DOI 10.36622/VSTU.2022.25.2.010
УДК 004.8 : 04.077

ОБЗОР МЕТОДОВ ДЛЯ ПОСТРОЕНИЯ РИСК-ОРИЕНТИРОВАННОЙ МОДЕЛИ КОНТРОЛЯ ДОСТУПА В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

С.А. Ермаков, А.А. Болгов

В работе рассматривается понятие риска безопасности и способы его оценки. Проводится подробный обзор методов количественной и качественной оценки рисков и анализ их преимуществ и недостатков. Проведен детальный анализ применений методов оценки рисков в различных риск-ориентированных моделях контроля доступа, с выделением их преимуществ и недостатков. Приведены результаты сравнительного анализа преимуществ и ограничений применимости различных методов оценки риска. Рассмотрен подход на основе нечеткой логики на основе экспертных оценок. На основании проведенного анализа и результатов сравнения выбран метод нечеткой логики с экспертным оценками в качестве подходящего метода для реализации риск-ориентированной модели контроля доступа для систем на построенных на базе технологии Интернета Вещей.

Ключевые слова: контроль доступа, интернет вещей, нечеткая логика, оценка риска, количественная оценка, качественная оценка, риск, безопасность.

Введение

Оценка риск безопасности является одной из основных функций, используемых в риск-ориентированных моделях контроля доступа и выступает в роли их фундаментальной основы. Использование риска безопасности в качестве критерия для принятия решения о доступе, может повысить безопасность до требуемого уровня [1].

Важным этапом внедрения модели контроля доступа, основанной на рисках, является процесс оценки рисков. Этот процесс основан на оценке возможности утечки и ценности информации. Основной целью операции оценки рисков является создание метода ранжирования рисков по степени важности для дальнейшего использования числовых значений риска в принятии решений о доступе, относительно конкретного контекста.

Риск безопасности может быть оценен либо с помощью качественных, либо количественных методов [2]. Методы количественной оценки рисков связаны с привязкой конкретных числовых значений к рискам безопасности. Эти значения используются для непосредственного определения решений о доступе. Методы количественной оценки риска являются хорошим инструментом, поскольку они дают численную оценку риска. Однако их трудно получить, не имея надлежащего набора данных, описывающего вероятность риска и его влияние на конкретное приложение [3].

Качественные методы оценки риска в свою очередь, используются для расчета риска на ранней стадии оценки системы. Это эффективно при классификации рисков и выборе соответствующих действий, которые следует предпринять. Качественные методы оценки риска не могут дать точных значений оценки. Однако они очень эффективны, при ограниченном времени на оценку рисков [2]. В табл. 1 представлены преимущества и недостатки количественных и качественных подходов оценки рисков.

Методы оценки рисков

При оценке рисков по абсолютно разным причинам могут возникнуть некоторые проблемы. Например, если целью процесса оценки риска является прогнозирование будущей возможности раскрытия информации в результате текущего доступа. Определить такую возможность – непростая задача. Более того, если оценка риска основывалась на неполной или неточной информации о соответствующих характеристиках риска, это приведет к сложности определения величины риска [4].

Таблица 1

Преимущества и недостатки количественных и качественных подходов к оценке рисков

Метод	Преимущества	Недостатки
Количественный	– Риски сгруппированы по их стоимости; – При расчете и оценке значений рисков используются объективные методы; – Для определения уровня безопасности используются доступность, целостность и конфиденциальность; – На основе анализа затрат выбираются наиболее подходящие меры; – По мере приобретения опыта, точность данных будет повышена.	– Сложные методы расчета; – Сложно реализовать без автоматического инструмента; – Нет стандартов для реализации этого метода; – Требуется много времени для обработки процесса расчета; – Полученные результаты представляются в виде численных значений, которые трудно понять человеку без опыта.
Качественный	– Легкость в понимании; – Легкость в определении уровня риска; – Легкость в реализации; – Процесс анализа рисков упрощается, поскольку не используется практическая ценность информации; – Не требуется количественная оценка вероятностей событий и последствий; – Не рассчитываются затраты на предполагаемую меру, которая должна быть реализована.	– Расчет риска и его результаты субъективны; – Субъективного расчета недостаточно для получения реальных и правильных оценок; – Из-за их субъективности трудно отслеживать эффективность управления рисками; – Анализ затрат и выгод не проводится, только субъективный расчет; – Точность результатов зависит от качества команды по управлению рисками.

Система нечеткой логики

Система нечеткой логики – это вычислительный подход, который имитирует мышление людей. В нем описывается мир в неточных терминах. Например, если температура высокая, то система нечеткой логики среагирует на это, заранее определенным точным действием. Компьютеры могут работать только с точными оценками, в то время как человеческий мозг умеет формировать рассуждения с неопределенностями и суждениями [5]. Система нечеткой логики рассматривается как попытка сочетать оба метода. На самом деле, система нечеткой логики – это точный подход решения проблем, который обладает способностью работать с числовыми данными и лингвистическими значениями одновременно. Это упрощает управление сложными системами, так как отсутствует необходимость их математического описания [6].

Система нечеткой логики имеет много преимуществ. Она гибкая, надежная и основана на естественном языке, что облегчает ее понимание. Она также устойчива к неточным данным, в которых она может работать даже при отсутствии правил. С другой стороны, она имеет некоторые недостатки. Например, ей нужны эксперты предметной области для определения

нечетких переменных системы. Помимо этого, она требует дополнительных тестов и моделирований, которые занимают много времени, особенного при наличии большого количества правил [7].

Процесс вычислений с использованием системы нечеткой логики состоит из трех основных этапов:

- Фазификация – большинство переменных являются четкими или классическими переменными. Процесс фазификации используется для преобразования четких переменных ввода и вывода в нечеткие переменные для их обработки и получения желаемого результата.
- Процесс нечеткого вывода – описание взаимосвязей между различными входными и выходными данными. Управление нечетким выводом осуществляется путем построения нечетких правил «ЕСЛИ – ТО». Нечеткое правило «ЕСЛИ-ТО» использует лингвистические переменные для описания взаимосвязи между определенным условием и результатом. Часть «ЕСЛИ», в основном используется для задания условия, а часть «ТО» используется для предоставления выходных данных в лингвистической форме. Правило «ЕСЛИ-ТО» обычно используется системой нечеткой логики для описания того, как входные данные соответствуют условию [5].
- Дефазификация – поскольку вывод должен быть четкой переменной, то эта фаза преобразует нечеткий вывод обратно в четкий [6].

Некоторые исследователи использовали систему нечеткой логики для оценки риска безопасности в моделях контроля доступа. Авторы [8] использовали систему нечеткой логики для построения модели контроля доступа MLS, которая применялась для доступа к информации систем IBM. Эта нечеткая модель MLS оценивала величину риска, связанную с запросом доступа, используя разницу между уровнем безопасности субъекта и уровнем безопасности объекта. То есть, чем больше разница, тем выше риск. Кроме того, авторы статьи [9] представили подход, основанный на нечетком моделировании, для оценки риска, связанного с запросом доступа к медицинской информации. Они использовали чувствительность данных, серьезность действий и историю рисков в виде нечеткого значения для определения решения о доступе. Помимо этой работы, в статье [4] описывается метод нечеткого вывода для оценки риска. В ней нечеткий подход использовался для оценки рисков доступа.

Экспертная оценка

Когда практических данных недостаточно для описания вероятности и последствий определенного инцидента, могут использоваться экспертные оценки. Они представляют собой субъективные оценки, основанные на опыте. Экспертные оценки обычно используются для измерения неопределенных параметров в вероятностной форме для оценки различных элементов выбранной модели [10].

Экспертные оценки являются мощным инструментом в риск-анализе. Они используются во многих областях, таких как психология, уголовное правосудие, финансовое прогнозирование, политология, анализ решений и т.п. Использование экспертных оценок вызывает много вопросов относительно точности результатов, однако существует множество обстоятельств, при которых экспертное заключение является единственным источником точной информации [10]. Определение вероятности возникновения инцидента при анализе рисков с учетом неопределенности, которая его окружает, является сложной задачей, особенно для редких и чрезвычайных ситуаций. Это относится и к оценке риска безопасности операций контроля доступа [11].

Оценка риска

Оценка риска используется для предотвращения потенциального ущерба при определенных сценариях. Оценка рисков может определяться как процесс прогнозирования возможных потерь с использованием комбинаций известной информации о возможных ситуациях [12]. Оценка риска используется для определения контекста риска и приемлемых значений риска в каждой ситуации. Этого можно

достичь, сравнив его с рисками аналогичных сценариев. Помимо этого, она направлена на предоставление различных решений для снижения риска и эффективного регулирования рисками [13].

Определение подходящего типа риск-анализа зависит от имеющихся данных, которые характеризуют вероятность риска и его влияние. Эффективная оценка рисков имеет много преимуществ. Например, хорошо проведенная оценка риска, может предоставить сбалансированное решение для предотвращения риска или, по крайней мере, снижения его воздействия. Однако, это субъективный процесс, который зависит от опыта, и он действителен только в определенный момент времени [13].

Оценка риска использовалась в существующих моделях контроля доступа, основанных на риск-анализе. Например, авторы [14] представили три различных подхода, для оценки рисков в модели контроля доступа, основанной на анализе рисков. Эти подходы используют уровень чувствительности объекта, уровень надежности субъекта и разницы между ними. Помимо этого, в работе [15] предлагается модель контроля доступа на основе рисков, которая использует доступность, конфиденциальность и целостность для оценки величины риска при каждом запросе на доступ.

Теория игр

Теория игр рассматривается как раздел прикладной математики, который используется в таких областях, как эволюционная биология, экономика, искусственный интеллект, политология и информационная безопасность. Теория игр используется для описания сценариев принятий решений с участием нескольких лиц в форме игры. В ней каждый игрок выбирает соответствующие действия, которые, по их мнению, могут привести к максимально возможному выигрышу. При этом они должны учитывать разумные действия игроков противника [16].

Теория игр является основным инструментом для моделирования и построения автоматизированных операций принятия решений в интерактивных средах. Это связано с тем, что с помощью теории игр можно создавать последовательные и математические платформы. Сила теории игр заключается в методологии, которую она поддерживает для анализа различных проблем, связанных со стратегическим выбором. Процесс моделирования ситуации, как игры, требует, чтобы лицо, принимающее решения, взаимодействовало с игроками и при этом принимало их стратегические решения, а также наблюдало за их предпочтениями и реакциями.

Теория игр состоит из четырех компонентов: игроков, их стратегий, вознаграждений и информации, которой они обладают. Игроки являются неотъемлемой частью игры, они принимают решения в рамках игры. В то время как стратегия – это план, который игрок использует в отношении действий противоположного игрока. Поэтому для игроков крайне важно выбрать подходящую тактику. Выигрыш – это вознаграждение для игроков в игре. На выигрыш каждого игрока влияют как их собственные действия, так и действия других игроков [17]. В теории игр риск-анализ проводится с использованием преимуществ пользователя, а не вероятности. Кроме того, теория игр рекомендуется в условиях, при которых отсутствуют практические данные [18]. Однако это очень сложно, особенно с более чем двумя игроками. Это приводит к случайным результатам при использовании смешанных стратегий.

Теория игр была использована в моделях контроля доступа, основанных на риск-анализе. Например, авторы работы [17] предложили метод анализа рисков, основанный на предпочтениях или величинах выгоды, которые могут получить субъекты, использую теорию игр.

Дерево решений

Дерево решений – это общая методология для многих операций в машинном обучении. Она используется в качестве инструмента помощи для принятия решений в зависимости от группы правил, представленных в виде дерева [19]. Построение модели дерева решений требует разделения данных на обучающие и проверочные наборы. Обучающие данные

используются для извлечения соответствующих правил, применительно к дереву. Проверка дерева и внесения необходимых изменений выполняются с использованием данных проверки.

Дерево решений представлено в виде блок-схемы, где каждый узел представляет собой прямоугольник, который описывает вероятность риска и его влияние. Эти прямоугольники соединены стрелками, которые ведут к другому прямоугольнику, представляющему процентную вероятность [19].

Методы, основанные на дереве решений просты для понимания. Они могут эффективно работать с недостаточным количеством данных, если эксперты предоставят все необходимые правила. Они также могут отображать всевозможные альтернативы и трассировки в едином представлении, которое обеспечивает простое сравнение с различными альтернативами. Однако у модели дерева решений помимо преимуществ имеется ряд недостатков. Например, ее масштабируемость вызывает сомнения, так как при увеличении масштаба дерева, полученную модель будет тяжело анализировать и ей потребуется больше дополнительных правил для проверки. Помимо этого, модель дерева решений основана на ожиданиях, поэтому может возникнуть такая ситуация, когда не удастся спланировать все непредвиденные обстоятельства, которые могут возникнуть в результате принятия решения [20].

Выбор подходящего метода оценки рисков, который соответствует требованиям Интернета вещей, является непростой задачей. В табл. 2 приводится краткое описание преимуществ и недостатков ранее рассмотренных методов оценки риска, чтобы получить краткое представление о каждом подходе к оценке риска.

Таблица 2

Преимущества и недостатки методов оценки риска

Подход	Преимущества	Недостатки
Система нечеткой логики	– Проста понимания, тестирования и обслуживания; – Гибкость, так как основан на естественном языке; – Надёжный, работает при отсутствии правил или неправильных правилах; – Устойчив к неточным данным; – Может быть построен на основе экспертных оценок; – Способен работать с любым набором входных-выходных данных, используя нейро-нечеткую систему (NFS); – Использует правила, которые выражают неточность реального мира.	– Необходимо большое количество тестов и моделирования; – Сложен в освоении; – Трудно установить корректные правила без помощи экспертов в данной области; – Отсутствует точная математическая модель; – Субъективность; – Требуется немалое количество времени, особенно при большом количестве входных правил; – Масштабируемость кажется сомнительной, при большом количестве правил.
Оценка экспертов	– Быстрый по производимости; – Требует мало ресурсов, с точки зрения времени и затрат; – Может быть столь же точным, как и другие дорогостоящее методы; – С опытными экспертами гарантирует точные данные.	– Субъективность; – Непоследовательность; – Оценка зависит от уровня квалификации экспертов; – Рискован и подвержен ошибкам; – Нужно большое количество экспертов в исследуемой области.

Продолжение табл. 2

Подход	Преимущества	Недостатки
Дерево решений	– Рассматривает широкий спектр последствий; – Прост в понимании, когда есть несколько решений и результатов; – Результаты улучшаются числовыми значениями решений; – Быстрая сборка и тестирование; – Хорошо работает с нелинейными данными; – Показывает все возможные альтернативы и отслеживает каждую альтернативу.	– Основан на ожиданиях, что приводит к невозможности запланировать все непредвиденные ситуации, которые могут возникнуть при приятии решений; – Более сложный и менее точный с большими деревьями; – Нестабильный, так как небольшие изменения входных данных, могут вызвать большие изменения в дереве; – Ограничение на хранение, так как перерисовка деревьев вручную, требует много свободного места; – Нужны существенные знания и навыки, что бы создать большое дерево решений; – Не принимает во внимание, динамическую структуру различных приложений.
Оценка риска	– Эффективный инструмент, используемый при принятии решений; – Оценивает, передаёт, организует риски и ожидаемые преимущества; – Приводит к оптимальной продуктивности; – Повышает прозрачность и понимание.	– Субъективный процесс, который зависит от опыта экспертов; – Действителен в определенный момент, но может измениться со временем; – Непоследовательный; – Накладные расходы времени и средств.
Теория игр	– Анализ риска основан на результатах, которые могут предоставить субъекты, а не на субъективной вероятности; – Риск анализ в форме игры с игроками и стратегиями; – Идеально подходит для стратегической ситуации с индивидуальным поведением.	– Сложный и трудно реализуемый с более чем двумя игроками; – Применение и использование данного метода нереалистичны; – Использование смешанных стратегий генерирует случайные результаты; – Не учитывает ограничение ресурсов; – Предполагается, что оба игрока умны и рациональны.

На сегодняшний день не существует простого подхода, который можно было бы использовать без ограничений. Так же, в анализе рисков никогда не будет подхода к оценке рисков без субъективности. Помимо этого, в большинстве подходов основной проблемой является масштабируемость. Поэтому, выбор оптимального подхода оценки рисков, должен зависеть в большей степени от контекста. Поэтому ниже приведена табл. 3, с преимуществами и ограничениями обсуждаемых выше методов оценки риска.

Таблица 3

Сравнение преимуществ и ограничений методов оценки риска

Характеристики	Методики оценки рисков				
	Нечетка логика	Экспертная оценка	Оценка риска	Теория игр	Дерево решений
Преимущества					
Пригодный	✓	✓	×	✓	×
Быстрый	×	✓	✓	×	✓
Масштабируемый	×	×	✓	×	×
Динамичный	✓	✓	✓	×	✓
Использует опыт экспертов	✓	✓	✓	×	✓
Недостатки					
Ресурсоемкость	×	×	×	✓	✓
Временные затраты	✓	×	✓	×	✓
Субъективность	✓	✓	✓	✓	✓

Предлагаемый подход к оценке рисков

Не существует универсального и лучшего метода для проведения риск-анализа. Однако, важно понимать сильные и слабые стороны различных подходов чтобы выбрать наиболее уместный подход относительно контекста [21]. Существует много споров о приемлемом методе оценки риска, для моделей контроля доступа, основанных на оценках риска для систем ИВ. Понимание различных преимуществ и недостатков ранее рассмотренных подходов оценки рисков, продемонстрированных в табл. 2 и 3, может помочь в выборе подходящего метода оценки рисков в контексте ИВ.

После изучения литературы посвященной методам оценки рисков, был выбран подход на основе нечеткой логики с экспертной оценкой. Он представляется наиболее подходящим для реализации в модели контроля доступа на основе рисков в контексте ИВ. Существует немало причин в пользу этого выбора. Во-первых, есть достоверные источники знаний, которые предоставляют всю необходимую информацию для оценки риска безопасности, относительно операций контроля доступа. Одним из главных источников является полученный опыт. У администраторов безопасности обычно есть некоторые навыки относительно различных параметров риска и применений подходящих правил и политик относительно каждого контекста. Эти навыки и знания могут быть легко конвертирован в правила для систем нечеткой логики [22].

Во-вторых, одной из важных проблем в исследованиях, посвященных безопасности, является нехватка надлежащих наборов данных из-за законов о защите информации. Для правильной оценки величины риска, связанной с конкретной ситуацией, необходимы данные описывающие, вероятность ситуации и её последствия. Как только данные будут доступны, их можно использовать для более точной оценки величины риска. Используя систему нечеткой логики с экспертными оценками, нет необходимости в наборах данных, поскольку необходимые данные будут предоставлены экспертами данной области. Экспертная оценка является важным источником информации в операциях принятия решения, основанных на рисках. Это связано с тем, что в большинстве моделей оценки риска отсутствуют корректные числовые данные, описывающие вероятность инцидента и его последствия [23]. Зачастую, определение числового значения риска с использованием классических подходов вызывает затруднения. Поэтому в таких случаях используется экспертная оценка, для определения точных значений риска. При этом точность этих значений будет зависеть от того, насколько правильно были выбраны соответствующие эксперты [24].

В-третьих, система нечеткой логики является гибкой [25], поэтому она отлично подходит для систем ИВ, чтобы уметь адаптироваться к ее изменяющимся условиям и ситуациям.

В-четвёртых, так как экспертные оценки добавляют субъективность в процессе оценки рисков, то ее необходимо снизить до приемлемого уровня. Система нечеткой логики, позволяет регулировать субъективность, так как она изменяется в процессе создания правил. Конечно, субъективность нельзя полностью устранить, так как на сегодняшний день еще не существует такого метода для анализа рисков, который исключал бы субъективность [21].

Наконец, стоит отметить, что существует много приложений, которые используют систему нечеткой логики, например, помощь в принятии решений, психология, медицина, бытовая техника и т.д. [26, 27].

Сочетание системы нечеткой логики с экспертными оценками (рис. 1) может генерировать реалистичные значения риска относительно определенных сценариев. Один из необходимых шагов по реализации подхода нечеткой логики для оценки рисков безопасности, это установка подходящих нечетких правил. Определение подходящих нечетких правил – это одна из основных целей, направленная на объединение экспертных знаний специалистов в предметной области с системами нечеткой логики.

Рис. 1. Сочетание системы нечеткой логики с экспертной оценкой для процесса оценки риска

Заключение

Таким образом, можно сделать вывод о том, что выбор подходящего метода оценки рисков, который соответствует требованиям систем Интернета вещей, является нетривиальной и противоречивой задачей, поскольку каждый метод обладает своими преимуществами и недостатками. Стоит отметить, что на сегодняшний день не существует единственного подхода, который можно было бы использовать без ограничений. Также, всем рассмотренным методам оценки риска свойственна субъективность, поскольку все они, так или иначе, опираются на экспертные оценки. Помимо этого, в большинстве подходов основной проблемой является масштабируемость.

В результате проведенного анализа был выбран подход, основанный на теории нечеткой логики с экспертным суждением в качестве наиболее подходящего метода оценки рисков для реализации модели контроля доступа на основе рисков для систем Интернета Вещей. Выбор основан на нескольких причинах. Во-первых, теория нечеткой логики позволяет реализовать гибкую модель, построенную на основе опыта экспертов. Во-вторых, система нечеткой логики устойчива к неточным данным, поэтому возможно применение в условиях отсутствия статистических данных. В-третьих, анализ рисков, основанный на теории нечеткой логики с согласованными экспертными оценками, позволяет реализовать эффективный метод оценки рисков в операциях контроля доступа. И в-четвертых, при последовательной обработке экспертных оценок субъективность выводов нечеткой логики может быть уменьшена.

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. Yin J. On estimating the security risks of composite software services. / J. Yin, C. Tang, X. Zhang, M. McIntosh // First Program Analysis for Security and Safety Workshop Discussion (PASSWORD 2006). 2006. P. 1-10.

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. 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.

5. Bai Y. Fundamentals of Fuzzy Logic Control – Fuzzy Sets, Fuzzy Rules and Defuzzifications. / Y. Bai, D. Wang // Advanced Fuzzy Logic Technologies in Industrial Applications. 1982. P. 17-36.

6. Kose U. Fundamentals of Fuzzy Logic with an Easy-to-use, Interactive Fuzzy Control Application. / U. Kose // International Journal of Modern Engineering Research (IJMER). 2012. No. 2(3). P. 1198-1203.

7. Shapiro A., Koissi M. Risk Assessment Applications of Fuzzy Logic. / Casualty Actuarial Society. Canadian Institute of Actuaries, 2015.

8. 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 // IEEE Symposium on Security and Privacy. 2007. P. 222-227.

9. Li Juan 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. Leung K., Verga S. Expert Judgement in Risk Assessment Expert Judgement in Risk Assessment. / Defence R&D Canada Centre for Operational Research & Analysis, 2007. P. 321-354.

11. Turisova R., Mihok J., Kadarova J. Verification of the Risk Assessment Model through An Expert Judgment. / R. Turisova, J. Mihok, J. Kadarova // Kvalita Inovacia Prosperita/Quality Innovation Prosperity. 2012. P. 37-48.

12. Shapiro A., Koissi M. Risk Assessment Applications of Fuzzy Logic. / Casualty Actuarial Society, Canadian Institute of Actuaries, 2015.

13. Stoneburner G. Risk Management Guide for Information Technology Systems. / G. Stoneburner, A. Goguen, A. Feringa // NIST Special Publication Sp. 2002. No. 19(30).

14. 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.

15. Diep N.N. Enforcing Access Control Using Risk Assessment. / N.N. Diep [etc.] // The Fourth European Conference on Universal Multiservice Networks, 2007, pp. 419–424.

16. Binmore K. Applying game theory to automated negotiation. / K. Binmore, N. Vulkan // Economic Research and Electronic Networking. 1999. No. 1. P. 1–9.

17. 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.

18. Hamdi M. Game-based adaptive security in the Internet of Things for eHealth. / M. Hamdi, H. Abie // IEEE International Conference on Communications (ICC 2014). 2014. P. 920-925.

19. Shang K. Applying Fuzzy Logic to Risk Assessment and Decision-Making. / K. Shang, Z. Hossen // Casualty Actuarial Society, Canadian Institute of Actuaries. Society of Actuaries. 2013. P. 1-59.

20. Wang S. A Vertical Handoff Method via Self- Selection Decision Tree for Internet of Vehicles. / S. Wang, C. Fan, C.H. Hsu, Q. Sun, F. Yang // IEEE Systems Journal. 2016. No. 10(3). P. 1183-1192.

21. Boc K. Fuzzy approach to risk analysis and its advantages against the qualitative

approach. // Proceedings of the 12th International Conference. Reliability and Statistics in Transportation and Communication. 2012. No. 12. P. 234-239.

22. Alberts C. J., Dorofee. A. Managing Information Security Risks: The Octave Approach. / Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

23. Tversky A. Judgment under uncertainty: heuristics and biases. / A. Tversky, D. Kahneman // Science. 1974. No. 185(4157). P. 1124-1131.

24. Pluess D. Expert Judegement in Risk Analysis: A Strategy to Overcome Uncertainities. / D. Pluess, A. Groso, T. Meyer // Chemical Engineering Transactions. 2013. No. 31. P. 307-312.

25. Da Ruan. Fuzzy Sets and Fuzzy Information Granulation Theory. / Bejing Normal Univeristy Press, 2000.

26. Zimmermann H.J. Practical Applications of Fuzzy Technologies. / The Handbooks of Fuzzy Sets. Springer Berlin Heidelberg, 2000.

27. 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.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 23.05.2022

Информация об авторах

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

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

OVERVIEW OF METHODS FOR BUILDING A RISK-BASED ACCESS CONTROL MODEL IN INTERNET OF THINGS SYSTEMS

S.A. Ermakov, A.A. Bolgov

The paper discusses the concept of security risk and ways to assess it. A detailed review of methods of quantitative and qualitative risk assessment and analysis of their advantages and disadvantages is carried out. A detailed analysis of the applications of risk assessment methods in various risk-oriented access control models has been carried out, highlighting their advantages and disadvantages. The results of a comparative analysis of the advantages and limitations of the applicability of various risk assessment methods are presented. An approach based on fuzzy logic based on expert assessments is considered. Based on the analysis and comparison results, the fuzzy logic method with expert assessments was chosen as a suitable method for implementing a risk-based access control model for systems based on Internet of Things technology.

Keywords: access control, Internet of Things, fuzzy logic, risk assessment, quantitative assessment, qualitative assessment, risk, security.

Submitted 23.05.2022

Information about the authors

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

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