DOI 10.36622/VSTU.2022.25.2.011
УДК 004.8 : 04.077

ОСНОВАННАЯ НА РИСКАХ АДАПТИВНАЯ ПРОЦЕДУРА КОНТРОЛЯ ДОСТУПА ДЛЯ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

В работе предложена адаптивная процедура контроля доступа на основе рисков для системы Интернета вещей. Выявлены ограничения существующих статических процедур контроля доступа применительно к системам Интернета вещей. Определена необходимость использования динамической процедуры контроля доступа, основанной на рисках. В работе проанализированы существующие на сегодняшний день проблемы в данном направлении. Сформулированы задачи и методы для решения выявленных при анализе различных источников проблем. Предложена адаптивная процедура контроля доступа, основанная на рисках. Подробно описаны ее основные элементы и представлена блок-схема работы алгоритма этой процедуры. Представлены методы исследования, которые необходимо использовать для решения поставленных задач исследования. В заключении, представлено краткое изложение основных результатов, полученных в данной статье.

Ключевые слова: нечеткая логика, риск, количественная оценка, качественная оценка, оценка риска, экспертная оценка.

Введение

Интернет вещей – это динамическая по своей природе система, в которой вся окружающая среда и разнородные объекты (вещи) могут быть соединены вместе для обмена различными данными и создания новых приложений и сервисов. Несмотря на то, что Интернет вещей обладает огромными преимуществами, возникает ряд проблем, особенно в области безопасности. Из-за неоднородного и распределенного характера системы Интернета Вещей достижение более высокого уровня безопасности является огромной проблемой. Кроме того, применение сложных алгоритмов безопасности может повлиять на удобство использования данной системы. Следовательно, для системы Интернета вещей конечной целью является создание эффективной системы безопасности с учетом удобства использования системы конечными потребителями [1].

Одним из важных элементов для решения проблем безопасности в системах ИВ, является процедура контроля доступа. Эта процедура используется для управления доступом к системным ресурсам, разрешая доступ только авторизованным пользователям, которые успешно прошли аутентификацию [2]. Основной целью системы Интернета вещей является увеличение пропускной способности обмена информацией для максимального использования преимуществ системы и в то же время применения максимально возможных мер безопасности для предотвращения раскрытия конфиденциальной информации. Однако статические процедуры контроля доступа строятся с использованием предопределенных политик, которые дают один и тот же результат в разных ситуациях. Данное бинарное решение (разрешить/запретить) не может обеспечить эффективный уровень безопасности в динамичной и гетерогенной среде, такой как система Интернета вещей [3, 4].

Статические процедуры контроля доступа не могут предоставить требуемую гибкость для различных приложений Интернета Вещей. Помимо этого, эти процедуры управляются системным администратором, который имеет доступ ко всем системным ресурсам. Компрометация учетной записи администратора может привести к утечке почти всех конфиденциальных данных системы [5, 6]. Следовательно, для системы Интернета

вещей требуется динамическая процедура управления доступом.

Процедура контроля доступа на основе рисков – это одна из динамических процедур, которая использует риск безопасности, связанный с запросом доступа, в качестве критерия для определения решения о доступе. Она оценивает величину риска, связанную с каждым запросом доступа. Затем оценка риска сравнивается с политикой управления рисками для принятия решения о доступе [7, 8].

Проблемы исследования

Большинство представленных моделей, основанных на оценке рисков, не были сосредоточены на контексте Интернета Вещей, где миллиарды датчиков могут использоваться для сбора данных в режиме реального времени, а контекстуальные функции – для динамического определения решений о доступе.

Получение числового значения риска угрозы безопасности – это одна из самых больших проблем, которую не удалось решить ранее. Большинство представленных методов оценки рисков не предлагают четкого и точного метода для определения числового значения риска, связанного с каждым запросом доступа.

Большинство представленных моделей, основанных на риске, предлагали использовать пороговое значение риска для разрешения или отказа в доступе без предоставления каких-либо подробностей о том, как определить это пороговое значение риска в различных приложениях.

В источниках [8-11] авторы использовали историю оценки рисков в качестве параметра для определения решений о доступе. Однако история оценки рисков будет недоступна в начале настройки новой процедуры, основанной на рисках, что сделает систему непригодной для использования, пока не будет собрана история оценок рисков.

Обеспечение четкого подхода к оценке рисков было не единственной проблемой, которую не удалось решить ранее. Учитывая рост числа устройств Интернета вещей, требуется быстрый и масштабируемый подход к оценке рисков. Этот подход также не был предложен или рассмотрен. Нет никаких доказательств того, что представленные ранее методы оценки рисков были протестированы на масштабируемость и время отклика, особенно в контексте Интернета вещей.

Большинство существующих процедур контроля доступа не используют метод обнаружения вредоносных действий после предоставления доступа. Помимо этого, в соответствующих процедурах контроля доступа на основе рисков отсутствуют возможности обнаружения отклонений, которые позволяют системе своевременно обнаруживать и предотвращать некорректное поведение во время сеансов доступа.

Конечная цель любого нового подхода – это гарантировать, что он применим в реальных сценариях. Соответствующие процедуры контроля доступа на основе рисков, обсуждаемые в изученной литературе, не имеют никаких способов проверки и оценки рисков их моделей с использованием реальных сценариев, особенно в контексте Интернета Вещей.

Таким образом, после обзора существующей литературы, касающейся процедур контроля доступа на основе рисков для системы Интернета вещей, удалось выявить ряд проблем, связанных с:

– выбором подходящей адаптивной процедуры контроля доступа на основе рисков для систем Интернета вещей;

– выбором подходящего метода для оценки риска, связанного с запросом на доступ;

– определением приемлемых значений риска для принятия решения о доступе в приложениях Интернета вещей;

– сложностью реализации процедуры оценки, основанной на рисках, которая сможет работать при первом использовании или подключении к системе Интернета вещей;

– отсутствием быстрого и масштабируемого метода оценки рисков, чтобы справиться с постоянным увеличением числа устройств Интернета вещей;

– отслеживанием поведения пользователя/агента во время сеанса доступа;

– оценкой применимости предлагаемой модели к реальным сценариям Интернета вещей.

На основе выделенных проблем были сформулированы следующие задачи:

1. Предложить динамическую процедуру контроля доступа на основе рисков для систем Интернета вещей.
2. Предложить четкую и эффективную методику оценки риска для количественной оценки величины риска, связанного с каждым запросом доступа в динамической среде.
3. Предоставить приемлемые значения риска, которые могут быть использованы для принятия решений о доступе.
4. Разработать такую процедуру контроля доступа на основе рисков, которая работает при первом подключении без настройки системным администратором.
5. Предусмотреть масштабируемый метод оценки рисков, который может справиться с постоянным увеличением числа устройств Интернета вещей.
6. Предложить способ обнаружения и предотвращения вредоносных действий во время сеансов доступа.
7. Предоставить способ оценки риска моделей контроля доступа на основе рисков с использованием реальных сценариев.

Для решения исследовательских проблем и выполнения поставленных задач, предлагается адаптивная процедура контроля доступа, основанная на риске. Эта процедура должна использовать контекстуальную информацию, собираемую из среды Интернета вещей, а также обрабатывать эту информацию в режиме реального времени.

Структура процедуры

Несанкционированное раскрытие информации является одной из важнейших проблем в системе Интернета вещей, которую необходимо решить. Существующие статические процедуры контроля доступа не могут решить эту проблему по трем причинам [9, 13]. Во-первых, они не в состоянии справиться с необычными для них ситуациями, в которых сама политика доступа должна быть переопределена, чтобы не останавливать систему. Во-вторых, они не отвечают требованиям обеспечения динамически защищенной информации и совместного использования разрешений в системах совместной работы. В-третьих, они недостаточно гибки, чтобы справиться с меняющейся моделью поведения пользователей, особенно в такой динамичной среде, как Интернет вещей.

Процедура контроля доступа на основе рисков – это одна из динамических процедур, которая выполняет анализ рисков безопасности, связанного с запросом доступа, для принятия решения о доступе. Эта процедура решает одну из основных проблем, как гибкость доступа к системным ресурсам [8, 14].

На рис. 1 представлена предлагаемая адаптивная процедура контроля доступа на основе рисков для системы Интернета Вещей. Данная процедура имеет четыре входных параметра: контекст пользователя/агента, оценка критичности ресурса, оценка критичности операции и история рисков. Эти входные параметры риска используются для оценки значения риска безопасности, связанного с запросом доступа. Затем оцененное значение риска сравнивается с политиками рисков для принятия решений о доступе. Помимо этого, отслеживается поведение пользователя для обнаружения и предотвращения вредоносных действий со стороны авторизованных пользователей во время сеансов доступа. Основная причина выбора только четырех параметров риска заключается в том, чтобы гарантировать, что предлагаемая модель является универсальной и может быть применена в различных приложениях Интернета Вещей. Кроме того, добавление дополнительных параметров риска увеличит вычислительную нагрузку предлагаемой процедуры. Конечная цель предлагаемой риск-ориентированной процедуры – это создать систему, которая умеет работать с большим потоком информации, сохраняя при этом ответственность пользователей за свои действия и предотвращая ожидаемый ущерб, который организация может понести из-за раскрытия конфиденциальной информации. Более того, организации смогут динамически контролировать небезопасные

информационные потоки, основываясь на своей политике принятия риска относительно выбранной системы Интернета вещей [15, 16].

Предлагаемая процедура, основанная на оценке рисков, может хорошо работать в непредвиденных ситуациях, которые часто требуют вмешательства в политики безопасности. Это может произойти из-за того, что политика является неполной или непоследовательной, иногда даже противоречивой. Наиболее распространенными примерами таких ситуаций являются медицинские и военные приложений, где необходимость принятия мер может спасти жизни, а статическое состояние системы может нанести серьезный вред [14].

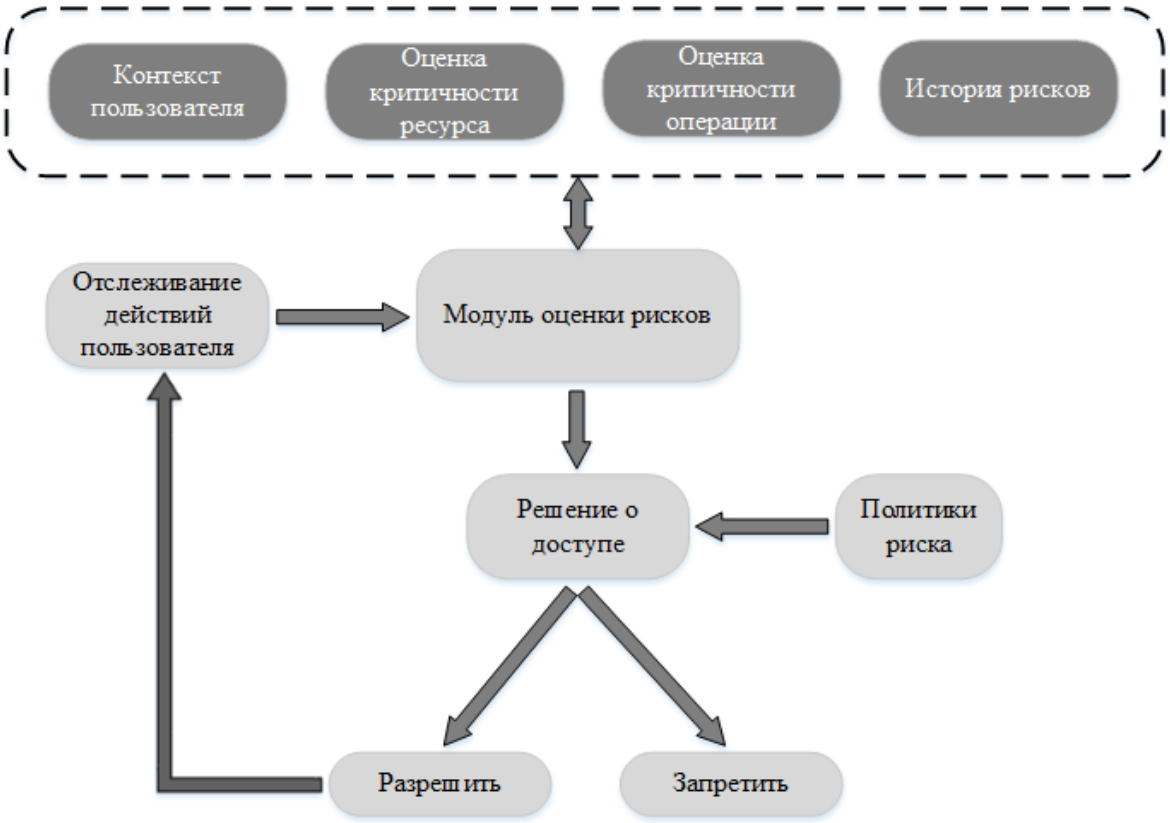

Рис. 1. Предлагаемая адаптивная процедура контроля доступа на основе рисков

К основным компонентам предлагаемой адаптивной процедуры контроля доступа на основе рисков относятся: параметры риска, модуль оценки рисков, политики рисков, принятие решений о доступе и мониторинг действий пользователей.

- Контекст пользователя/агента: Он представляет контекстуальные функции, встроенные в пользователя/агента во время выполнения запроса на доступ. Эти функции обрабатываются при выполнении запроса доступа для определения значения риска безопасности, связанного с запрашивающим пользователем. Местоположение, личность, время, история событий и действий являются наиболее распространенными контекстными функциями пользователя/агента [17]. Определение агент используется для выражения разнообразия приложений в системе Интернета вещей. Агент представляет собой любой системный объект, который имеет возможность сделать запрос на доступ [18]. В остальной части этой статьи слово «Пользователь» будет использоваться, как и для обозначения пользователя, так и для обозначения агента.

- Оценка критичности ресурса: Она описывает, насколько ценен ресурс для владельца или поставщика услуг. Например, данным может присваиваться уровень секретности в зависимости от того, кто должен иметь к ним доступ и какой ущерб

будет нанесен, если они будут раскрыты. Каждому ресурсу в системе Интернета вещей присваивается метрика риска в зависимости от того, насколько ценны данные ресурса для владельца. Следовательно, чем выше оценка критичности ресурса, тем выше показатель риска, связанный с ресурсом.

- Оценка критичности операции: Она представляет последствия определенной операции для конкретного ресурса с точки зрения конфиденциальности, целостности и доступности. Различные операции оказывают разное воздействие и, следовательно, имеют разную величину риска. Например, риск операции «просмотр» ниже, чем риск операции «удаление».
- История рисков: Она содержит предыдущие значения рисков пользователя в отношении конкретного ресурса. Это связано с тем, что история рисков отражает модели поведения пользователей. Более того, она используется для определения хороших и плохих авторизованных пользователей, а также прогнозирование их будущего поведения [9].
- Модуль оценки рисков: Это главный элемент процедуры контроля доступа, основанной на рисках. Он отвечает за учет входных параметров риска для определения количественной оценки значения риска безопасности, связанного с каждым запросом доступа. Существует два способа оценки риска: количественный и качественный. Однако конечной целью в контексте контроля доступа является определение числового значения риска безопасности, связанного с каждым запросом доступа, для определения решения о доступе.
- Политики в отношении рисков: Они в основном используются модулем оценки рисков для принятия решений о доступе. Эти политики создаются владельцем ресурса или администратором системы безопасности для определения условий предоставления или отказа в доступе к определенному ресурсу. Чтобы определить решение о доступе, оценочная величина риска, полученная из модуля оценки риска, сравнивается с политиками рисков для определения решения о доступе. Определение порогового значения риска является одним из распространенных способов построения политики рисков в моделях контроля доступа на основе рисков, в которых доступ предоставляется только в том случае, если оцененное значение риска ниже порогового значения риска.
- Отслеживание действий пользователя: В существующих процедурах контроля доступа, при предоставлении доступа авторизованному пользователю, нет никакого способа для обнаружения или предотвращения деструктивных действий над данными. Поэтому появляется необходимость в модуле отслеживания, который необходим для адаптивной корректировки значения риска на основе поведения пользователя во время сеанса доступа. Предлагаемая процедура, основанная на рисках, использует смарт-контракты для анализа поведения пользователя во время сеанса доступа. Применение смарт-контрактов для выполнения этого процесса является нелегкой задачей, особенно по тому, что это будет первый в истории случай использования смарт-контрактов в данном контексте. Смарт-контракты рассматриваются как программный код для обеспечения функциональной реализации конкретных требований и подтверждения того, что определенные условия и правила были выполнены [19]. Для каждого пользователя будет создан смарт-контракт, отражающий права пользователя. Следовательно, для каждого сеанса доступа будет сравниваться поведение пользователя со смарт-контрактом, чтобы убедиться, что пользователь соблюдает условия смарт-контракта, для предотвращения любого потенциального нарушения безопасности во время сеансов доступа.
- Решение о доступе: Это решение о том, предоставлять или отказывать в доступе. Решение о доступе не связано с разрешениями. Оно связано с тем, какие ресурсы использует пользователь и какие действия выполнит при запросе доступа. Таким образом, будут предоставлены или отклонены только запрошенные разрешения. Решение о доступе в процедуре контроля доступа, основанной на риске, принимается на основе расчетной величины риска каждого

запроса на доступ. Затем оцененное значение риска сравнивается с политиками рисков, чтобы определить, следует ли предоставить или запретить доступ. Поскольку смарт-контракты используются в качестве средства выявления аномалий для обнаружения и предотвращения деструктивных действий во время сеансов доступа, то для принятия решения о доступе были предложены три диапазона риска, как показано на рис. 2.

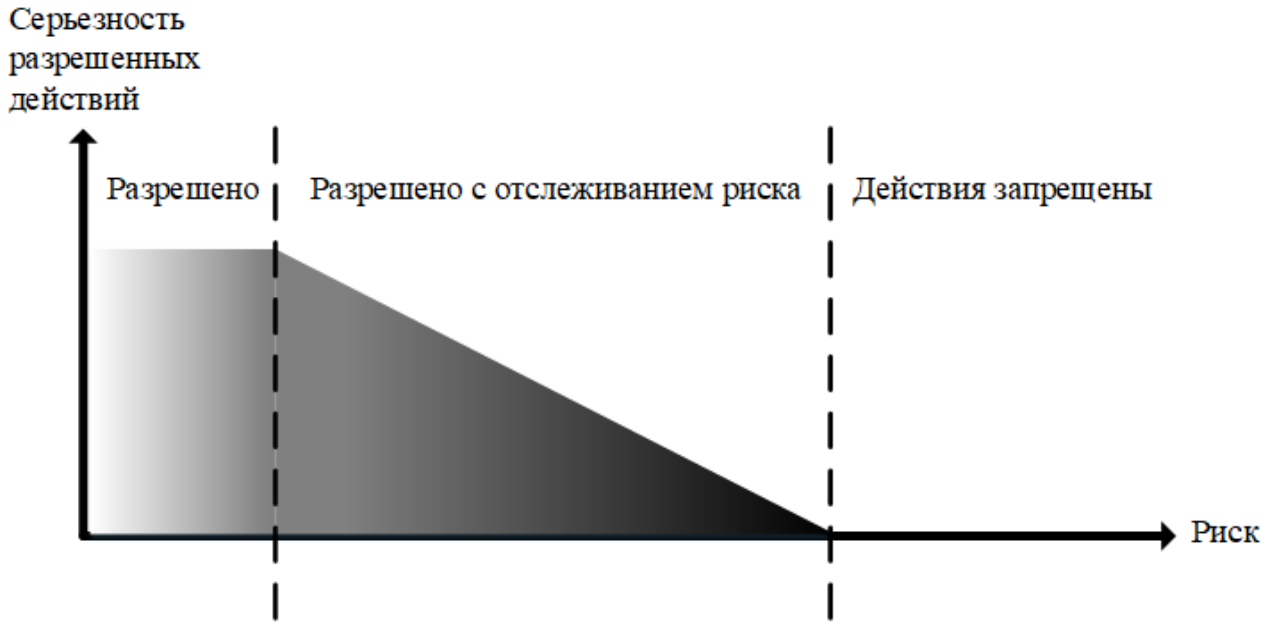

Рис. 2. Диапазоны принятия решений о доступе

– Диапазон разрешения: Этот диапазон используется для предоставления доступа без отслеживания действий пользователя во время сеанса доступа, чтобы сохранить конфиденциальность пользователя. Этот диапазон очень узок с точки зрения величины риска. Он используется в основном для обеспечения доступа пользователей, связанных с очень низким уровнем риска, без контроля, например, владельца устройства или администратора системной безопасности.

– Диапазон разрешения с отслеживанием риска: Этот диапазон используется для предоставления доступа с отслеживанием поведения и действий всех пользователей во время сеанса доступа для обнаружения и предотвращения любой потенциальной вредоносной активности. Конечная цель предлагаемой процедуры контроля доступа на основе рисков – увеличить обмен информацией и в то же время гарантировать безопасность системных ресурсов. Поэтому для отслеживания действий пользователя, во время сеанса доступа, используются смарт-контракты. Таким образом, этот диапазон достаточно широк, что содержит в себе большую часть доступа к системным ресурсам.

– Диапазон запрета: Из-за высокого значения риска, доступ будет запрещен внутри этого диапазона.

Алгоритм работы предлагаемой процедуры

Предлагаемая процедура контроля доступа на основе рисков обеспечивает динамический метод авторизации различных типов пользователей в системе Интернета вещей путем оценки значения риска безопасности, связанного с каждым запросом доступа. Чтобы понять предлагаемую модель, основанную на оценке рисков, на рис. 3 представлено подробное описание процесса обработки запроса на доступ.

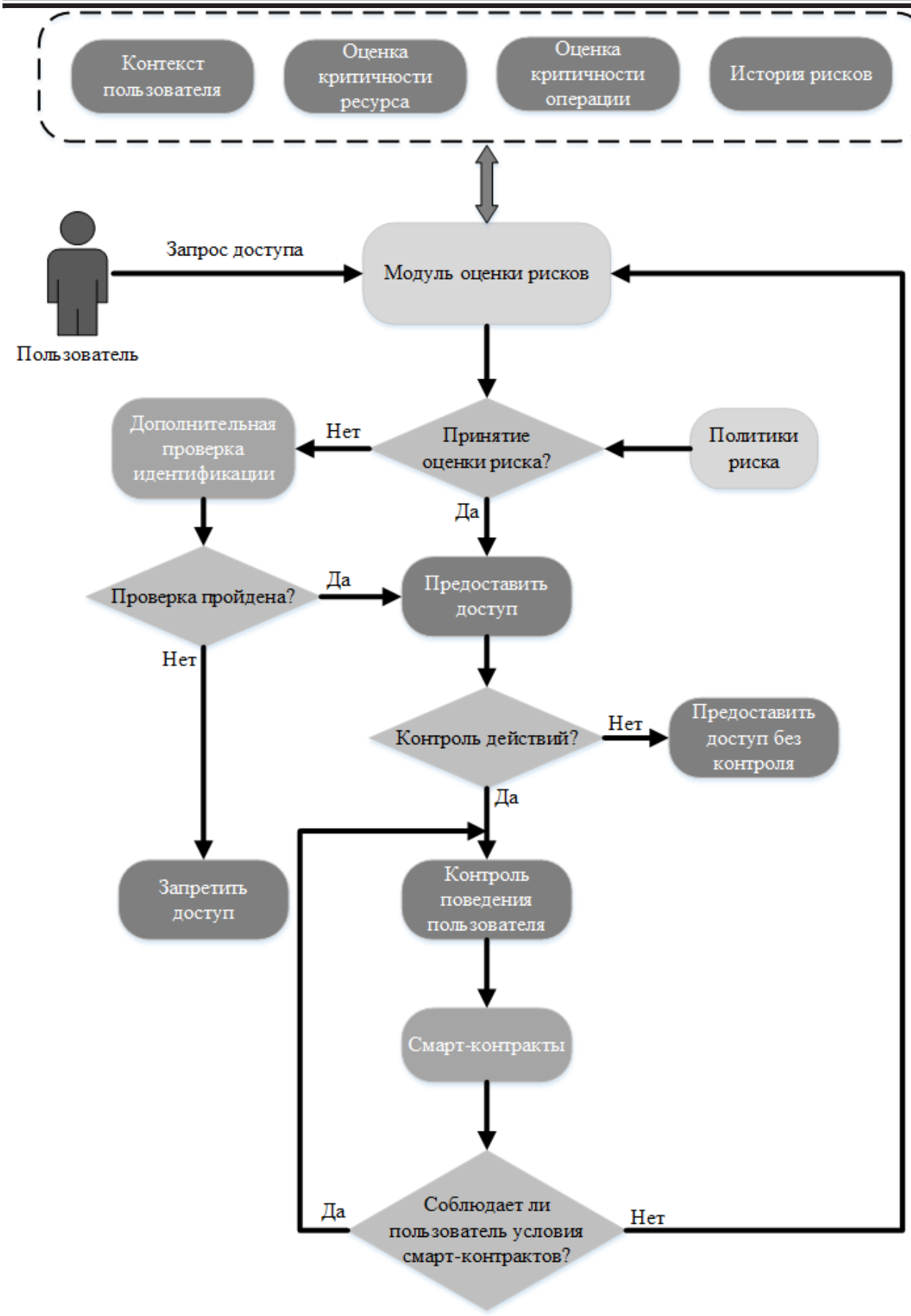

Рис. 3. Блок-схема алгоритма работы, предлагаемой адаптивной процедуры контроля доступа на основе рисков

Работа процедуры начинается, когда диспетчер контроля доступа получает запрос на доступ от пользователя. Диспетчер контроля доступа запрашивает значения параметров риска (контекстные характеристики пользователя, оценку критичности ресурса, оценку критичности операции и историю рисков) запрашивающего пользователя. Модуль оценки риска использует эти значения для оценки общего значения риска, связанного с запросом доступа. Затем оцененное значение риска сравнивается с политиками рисков для определения решения о доступе. На данный момент есть два решения:

а) Если доступ предоставлен, то возможны два сценария. Первый сценарий заключается в том, что, если оценочное значение риска запроса доступа находится в пределах разрешенной полосы, доступ будет предоставлен без контроля действий пользователя во время сеанса доступа. Второй сценарий заключается в том, что, если оценочное значение риска запроса доступа находится в пределах диапазона «Разрешить с отслеживанием риска», модуль мониторинга будет отслеживать и записывать поведение и действия пользователя для обнаружения и предотвращения потенциальных вредоносных действий. Смарт-контракт будет анализировать отслеживаемые данные, чтобы определить, соблюдает ли пользователь условия контракта или нет. Если пользователь соблюдает условия контракта, система будет продолжать отслеживать поведение пользователя, а если нет, то она вернется к модулю оценки рисков, чтобы уменьшить права доступа пользователя или завершить сеанс доступа, тем самым, остановив любую потенциальную вредоносную активность.

б) Если в доступе отказано, система попросит пользователя предоставить дополнительные данные для идентификации, чтобы не блокировать авторизованного пользователя и снизить частоту ложных срабатываний. Если пользователь предоставил необходимые идентификационные данные, доступ будет предоставлен, и работа процедуры продолжится, как в решении «а». Если пользователь не предоставит правильные идентификационные данные, система откажет в доступе.

Решения исследовательских задач

Существует ряд исследовательских проблем, которые были описаны выше. Цель этого исследования – предложить наилучшие решения этих проблем. В табл. 1 представлено краткое изложение предлагаемых решений.

Таблица 1

Предлагаемые решения исследовательских проблем

Исследовательские проблемы	Предлагаемые решения
Выбор подходящей адаптивной процедуры контроля доступа на основе рисков для систем Интернета вещей.	Предлагается динамическая и адаптивная процедура контроля доступа на основе рисков, которая использует контекстную информацию в режиме реального времени, собираемую из среды Интернета вещей, для принятия решений о доступе. Эта процедура может быть использована в различных приложениях Интернета вещей для адаптации к неожиданным ситуациям и обеспечения гибкого способа определения решений о доступе.
Выбор подходящего метода для оценки риска, связанного с запросом на доступ.	Предоставление четкой и точной методики для получения количественной оценки риска при каждом запросе доступа. После рассмотрения существующих методов оценки рисков для реализации процесса оценки рисков в предлагаемой процедуре была выбрана система нечеткой логики с экспертными оценками. Будет предоставлена четкая и подробная реализация подхода к оценке рисков.

Продолжение табл. 1

Исследовательские проблемы	Предлагаемые решения
Определение приемлемых значений риска для принятия решения о доступе в приложениях Интернета вещей.	Предлагаются три диапазона принятия решений о риске для предоставления или отказа в доступе. Первый диапазон предоставляет доступ. Второй диапазон так же предоставляет доступ, но уже с отслеживанием риска. Третий диапазон запрещает доступ. В ходе этого исследования будут опрошены эксперты по безопасности, чтобы определить приемлемые значения риска для каждого диапазона.
Сложность построения процедуры, основанной на рисках, которая сможет работать при первом использовании или подключении к системе Интернета вещей.	Одна из проблем в существующих процедурах, основанными на риске, заключается в том, что они не могут работать при первом включении, пока не будут собраны данные о предыдущих значениях риска. Поэтому можно решить эту проблему путем внедрения процесса «холодного запуска», которое позволит предлагаемой процедуре, основанной на рисках, работать при первом же использовании или подключении.
Отсутствие быстрого и масштабируемого метода оценки рисков, который мог бы справиться с постоянным увеличением числа устройств Интернета вещей.	Для решения этой проблемы предлагается адаптивная система нейро-нечеткого вывода (ANFIS). Эта система выбрана из-за того, что обычная система нечеткой логики требует больших временных затрат и не обладает необходимой масштабируемостью.
Отслеживание поведения пользователя/агента во время сеанса доступа.	Предлагаемая процедура, основанная на рисках, обеспечивает возможность обнаружения деструктивных действий с использованием смарт-контрактов. Она отслеживает и анализирует поведение пользователя во время сеанса доступа для обнаружения и предотвращения потенциальных вредоносных действий.
Оценка применимости предлагаемой модели к реальным сценариям Интернета вещей.	Чтобы оценить и доказать применимость предложенной риск-ориентированной процедуры в реальных сценариях, будут рассмотрены несколько тематических приложений Интернета Вещей.

Методология исследования

Построение адаптивной процедуры контроля доступа на основе рисков для системы Интернета вещей включает в себя множество методов исследования для достижения поставленных целей.

Для проведения исследований могут использоваться две исследовательские методологии: качественная и количественная.

Количественная методология исследований зависит от измерений и анализа данных для определения взаимосвязи между одним набором данных и другим, для объяснения определенного явления. Измерение этих переменных может привести

к количественной оценке, которые поддаются выводам. Таким образом, в данной методологии делается акцент на статистические показатели достоверности [20]. В ней используются стандартные инструменты, содержащие закрытые вопросы, такие как опросы [21]. Количественные исследования оцениваются либо с помощью описательной, либо с помощью логической статистики [22]. Описательная статистика используется для описания характеристик конкретной выборки данных, в то время как логическая статистика используется для определения вероятности обобщения характеристик от небольших выборок к более крупным [22].

Методология качественного исследования связана только с определением значения и пониманием того или иного явления. Она не связана с количественной оценкой явления, а обеспечивает понимание явления посредством наблюдения [20, 23, 24]. Качественные методы направлены на то, чтобы ответить на вопрос «что» и «как» [22]. Эти методы могут включать в себя опросы, наблюдения, документы, открытые вопросы и аудиовизуальные данные.

Таблица 2

Предлагаемые методы исследования, для решения выявленных проблем

Исследовательские проблемы	Метод исследования	Описание
Выбор подходящего метода для оценки риска, связанного с запросом на доступ.	Опрос экспертов	После рассмотрения существующих методов оценки рисков в соответствующих моделях, основанных на риске, в качестве подходящего метода была выбрана нечеткая логика с экспертными оценками. Необходимо опросить экспертов по безопасности Интернета вещей, чтобы проверить предложенную модель и задать нечеткие правила.
Определение приемлемых значений риска для принятия решения о доступе в приложениях Интернета вещей.	Опрос экспертов	Опросить экспертов по безопасности Интернета вещей, чтобы определить приемлемые значения риска для предложенных трех диапазонов рисков.
Сложность построения процедуры, основанной на рисках, которая сможет работать при первом использовании или подключении к системе Интернета вещей.	Опрос экспертов	Чтобы внедрить решение проблемы «холодного запуска», необходимо опросить достаточное количество научных сотрудников по безопасности, для установки нечетких правил.
Отсутствием быстрого и масштабируемого метода оценки рисков, чтобы справиться с постоянным увеличением числа устройств Интернета вещей.	Эксперименты	Для решения проблем временных затрат и масштабируемости, связанных с системой нечеткой логики, предлагается использовать систему ANFIS. Также необходимо провести несколько экспериментов по внедрению процесса оценки рисков с использованием подходов ANFIS.

Продолжение табл. 2

Исследовательские проблемы	Метод исследования	Описание
Отслеживание поведения пользователя/агента во время сеанса доступа.	Моделирование	В этом исследовании для отслеживания поведения пользователей во время сеансов доступа, будут использоваться смарт-контракты. Для моделирования работы смарт-контрактов используются диаграммы MATLAB Simulink и Stateflow, чтобы оценить работу смарт-контрактов при обнаружении вредоносных действий.
Оценка применимости предлагаемой процедуры к реальным сценариям Интернета вещей.	Сценарии доступа	Чтобы проверить применимость предложенной процедуры контроля доступа на основе рисков в реальных приложениях Интернета вещей, предложены сценарии управления доступом для трех приложений Интернета вещей.

Количественные модели требуют точной числовой информации о структуре системы и ее начальном состоянии, которая представлена количественно [22]. Когда такие данные недоступны, количественные модели сталкиваются со многими ограничениями. Тогда как, качественные модели отображают все возможные варианты поведения, но только в качественных терминах [23]. Основная цель этого исследования – создать динамическую и адаптивную процедуру управления доступом на основе рисков для систем Интернета Вещей, которая может работать в непредсказуемых ситуациях, используя не только политики доступа, но и функции контекста в режиме реального времени при принятии решения о доступе. Для достижения поставленной цели в этом исследовании предлагается множество различных методов. В табл. 2 представлено краткое описание методов исследования, используемых для решения исследовательских проблем.

Описание методов исследования, предложенных в данной работе

– Опрос является одним из распространенных методов сбора качественных данных. Он может быть структурированным, полуструктурированным и неструктурированным [24]. Он считается неофициальным методом проверки, поскольку основаны на человеческой субъективности. Данные, полученные в результате этих опросов, могут быть как качественными, так и количественными, в зависимости от вопросов, предлагаемых в опросе [25]. В этом исследовании предлагается использование полуструктурированных опросов. Этот тип опроса дает возможность более подробно отвечать на вопросы. Вопросы в рамках полуструктурированных опросов позволяют получить ожидаемую информацию наряду с другой непредвиденной информацией [24].

– Моделирование позволяет исследователям смоделировать реальное поведение системы с учетом ее организационной сложности. Если другие методы отвечают на вопросы «Что произошло, как и почему?», то моделирование помогает ответить на вопрос «Что, если?». Моделирование позволяет изучать сложные системы, потому что оно создает наглядное представление о будущем, «продвигаясь вперед», в то время как другие методы исследования пытаются оглядываться назад через историю, чтобы определить, что произошло и как [25]. В этом исследовании предлагается использовать моделирование, как метод имитации работы смарт-контрактов для отслеживания действий пользователей во время сеансов доступа к системе Интернета вещей.

– Эксперименты – это систематический научный подход, который позволяет исследователю управлять одной или несколькими переменными и анализировать результат работы исследуемой системы. Настоящее экспериментальное исследование считается успешным только тогда, когда исследователь подтверждает, что изменение зависимой переменной происходит исключительно из-за манипулирования независимой переменной [25]. Результаты экспериментальных исследований, однажды проанализированные, могут быть применены к другим подобным аспектам. В этом исследовании предлагается использовать эксперименты для построения процесса оценки рисков с использованием подходов ANFIS и NFS.

Заключение

Одной из основных проблем, выявленных при изучении данной предметной области, является отсутствие динамической процедуры контроля доступа, основанной на рисках, которая могла бы адаптироваться к различным априорно неизвестным обстоятельствам в системах Интернета Вещей. Поэтому была предложена адаптивная модель контроля доступа на основе рисков для системы Интернета Вещей. Эта модель использует риск безопасности в качестве критерия для принятия решения о доступе. Она оценивает величину риска, связанную с каждым запросом доступа, используя четыре входных параметра: контекст пользователя/агента, оценку критичности ресурса, оценку критичности операции и историю рисков. Затем оцененное значение риска сравнивается с политиками рисков для определения решения о доступе. Чтобы предотвратить и обнаружить деструктивное действие со стороны авторизованных пользователей во время сеанса доступа, предлагаемая процедура использует смарт-контракты для контроля действий пользователей и адаптивной корректировки их значений риска. Помимо этого, были представлено описание того, как предлагаемая адаптивная процедура, основанная на риске, будет решать исследовательские проблемы, выявленные из анализа существующих подходов и методов.

В итоге, были представлены методы исследования, которые могут быть использованы для решения поставленных задач, в контексте тематики выбранного исследования.

Список литературы

1. Habib K. Context-Aware Authentication for the Internet of Things. / K. Habib, W. Leister /// The Eleventh International Conference on Autonomic and Autonomous Systems Fined, 2015. P. 134-139.

2. Liu J.K. Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. / J.K. Liu, M.H. Au, X. Huang, R. Lu, J. Li // IEEE Transactions on Information Forensics and Security. 2016. No. 11(3). P. 484-497.

3. Ramona S.E. Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. / S.E. Ramona // Chinese Business Review. 2011. No. 10(12). P. 1106-1110.

4. Diep N.N. Enforcing Access Control Using Risk Assessment. / N.N. Diep, L.X. Hung, Y. Zhung, S. Lee, Y Lee., H. Lee // The Fourth European Conference on Universal Multiservice Networks. 2007. P. 419-424.

5. Castiglione A. Hierarchical and shared access control. / Castiglione A. [etc.] // IEEE Transactions on Information Forensics and Security. 2016. No. 11(4). P. 850-865.

6. Shen J. Anonymous and Traceable Group Data Sharing in Cloud Computing. / T. Zhou, X. Chen, J. Li, W. Susilo // IEEE Transactions on Information Forensics and Security. 2018. No. 13(4). P. 912-925.

7. Ye N. An efficient authentication and access control scheme for perception layer of internet of things. / N. Ye, Y. Zhu, R.C. Wang, R. Malekian, Q.M. Lin // Applied Mathematics and Information Sciences. 2014. No. 8(4). P. 1617-1624.

8. Shaikh R.A. Dynamic risk-based decision methods for access control systems. / R.A. Shaikh, K. Adi, L. Logrippo // Computers and Security. 2012. No. 31(4). P. 447-464.

9. Li J. A fuzzy modeling approach for risk-based access control in eHealth cloud. / J. Li, Y.

Bai, N. Zaman // Proceedings of 12th IEEE International Conference on Trust. Security and Privacy in Computing and Communications. TrustCom. 2013. P. 17-23.

10. Khambhammettu H. A framework for risk assessment in access control systems. / H. Khambhammettu, S. Boulares, K. Adi, L. Logrippo // Computers & Security. 2013. No. 39. P. 86-103.

11. Namitha S. Risk Based Access Control In Cloud Computing. / S. Namitha, S. Gopalan, H.N. Sanjay, K. Chandrashekaran // International Conference on Green Computing and Internet of Things (ICGCloT). 2015. P. 1502-1505.

12. Britton D., Brown I. A security risk measurement for the RAdAC model. / Naval Postgraduate School (U.S.), 2007. URL: pttps://apps.dtic.mil/dtic/tr/fulltext/u2/a467180.pdf (дата обращения: 15.01.2022).

13. Lee S. Contextual Risk-based access control. / S. Lee, Y.W. Lee, N. Diep, Y. Lee, H. Lee // Proceedings of the 2007 International Conference on Security & Management. 2007. P. 406-412.

14. Dos Santos D.R. A dynamic risk-based access control architecture for cloud computing. / D.R. Dos Santos, C.M. Westphall, C.B. Westphall // IEEE Network Operations and Management Symposium (NOMS). 2014. P. 1-9.

15. Chen P. Fuzzy Multi-Level Security: An Experiment on Quantified Risk – Adaptive Access Control. / P. Chen, C. Pankaj, P.A. Karger, G.M. Wagner, A. Schuett // 2007 IEEE Symposium on Security and Privacy(SP'07). 2007. P. 222–227.

16. Abie H. Risk-Based Adaptive Security for Smart IoT in eHealth. / H. Abie, I. Balasingham // Proceedings of the 7th International Conference on Body Area Networks, (SeTTIT). 2012. P. 269-275.

17. Perera C. Context aware computing for the internet of things: A survey. / C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos // IEEE Communications Surveys and Tutorials. 2014. No. 16(1). P. 414-454.

18. Feitosa E. L. O. Security Information Architecture for Automation and Control Networks. // VIII Brazilian Symposium on Information Security and Computational Systems. 2014. P. 17-30.

19. Watanabe H. Blockchain contract: Securing a blockchain applied to smart contracts. / H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami // IEEE International Conference on Consumer Electronics (ICCE). 2016. P. 467-468.

20. Eldabi T. Quantitative and qualitative decision-making methods in simulation modelling. / T. Eldabi, Z. Irani, R.J. Paul, P. Love // Management Decision. 2002. No. 40(1). P. 64-73.

21. Creswell J.W. Research Design Qualitative, Quantitative, and Mixed Methods Approaches. / Second Edition; SAGE Publications Inc, 2003.

22. Taylor G.R. Integrating Quantitative and Qualitative Methods in Research. / University Press of America, 2nd revise edition, 2005.

23. Berleant D. Qualitative and quantitative simulation: bridging the gap. / D. Berleant, B.J. Kuipers, //Artificial Intelligence. 1997. No. 95. P. 215-255.

24. Pang W. Qualitative, semi-quantitative, and quantitative simulation of the osmoregulation system in yeast. / W. Pang, G.M. Coghill // BioSystems. 2015. No. 131. P. 40-50.

25. Omar A.S. Application of Fuzzy Logic in Qualitative Performance Measurement of Supply Chain Management. / A.S. Omar, M. Waweru, R. Rimiru // International Journal of Information and Communication Technology Research. 2015. No. 5(6). P. 42-55.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 24.05.2022

Информация об авторах

Ермаков Сергей Александрович – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

RISK-BASED ADAPTIVE ACCESS CONTROL PROCEDURE FOR INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The paper proposes an adaptive access control procedure based on risks for the Internet of Things system. The limitations of the existing static access control procedures in relation to the Internet of Things systems are revealed. The necessity of using a dynamic access control procedure based on risks is determined. The paper analyzes the current problems in this direction. The tasks and methods for solving the problems identified in the analysis of various sources are formulated. An adaptive access control procedure based on risks is proposed. Its main elements are described in detail and a flowchart of the algorithm of this procedure is presented. The research methods that need to be used to solve the research tasks are presented. In conclusion, a summary of the main results obtained in this article is presented.

Keywords: fuzzy logic, risk, quantitative assessment, qualitative assessment, risk assessment, expert assessment.

Submitted 24.05.2022

Information about the authors

Sergey A. Ermakov – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

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