирования РАН*. 2019. Т. 31, № 3. С. 177-189.
12. Абдусаломова Н.М. Математическое моделирование научных знаний как отдельная позиция между теорией и экспериментом. *Мировая наука*. 2024. № 6. С. 44-47.
13. Истратова Е.Е. Применение нейронных сетей для обнаружения аномального трафика в сетях Интернета вещей. *International Journal of Open Information Technologies*. 2024. № 1. С. 65-70.
14. K. E. Jeon, J. She, P. Soonsawad and P. C. Ng. BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities. *IEEE Internet of Things Journal.* V. 5, № 2, P. 811-828, April 2018, DOI: 10.1109/JIOT.2017.2788449.
15. Prathibha Muraleedhara, Christo S, Jaya J, D. Yuvasini. Any Bluetooth Device Can be Hacked. Know How? *Cyber Security and Applications*. 2024 Feb 1;100041–1. DOI:10.1016/j.csa.2024.100041

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Представленная статья на тему «Подход к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с двумя критериями» соответствует тематике журнала «Программные системы и вычислительные методы» и посвящена актуальной проблеме – разработке эффективных методов обеспечения безопасности IoT- и PIoT -устройств. По мнению авторов это связано с тем, что большинство среднестатистических пользователей регулярно взаимодействует с портативными умными устройствами, начиная от фитнес-трекеров и заканчивая наушниками с беспроводной передачей данных. Подобные устройства относятся к классу персонального Интернета Вещей (PIoT, Personal Internet of Things). Количество брендов, под которыми они разрабатываются и распространяются, стремительно растет. Несмотря на имеющиеся преимущества, IoT- и PIoT- устройства сохраняют ряд уязвимостей, тем самым создавая возможности для проведения различных видов атак.
В статье представлен достаточно широкий анализ литературных российских и

зарубежных и интернет-источников по теме исследования. Указана теоретико-методологическая основа исследования.
Авторами самостоятельно проведен комплексный анализ PIoT-устройств с учетом таких тактико-технических характеристик устройств, как семейство микроконтроллеров, выполняющих роль основного управляющего элемента системы, вспомогательные модули и платы расширений, являющиеся наиболее уязвимыми компонентами IoT-устройств, а также программные компоненты и библиотеки, исследование которых может предоставить важную информацию о возможных уязвимостях программного обеспечения устройства. Также авторами проведен расчет показателей приоритета механизмов защиты.
Стиль и язык изложения материала является достаточно доступным для широкого круга читателей. Практическая значимость статьи четко обоснована. Статья по объему соответствует рекомендуемому объему от 12 000 знаков.
Статья достаточно структурирована - в наличии введение, заключение, внутреннее членение основной части (анализ литературы, методология, результаты исследования и обсуждение).

Авторами проведено исследование, в результате которого разработан подход к обеспечению безопасности устройств персонального Интернета вещей на основе математической модели с двумя критериями: универсальность механизма защиты и сложность реализации. Применение данного подхода позволяет определить и ранжировать механизмы защиты, оптимизируя их выбор с учётом ограничений ресурсов и специфики разрабатываемого устройства.

К недостаткам можно отнести следующие моменты: из содержания статьи не прослеживается научная новизна. Отсутствует четкое выделение предмета, объекта исследования.
Рекомендуется четко обозначить научную новизну исследования, сформулировать предмет, объект. Также будет целесообразным добавить о перспективах дальнейшего исследования.

Статья «Подход к выбору механизмов защиты устройств персонального Интернета вещей на основе математической модели с двумя критериями» требует доработки по указанным выше замечаниям. После внесения поправок рекомендуется к повторному рассмотрению редакцией рецензируемого научного журнала.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Статья посвящена вопросам обеспечения безопасности устройств персонального Интернета вещей (PIoT), которые активно внедряются в повседневную жизнь. Исследование акцентируется на разработке методологии выбора механизмов защиты с использованием математической модели, что позволяет учесть ограниченность ресурсов и специфические угрозы. Авторы также рассматривают практические аспекты реализации предложенного подхода для достижения оптимальной защищенности устройств.
Исследование опирается на использование математической модели, включающей два ключевых критерия: универсальность механизма защиты и сложность его реализации.

Представленный подход базируется на использовании булевого программирования, что способствует минимизации субъективности при выборе защитных решений. Авторы подробно описывают этапы реализации модели, включая формирование множества угроз, определение механизмов защиты, построение модели угроз и последующее ранжирование механизмов по степени приоритета. Методология дополнена примерами расчетов, что подтверждает её применимость и достоверность.

Актуальность исследования обусловлена стремительным ростом числа PIoT-устройств, что увеличивает риски утечек данных и уязвимостей. Представленные статистические данные, включая прогнозы роста числа устройств до 29 миллиардов к 2030 году, подтверждают важность создания эффективных решений для защиты данных. Учитывая растущее число угроз и отсутствие универсальных стандартов защиты, статья предлагает своевременный и практически значимый подход.

Предложение метода оценки механизмов защиты с использованием математической модели является ключевым элементом научной новизны работы. Модель базируется на учете ограниченности ресурсов разработчиков и интеграции двух критериев, что делает её уникальной в контексте PIoT. Авторы также подчеркивают, что их подход позволяет учитывать индивидуальные особенности каждого устройства, что является значимым шагом в создании адаптивных систем защиты.

Статья написана академическим стилем с высоким уровнем технической проработки.

Структура работы:

- Введение четко формулирует цели исследования и подчеркивает актуальность проблемы.
- Анализ текущего состояния дает всесторонний обзор существующих подходов и их ограничений, подкрепленный статистическими данными.
- Методология подробно описывает этапы разработки математической модели, включая формирование критериев, оценку ресурсов и анализ угроз.
- Результаты и обсуждение акцентируют внимание на применении модели для практических задач.
- Выводы содержат рекомендации и намечают пути дальнейшего исследования.

Текст сопровождается таблицами и диаграммами, что упрощает восприятие материала. Однако было бы полезно включить иллюстрацию полной схемы процесса выбора механизмов защиты.

Список литературы разнообразен и включает актуальные работы, посвященные вопросам безопасности IoT, статистическим исследованиям и нормативной базе. Указанные источники подтверждают глубину проведенного анализа. Тем не менее, добавление большего числа примеров практического применения предложенного подхода могло бы усилить значимость работы.

Авторы аргументированно обосновывают свой подход, признавая, что универсальные механизмы защиты для PIoT-устройств создать сложно. Однако предложенная модель позволяет адаптироваться к индивидуальным условиям каждого устройства, что снижает вероятность критики со стороны оппонентов. При этом они подчеркивают необходимость дальнейшей стандартизации критериев, что открывает новые горизонты для дискуссии и совместных исследований.

В заключении авторы четко обозначают практическую ценность своей работы, подчеркивая, что предложенный подход может быть использован как производителями PIoT-устройств, так и исследователями в области информационной безопасности. Статья вызывает интерес как у научного сообщества, так и у представителей отрасли, предоставляя инструменты для повышения уровня защиты умных устройств.

Статья представляет собой высококачественное исследование, основанное на инновационной методологии и актуальных данных. Работа отличается высокой

практической значимостью и научной новизной, что делает её достойной публикации.

Рекомендация: принять статью к публикации. Более того, в случае её доработки (например, добавления дополнительных иллюстраций процесса или расширения обзора практического применения), она может быть рекомендована к включению в список лучших публикаций месяца.