DOI 10.36622/VSTU.2022.25.3.006
УДК 004.735

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «УМНЫЙ ДОМ»: АЛГОРИТМ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

С.А. Ермаков, Ю.А. Гусарева, А.А. Болгов, В.Н. Кострова

В статье предложена методика повышения защищенности автоматизированной системы «Умный дом» от атак, направленных на нарушение конфиденциальности передаваемой и обрабатываемой информации в каналах передачи информации и на конечных устройствах. В основе методики лежит алгоритм оценки рисков и выявления уязвимых компонентов автоматизированной системы «Умный дом». В работе представлены структурно-параметрическая и логическая модели, учитывающие архитектуру и топологию автоматизированной системы «Умный дом», построенной на основе облачного сервиса, модель угроз, включающая описание злоумышленников и атак для каждой структурной составляющей автоматизированной системы, и предложен инструментарий численной оценки рисков. Полученные результаты в виде численной оценки позволяют выполнять анализ рисков нарушения конфиденциальности информации для каждого компонента системы, выявлять и информировать разработчиков и пользователей системы «Умный дом» об уязвимых сегментах системы и соответствующих угрозах с точки зрения нарушения конфиденциальности информации.

Ключевые слова: интернет вещей, риск, атака, конфиденциальность, умный дом.

Введение

В ходе развития технологий интернета вещей в отдельный класс стали выделять устройства системы «Умный дом», которая сейчас является одним из самых известных приложений интернета вещей, включающим разнородные устройства от интеллектуальных микрофонов до электронных дверных замков, подключенных к домашней сети и управляемых удаленно через сеть Интернет [1]. Эти устройства обмениваются собранными данными между собой и пользователями, что дает различные преимущества, такие как удобство применения, энергоэффективность и другие. Прогнозировалось, что мировой рынок систем «Умного дома» достигнет примерно 53,45 млрд долларов в 2022 году, что больше на 14,5%, чем в 2017 [2].

При этом «Умные дома» становятся объектами кибернетических атак. Распространенность «умных» устройств сопровождается значительными рисками нарушения конфиденциальности информации, что связано с хранением данных, которые могут быть неправомерно использованы злоумышленниками [3-5]. Автоматизированная система «Умный дом» может включать в себя различные устройства с камерами, микрофонами, трекерами местоположения, которые могут иметь уязвимости, позволяющие злоумышленнику получить доступ к обрабатываемой конфиденциальной информации. Это делает их уязвимыми для кибератак, которые могут раскрыть личные данные и информацию о проживающих на территории дома, в том числе детях и посетителях. Некоторые примеры распространенных векторов атак (т.е. методы, используемые для обходов средств обеспечения безопасности или конфиденциальности системы) направлены на подключенные устройства с уязвимыми службами, слабой системой аутентификации и конфигурацией по умолчанию [6, 7]. Компоненты системы «Умного дома» сильно взаимосвязаны, например, атакующему достаточно эксплуатировать уязвимость только в одном компоненте, таком как шлюз дома, для получения доступа ко всей домашней сети, а также как способ получения доступа ко всем конфиденциальным данным, циркулирующим в сети.

Таким образом, крайне важно понимать последствия для конфиденциальности подключённых устройств, чтобы потребители знали о рисках, а также как можно минимизировать ущерб от рисков [8, 9, 10].

В данной работе рассматривается система «Умный дом» как объект реализации рисков нарушения конфиденциальности информации с использованием различных устройств, обеспечивающих взаимодействие пользователя с системой. Важно также учесть, что устройства и сети имеют встроенные средства обеспечения безопасности, различные конфигурации и требования. Поэтому важно рассматривать риски нарушения конфиденциальности всесторонне, учитывая различные каналы утечки информации и векторы атак.

Угрозы нарушения конфиденциальности, влияющие на системы интернета вещей, а, следовательно, и на «Умные дома», направлены на получение доступа, сбор, обработку и раскрытие конфиденциальной информации вопреки ожиданиям пользователей. Как правило, злоумышленники ставят перед собой одну из целей [11, 12]:

1. Компрометация информации, например, учетных данных пользователей;
2. Отслеживание местоположения пользователя;
3. Получение контроля над системой, например, внедрение вредоносного кода или изменение настроек и конфигурации устройства.

Для того, чтобы оценить риски систем на предмет угроз нарушения конфиденциальности, необходимо рассмотреть сценарии успешных реализаций атак, когда доступ к конфиденциальной информации получен и использован против исходных информационных норм и контроля [8]. Атака с целью получения конфиденциальных данных считается успешной, если личность пользователя раскрывается или становится связанной с скомпрометированными данными, которые субъект считает частными [1].

Таким образом, актуальность исследования обусловлена следующими факторами:

– стремительным ростом спроса на устройства системы «Умный дом», которые взаимодействуют друг с другом централизованно и не безопасно;

– необходимостью повышения защищенности автоматизированной системы «Умный дом» в условиях повышенных рисков нарушения конфиденциальной информации;

– наличием широкого спектра подходов в построении системы, применение новых технологий взаимодействия и подключения;

– потребность создания инструментария количественной оценки рисков в условиях реализации атак на нарушение конфиденциальности информации в автоматизированной системе «Умный дом».

При анализе имеющихся подходов оценки рисков и защищенности системы «Умный дом» с использованием сетей интернета вещей, а также изучением предложенных ранее мер защиты были выявлены следующие противоречия между:

1. Необходимостью построения специализированной модели автоматизированной системы «Умный дом», учитывающей все особенности системы для оценки рисков нарушения конфиденциальности информации и доступностью только универсальных моделей систем на базе технологии «Интернет вещей»;
2. Необходимостью численной оценки рисков нарушения конфиденциальности информации в автоматизированной системе «Умный дом» в условиях реализации атак и наличием лишь качественных подходов к оценке рисков нарушения конфиденциальности информации в автоматизированной системе «Умный дом»;
3. Необходимостью выявления наиболее уязвимых компонентов автоматизированной системы «Умный дом» к атакам, направленным на нарушение конфиденциальности информации и отсутствием адекватных алгоритмов оценки и методик регулирования рисков нарушения конфиденциальности информации в автоматизированной системе «Умный дом».

Объектом исследования является автоматизированная система «Умный дом», построенная на основе облачного сервиса.

Предметом исследования является инструментарий численной оценки и регулирования рисков в автоматизированной системе «Умный дом» в условиях успешной реализации атак, направленных на нарушение конфиденциальности информации в каналах передачи данных и на конечных устройствах.

Постановка задач исследования

Основная цель работы состоит в повышении защищенности автоматизированной системы «Умный дом» от атак, направленных на нарушение конфиденциальности передаваемой и обрабатываемой информации в каналах передачи данных и на конечных устройствах, за счет разработки алгоритма оценки рисков для выявления уязвимых компонентов автоматизированной системы «Умный дом».

Для достижения цели необходимо решить задачи:

1. Построить структурно-параметрическую модель автоматизированной системы «Умный дом», учитывающую архитектуру, топологию, устройства, каналы и используемые протоколы передачи конфиденциальной информации;
2. На основе построенной модели автоматизированной системы «Умный дом» разработать методику получения численной оценки рисков нарушения конфиденциальности информации;
3. Предложить (для дальнейшей программной реализации) алгоритм выявления компонентов автоматизированной системы «Умный дом» с высоким уровнем риска нарушения конфиденциальности информации на основе ранее полученных количественных оценок.

Анализ методик оценки рисков нарушения конфиденциальности информации

Модель STRIDE была предложена Майкрософт как методика идентификации угроз безопасности с классификацией угроз на 6 категорий: спуфинг, подделка, отказ, раскрытие информации, отказ в обслуживании и повышение привилегий. Хотя данная модель полезна для анализа угроз, но предназначена для анализа безопасности, поэтому ее использование ограничено для исследования и анализа обеспечения конфиденциальности.

LINDDUN представляет собой технику моделирования угроз конфиденциальности, аналогичную STRIDE, позволяющую систематически идентифицировать угрозы конфиденциальности и выбирать технологии для повышения обеспечения конфиденциальности в целях снижения рисков. Аббревиатура LINDDUN происходит от категорий угроз конфиденциальности, которые она может идентифицировать, а именно: связность, идентификация, невозможность отказа, возможность обнаружения, раскрытие информации, неосведомленность и несоблюдение. Несмотря на то, что данная модель полезна для моделирования программных систем, но не предоставляет средств для количественной оценки рисков.

Методология количественного анализа угроз QTMM представляет собой методологию количественного моделирования угроз, позволяющую объективно делать выводы об атаках, связанных с нарушением конфиденциальности информации.

Подобно LINDDUN, QTMM основан на подходе STRIDE и использует те же этапы моделирования. Тем не менее, QTMM фокусируется на трех категориях угроз, связанных с конфиденциальностью: связность, неосведомленность и возможность вмешательства, которые ограничены по сравнению с LINDDUN. В QTMM используются измеримые деревья атак, чтобы помочь аналитику принимать объективные решения об угрозах, атаках и механизмах уменьшения последствий. В модели LINDDUN отсутствует количественная оценка с помощью деревьев атак. QTMM предоставляет методологию анализа и оценки угроз нарушения конфиденциальности информации, но она не касается конкретно исследования системы «Умный дом».

EPIC – операционная методология, предназначенная для выявления и оценки угроз нарушения конфиденциальности информации, возникающих в результате развертывания организационной системы кибербезопасности (CSS). Эта система, как

правило, обрабатывает большое количество конфиденциальной информации, касающейся сетевого трафика, проходящего в организации. В частности, эта модель предназначена для предоставления специалистам по безопасности и конфиденциальности инструкций от моделирования и раскрытия в CSS до оценки рисков нарушения конфиденциальности информации. В методике EPIC считается, в отличие от LINDDUN и QTMM, любое раскрытие данных, которое может позволить получить доступ к конфиденциальной информации субъекта (обладателя). Тем не менее, данная модель также отображает методику оценки рисков конфиденциальности информации, но не рассматривает угрозы и злоумышленников в рамках «Умного дома».

Другие известные подходы и системы моделирования угроз конфиденциальности, например, FPFSD и PriS, существуют в научной литературе, однако их цели отличаются от целей, поставленных в данной работе [18, 19].

Описание методики численной оценки рисков нарушения конфиденциальности информации

Описание методики взято на основе моделей STRIDE и PRASH [8], представленных ранее и дополнено компонентами, описывающими систему, включая политики конфиденциальности и передаваемые/обрабатываемые типы конфиденциальных данных.

Модель автоматизированной системы «Умный дом» объявляется следующим образом, как S = (H, N, U, L, D, P), имея в своем составе 6 компонент.

– H (Дом) - представляет собой физическую среду, где проживают пользователи. Среду проживания можно описать как совокупность различных зон, таких как комнаты, определенные территории, то есть части для проведения времени и активности пользователей. $H = \{z_1, z_2 \ldots z_n\}$, где $z_i \in LC$ – описывает жилую зону дома;

– N (Устройства) – совокупность физических компонентов, которые включены в систему «Умный дом». $N = C \cup M \cup B$, где C – это подключенные устройства внутри среды «Умного дома» (такие как удаленно подключенные и управляемые пользователем устройства), M – устройства конечных пользователей (устройства для удаленного управления подключенными устройствами), B – обработчики данных (удаленный центр обработки данных, но также может являться и конечным устройством). Предполагается, что существует конечное множество CP, то есть возможностей, описываемых отношением $I \subseteq N \times CP$, где $I(n, cp)$ – представляет, что узел n реализует возможности и описывается отображением $f_{nl} : N \to LC$;

– U (Пользователи) – компонент представляет собой пользователей, которые взаимодействуют с автоматизированной системой. Пользователь может контактировать с N напрямую или косвенно через устройства (приложения), которые встроены в устройства (узлы). Здесь также представлены роли, которые могут быть назначены пользователю R = {субъект данных, контроллер данных, пользователь данных}. Описывается тернарным отношением $At \subseteq U \times R \times N$, где $At(u, t, n)$ значит, что пользователь с определенной ролью имеет отношение к определенному устройству;

– L (Каналы) – это набор каналов для коммуникации, то есть физические или логические каналы, соединяющие N (узел) и U (пользователь), где могут быть переданы D (данные). Отношение $L \subseteq (N \times N) \cup (N \times U) \cup (U \times N)$ представляет потоки данных;

– D (Информация) – это набор элементов данных, собираемых и обрабатываемых N (узлом). D представлен в виде кортежем $s(d_i, d_s, d_p, d_t, d_l, d_e)$, где значение каждого атрибута является описанием собираемых и обрабатываемых метаданных:

– d_i – это элементы данных, которые собирает и обрабатывает подключенное к системе устройство N. Элементом может быть, как имя, так и более обширный тип

данных в зависимости от рассматриваемого устройства N;

– d_s – это субъект данных. Представляет собой лицо, чьи данные собираются и обрабатываются устройством. Это могут быть следующие значения: {пользователь, система}, где пользователь — это сущность U, а система - N;

– d_p – характеризует цель обработки данных (например, для однозначной идентификации человека, сбора или переработки информации d_i);

– d_t – это время хранения данных, которое характеризуется условиями хранения d_i с возможными значениями ∈ {неопределенно, цель, дата}. Таким образом, неопределенное значение, указывает на отсутствие ограничений по времени для удаления данных; цель характеризует процесс удаления данных, когда достигнуто d_p; дата характеризует фактическую дату и назначенное время удаления d_i;

– d_l – явный идентификатор, представляющий собой логическое значение, указывающее является ли d_i явно идентичным (номер социального страхования, голос, MAC-адрес и т. д.) d_s;

– d_e – характеризует управление конфиденциальными данными. Представляет собой набор кортежей (управление, фаза), где управление представляет собой технологию повышения уровня конфиденциальности информации с возможными значениями ∈ {анонимизация, деидентификация, шифрование}, а фаза – указывает на фазу жизненного цикла данных с возможными значениями {генерация, сбор, обработка, раскрытие}, над которыми производится контроль.

– P (Правила) – представляет собой набор правил, описывающих настройку и работу автоматизированной системы «Умный дом».

На основе представленных классификаций, функционального описания и представленных типов конфиденциальных данных можно построить модель автоматизированной системы «Умный дом», включающую схематичное представление, логику взаимодействия, каналы и компоненты системы.

Оценки, представленные ниже, помогают получить меру риска нарушения конфиденциальности информации для субъекта данных. Предлагаются три оценки, характеризующие состояние конфиденциальности информации в автоматизированной системе «Умный дом»:

1. Оценка успешности реализации атаки (α_l);

2. Оценка негативных последствий от атаки (α_i);

3. Показатель для оценки меры риска нарушения конфиденциальности информации (r_μ).

α_l - это оценка того, что t_a успешно достиг своей цели и получил доступ к конфиденциальным данным пользователя системы «Умный дом». Оценка $\alpha_l \in [0;1]$. Если значение $\alpha_l \le 0{,}3$, то оценка успеха атаки крайне минимальна и атакующему трудно получить доступ к устройству/каналу. Если $\alpha_l \ge 0{,}7$, то оценка успешности реализации атаки крайне велика. На основе построенной ранее модели оценки риска нарушения конфиденциальности информации PRASH и DREAD можно выделить метрики, которые позволяют просчитать оценку успешности реализации атаки, направленной на нарушение конфиденциальности информации.

Путем экспертной оценки для параметров была разработана следующая градация:

1) Оценка популярности уязвимости (D):

– уязвимость существует в наиболее часто используемой функции устройства автоматизированной системы «умный дом». есть опубликованная информация, объясняющая возможность атаки. значения оценки в промежутке: [0,7; 1];

– нахождение уязвимости довольно редко, поэтому использование злоумышленником уязвимости потребует больше затрат на поиск, а также принесет ущерб меньшему количеству пользователей устройств системы. значения оценки в промежутке: [0,4; 0,69];

– уязвимость почти неизвестна, следовательно, атака маловероятна. значения оценки в промежутке: [0; 0,39];

2) Оценка простоты реализации атаки (R):

– атака может быть реализована каждый раз вне зависимости от уровня привилегий в системе во время определенного временного окна взаимодействия с пользователем. значения оценки в промежутке: [0,7; 1];

– атака может быть реализована, но при имении в системе привилегий базового пользователя, а также может потребоваться некоторое взаимодействие с пользователем для реализации. значения оценки в промежутке: [0,4; 0,69];

– атаку трудно воспроизвести, требуются высокие привилегии в системе, взаимодействие с пользователем или физическое взаимодействие непосредственно с устройством системы. значения оценки в промежутке: [0; 0,39];

3) Оценка доступности инструментов для использования уязвимости (E):

– атакующий может найти эксплойты в открытом доступе или же иметь навыки для реализации атаки. значения оценки в промежутке: [0,7; 1];

– атакующий должен иметь более обширные знания, чтобы провести атаку. значения оценки в промежутке: [0,4; 0,69];

– для реализации атаки злоумышленник должен иметь высокую степень квалификации, специальное оборудование и ПО, глубокие знания в области эксплуатации уязвимостей. Значения оценки в промежутке: [0; 0,39];

Вычисляется α_l по формуле:

$$\alpha_l = D \times R \times E,$$

где α_l – это оценка успешности реализации атаки;

D – оценка популярности уязвимости;

R – оценка простоты реализации атаки;

E – оценка доступности инструментов для использования уязвимости.

Расчет оценки успешности реализации атаки производится по следующему правилу агрегации. В первом случае, если атаки рассматриваются одновременно с условием «И», то оценка успешности реализации атаки является произведением оценок нескольких успешных атак на компонент системы. Если же атаки рассматриваются с условием «ИЛИ», то выбирается максимальное значение оценки:

$$\alpha_l = \begin{cases} \prod_{i=1}^{n} \alpha_{l.i} \\ \alpha_l = \max(\alpha_{l.i}), i = 1...n \end{cases},$$

где n- количество оценок успешности реализации атаки, соответствующих каждой угрозе для одного компонента системы.

α_i – эта оценка характеризует, какие потенциальные потери несет пользователь при утрате или раскрытии конфиденциальных данных. Компрометация данных возникает при успешном достижении поставленной цели злоумышленником. Показатель представляет собой максимальный потенциальный вред, наносимый субъекту данных при достижении поставленной цели. Если значение $\alpha_i \le 0{,}3$, то влияние злоумышленника на конфиденциальные данные минимально, в противном случае, если $\alpha_i \ge 0{,}7$, то влияние высокое, следовательно, конфиденциальные данные пользователя находятся под угрозой компрометации.

При определении α_i основой является расчет уровня идентификации субъекта данных и чувствительность контекста конфиденциальной информации. Формально, предполагается, что существует матрица решений $\gamma = M(i_l, d_c)$, где i_l – это уровень идентификации, d_c – уровень чувствительности конфиденциальных данных, для расчета влияния. Существует соответствующая функция поиска $f_\theta : i_l, d_c \to \alpha_i$, для γ.

Уровень идентификации (i_l) – это показатель $i_l \in [0;10]$, определяющий степень идентификации субъекта данных. Идентификация может быть произведена за счет явных идентификаторов пользователя в системе (например, адрес электронной почты, идентификаторы устройств (MAC-адрес,

серийный номер, IMEI), биометрические идентификаторы и т.д.

Уровень чувствительности конфиденциальных данных (d_c) – это показатель $d_c \in [0;10]$, который определяет нарушение конфиденциальности информации, воспринимаемое субъектом данных в определенном контексте. Значение показателя $d_c \le 3$ указывает на то, что данные используются и обрабатываются устройствами с низким воздействием на уровень конфиденциальности информации, $d_c \ge 7$ указывает, что данные используются в контексте «критический» уровень конфиденциальности информации, что предполагает возможность зависимости уровня конфиденциальности от показателя i_l. Также показатель может быть зависим от места, где установлено устройство, тогда в зависимости от политики автоматизированной системы «Умный дом» можно назначать уровень чувствительности данных.

Путем экспертной оценки параметры были определены в виде градации:

1) Оценка степени подверженности пользователей (U):

– затронута вся семья, а также более широкий круг лиц, связанный непосредственно с семьей. Значение оценки равно 3;

– поражены несколько членов семьи. Значение оценки равно 2;

– пострадал один пользователь. Значение оценки равно 1;

2) Оценка степени негативного воздействия (Dm):

– происходит утечка личной конфиденциальной информации о устройстве системы «умного» дома, включая информацию об уязвимых субъектах данных, вызывающая финансовый/психологический/физический ущерб. значение оценки 4-5;

– произошла утечка конфиденциальных данных, при этом ущерб не несет значительных потерь, не наносит прямого или косвенного ущерба. значение оценки 2-3;

– произошла утечка конфиденциальных данных, при этом, пользователи никак не ощущают воздействия на их безопасность. значение оценки 0-1.

Вычисляется α_i:

$$\alpha_i = U \times Dm,$$

где α_i – оценка негативных последствий от атаки;

U – оценка степени подверженности атакам пользователей;

Dm – оценка степени негативного воздействия;

Чтобы посчитать α_i используется правило агрегации и определяется уравнением:

$$\alpha_i = \max(\alpha_{i.i}), i = 1...n,$$

где n – количество оценок негативных последствий от атаки, соответствующих каждой угрозе для одного компонента системы.

Исходя из общепринятой методики оценки рисков в сфере компьютерной безопасности, риск нарушения конфиденциальности информации — это комбинация оценки успешности реализации атаки и последствий (ущерб). В частности, при умножении получается численная мера риска. Это значение указывает на приоритеты в мерах регулировании рисков, которые нужно предпринять для повышения защищенности автоматизированной системы «Умный дом».

Описывается мера риска следующим уравнением:

$$r_\mu = \alpha_{l.\mu} \times \alpha_{i.\mu}, \mu = 1...n,$$

где r_μ – мера риска для компонента автоматизированной системы;

n – количество компонентов автоматизированной системы.

Численные значения показателей риска нарушения конфиденциальности информации:

1) Уязвимость в компоненте системы «Умный дом» можно с легкостью эксплуатировать в целях нарушения

конфиденциальности информации. Мера в промежутке [7; 10];

2) Уязвимость в компоненте системы «Умный дом» сложнее использовать, но при определенных условиях она может поставить под угрозу конфиденциальность информации пользователей. Мера в промежутке [4; 6,9];

3) Уязвимость в компоненте системы «Умный дом» требует больших усилий для возможности эксплуатации или эксплуатация уязвимости приводит к незначительным последствиям нарушения конфиденциальности информации. Мера в промежутке [0,1; 3,9];

4) Нет риска эксплуатации уязвимости в системе «Умный дом». Мера риска равна 0.

Исходя из выявленных угроз для каждого компонента системы, оценки успешной реализации атак и негативных последствий от атак указаны в табл. 1.

Результаты проведенной оценки мер риска представлены на рис. 1.

Таблица 1

Данные для расчета показателя риска нарушения конфиденциальности информации автоматизированной системе «Умный дом»

Устройство/ Канал/ Субъект	Тип атаки	Подверженная угрозе информация	α_l	α_i
Устройство 0 (Облачный сервис)	Атака на сетевую службу	-	0,3	8
Устройство 1 (Мобильное устройство)	Захват узла	-	0,5	7
	Атака на сетевую службу	-	0,5	2
Устройство 2 (Умная колонка)	Атака на сервис	-	0,7	4
Устройство 3	Атака на сервис	-	0,8	10
(Дверной звонок)				
Устройство 4 (Дверной замок)	Кража узла	-	0,7	10
Устройство 5 (Голосовой помощник)	Атака на сервис	-	0,5	6
Канал 0	MiTM	Данные команд управления	0,6	4
Канал 1	Подслушивание	Видео	0,5	4
Канал 2	Подслушивание	Видео	0,7	6
	MiTM	Видео	0,8	8

Продолжение табл. 1

Данные для расчета показателя риска нарушения конфиденциальности информации автоматизированной системе «Умный дом»

Устройство/ Канал/ Субъект	Тип атаки	Подверженная угрозе информация	α_l	α_i
Канал 3	Подслушивание	Аудио	0,5	5
Канал 4	MiTM	Данные команд управления	0,7	4
Канал 5	Подслушивание	Аудио	0,5	4
Канал 6	Подслушивание	Аудио	0,5	6
Провайдер	Социальная инженерия	-	0,4	10
Пользователь 1	Социальная инженерия	-	0,2	6
Пользователь 2	Социальная инженерия	-	0,2	6

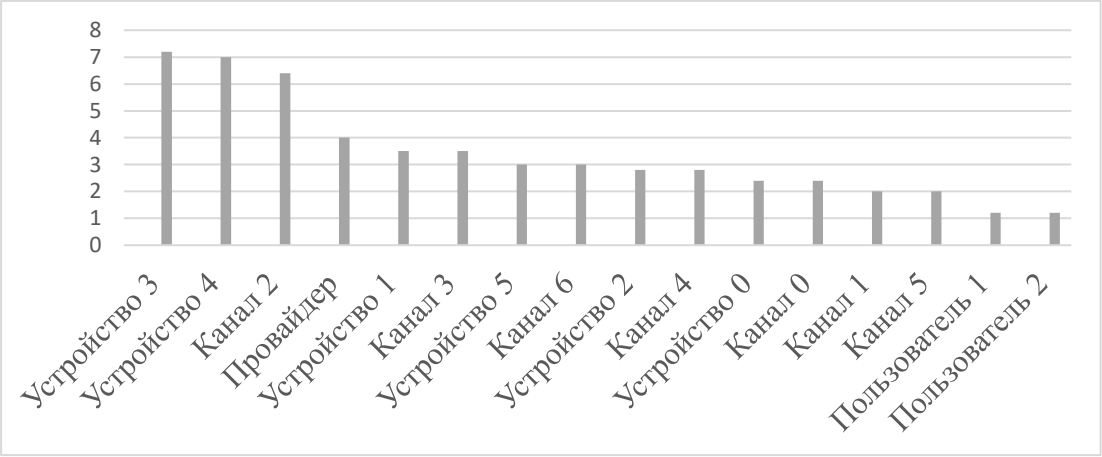

Рис. 1. Меры риска для компонентов системы «Умный дом»

Алгоритм оценки рисков нарушения конфиденциальности информации в автоматизированной системе «Умный дом»

Для детального рассмотрения угроз необходимо построить модель автоматизированной системы «Умный дом», включая среду дома, настройки системы, способы обработки и виды конфиденциальной информации, передаваемой между устройствами, каналы передачи информации. Таким образом, сформировав структурно-параметрическую и логическую модели системы.

В представленном программном алгоритме из собранных данных об исследуемой системе понадобится количество каналов и конечных устройств, параметры которых будут вводится в следующих итерациях.

Алгоритм получения меры риска нарушения конфиденциальности информации для каждого компонента автоматизированной системы «Умный дом» представлен на рис. 2.

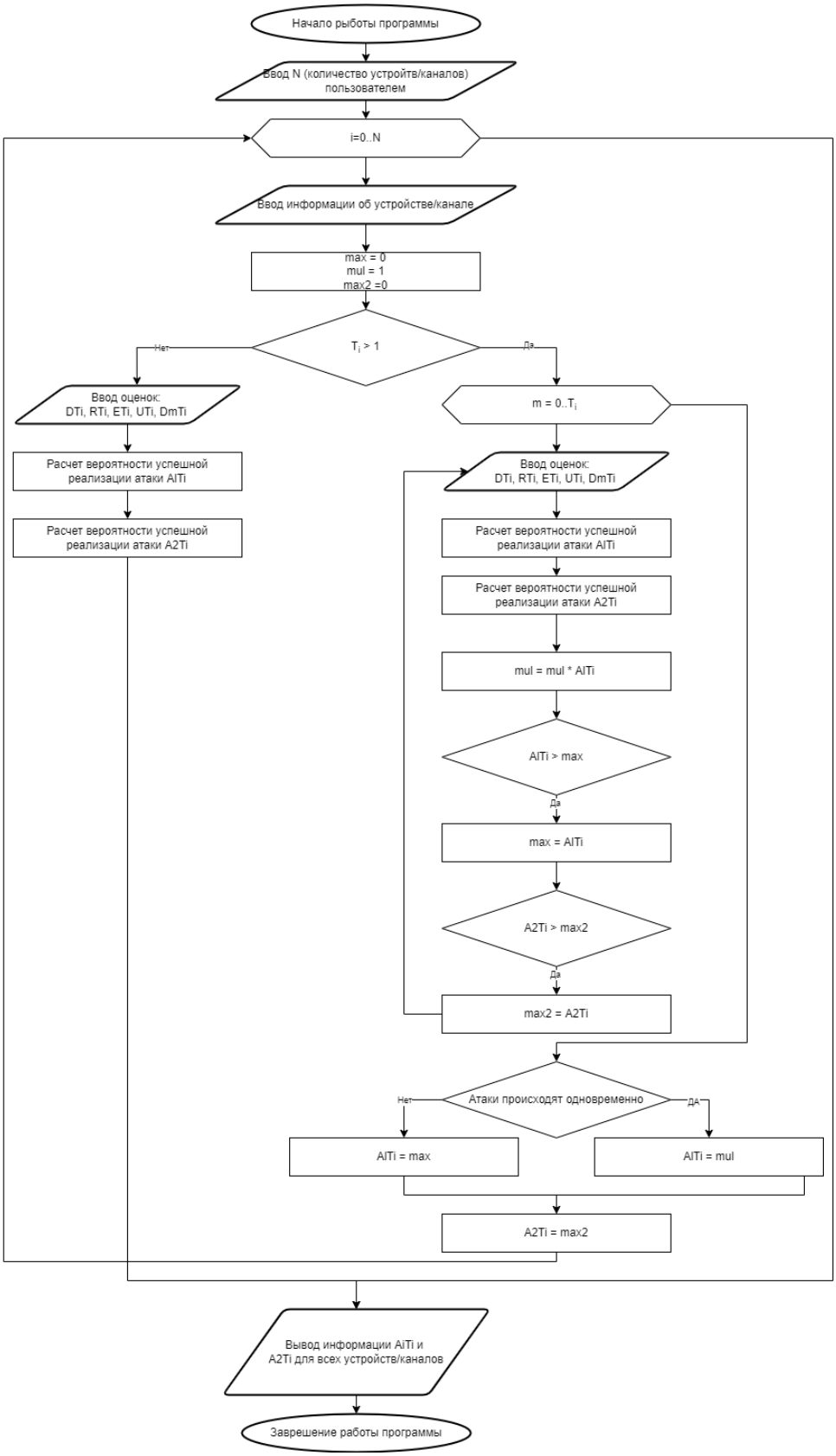

Рис. 2. Алгоритм расчета меры риска нарушения конфиденциальности информации

Заключение

Предложенный алгоритм оценки рисков нарушения конфиденциальности информации в автоматизированных системах «Умный дом» на базе облачных сервисов может быть использован в рамках проведения аудита системы на предмет обеспечения допустимого уровня конфиденциальности информации. Перспектива данного исследования заключается в получении общей оценки защищенности автоматизированной системы «Умный дом».

Список литературы

1. Sarkar H. A., Subhi R. M. A survey on Security and Privacy Challenges in Smarthome based IoT, International Journal of Contemporary Architecture "The New ARCH", 2021, no. 2(8), pp. 489 – 510.

2. Hammi B., Zeadally S., Khatoun R., Nebhen J. Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. Article in Computers & Security, 2022.

3. Ling Z., Luo J., Xu Y., Gao C., Wu K., Fu X. Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet Things, 2017, no. 4, pp. 1899–1909.

4. Notra S., Siddiqi M., Gharakheili H.H., Sivaraman V., Boreli R. An experimental study of security and privacy risks with emerging household appliances. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 2014, pp. 79–84.

5. Sivaraman V., Chan D., Earl D., Boreli R. Smart-phones attacking smart-homes. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 2016, pp. 195–200.

6. Alrawi O., Lever C., Antonakakis M., Monrose F. Security evaluation of home-based iot deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 1362–1380.

7. Nicklas J.P., Mamrot M., Winzer P., Lichte D., Marchlewitz S., Wolf K.D. Use case-based approach for an integrated consideration of safety and security aspects for smart home applications. In Proceedings of the 2016 11th System of Systems Engineering Conference (SoSE), Kongsberg, Norway, 2016, pp. 1–6.

8. Bugeja J., Jacobsson A., Davidsson P. PRASH: A Framework for Privacy Risk Analysis of Smart Homes. Internet of Things and People Research Center, Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden, 2021, no. 21, pp. 1–29.

9. Lopez, J., Rios, R., Bao, F., Wang, G. Evolving privacy: From sensors to the Internet of Things. Future Gener. Comput. Syst., 2017, no. 75, pp. 46–57.

10. Li, C., Palanisamy, B. Privacy in internet of things: From principles to technologies. IEEE Internet Things J., 2018, no. 6, pp. 488–505.

11. Kenneally, E. Privacy and Security. IEEE Internet Things Mag., 2018, no. 1, pp. 8–10.

12. Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., Lepri, B. The privacy implications of cyber security systems: Atechnological survey. ACM Comput. Surv. (CSUR), 2018, no. 51, pp.1–27.

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

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 14.07.2022

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, начальник отдела, Концерн «Созвездие», e-mail: s.a.ermakov@sozvezdie.su

Гусарева Юлия Александровна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Болгов Андрей Александрович – аспирант, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Кострова Вера Николаевна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

IMPROVING THE SECURITY OF THE SMART HOME AUTOMATED SYSTEM: ALGORITHM FOR ASSESSING THE RISKS OF BREACH THE CONFIDENTIALITY OF INFORMATION

S.A. Ermakov, Yu.A. Gusareva, A.A. Bolgov, V.N. Kostrova

The article proposes a procedure for calling a secure "Smart Home" security system from attacks aimed at violating the confidentiality of potential and detected information in the information transmission channel and at the output. It is based on algorithms for assessing risk and sensitivity to the sensitivity of the Smart Home system. In the work, structural-parametric and logical models are carried out that take into account the architecture and topology of the autonomous system "Smart Home", built on the basis of a cloud service, a danger model that includes a description of detection and attacks for each structural area of system coverage, and a toolkit for calculating risk assessments is proposed. The obtained results in the form of a numerical assessment make it possible to perform an analysis of the risk of confidentiality violation for each component of the system, to identify and inform about the risks and users of the United Home system about the detection of system segments, and to consider it from the perspective of information confidentiality violation.

Keywords: internet of things, risk, attacks, privacy, smart home.

Submitted 14.07.2022

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Head of Department, Concern «Sozvezdie», e-mail: s.a.ermakov@sozvezdie.su

Yuliya A. Gusareva – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Andrey A. Bolgov – graduate student, Voronezh State Technical University, e-mail: mnac@comch.ru

Vera N. Kostrova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru