DOI 10.36622/VSTU.2022.25.2.008
УДК 004.8 : 04.077

ОБЗОР СУЩЕСТВУЮЩИХ ПРОЦЕДУР КОНТРОЛЯ ДОСТУПА В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

Работа посвящена обзору существующих подходов к реализации контроля доступа, произведен анализ известных процедур контроля доступа и выполнено их сравнение применительно к обеспечению безопасности систем Интернета вещей. Подробно рассмотрены три способа реализации контроля доступа в системах Интернета вещей. Проведен анализ и сравнение статических и динамических процедур контроля доступа. Проанализированы наиболее распространённые процедуры контроля доступа. Рассмотрена процедура контроля доступа по критерию допустимости оценки риска безопасности авторизуемого объекта. Проведен анализ существующих процедур-аналогов для контроля доступа по критерию величины риска. Описаны основные параметры оценки риска для процедуры контроля доступа. Выделены преимущества и недостатки известных процедур и методик контроля доступа в контексте безопасности систем Интернета вещей.

Ключевые слова: контроль доступа, интернет вещей, конфиденциальность, аутентификация, целостность, доступность, риск, параметры риска, безопасность.

Введение

Основная цель процедуры контроля доступа – это запрет на выполнение регламентированных операций неавторизованными пользователями. Таким образом, процедура контроля доступа запрещает любую деятельность, которая может привести к нарушению безопасности [1]. Качественная процедура контроля доступа должна удовлетворять требованиям по обеспечению свойств конфиденциальности, целостности и доступности информации [2].

Дадим определение терминам аутентификация, авторизация и контроль доступа для однозначной интерпретации последующих положений. Аутентификация – это операция по проверки личности пользователя [3]. Авторизация – это разрешение или отказ в доступе аутентифицированному пользователю для выполнения определенных операций с определенными ресурсами. Контроль доступа – это процесс применения политик авторизации. Как только пользователь (агент) аутентифицируется и проходит уровень авторизации, контроль доступа будет обеспечивать соблюдение пользовательских разрешений, то есть будет запрещать пользователю доступ ко всему, что ему не было разрешено [2].

Исторически термин контроль доступа появился при организации дорожного движения в первой половине двадцатого века. [3]. Позднее электронные устройства стали использовать системы контроля доступа для определения попыток доступа с помощью ранее утраченных ключей и ограничения доступа с помощью них. Ранние решения для контроля доступа использовали клавиатуры для ввода персональных идентификационных кодов доступа, а затем они были обновлены до считывателей карт, которые используются до настоящего времени.

На текущий момент контроль доступа реализован на разных уровнях в различных применениях, таких как операционные системы и системы управления базами данных, чтобы контролировать доступные системные ресурсы и разрешать их использовать авторизованным способом только легальным пользователям.

Структурная модель процедуры контроля доступа включает в себя пять основных элементов: субъекты, объекты, действия, привилегии и политики доступа.

- Субъекты – активные сущности в виде пользователей и процессов, которые запрашивают доступ к объектам;
- Объекты – пассивные сущности, содержащие информацию, к которой обращаются субъекты;
- Действия – операции чтения, записи, выполнения и т.д., выполняемые с определенными объектами;
- Привилегии – разрешения на выполнение определенных действий с определенными объектами;
- Политики доступа – набор правил, определяющие решения о доступе (предоставление или отказ в доступе).

Процесс управления доступом проиллюстрирован на рис. 1. Сначала субъект/пользователь для доступа к определенному объекту отправляет запрос диспетчеру контроля доступа. Затем, диспетчер контроля доступа на основании учетных данных субъекта принимает решение о доступе на основе политики контроля доступа. Запрос будет либо удовлетворен, либо отклонен. Если доступ предоставлен, пользователь получает доступ к объекту, если же доступ запрещен, диспетчер завершит сеанс контроля доступа после отправки предупреждающего сообщения о недостаточных полномочиях.

Рис. 1. Последовательность операций контроля доступа

Архитектуры процедуры контроля доступа для Интернета вещей

Основная проблема, связанная с построением модели системы контроля доступа для Интернета вещей, заключается в отсутствии возможности обработать запрос на доступ и принять требуемое решение, поскольку устройства Интернета вещей имеют сильно ограниченные вычислительные ресурсы и память для хранения данных.

Глобально, в настоящее время известны и применимы для систем Интернета вещей три принципа построения системы контроля доступа: централизованный, распределенный, а также централизованно-контекстный [4].

Централизованный подход

При таком подходе логика контроля доступа находится в центральном объекте. Этим объектом, например, может быть сервер, имеющий прямую связь с устройствами Интернета вещей, которыми он управляет. Устройства Интернета вещей отправляют собранные данные в центральный объект, который принимает решение для контроля доступа, как показано на рис. 2. Ключевым преимуществом этого подхода является то, что логика управления доступом расположена во внешнем объекте, у которого нет ограничений по ресурсам, что позволяет использовать стандартные технологии обеспечения безопасности и передовые технологии контроля доступа [4].

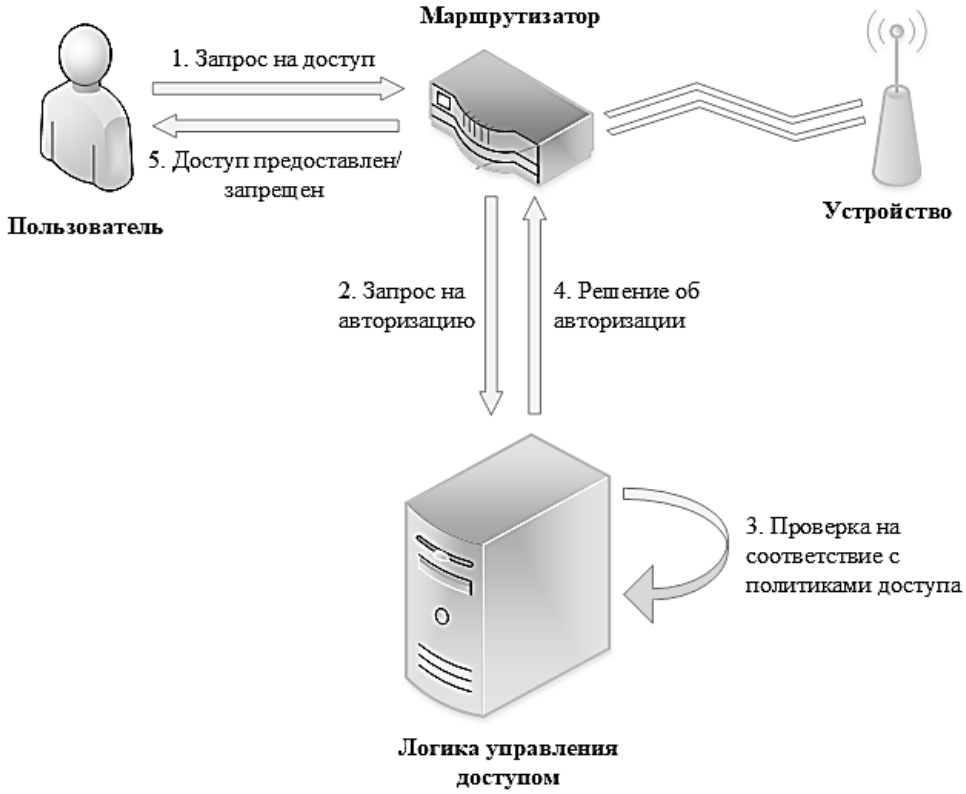

Рис. 2. Процесс управления доступом при централизованном подходе

С другой стороны, централизованный подход имеет и ряд существенных недостатков. При принятии решения о доступе не используется контекстная информация, относящейся непосредственно к устройствам Интернета вещей. Кроме того, поскольку для принятия решений о доступе необходим центральный объект, то этому объекту необходимо анализировать содержимое запроса доступа, что создает угрозу нарушения конфиденциальности для запрашивающей стороны. Также, поскольку единый объект хранит и управляет всеми данными, поступающими с разных устройств Интернета вещей, он становится единой точкой отказа, в которой злоумышленник может скомпрометировать весь объем конфиденциальной информации.

Распределенный подход

При таком подходе логика управления доступом распределена по устройствам Интернета вещей. Эти устройства должны обладать необходимыми аппаратными ресурсами для получения, обработки и отправки информации другим службам и сервисам. Таким образом, устройства Интернета вещей принимают решения о доступе без участия центрального объекта. Процесс управления доступом с использованием распределенного подхода показан на рис. 3. Использование распределенного подхода обладает рядом принципиальных преимуществ. Устройства Интернета вещей перестают быть пассивными объектами и у них появляется возможность управлять циркулирующей информацией. Также, очевидно, что устранятся единая точка отказа [5].

Одной из проблем такого подхода является необходимость расширения функционала устройств Интернета вещей путем добавления логики управления доступом. Кроме того, реализация статических процедур управления доступом будет затруднена в устройствах Интернета вещей с ограниченными аппаратными ресурсами. В дальнейшем целесообразно провести исследование на предмет анализа реализуемости различных известных моделей контроля доступа или внедрения новых предложений, отвечающих требованиям распределенного подхода [4].

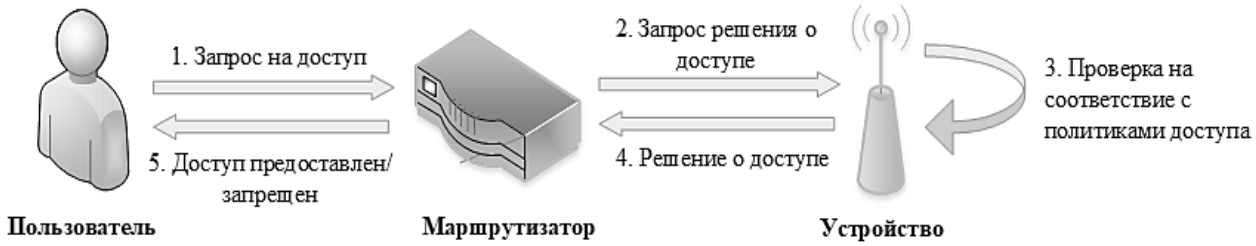

Рис. 3. Процесс управления доступом при распределенном подходе

Централизованно-контекстный подход

Это гибридный подход, при котором устройства Интернета вещей не являются полностью пассивными объектами, поскольку они частично участвуют в принятии решений о доступе. Логика управления доступом реализована в центральном объекте, как и при централизованном подходе, но дополнительно в центральный объект еще отправляется контекстная информация с устройств Интернета вещей, которая используется для принятия решений о доступе, как показано на рис. 4.

Этот подход основан на предоставлении контекстной информации об устройствах Интернета вещей во время запроса доступа. Из-за этого возникает задержка при передаче данные центральному объекту, и соответственно нарушается обработка в реальном масштабе времени.

Модели систем контроля доступа

Реализация эффективного механизма контроля доступа для систем Интернета вещей является одной из основных задач при обеспечении безопасности системы. Устройства Интернета вещей должны получать доступ к службам или приложениям только после правильного предоставления своих идентификационных данных [6]. Для обеспечения конфиденциальности и целостности системы, процедура контроля доступа гарантируют то, что авторизованным пользователям будут предоставлены соответствующие разрешения и доступ [7]. Существует множество моделей систем контроля доступа, которые можно разделить на два класса: статические и динамические.

Рис. 4. Процесс управления доступом при централизованно-контекстуальном подходе

Модели статического контроля доступа

В основе моделей статического контроля доступа (также называемого классическим или традиционным) лежат заранее предопределенные политики доступа, которые вне зависимости от ситуации принимают одинаковое решение при заданных исходных данных, т.е. не чувствительны к контексту.

Несмотря на то, что статические подходы контроля доступа успешно применяются в различных сферах для решения различных проблем, эти подходы предназначены для установления взаимно-однозначного соответствия между правилами контроля доступа, и ресурсами, к которым необходим доступ. Такой подход контроля доступа подвержен атакам, использующим недокументированные состояния в политики доступа, использующие ложные объекты для получения доступа к набору существующих учетных записей. Таким образом, статические подходы контроля доступа обладают рядом недостатков, в частности, такие подходы не способны обрабатывать непредсказуемые ситуации, поскольку основаны на статических и предопределенных политиках [8].

Проведем краткий обзор основных типов статических моделей управления доступом, выделяя преимущества и недостатки каждого из них.

Список контроля доступа

Управление доступом может реализовываться в виде таблицы, называемой матрицей контроля доступа (ACM), где каждая строка и столбец состоят из субъекта и объекта соответственно. Каждая запись представляет собой набор прав доступа для соответствующего субъекта [8].

Также существует реализация в виде списка контроля доступа (ACL). ACL – это списки для каждых объектов, которые включают в себя перечень легальных субъектов вместе с их правами доступа. Списки управления доступом – это

представление прав доступа по умолчанию в системах UNIX. Хотя ACL является действенным и эффективным способом, но он не масштабируется на большое количество субъектов и объектов. Кроме того, затруднительно изменить права на несколько объектов для отдельных пользователей [8].

Избирательный контроль доступа

Избирательный контроль доступа (DAC) предназначен для многопользовательских баз данных и систем с небольшим количеством заранее известных пользователей. Все системные ресурсы находятся под полным контролем пользователя. DAC предоставляет доступ в зависимости от идентификатора пользователя и результата авторизации, которые определяются с помощью открытых политик. Владелец ресурса может предоставить доступ любому пользователю. DAC в основном занимается наследованием разрешений, авторизацией пользователей, аудитом системных событий и административными привилегиями [7].

Ключевым преимуществом, связанным с использованием DAC, является возможность обеспечения комплексного управления системными объектами. Кроме того, DAC прост в реализации и предоставляет гибкие настройки разрешений владельцам системы или системным администраторам для создания индивидуальных политик доступа для каждого пользователя. Например, при доступе к некоторому ресурсу одному пользователю может быть предоставлен доступ на чтение и запись, а другому только на чтение.

С другой стороны, модель DAC обладает некоторыми уязвимостями. Возможность предоставления пользователю полного контроля по разрешению доступа к объектам, создает условия для реализации троянских атак. Кроме того, в системах DAC обслуживание системы и проверка политик безопасности является чрезвычайно сложным, поскольку права доступа пользователей задаются отдельно по каждому объекту системы.

Мандатный контроль доступа

В модели мандатного контроля доступа (MAC) каждому объекту присваивается метка, которая на основании степени конфиденциальности информации определяет требуемый уровень привилегий для доступа к каждому объекту. Помимо этого, каждому субъекту присваивается метка, указывающая, к каким объектам он может получить доступ [10]. Модель MAC обеспечивает условия, при которых пользователь может выполнять только задачи, соответствующие уровню его привилегий. В MAC политика безопасности контролируется администратором политики безопасности, и пользователь не может ее переопределить. Модель MAC призвана обеспечивать конфиденциальность и целостность информации, поэтому она в обычно применяется в специальных системах [9].

По сравнению с DAC, MAC не имеет уязвимости для реализации троянских атак. Кроме того, модель MAC проста и может применяться в коммерческих системах, работающих в условиях деструктивных воздействий, где риск атак очень высок, а конфиденциальность защищаемых объектов имеет высокую важность [8].

MAC на сегодняшний день является наиболее безопасной процедурой контроля доступа, но платой за это является существенные затраты на ее поддержку. Возникают большие накладные расходы на управление системой из-за постоянной необходимости обновлять метки объектов и субъектов для размещения новых данных, внесения изменений в классификацию для добавления новых пользователей или внесения изменений для уже существующих пользователей [10].

Управление доступом на основе ролей

Управление доступом на основе ролей (RBAC) является широко распространённой моделью, применяемой в различных системах [16]. Модель RBAC состоит из трех основных элементов: пользователи (субъекты, запрашивающие доступ), роли (набор разрешений) и операции (действия над целевыми ресурсами). Права доступа

связаны с ролями, где пользователю предоставляется соответствующая роль. Один пользователь может быть связан с одной или несколькими ролями, и одна роль может относиться к одному или нескольким пользователям. RBAC предоставляет классификацию пользователей в зависимости от их ролей [10].

Модель RBAC ограничивает доступ к объектам на основе роли субъекта, а не его идентификации. Роли распределяются между субъектами в соответствии с их допуском, квалификацией и обязанностями внутри организации. Набор разрешений группируется вместе, образуя роль. Модель RBAC может иметь множество пользователей, где каждому пользователю будет назначена определенная роль или несколько ролей, где каждая роль состоит из набора разрешений/прав. RBAC помогает обеспечить целостность и доступность данных в системе, явно контролируя не только то, какие ресурсы могут быть доступны, но также и то, какие действия разрешены над ресурсами. Кроме того, консолидация контроля доступа для многих пользователей в рамках одной роли позволяет значительно упростить управление всей системой и значительно повысить эффективность политик безопасности [10].

Хоть RBAC и обладает существенными преимуществами в области контроля доступа, но проблемы управления большими системами в ней все еще присутствуют. В больших системах настройка членства, наследование ролей и необходимость в детализированных настраиваемых привилегиях делают процесс администрирования потенциально непрактичным. Кроме того, RBAC нельзя использовать для предоставления разрешений на последовательности операций/действий [10].

Модели динамического контроля доступа

Основной принцип динамических моделей контроля доступа заключается в том, что они учитывают не только политику доступа для принятия решения о доступе, но также динамические характеристики и контекст, которые оцениваются в момент запроса доступа [10]. Это обеспечивает большую гибкость и позволяет адаптироваться к различным ситуациям и условиям при принятии решения о доступе.

Для обеспечения эффективного и гибкого контроля доступа необходимо внедрение динамических подходов. Однако большинство существующих подходов для обеспечения контроля доступа основаны на статических, фиксированных политиках доступа. Отсутствие автоматизации приводит к проявлению человеческого фактора, что сопровождается ошибками и является уязвимостью для различных типов атак, основанных на социальной инженерии. Кроме того, классические подходы не позволяют выполнять управление рисками в режиме реального времени, особенно при воздействии угроз нулевого дня. Это связано с тем, что решение о доступе в этих подходах принимаются на основе заранее разработанного аналитиками по безопасности набора политик. Соответственно они не позволяют в режиме реального времени разрешать ранее не возникавшие проблемы с контролем доступа [10].

Помимо этого, в существующих подходах по контролю доступа отсутствует обратная связь и альтернативные варианты разрешения ситуаций контроля доступа. Например, рассмотрим ситуацию, когда легальный пользователь пытается получить доступ к определенному ресурсу или услуге, но система контроля доступа по какой-то причине отказывает ему и он не может продолжать работу. При этом пользователь получает сообщение об отказе в доступе без предоставления каких-либо подробностей. Такое сообщение вынуждает пользователя обращаться к системному администратору, что в свою очередь приводит к временному простою в работе и увеличивает нагрузку на системных администраторов. Причем, подходы со статическим контролем доступа предполагают, наличие системного администратора с широкими привилегиями доступа к службам, данным без ограничений по времени этого доступа. Компрометация

учетной записи системного администратора подвергает всю систему угрозе деструктивного воздействия, причем ограничить риск взлома такой учетной записи не представляется возможным [2, 10].

В отличии от статических политик динамические подходы по контролю доступа для принятия решения используют дополнительную информацию и функционируют в режиме реального времени. Дополнительным контекстом в режиме реального времени могут быть оценки степени доверенности субъекта, риска, временные показатели и др. Динамические модели позволяют адаптироваться к различным условиям при принятии решений о доступе [11].

Контекстная информация в сетях Интернета вещей

В связи с быстрым развитием сенсорных технологий датчики и сенсоры становятся неотъемлемой частью при получении и сборе соответствующих данных о параметрах окружающей среды. Датчики становятся все более мощными, дешевыми и малогабаритными, что стимулирует их широкое распространение. С ростом числа применяемых датчиков, возрастает и объем генерируемых ими данных. Данные должны интерпретироваться и анализироваться для извлечения полезной информации. Контекстно-зависимые вычисления имеют ключевую роль в достижении этой цели. Это облегчает хранение контекстной информации, поступающей с датчиков. Поэтому интерпретация полученных данных может быть выполнена проще и более осмысленно. Кроме того, понимание контекста облегчает реализацию межмашинного взаимодействия (M2M), которое является ключевым принципом технологии Интернета вещей [11].

Контекстная осведомленность является важной отличительной особенностью современных вычислительных систем. Это ключевая технология, обеспечивающая интеллектуальное взаимодействие между пользователями и системами Интернета вещей. Как правило, контекстная осведомленность подразумевает устройства, которые обладают способностью воспринимать свое физическое окружение и соответствующим образом менять свое поведение.

Под термином контекст будем понимать [11] любую информацию, которую можно использовать для характеристики ситуации в которой находится сущность. Сущность – это человек, место или объект, которые относятся к взаимодействию между пользователем и приложением, включая самого пользователя и приложения. Например, местоположение, личность, время, журнал событий и активность представляют собой основные типы контекста для характеристики ситуации, в которой находится конкретный объект [11].

Типы контекста и их классификация

В различных исследованиях выделяются определенные виды контекста. В [12] представлен наиболее распространенный механизм определения видов контекста. Авторами в качестве основных видов контекста были определены: местоположение, личность, время и активность. Также, было предложено разделить виды контекста на две категории: первичный и вторичный контексты.

Первичный контекст – это любая информация, полученная без использования существующего контекста и без выполнения каких-либо операций объединения данных с датчиков, таких как показания датчиков GPS, а также информация о местоположении.

Вторичный контекст – это любая информация, которая может быть вычислена с использованием первичного контекста. Вторичный контекст может быть вычислен с помощью операции объединения данных с датчиков или операций извлечения данных, таких как вызов веб-служб, и определения расстояния между двумя датчиками путем применения операций объединения данных с датчиков по двум сырым значениям с датчиков GPS. Также, контекст, полученный на основе личных данных, например, номер телефона, адрес, адрес электронной почты, день рождения, список друзей, также может быть идентифицирован как вторичный контекст.

Также, в [11] представлен принцип классификации первичного и вторичного контекста. Местоположение, личность, время и активность были отмечены как наиболее важные виды контекстной информации. В табл. 1 представлены способы получения первичного и вторичного контекста о местоположении, личности, времени и активности.

Таблица 1

Классификация наиболее распространенной контекстной информации

Контекстная информация	Вид контекста	
	Первичный	Вторичный
Местоположение	Данные о местоположении с датчиков GPS	– Определение расстояния между двумя датчикам, вычисленное с использованием системы GPS; – Предоставление карты, полученное от поставщика картографических услуг.
Личность	Идентификация пользователя на основе RFID метки	– Извлечение списка друзей из профиля пользователя в соц. сетях; – Идентификация лица человека, с помощью системы распознавания лиц;
Время	Считывание текущего времени	– Определение времени года, основываясь на информации о погоде; – Предсказывание времени на основе календаря и текущей активности солнца.
Активность	Определение открывания двери, с помощью дверного датчика	– Определение активности пользователя на основе датчиков мобильного телефона, таких как GPS и акселерометр; – Прогнозирование активности пользователя на основе предыдущих действий.

Контекстно-зависимые функции

Контекстно-зависимые приложения обладают некоторыми общими свойствами. В [12] выделили три основных функции, которые реализуются в контекстно-зависимых приложениях: предоставление, исполнение и маркировка (тегирование).

- Предоставление: это функция анализа соответствующей информации, связанной с определенным контекстом, с целью определения и принятия решения о том, какая информация или услуга должны быть предоставлены пользователю. Например, когда пользователь заходит в супермаркет и достает свой смартфон, контекстно-зависимое мобильное приложение должно поддерживать возможность подключение к домашнему умному холодильнику, для формирования списка покупок и передачи его пользователю. Это один из возможных вариантов реализации идеи представления информации на основе контекста, такого как время, местоположение и т.д.
- Исполнение: система Интернета вещей имеет возможность использовать собранные и проанализированные данные для автоматического принятия решений на основе контекста без вмешательства человека. Например, когда пользователь едет домой с работы, приложение в системе умного дома, может включить систему кондиционирования воздуха и кофеварку, чтобы все было готово к тому времени, когда пользователь войдет в дом. Эти действия должны выполняться автоматически в зависимости от контекста. В этой связи важным аспектом является организация M2M взаимодействия, которое позволяет автоматизировать сервисы Интернета вещей с использованием контекстной информации.

Маркировка (тегирование): системы Интернета вещей включают в себя большое

число датчиков, как правило встроенных в бытовые предметы. Эти датчики генерируют большой объем данных, который необходимо собирать, анализировать и интерпретировать. Причем данных от одного датчика, недостаточно для предоставления необходимой информации о системе в целом. Поэтому необходима агрегация данных, собранных с помощью нескольких датчиков. Вместе с данными от датчиков, которые позже будут обработаны и интерпретированы, должна быть помещена контекстная информация. Таким образом, контекстная маркировка данных играет важную роль в контекстно-зависимых приложениях.

Риск-ориентированный контроль доступа

Как известно, риск — это вероятность возникновения ущерба определенной величины. Риск связан с угрозой – событием, которое может произойти в будущем и привести к ущербу [13]. Показатель риска достаточно универсален и широко применяется в различных дисциплинах. С точки зрения безопасности информации, риск безопасности определяется как вероятность нанесения ущерб владельцу информации при реализации угрозы. Под управлением рисками (риск-менеджментом) понимается выявление и нейтрализация угроз, которые могут привести к нарушению конфиденциальности, целостности или доступности информации [13].

Риск безопасности в контексте контроля доступа может быть определен как возможность нарушения конфиденциальности (утечки) и целостности этой информации, в результате получения доступа к системным ресурсам [1]. Модель управления доступом, основанная на рисках, использует риск безопасности в качестве критерия для принятия решения о доступе. Эта модель принимает или отклоняет запросы на доступ динамически на основе расчетной величины риска [14]. В этой модели для принятия решения о доступе анализ рисков выполняется при каждом пользовательском запросе доступа.

Модели управления доступом, основанные на риске делятся на два типа: неадаптивные и адаптивные. При неадаптивном подходе для каждого запроса доступа оценивается величина риска. Затем рассчитанное значение риска сравнивается с пороговым значением для принятия решения о доступе. При адаптивном подходе после предоставления доступа выполняется дополнительная процедура мониторинга активности с целью обнаружения аномального поведения в течении сеанса доступа. В случае обнаружения порог риска должен быть автоматически снижен, чтобы предотвратить высокорискованные операции. Пользователь должен быть оповещен о том, что сеанс доступа может быть прекращен [14]. Фундаментальное отличие адаптивной и неадаптивной моделей заключается в том, что при адаптивном подходе требуется системный процесс мониторинга, в котором пороговое значение риска адаптивно корректируется на основе действий пользователей во время сеансов доступа, в то время как неадаптивный подход позволяет только оценивать мгновенное значение риска и не обладает возможностью обнаружения аномалий [15].

Существует несколько способов реализации риск-ориентированных моделей управления доступом. Все эти способы основываются на общем принципе. Процесс управления доступом, на основе рисков проиллюстрирован на рис. 5.

Реализация управления доступом на основе рисков включает в себя три модуля. Основным модулем является оценка риска. Он получает запросы от пользователей, анализирует их, собирает контекстную информацию и оценивает величину риска, связанного с запросом доступа. Затем оцененное значение риска сравнивается с пороговыми значениями на основе политики доступа для принятия решения о доступе [16].

В последнее время было опубликовано несколько исследований подходов, направленных на повышение гибкости статического контроля доступа за счет реализации функций обработки контекстной информации и непредвиденных ситуаций.

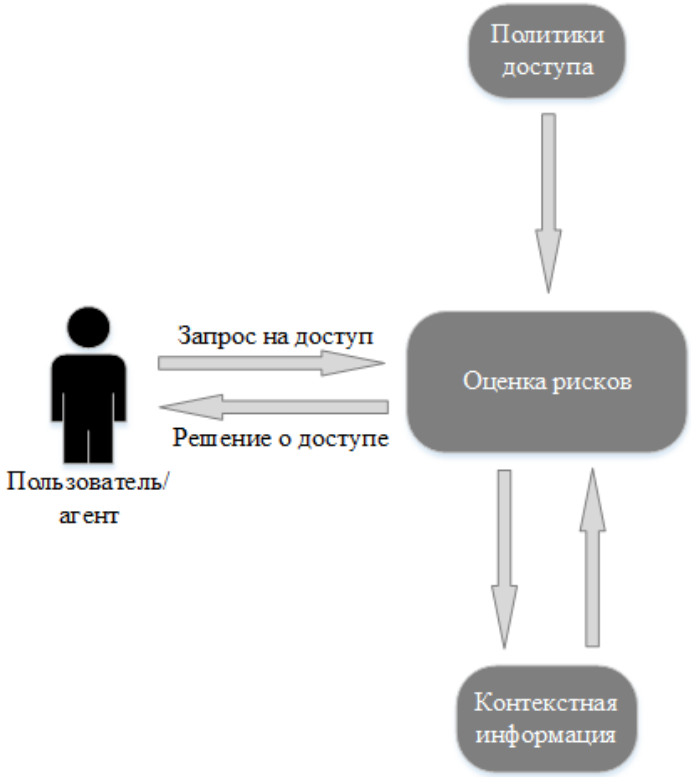

Рис. 5. Процесс управления доступом на основе рисков

Контекстно-зависимые модели

Построение гибкой, и детализированной модели контроля доступа является одним из наиболее важных аспектов обеспечения эффективного контроля доступа к системным ресурсам. Это может быть достигнуто путем реализации контекстно-зависимых моделей контроля доступом, которые используют не только политики доступа, но и контекстную информацию для принятия решения о доступе.

Контекстно-зависимые модели контроля доступа предполагают использование контекстной и другой информации для обеспечения детального контроля доступа. Эти модели не дают однозначного представления о риске доступа, но контекст может предоставить дополнительную информацию, которая позволяет уточнить оценку риска доступа. В таких моделях при принятии решения об удовлетворении запроса на доступ учитывается контекстная информация, но не путем статической проверки соответствующего условия в политике безопасности, а путем применения в качестве дополнительного параметра при оценке значения риска безопасности, связанного с запросом доступа.

Известно несколько контекстно-зависимых моделей, которые дополняют модель RBAC с помощью атрибутов контекста для обеспечения соответствующей гибкости модели контроля доступа. В работе [17] предложили обобщенную ролевую модель контроля доступа (GRBAC). Эта модель расширяет традиционную RBAC, распространяя роли на все объекты в системе (в концепции RBAC роли используется только для субъектов). Было определено три основные роли: субъект, среда и объект. Модель GRBAC использует контекстную информацию, как параметр при принятии решения о доступе. Также, в [18] предложены две ключевые идеи: 1) при изменении контекста права доступа пользователя должны изменяться; 2) ресурс должен изменить свои разрешения на доступ, при изменении системной информации

(например, пропускная способность сети, загрузка процессора, использование памяти). Однако, в этих статьях не рассматриваются аспекты безопасности в процессе принятия решений и влияния угроз безопасности на систему. В них также не применен адаптивный контроль для предотвращения деструктивных атак во время сеанса доступа.

Также известны контекстно-зависимые модели с динамической моделью контроля доступа для здравоохранения. В работе [19] предложена модель контроля доступа для чрезвычайных ситуаций в медицинских учреждениях. Эта модель позволяет реагировать на изменения ситуации путем их пошагового анализа в соответствии с приоритетами и путем установления соответствующих политик и разрешений для различных ситуаций.

В дополнение к работам по интерпретации контекста известны и другие работы, предлагающие использовать уровень потребности для повышения гибкости модели контроля доступа. В работе [20] предложен адаптируемый к рискам контроль доступа (RAdAC), который основан на оценке риска безопасности и уровня потребности для предоставления доступа. Эта модель предназначена для предварительной оценки риска, связанного с запросом доступа. Затем оцененный риск соотносится с правилами политики контроля доступа. После чего система проверяет уровень потребности в ресурсе, если потребности могут быть удовлетворены и соответствуют политике безопасности, то доступ предоставляется. Однако эта модель не содержит подробных сведений о том, как количественно оценивать риск и уровень потребности. В работе [21] авторы применили модель (RAdAC) для определения параметров риска и уровня потребности, но использовали собственную модель контроля доступа на основе атрибутов (ABAC).

В ряде работ предлагается для принятия решения о доступе интегрировать показатели доверия и риска. В работе [22] авторы предложили процедуру, которая расширяет модель RBAC путем учета оценок доверенности и риска при принятии решения о доступе. В работе утверждается, что процедура позволяет адаптироваться к подозрительным изменениям в поведении пользователей, удаляя привилегии, когда доверие к пользователю падает ниже определенного порога. Этот порог вычисляется на базе оценки риска, который включает обусловлен несанкционированным доступом к информации. Еще в одной работе [23] авторы предложили процедуру контроля доступа, учитывающую показатели доверенности и риска, на основе правил политик безопасности и динамических решений о доступе. Авторы ввели понятие зональной политики, которая позволяет владельцу данных иметь полный контроль над своими собственными данными. Показатель доверия используется для выполнения проверки соблюдения заявителем возложенных на него обязательств. В процедуре применяется вероятностная расчетная модель доверия, получившая название субъективной логики для формулирования оценки доверия. При этом оценка риска выполняется с использованием классического метода оценки ожидаемого ущерба от нарушения конфиденциальности информации.

Модели контроля доступа на основе рисков

Модели контроля доступа, основанные на оценках риска, призваны в первую очередь обеспечить требуемую гибкость и детализацию контроля доступа. Известен ряд реализаций моделей, основанных на оценке риска, призванных расширить возможности статических моделей контроля в части обработки неожиданных ситуаций.

Одну из реализаций модели управления доступом, основанной на рисках, предложена в [24]. Авторы предложили три этапа реализации модели. Это оценка риска, определение приемлемых уровней риска и контроль обмена информацией. Эта идея была использована в [25] для построения динамической модели, основанной на оценке рисков, путем сбора вспомогательной информации из окружения, оценки ее с точки зрения безопасности и принятия решения о доступе на основе оценки рисков. Аналогичным образом, в [25] представлена

модель контроля доступа на основе оценки риска и контекста. Эта модель подразумевает сбор дополнительной информации из окружения и ее интерпретацию с точки зрения безопасности с помощью многопараметрической оценки рисков (MFEP). В этом подходе риск оценивается с точки зрения обеспечения конфиденциальности, целостности и доступности информации. Эта модель апробировалась при контроле доступа к информации в больнице. Однако, учитывая дополнительные параметры риска, связанные со спецификой объекта, данному подходу не хватает адаптивных функций для повышения эффективности принятия решений. В работе [26] авторы предложили подход, основанную на оценке критичности и достоверности объекта с использованием оценки риска. Однако в работе не описывается, как оценить величину риска в различных окружениях. Кроме того, эти модели требуют наличия эксперта - системного администратора с большим опытом работы, чтобы давать оценки каждому входному параметру на ранних стадиях процесса оценки риска. Кроме того, в этих моделях отсутствует адаптивный контроль обнаружения вредоносных программ и пользователей во время сеансов доступа.

Модели управления, основанные на рисках, опираются на общие идеи, но предлагаются различные параметры и методы оценки риска для повышения эффективности по определенному критерию. Например, в работе [27] использованы те же элементы риск-ориентированной модели, что и в рассмотренной ранее работе [16], но при этом используется метод нечеткой логики для оценки величины риска, связанного с запросом доступа. В работе показано, что нечеткий вывод является хорошим решением для оценки риска безопасности доступа. Однако в обеих моделях игнорировалась информация об истории поведения пользователей в процессе оценки рисков, а также отсутствовали адаптивные функции. Аналогичным образом, в работе [25] использован метод нечеткой логики для оценки риска, связанного с доступом к медицинской информации. В качестве меры риска для принятия решения о возможности доступа к медицинской информации использовалась комбинация оценок конфиденциальности данных, критичности операций и история рисков. Однако эта модель не дает количественной оценки риску. Кроме того, она требует статистики реализации угроз и не позволяет предотвратить деструктивные действия во время сеанса доступа. В работе [23] авторы также применили метод нечеткой логики для разработки многоуровневой модели безопасности (MLS), основанной на рисках. Эта модель измеряла риск, используя разницу между уровнями привилегий объекта и субъекта. Так, что, если разница велика, величина риска, связанная с доступом, будет высокой. Полученный результат оценки риска представлялся в виде двоичного числа, где 0 – разрешает доступ, а 1 – запрещает доступ.

В работе [28] авторы предложили модель контроля доступа, основанную на количественной оценке риска. Величина риска оценивалась на основе интерпретации цели доступа к конфиденциальным данным различной критичности. Оценка риска осуществляется с использованием принципов теории информации. Авторами реализован прототип и выполнена апробация на реальных записях истории болезни для демонстрации эффективности предложенного подхода. Однако цель доступа как параметр недостаточен для оценки величины риска для принятия решения о доступе. Также подход не является адаптивным, не использует контекст и не работает в реальном времени. В работе [27] представлен подход к анализу рисков, основанный на положениях теории игр. Однако использование только оценок выигрыша субъекта для принятия решения о доступе недостаточно для разработки гибкой масштабируемой модели контроля доступа. Подход также не является адаптивным и не использует контекст.

В ряде работ предложены аналитические подходы и алгоритмы для оценки рисков безопасности при управлении доступом. Например, в работе [30] предложена модель контроля доступа, в которой величину риска

оценивается на основе выполняемых действий. В этой модели величина риска оценивается с точки зрения различных действий и их соответствующих проявлений. Модель не предусматривает количественную оценку величины риска, требует статистики вредоносных воздействий и не позволяет предотвращать деструктивные действия во время сеанса доступа. В работе [31] реализована модель контроля доступа на основе рисков, основанная на аналитической оценке полномочий пользователя. Но в данной модели не используются никакие другие параметры, учитывающие конфиденциальность информации, критичность операции или историю рисков. А также отсутствует возможность прогнозирования рисков и адаптации.

В работе [1] предложена модель контроля доступа на базе риска, основанная на его количественной оценке частных показателей и их последующего агрегирования. Эта модель основана на идее политик рисков, которые позволяют поставщикам услуг и владельцам ресурсов определять частные показатели, обеспечивая гибкость системы контроля доступа. Модель реализована в виде прототипа. Данный подход получил развитие за счет внедрения функций анализа контекста и введения весовых коэффициентов для каждой метрики риска в зависимости от их количества. Данный подход обеспечивает большую гибкость, позволяя владельцам ресурсов определять свои собственные метрики, но при этом требуется администратор безопасности для обеспечения безопасности системы и отсутствует возможность адаптации. В работе [31] предложен динамический риск-ориентированный метод для принятия решений. Этот метод использует информацию о прошлом поведении пользователя для оценки риска. Оценка формируется путем начисления пользователям штрафных баллов после завершения транзакции. Подход также не обеспечивает возможности динамического контроля доступа, и не является адаптивным.

В работе [30] представлен метод количественной оценки для модификации модели RAdAC. В предложенной модели 27 метрик были разделены на 6 категорий, которые оценивались для каждого запроса доступа и агрегировались для получения оценки интегрального риска безопасности. В качестве параметров риска выступают оценки вероятности и ущерба на основе трехуровневой шкалы. Опираясь на треугольное распределение, с помощью метода Монте-Карло определяется вероятность каждого события, которая затем умножается на весовой коэффициент, оцениваемый экспертным методом по каждой метрике. Данный метод создан для специальных приложений, поэтому некоторые показатели не подходят для приложений технологии Интернета вещей. В работе [32] предложен принцип контроля доступа, основанный на шансах и рисках. Подход использует оценки риска безопасности и шанса успешного функционирования для принятия решения о доступе. Для каждого действия определяется вектор рисков и шансов. Доступ для выполнения определенного действия разрешается только в том случае, если оценка шанса превышает значение риска. Система формирует граф с описанием разрешенных пользователю действий для доступа к системным ресурсам. Для управления доступом применяется фиксированный и заранее определенный граф действий и достаточно его достаточно сложно обновлять.

В работе [14] представлена динамическая модель контроля доступа на основе рисков для облачных технологий. Подход сочетает в себе ABAC с методом оценки риска и степени доверия. В модели задается пороговое значение риска на основе журнала истории и применяется потоковая концепция обработки данных. Тем не менее модель не обеспечивает работу в режиме реального времени. В работе [33] представлена основа для разработки контекстно-зависимой модели на базе риска для медицинских информационных систем. В модели для расчета величины риска информация классифицируется с помощью профилирования разрешений. Процедура выдает решение о доступе на основе критичности контекста. Эта модель также является качественной, ограничена

медицинскими информационными системами и не является адаптивной. В работе [34] авторы предложили модель контроля доступа, которая обеспечивает баланс между предоставлением доступа и защитой конфиденциальной информации о пациентах. Она использует оценки уровня важности объекта и доверия к субъекту для принятия решения о доступе. В модели задается порог риска на основе текущих условий, но не предусмотрена количественная оценка величины риска и методика определения порогового значения риска в зависимости от условий. Также эта модель ориентирована только на медицинские информационные системы и не является адаптивной.

Параметры риска

Одной из важных задач при разработке модели контроля доступа, основанной на рисках, является выбор параметров риска, которые способствуют эффективному принятию решения о разрешении доступа. Существует множество параметров, которые возможно применить для оценки величины риска, связанного с предоставлением доступа для эффективного принятия решения в динамике. Наиболее подходящими для этого параметрами риска являются следующие:

- **Оценка привилегий субъекта:** представляет собой уровень привилегий субъекта, полученных от системного администратора. Различные разрешения на доступ предоставляются в зависимости от роли субъекта в организации. Каждая роль связана с определенными разрешениями [33].
- **Оценка важности объекта:** представляет собой уровень важности объекта. В зависимости от роли субъекта доступ к объектам определенной важности может быть предоставлен или запрещен.
- **Оценка критичности ресурса:** описывает уровень критичности ресурсов, к которым пользователь хочет получить доступ. Разные уровни критичности определяют степень риска. Чем выше критичность ресурса, тем выше потенциальный риск, при предоставлении доступа к этому ресурсу [35].
- **Оценка критичность операции:** представляет собой оценку последствий от определенных операций над определенным ресурсом с точки зрения конфиденциальности, целостности и доступности. Одна и та же операция может привести к различному ущербу, а значит и потенциальному риску.
- **История рисков:** представляет собой журнал значений рисков пользователей для определенного ресурса. История рисков может быть использована для прогнозирования поведения пользователя по отношению к определенному ресурсу.
- **Уровень доверия:** представляет оценку доверия субъекта определенному ресурсу. Уровень доверия разделяется на две категории: доверие к личности и доверие к поведению. Доверие к личности связано с проверкой подлинности объекта и фокусируется на учетных данных. В то время как поведенческое доверие связано с надежностью субъекта, которая зависит от определенных контекстов [35]. В моделях контроля доступа, основанных на риске, используется только поведенческое доверие.
- **Уровень квалификации:** этот параметр оценивает уровень квалификации в сфере безопасности, которую имеет запрашивающий. Как правило, чем выше квалификация, тем меньше вероятность того, что запрашивающий допустит противоправное действие и потенциальный риск ниже [35].

Заключение

В результате проведенного анализа, можно сделать вывод о том, что ввиду динамической и распределенной сущности технологии Интернета вещей наиболее перспективным направлением исследований в сфере идентификации, аутентификации и авторизации является разработка динамической процедуры контроля доступа. Однако известные процедуры управления доступом, основанные на оценке рисков, сосредоточены только на принятии решений о доступе, не предоставляя никаких способов предотвращения несанкционированного доступа к данным со стороны авторизованных пользователей. Помимо

этого, они не имеют функции отслеживания изменений в режиме реального времени и контекстно зависимых функций, которые для определения решения о доступе позволяют использовать информацию об окружении.

По сравнению с традиционными, рассмотренные в ходе анализа процедуры контроля доступа являются существенно более гибкими, но несмотря на эти преимущества, необходимо провести дополнительные исследованиях в этой области и предложить более универсальный подход к контролю доступа в системах Интернета вещей.

Список литературы

1. 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.
2. Suhendra V. A Survey on Access Control Deployment. Communications // Computer and Information Science. 2011. P. 11–20.
3. Hulsebosch R.J. Context Sensitive Adaptive Authentication. / R.J. Hulsebosch, M.S. Bargh, G. Lenzini, W.G. Ebben, S.M. Iacob // Kortuem G., Finney J., Lea R., Sundramoorthy V. (eds) Smart Sensing and Context. EuroSSC 2007. Lecture Notes in Computer Science. 2007. V. 4793.
4. Hernández-Ramos J., Jara A. Distributed Capability-based Access Control for the Internet of Things. // Journal of Internet Services and Information Security (JISIS). 2013. No. 3. P. 1-16.
5. Bijon K. Z. A framework for risk-aware role-based access control. / K.Z. Bijon, R. Krishnan, R. Sandhu // IEEE Conference on Communications and Network Security (CNS). 2013. P. 462-469.
6. Kumar A. Context sensitivity in role-based access control. / A. Kumar, N.M. Karnik, G. Chafle // Operating Systems Review. 2002. No. 36(3). P. 53-66.
7. Sandhu R. S. Role-based access control models. / R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman // Computer. 1996. No. 29(2). P. 38-47.
8. Wang Q., Jin H. Quantified risk-adaptive access control for patient privacy protection in health information systems. // Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS ’11), 2011. P. 406–410.
9. Zhou L. Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. / L. Zhou, V. Varadharajan, M. Hitchens // IEEE Transactions on Information Forensics and Security. 2013. No. 8(12). P. 1947-1960.
10. 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.
11. 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.
12. Abowd G.D. Towards a Better Understanding of Context and Context-Awareness. / G.D. Abowd [etc.] // Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing. 1999. P. 304–307.
13. Elky S. An Introduction to Information System Risk Management. / SANS Institute, 2006.
14. 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.
15. 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, pp. 269–275.
16. Diep N. N. Enforcing Access Control Using Risk Assessment. / N.N. Diep [etc.] // The Fourth European Conference on Universal Multiservice Networks. 2007. P. 419–424.
17. Covington M.J. Generalized role-based access control for securing future applications. / M.J. Covington, M.J. Moyer, M. Ahamad // Proceedings of the 23rd National Information Systems Security Conference (NISSC). 2000. P. 40-51.
18. Zhu Z. A Context-Aware Access Control Model for Pervasive Computing in Enterprise Environments. / Z. Zhu, R. Xu // 4th International Conference on Wireless

Communications. Networking and Mobile Computing. 2008. P. 1–6.

19. Garcia-Morchon O. Modular context-aware access control for medical sensor networks. / O. Garcia-Morchon., K. Wehrle // Proceeding of the 15th ACM Symposium on Access Control Models and Technologies - SACMAT ’10. 2010. P. 129–138.

20. McGraw R. Risk-Adaptable Access Control (RAdAC): Access Control and the Information Sharing Problem. / R. McGraw // Proceedings of NIST & NSA Privilege Management Workshop, 2009.

21. Kandala S. An Attribute Based Framework for Risk-Adaptive Access Control Models. / S. Kandala, R. Sandhu, V. Bhamidipati // Proc. of the 6th International Conference on Availability, Reliability and Security. 2011. P. 236-241.

22. Baracaldo N. A trust-and-risk aware RBAC framework: tackling insider threat. / N. Baracaldo, J. Joshi / Proceedings of the 17th ACM Symposium on Access Control Models and Technologies - SACMAT ’12. 2012. P. 167-176.

23. Burnett C. TRAAC: Trust and risk aware access control. / C. Burnett, L. Chen, P. Edwards, T.J. Norman // Twelfth Annual International Conference on Privacy. Security and Trust. 2014. P. 371–378.

24. Jason C. Horizontal integration: Broader Access Models for Realizing Information Dominance. // MITRE Corporation, Tech. Report, 2004.

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

26. 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.

27. Ni Q. Risk-based access control systems built on fuzzy inferences. / Q. Ni, E. Bertino, J. Lobo // Proceedings of the 5th ACM Symposium on Information. Computer and Communications Security, New York, USA. 2010. P. 250-260.

28. Wang Q. Quantified risk-adaptive access control for patient privacy protection in health information systems. / Q. Wang, H. Jin // Proceedings of the 6th ACM Symposium on Information. Computer and Communications Security (ASIACCS ’11). 2011. P. 406-410.

29. Rajbhandari L. Using game theory to analyze risk to privacy: An initial insight. / L. Rajbhandari, E. A. Snekkenes // Privacy and Identity Management for Life. Springer Berlin Heidelberg. 2011. P. 41–51.

30. Sharma M. Using risk in access control for cloud-assisted ehealth. / M. Sharma, Y. Bai, S. Chung, L. Dai // High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS). 2012. P. 1047-1052.

31. 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.

32. Britton D. A security risk measurement for the RAdAC model / D. Britton, I. Brown. // Naval Postgraduate School (U.S.). 2007. // URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a467180.pdf (дата обращения: 29.01.2021).

33. Choi D. A Framework for Context Sensitive Risk-Based Access Control in Medical Information Systems. / D. Choi, D. Kim, S. Park // Computational and Mathematical Methods in Medicine. 2015. P. 1–9.

34. Abomhara M. Towards Risk-aware Access Control Framework for Healthcare Information Sharing. / M. Abomhara, M. Koien, V.A. Oleshchuk, M. Hamid // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018). 2018. P. 312-321.

35. Maw H. A. An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks. / H.A. Maw, H. Xiao, B. Christianson // Proceedings of the 8h ACM Symposium on QoS and Security for Wireless and Mobile Networks. 2012. P. 81-86.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 23.05.2022

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

OVERVIEW OF EXISTING ACCESS CONTROL PROCEDURES IN THE CONTEXT OF ENSURING THE SECURITY OF INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The work is devoted to the review of existing approaches to the implementation of access control, the analysis of known access control procedures and their comparison in relation to the security of Internet of Things systems. Three ways of implementing access control in Internet of Things systems are considered in detail. Static and dynamic access control procedures are analyzed and compared. The most common access control procedures are analyzed. The procedure of access control according to the criterion of the admissibility of the assessment of the security risk of the authorized object is considered. The analysis of existing analogous procedures for access control according to the criterion of risk magnitude is carried out. The main risk assessment parameters for the access control procedure are described. The advantages and disadvantages of well-known access control procedures and techniques in the context of the security of Internet of Things systems are highlighted.

Keywords: access control, Internet of Things, confidentiality, authentication, integrity, availability, risk, risk factors, security.

Submitted 23.05.2022

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