УДК 004.056

С. С. Чупров, Р. И. Гатауллин, И. И. Викснин
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Оценка уязвимостей в механизме группового управления мобильной робототехнической системой

Рассмотрено понятие мобильных робототехнических систем (МРТС): дано определение, область применения, основные преимущества использования. Описаны стратегии управления, среди которых групповое управление определено как наиболее полезное для целей исследования. Описаны типичные уязвимости МРТС и методы обеспечения их защищенности, снижающие вероятность использования таких уязвимостей. Выбран метод реализации модели полицейских участков (Police Office Model, POM), позволяющий назначить для каждого участка местности, на которой работает МРТС, отдельного робота, ответственного за обеспечение функционирования системы на вверенной ему области. Определены наиболее актуальные уязвимости, для которых впоследствии оценивается степень риска их возможного использования злоумышленником. Оценка проводится на основе открытого стандарта CVSS, который содержит ряд метрик, позволяющих описать МРТС как информационную систему. Впоследствии оценки по методике CVSS для исходной МРТС и для МРТС, в которой внедрена модель полицейских участков, сравниваются.

Мобильная робототехническая система, мобильный агент, информационная безопасность, модель полицейских участков, CVSS

Формализация понятия МРТС. Промышленная робототехника затрагивает самые различные области науки и техники, в частности – вопросы создания, сборки, конструирования отдельных роботов, разработки систем управления как отдельными компонентами робота, так и группой роботов. Робототехника активно внедряется в различные сферы жизнедеятельности человека, подстраиваясь под современные запросы. С развитием отдельных сфер науки и техники стало возможным и развитие робототехнических устройств в составе так называемых автономных мобильных робототехнических систем (МРТС), применяемых для решения комплексных задач, требующих высокой надежности [1].

Как правило, для решения большинства задач применяются либо отдельные роботы, либо их объединение (группа, рой), в которых каждый робот способен выполнять свои задачи автономно. Спектр задач, которые будет выполнять отдельный робот, ограничивается доступными для его функционирования ресурсами, и, соответственно, для расширения его функциональности разработчикам необходимо совершенствовать робота, тем самым увеличивая его конечную стоимость. При использовании одиночных роботов надежность системы в целом обусловлена наименее отказоустойчивой составляющей, что делает ее зависимой от одного из компонентов робототехнического устройства, который при отказе функционирования может повлиять на деятельность всей системы. Когда для решения задачи привлекается группа роботов, то разбиение подзадач происходит между отдельными автономными роботами, при этом они по структуре могут быть относительно простыми, что положительно сказывается и на возможности расширить группу роботов при усложнении решаемых задач, и на надежности всей системы. Таким образом, для эффективного решения комплексных задач широкое применение получили группы взаимодействующих роботов, представляющие собой интеллектуальные МРТС.

Мобильная робототехника как отдельная область исследований включает в себя вопросы изучения организации частично или полностью автономных мобильных робототехнических устройств, способных в определенных условиях выполнять свои функции без вмешательства человека-оператора [2]. Отличительной особенностью данной области исследований от таких областей, как, например, искусственный интеллект

или машинное зрение, служит ориентированность на решение проблем и выполнение задач, распределенных по местности функционирования. В частности, использование МРТС актуально для передвижения в пространстве, получения информации об окружающей среде сканированием местности с помощью датчиков и сенсоров, принятия решений на основе информации, полученной из окружающей среды, в том числе без участия человека.

В настоящее время МРТС находят широкое применение в различных сферах деятельности человека в целях автоматизации и оптимизации выполнения тяжелой и/или опасной для человека работы. Применение МРТС позволяет автоматизировать процессы в различных сферах. Мотивация для использования именно мобильных робототехнических систем обусловлена следующими факторами:

– наличие обстоятельств, не позволяющих человеку выполнить задачу (например, долгое нахождение в воздухе);

– наличие враждебной окружающей среды, опасной для человека;

– задача подразумевает несоизмеримо большие затраты ресурсов и/или времени, если ее будет выполнять человек.

Использование группы мобильных роботов (агентов) для решения задач в сравнении с одним многофункциональным робототехническим устройством имеет ряд преимуществ [3]. В их число входят:

– избыточность, надежность и масштабируемость: участники группы мобильных роботов устроены проще, более надежны (надежность каждого отдельного робота обусловлена степенью надежности наименее отказоустойчивого компонента), а также способны выполнять большое количество задач, связанных с распределением на местности;

– способность использовать децентрализованную стратегию группового управления: в системе отсутствует центральное управляющее устройство, т. е. мобильные агенты самостоятельно принимают решение на основе данных, полученных из окружающей среды, и коммуникации между собой;

– способность выполнять сложные задачи, которые, по определенным причинам, не могут быть выполнены одним роботом;

– за счет групповых действий возможно повышение быстродействия системы и оптимизации ее действий;

– отдельные простые роботы более дешевы в производстве и обслуживании.

Обеспечение информационной безопасности в МРТС. Мобильная робототехника, подразумевающая групповое взаимодействие некоторого количества отдельных робототехнических устройств, обладает такими характеристиками, как автономность; наличие системы группового управления, некоторого количества участников группы, коллективного «поведения»; способность получать информацию из окружающей среды и осуществлять коммуникацию с другими участниками группы. С точки зрения информационной безопасности (ИБ), в связи с вышеупомянутыми характеристиками функционирование группы робототехнических устройств (и, в частности, информационное воздействие элементов системы между собой и с окружающей средой) может быть сопоставимо с функционированием компьютерных коммуникационных сетей.

Обеспечение информационной безопасности МРТС на текущий момент сохраняет свою актуальность: существует ряд методов, повышающих защищенность как отдельных роботов-агентов, так и всей системы в целом, однако они могут применяться только в рамках обособленной области определения, т. е. универсальных методов на данный момент не существует. Использование различных методов обеспечения ИБ, тем не менее, позволяет снизить риск деструктивного воздействия на МРТС со стороны возможного злоумышленника, что далее будет рассмотрено на примере внедрения в стандартную МРТС модели полицейских участков (Police Office Model, POM), разработанной китайскими исследователями в 2000 г. [4] и усовершенствованной российскими учеными в 2014 г. [5].

Модель функционирования сетевых хостов, обслуживающих мобильных агентов, предполагает разделение всей сети на определенные участки – регионы. В каждом из регионов назначается так называемый «полицейский участок» – агент, ответственный за обеспечение функций безопасности в пределах своего региона. Мигрируя из одного региона в другой, каждый мобильный агент обязан зарегистрироваться в соответствующем полицейском участке и получить разрешение на выполнение своих функций. Также предусмотрено разделение мобильного агента на две части – главную и вспомогательную. Главная часть находится в полицейском участке, отвечает за обеспе-

чение функций информационной безопасности и хранит все необходимые данные, вспомогательная же часть может быть отправлена на хост в пределах региона для выполнения каких-либо действий (сбор данных и т. п.). В статье российских ученых [5] рассмотрена возможность совершенствования модели РОМ для обеспечения безопасности роевых робототехнических систем. В ней приводится механизм, позволяющий повысить защищенность алгоритма выбора кратчайшего пути (муравьиный метаэвристический алгоритм), показано влияние роботов-диверсантов на систему при их различной концентрации в рое. С помощью численного эксперимента обоснована помехоустойчивость РОМ в случае, если время воздействия помех на систему меньше, чем время миграции робота из одного региона в другой. Таким образом, подобная структура функционирования системы позволяет противодействовать шпионским атакам (анализ программного кода и информации, которую содержат в себе мобильные агенты), атакам по выводу агентов из строя, дает возможность интегрирования в модель функций агентов, позволяющих им выполнять свои задачи.

Источники угроз и уязвимости МРТС. В соответствии с [3] к основным источникам угроз в МРТС относятся:

– уязвимости в системе мониторинга и контроля в связи с децентрализованной организацией системы;

– уязвимости коммуникационных каналов;

– уязвимости процесса аутентификации;

– уязвимости системы реагирования роя на окружающую среду;

– ограниченность ресурсов отдельных роботов;

– физический захват или подделка роботов (внедрение в группу агентов-диверсантов, с помощью которых злоумышленник способен нарушить работу системы);

– постоянная подвижность роя;

– необходимость организации хранения криптографических ключей при использовании шифрования канала связи;

– необходимость наличия системы предотвращения вторжений, адекватной используемым в системе технологиям и уязвимостям.

Многие из перечисленных угроз связаны со свойством автономности элементов МРТС, что значительно отличает их от других распределенных информационных систем. Перечисленные способы обеспечения ИБ в МРТС не универсальны и имеют определенные недостатки. Решение задач обеспечения ИБ в подобных системах имеет не только теоретическую значимость, но и позволит в дальнейшем проектировать и разрабатывать МРТС, более устойчивые к деструктивным информационным воздействиям, как явным, так и скрытым.

Уязвимости в программном, аппаратном и программно-аппаратном обеспечении представляют серьезный риск для эксплуатантов МРТС. Необходимо определить уязвимости, оценку которых предстоит выполнить. Так, уязвимости, эксплуатация которых подразумевает использование побочных электромагнитных излучений и наводок, физическое воздействие на систему (кража робота, подключение к портам робота, влияние агрессивной внешней среды и т. п.), «жесткое» воздействие на систему (атаки типа «отказ в обслуживании», «переполнение буфера» и т. п.) в контексте данной работы не рассматривались.

Таким образом, далее в качестве актуальных для мобильной робототехнической системы уязвимостей будут рассмотрены следующие:

– уязвимость А: уязвимость в системе группового управления МРТС, позволяющая роботам-агентам умышленно либо в результате нарушения корректных режимов работы программно-аппаратных устройств предоставлять другим агентам недостоверные данные об остатке энергоресурсов, о задачах, подлежащих выполнению, своем местоположении и статусе выполнения задачи. В результате успешной эксплуатации данной уязвимости система группового управления МРТС подвергается деструктивному информационному воздействию со стороны легитимных агентов, что приводит к снижению эффективности функционирования системы. К тому же, успешная эксплуатация данной уязвимости позволяет злоумышленнику внедрить в МРТС своего агента, передающего другим агентам заведомо ложные данные;

– уязвимость В: уязвимость канала связи между агентами к атакам типа «человек посередине». В результате успешной эксплуатации данной уязвимости злоумышленником может быть совершен перехват информации, передаваемой по каналу связи, и дальнейшая возможная ее несанкционированная модификация и передача легитимным агентам системы. Таким образом, в зависимости от намерений злоумышленника может как пострадать конфиденциальность переда-

ваемой информации, так и в результате дальнейших действий злоумышленника может оказываться влияние на целостность передаваемой информации.

Задача исследования. Оценить наиболее актуальные уязвимости, ранее определенные как уязвимости A и B, присутствующие в двух видах МРТС: в классической МРТС и в усовершенствованной МРТС, элементы которой взаимодействуют между собой на основе модели полицейских участков.

Оценка уровня защищенности. Для решения задачи использовалась методика Common Vulnerability Scoring System (CVSS). Методика предоставляет возможность определения основных характеристик уязвимости и получения числовой оценки, отражающей ее опасность для функционирования системы. Числовая оценка затем может быть переведена в качественное представление (степень риска обозначается как «низкая», «средняя», «высокая» и «критическая»), что может помочь эксплуатантам МРТС должным образом оценить и расставить приоритеты в своих процессах управления уязвимостями.

Основные преимущества использования методики CVSS для оценки уязвимостей:

– CVSS предоставляет стандартизированные оценки уязвимостей, что позволяет сформировать единую политику управления уязвимостями, определяющую максимально допустимое время для проверки и устранения данной уязвимости;

– использование CVSS подразумевает наличие открытой (доступной для ознакомления) структуры оценки уязвимостей, что позволяет исключить неоднозначную трактовку степени влияния уязвимостей на систему в целом. Характеристики, используемые для расчетов, также прозрачны;

– CVSS позволяет назначать приоритет отдельным рискам: иными словами, использование этой методики позволяет определить уязвимости, актуальные именно для конкретной информационной системы (организации, эксплуатирующей ее).

– данная методика используется Федеральной службой по техническому и экспортному контролю Российской Федерации для формирования оценок уязвимостей, содержащихся в банке данных угроз информационной безопасности.

Отзывы организаций, использующих CVSS, показали, что при эксплуатации первой версии возникали существенные проблемы. Работа над CVSS второй версии началась в апреле 2005 г., а окончательная спецификация была запущена в июне 2007 г. Дальнейшее развитие привело к тому, что работа над CVSS третьей версии началась в 2012 г. и закончилась выпуском CVSS v3.0 в июне 2015 г. На данный момент актуальна версия методики CVSS v3.1, выпущенная в июне 2019 г. Эта версия не вносит новых изменений в стандарт, но детализирует описание некоторых используемых метрик для лучшего их понимания.

Методика делит оценку уязвимостей на три группы метрик: базовые, временные, контекстные.

Базовые метрики описывают характеристики уязвимости, которые не зависят от среды и не меняются со временем. Они подразделяются на две подгруппы: метрики эксплуатации (определяющие контекст использования уязвимости: вектор атаки; сложность атаки; уровень привилегий; взаимодействие с пользователем; сфера воздействия) и метрики влияния на свойства системы (влияние на конфиденциальность, целостность и доступность информационных ресурсов, управляемых компонентом, на который направлена атака).

Временные метрики отражают текущее состояние методов реализации атаки либо их доступности возможному злоумышленнику, а также степень уверенности в том, что описанная уязвимость не имеет других возможностей ее эксплуатации. К временным метрикам относятся следующие: доступность средств эксплуатации; доступность средств устранения уязвимости; степень доверия к информации об уязвимости.

Контекстные метрики позволяют оценивать уязвимость с поправкой на характеристики информационной среды. Они подразделяются на требования к безопасности (условно «модифицированное» влияние на конфиденциальность, целостность и доступность информации) и модифицированные базовые метрики (к примеру, «модифицированный вектор атаки», «модифицированная сфера воздействия»).

Для всех описанных метрик определен ряд возможных значений, который, в свою очередь, для проведения оценки переводится в числовые значения. Более подробно с алгоритмом вычисления оценки уязвимостей по методике CVSS третьей версии можно ознакомиться в документе о спецификации [6] и в руководстве пользователя по проведению оценки.

Таблица 1

Описание	Обозначение	Уязвимость A	Уязвимость A + POM	Уязвимость B	Уязвимость B + POM
Вектор атаки	AV	Смежная сеть (A)	Смежная сеть (A)	Смежная сеть (A)	Смежная сеть (A)
Сложность атаки	AC	Низкая (L)	Высокая (H)	Высокая (H)	Высокая (H)
Уровень привилегий	PR	Низкий (L)	Высокий (H)	Не требуется (N)	Высокий (H)
Взаимодействие с пользователем	UI	Не требуется (N)	Не требуется (N)	Не требуется (N)	Не требуется (N)
Влияние на другие компоненты системы	S	Оказывает (C)	Оказывает (C)	Оказывает (C)	Оказывает (C)
Влияние на конфиденциальность	C	Не оказывает (N)	Не оказывает (N)	Высокое (H)	Высокое (H)
Влияние на целостность	I	Высокое (H)	Низкое (L)	Низкое (L)	Низкое (L)
Влияние на доступность	A	Не оказывает (N)	Не оказывает (N)	Не оказывает (N)	Не оказывает (N)
Доступность средств эксплуатации	E	Высокая (H)	Есть сценарий (F)	Есть сценарий (F)	Есть сценарий (F)
Доступность средств устранения	RL	Не определено (X)	Не определено (X)	Рекомендации (W)	Рекомендации (W)
Степень доверия к информации об уязвимости	RC	Не определено (X)	Не определено (X)	Не определено (X)	Не определено (X)
Требования к конфиденциальности	CR	Высокие (H)	Высокие (H)	Высокие (H)	Высокие (H)
Требования к целостности	IR	Высокие (H)	Высокие (H)	Высокие (H)	Высокие (H)
Требования к доступности	AR	Высокие (H)	Высокие (H)	Высокие (H)	Высокие (H)
Модифицированные базовые метрики	MAV, MAC, MPR, MUI, MS, MC, MI, MA	Аналогично немодифицированным базовым метрикам			

В третьей версии методики были определены качественные уровни оценки в соответствии с числовой оценкой: None (отсутствует, 0), Low (низкая, 0.1…3.9), Medium (средняя, 4.0…6.9), High (высокая, 7.0…8.9) и Critical (критическая, 9.0…10.0).

Для проведения оценки используется калькулятор CVSS V3.1, размещенный в свободном доступе на сайте ФСТЭК [7].

Показатели метрик для оценки уровня риска эксплуатации уязвимостей A и B в исходной МРТС и с использованием модели полицейских участков (Police Office Model) приведены в табл. 1. Описание, обозначения и качественные значения метрик приведены в соответствии с методикой CVSS v3.1.

Результаты оценки описанных уязвимостей МРТС без использования логики POM, с ее использованием и шифрования канала связи представлены в табл. 2.

Таблица 2

Уязвимости	Метрики	Исходная МРТС	МРТС + POM
Уязвимость A	Базовые	6.8 – M	2.6 – L
	Временные	6.8 – M	2. 6 – L
	Контекстные	8.9 – H	3.4 – L
Уязвимость B	Базовые	6.9 – M	6.2 – M
	Временные	6.5 – M	5.9 – M
	Контекстные	8 – H	7.2 – H

Интерпретация результатов. В ходе проведения оценки описанных ранее уязвимостей по методике CVSS последней версии определено, что при использовании метода внедрения модели полицейских участков в МРТС оценки уязвимости A (недостоверные данные от агента) по различным метрикам снизилась значительно (с 6.8 до 2.6; с 8.9 до 3.4; в целом оценка уязвимости сменилась со «средней»/«высокой» на «низкую»); оценка уязвимости B (перехват и модификация информации внутри МРТС), в свою очередь, существенно не изменилась (осталась на «среднем»/«высоком» уровне). При использовании метода полицейских участков в МРТС общая степень риска реализации уязвимости A была заметно снижена, что показывает пользу применения такого метода в случаях, когда эксплуатантами МРТС предусматривается необходимость принятия мер по снижению степени наступления подобного риска. В свою очередь, внедрение такого метода не помо-

жет значительно снизить риск эксплуатации уязвимости В («человек посередине»), а значит, использования только одного метода для всестороннего обеспечения ИБ в МРТС будет явно недостаточно.

Определено, что выбранная для проведения оценки уязвимостей методика не в полной мере подходит для оценки уязвимостей в робототехнических системах.

Данная методика создавалась для оценки опасности уязвимостей в традиционных компьютерных системах и, в случае робототехнических систем, не позволяет учесть специфические особенности таких систем и предоставить точную с точки зрения реальной опасности уязвимости оценку той или иной уязвимости. В подобных системах роботы – это физические объекты, которые могут взаимодействовать с другими роботами, окружающей средой и человеком, что создает дополнительные векторы атак. Методика CVSS позволяет наиболее полно оценить лишь уязвимости информационного взаимодействия элементов МРТС, при этом необходимо получить и оценку физического влияния окружающей среды на систему (либо системы на окружающую среду). Концепция использования робототехнических систем построена именно на взаимодействии информационных и физических компонентов. Если предположить, что следующая версия методики CVSS будет затрагивать и такие аспекты взаимодействия, то не исключено, что она будет более пригодна для оценки уязвимостей функционирования МРТС.

В качестве дальнейших исследований в данной области планируется разработка физической модели мобильной робототехнической системы для проведения имитационного моделирования на реальных физических объектах в условиях внешней среды реального мира.

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации (проект «Госзадание» № 075-01024-21-02 от 29.09.2021).

СПИСОК ЛИТЕРАТУРЫ

1. Конюх В. Л. Основы робототехники. Ростов-н/Д.: Феникс, 2008.

2. Dudek G., Jenkin M. Computational principles of mobile robotics. Cambridge: Cambridge University Press, 2010.

3. Higgins F., Tomlinson A., Martin Keith M. Threats to the swarm: Security considerations for swarm robotics // Intern. J. on Advances in Security. 2009. Vol. 2, № 2&3. P. 288–297.

4. Guan X., Yang Y., You J. POM-a mobile agent security model against malicious hosts // Proc. Fourth Intern. Conf. «Exhibition on High Performance Computing in the Asia-Pacific Region» IEEE. 2000. Vol. 2. P. 1165–1166.

5. Совершенствование Police Office Model для обеспечения безопасности роевых робототехнических систем / И. А. Зикратов, А. В. Гуртов, Т. В. Зикратова, Е. В. Козлова // Науч.-техн. вестн. информационных технологий, механики и оптики. 2014. № 5 (93). С. 99–109.

6. Team C. Common vulnerability scoring system v3.0: Specification document // First. org. 2015. URL: https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf (дата обращения 16.11.2021).

7. БДУ – Калькулятор CVSS V3.1. URL: https://bdu.fstec.ru/calc31 (дата обращения 11.11.2021).

S. S. Chuprov, R. I. Gataullin, I. I. Viksnin
Saint Petersburg Electrotechnical University

VULNERABILITY ASSESSMENT IN THE GROUP MANAGEMENT OF MOBILE ROBOTIC SYSTEM

Describes the concept of mobile robotic systems (MRTS): the definition, scope, main advantages of use are given. Management strategies are described, among which group management is identified as the most useful for research purposes. The typical vulnerabilities of MRTS and methods of ensuring the security of MRTS, which reduce the likelihood of exploiting such vulnerabilities, are described. The method of implementation of the Police Office Model (POM) was chosen, which allows assigning for each site of the terrain in which the MRTS operates, a separate robot responsible for ensuring the functioning of the system in the area entrusted to it. The most relevant vulnerabilities have been identified, for which the risk of their exploitation by a possible attacker is subsequently assessed. The assessment is carried out using the open CVSS standard, which contains a number of metrics that allow describing the MRTS as an information system. Subsequently, the estimates are compared using the CVSS methodology for the original MRTS and for the MRTS with POM implemented.

Mobile robotic system, mobile agent, information security, police office model, CVSS