УДК 519.8

DOI: http://doi.org/10.25728/pu.2020.3.6

МЕТОДЫ ОЦЕНКИ ИНФОРМАЦИОННОЙ УГРОЗЫ ДЛЯ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ В СРЕДЕ «УМНОГО ГОРОДА[1]»

В.Г. Промыслов, К.В. Семенков, Е.Ф. Жарко

Аннотация. Представлена комплексная модель кибербезопасности системы беспилотных транспортных средств (БТС) в среде «умного города». Рассмотрены проблемы описания информационных потоков в реальной системе БТС с помощью дискреционных моделей безопасности. Введено понятие безопасной передачи данных для задания специальных типов информационного обмена между активами в системе. Предложены методы классификации активов с учетом информационной связанности активов в рамках моделей Биба и Белла — Лападулы для целостности и конфиденциальности соответственно. Обсуждена комплексность понятия «целостность» в контексте обеспечения кибербезопасности системы и подчеркнута важность его расширения на оборудование и методы обработки данных. Отмечено, что такой подход позволяет перенести основное внимание на анализ и ликвидацию уязвимостей системы и строить ее защиту, основываясь на ее внутренних свойствах. Рассмотрены динамические методы синтеза архитектуры кибербезопасности транспортных систем с БТС. Показано, что динамические методы позволяют уменьшить вычислительную сложность моделирования системы с БТС. Для выбранного БТС анализ проведен не на полном графе безопасности, а на некотором его индуцированном подграфе. При этом вершины (активы) в полном графе безопасности исключены из рассмотрения, при условии, что они находятся на большом «расстоянии» от актива, для которого проводится анализ. Предложены формулы расчета «расстояний» в графе безопасности. Приведены примеры анализа и синтеза архитектуры кибербезопасности для БТС.

Ключевые слова: кибербезопасность, беспилотное транспортное средство, «умный город», архитектура кибербезопасности, классификация, кластеризация, граф безопасности, модель «take-grant».

ВВЕДЕНИЕ

Применение беспилотных транспортных средств (БТС) рассматривается в мире не только как способ повышения экономической эффективности транспортных перевозок, но и как технология повышения безопасности и эффективности дорожного движения [1]. Правительство России разработало проекты нормативных документов, определяющих методы обеспечения безопасности беспилотного транспорта на дорогах [2]. Беспилотным транспортным средством предлагается считать высоко или полностью автоматизированное транспортное средство, функционирующее без вмешательства человека (в беспилотном режиме). Проблемы безопасности, а также нравственные и юридические проблемы, связанные с применением как автономных роботов в общем случае, так и выведением БТС на дороги общего пользования активно обсуждаются на экспертном уровне [3, 4]. Одна из ключевых характеристик БТС — реализация функции обмена информацией с другими участниками движения и инфраструктурой «умного города», что позволяет БТС получать информацию не только от собственных встроенных сенсоров, но и других объектов [5]. Это обеспечивает расширение условного «поля зрения» БТС за границы доступного для изолированного БТС и, в конечном счете, повышает его безопасность и эффективность его применения.

В контексте информационного обмена БТС можно выделить несколько типов связей: между

[1] Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-29-06044, гл. 3 и 4.

транспортными средствами (Б2Б), БТС — инфраструктура (Б2И), БТС — пешеход (Б2П) и др.

Отметим, что возможностью передавать и получать информацию в реальном времени будут обладать не только БТС, но и обычные транспортные средства с водителем. Предполагается, что к 2025 г. начнут эксплуатироваться автоматизированные беспилотные транспортные системы в рамках ограниченных территорий, а на дорогах общего пользования начнут появляться беспилотные автомобили [6]. Такова новая реальность интеллектуальных транспортных систем.

Указанные возможности приведут к появлению инновационных решений для пассивной и активной безопасности дорожного движения, вспомогательных услуг для водителей, «умной мобильности» и услуг управления движением.

Следует учитывать, что применение большинства современных технологий имеет двойственный характер. Они служат как средства повышения безопасности, однако и сами по себе могут индуцировать новые угрозы окружающим. Наличие обширных каналов обмена информацией БТС с различными активами в системе приводит к появлению угроз и уязвимостей в сфере информационной и кибербезопасности (ИБ). Термин «кибербезопасность» имеет широкий смысл и часто интерпретируется для промышленных систем как «Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли от/или повреждения критических систем или информационных объектов» [7]. Однако в настоящей работе кибербезопасность рассматривается более узко, как свойство объекта не быть опасным для окружающей среды при его функционировании во всех режимах работы [8].

Применяемая в БТС технология информационного обмена в значительной степени зависит от компьютерных технологий управления объектом и технологий беспроводной и мобильной связи для обмена данных между объектами. Все относящиеся к ним угрозы и уязвимости, а также атаки с их применением могут влиять на функционирование БТС [9, 10] и ставят под угрозу безопасность других участвующих в транспортном движении субъектов. Существуют и специфические угрозы интеллектуальным транспортным средствам, к которым относится и БТС, угрозы приведены в работах [11—13].

Необходимо оценивать уязвимости в системе и уметь противостоять угрозам ИБ, чтобы реализовать потенциал взаимодействия БТС со средой «умного города» и другими участниками движения.

В настоящей работе приведен обзор текущих проблем обеспечения информационной безопасности БТС, анализируется ее влияние на функционирование БТС и других субъектов в среде «умного города». Рассмотрены методы анализа и управления информационной безопасностью БТС на основе расширенной дискреционной модели доступа и предложен механизм учета динамического характера поведения системы. Приведены примеры, иллюстрирующие предложенный подход.

1. КОМПЛЕКСНАЯ МОДЕЛЬ КИБЕРБЕЗОПАСНОСТИ В ПРИМЕНЕНИИ К БЕСПИЛОТНЫМ ТРАНСПОРТНЫМ СРЕДСТВАМ

Для описания ИБ в системе «БТС — умный город» рассмотрим комплексную аналитическую модель ИБ системы, аналогичную предложенной в работе [14] для промышленных систем управления.

Определение 1. Комплексная аналитическая модель информационной безопасности БТС — это совокупность компонентов $ICM = \langle DM, R\rangle$, где компонент DM (*data model*) задает порядок обмена информации между активами. Набор операторов R задает опциональное правило ранжирования активов в модели DM. Активы в модели представляют собой идентифицированные как важные в смысле ИБ объекты системы. ♦

В качестве комплексной аналитической модели информационной безопасности БТС принята расширенная дискреционная модель безопасности «take-grant» («*брать-давать*») [15], которая применяется для задания информационных связей. Решеточная модель доступа, предложенная в работе [16], описывает архитектуру кибербезопасности в системе.

Под термином «архитектура кибербезопасности» будем понимать связанную с ИБ структуру системы как системы систем, включая основные функции, класс и границы каждой системы, а также взаимосвязь или независимость систем, приоритетность целей ИБ, действующих в системе и порядок взаимодействия между активами.

Далее рассмотрим компоненты модели подробнее.

1.1. Модель обмена информацией

В дискреционной модели безопасности компонент $DM = \langle G^*, OP\rangle$, где $G^* = \langle\{G_i | i = 1, N\}\rangle$ — все возможные состояния системы, которые описываются ориентированным графом $\{A_i\}$ соответствует активам, ребра, соответственно, задают бинарные отношения между $\langle A, \{\mapsto, \neg\}\rangle$.

Представим информационную модель системы «умный город плюс БТС» в виде графа (графа безопасности), отражающего физическую природу описываемой системы. Свойства такого графа приведены в табл. 1.

В модели графы служат для описания отношений доступа между объектами и субъектами поли-

тики безопасности. В рамках данной модели ИБ описывается в виде графа безопасности G, где G — это конечный помеченный ориентированный взвешенный мультиграф, описывающий состояние системы: $G = G(A, E)$, где A — множество вершин, E — множество ребер.

В графе выделяются два типа вершин: один соответствует субъекту, другой — объекту, которые отражают активные и пассивные активы моделируемой системы.

Наличие ребра, направленного из вершины A к вершине B, означает, что A имеет некоторое право (права) доступа к B. Обычно стандартными считаются такие права доступа: чтение r (*read*), запись w (*write*) — в части передачи информации, взятие t (*take*), выдача g (*grant*) — в части передачи прав. Отношения, связанные с передачей прав доступа $R = \{r_1, r_2, ..., r_n\} \cup \{t, g\}$, принято называть отношениями «де-юре», а $R = \{r_1, r_2, ..., r_n\} \cup \{w, r\}$ — отношениями «де факто». Для отношений «де факто» введен набор элементарных преобразований для описания передачи информации (*Post*, *Pass*, *Spy*, *Find*) и модификации графа — добавления и удаления вершин и ребер (*Create*, *Delete*).

Достоинство модели «take-grant» заключается в ее вычислительной эффективности.

Начальный граф доступа G_0, задаваемый формальной моделью безопасности, может быть трансформирован последовательным применением элементарных правил в новый граф G' (трансформация обозначается как $G_0 \mapsto G'$). Информационная безопасность системы рассматривается в смысле возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения элементарных команд. Рассматриваются условия санкционированного, т. е. законного получения прав доступа, и «похищения» прав доступа.

Базовым отношением на графе, употребляемым при моделировании, является отношение *can_know*. Следуя работе [15], приведем условия, при которых субъект может осуществить доступ типа $\{r, w, t, g\}$ к активу для указанного выше набора прав доступа и элементарных правил преобразования графа.

Определение 2. Отношение *can_know* $f(x, y, G_0)$ верно тогда и только тогда, когда существует последовательность графов безопасности $G_0, G_1, ..., G_n$ такая, что $G_0 \mapsto G_n$, и в графе G_n либо существует ребро (x, y), обозначаемое как r, либо существует ребро (y, x), обозначаемое как w, и если ребро явное, то его начало — субъект. ♦

При моделировании системы нужно учитывать особенности отношений: все операции являются обратно симметричными операциями, если они выполняются между субъектами [17]. Например, для отношений $\{w, r\}$, если субъект A может прочесть данные от субъекта B, то это означает, что актив B может записать в A. Сопряженную вторую часть таких симметричных отношений называют неявными отношениями. В такой модели инфор-

Таблица 1

Соответствие физических свойств системы «БТС — инфраструктура умного города» ее представлению в виде графа безопасности

Физическое свойство системы	Свойство графа $G(A, E)$
В процессах передачи информации существуют источник и получатель	Направленность отношений
Имеются разные типы объектов (активные и пассивные)	Вершины могут соответствовать как объектам, так и субъектам, следовательно, в общем случае вершины окрашены
Имеются различные виды отношений между активами	Ребра могут относиться к разным типам, например: передача прав на управление БТС, передача информации между БТС и другими активами, получение команд управления. Следовательно, ребра графа в общем случае окрашены
В общем случае, в системе, включающей в себя БТС, есть иерархия, как-то: диспетчеры, объекты дорожной инфраструктуры, централизованные системы управления движением, сами БТС и пр.	В графе выделяется подмножество вершин $\hat{A} \subset A \in G(A, E)$, на котором можно ввести отношение порядка
Наличие в системе барьеров на пути передачи информации (шлюзов, брандмауэров и др.)	Граф, вообще говоря, не транзитивен, т. е. из отношения порядка между вершинами $a_1 \le a_2$, не следует, что эти вершины соединены ребром $(a_1, a_2) \in E$
Реальные системы содержат конечное число элементов	Граф конечен
Двойственность, симметричность отношений между активами	Граф может содержать циклы
Активы, взаимодействующие с БТС, и отношения, возникающие между ними и БТС, зависят от времени	Граф динамически обновляемый

мация о субъекте может быть получена двояко: либо если субъект A, интересующийся субъектом B, имеет отношения типа r с субъектом B, либо если субъект B имеет отношения w с субъектом A.

Неявная запись означает, что если субъект A имеет отношения типа r с субъектом B, то чтение информации от B может рассматриваться как передача (запись) информации от B в A. Неявное чтение несколько более абстрактно. Проиллюстрируем его примером: представим, что актив B не содержит никакой информации до начала записи в него информации от A. После завершения записи B будет содержать только ту информацию, которую передал ему A, так как A очевидно знает, что он передавал. Следовательно, A будет иметь полное знание об информации в B, как если бы он ее прочитал.

В настоящей работе основное внимание уделено применению дискреционной модели к анализу свойств ИБ, связанных с передачей в виде чтения и записи информации между активами в системе (отношений «де факто»), а не прав на нее (отношений «де юре»).

Дискреционная модель позволяет описывать разнообразные сценарии поведения систем БТС и допускает различные способы отображения объектов и отношений реальной системы в модель. В нашем случае мы принимаем способ представления системы с БТС в дискреционной модели в соответствии с табл. 2.

Симметрия отношений «де факто» в дискреционной модели приводит к тому, что невозможно организовать обмен информацией между активами по чтению без нарушения целостности или запись без нарушения конфиденциальности (модели Биба и модель Белла — Лападулы соответственно) [18, 19] между различными уровнями системы, если в процессе передачи информации учувствуют только субъекты.

Это ограничение в некоторых случаях можно обойти [14, 17], вводя несимметричные отношения или используя промежуточные объекты в цепи. Далее мы проведем рассуждения в рамках модели Биба, так как в основном ИБ систем управления технологическими объектами нацелена на сохранение целостности, а не конфиденциальности (см., например, п. 5.2 ГОСТа [7] или работу [20]). Анализ модели Белла — Лападулы может быть проведен аналогичным путем.

Модель Биба определяет, что граф доступа безопасный, если актив с более низким уровнем безопасности не может осуществить запись в актив с более высоким уровнем ИБ и изменить в нем информацию.

Определим, что передача информации в безопасном виде означает, что на пути передачи информации установлены определенные барьеры безопасности. Если на пути передачи информации барьеров между активами не установлено, то будем говорить о простой передаче информации. Мы не конкретизируем вид этих барьеров, так как он зависит от реализации моделируемой системы, однако далее, в § 3, мы приведем примеры архитектуры, обеспечивающей безопасную передачу информации.

Ребра r, w в графе доступа относятся к одному из двух типов: простая передача информации $\mapsto$, безопасная передача информации $\rightharpoonup$.

Запись $a \mapsto b$ означает, что информация от актива a передается активу b простым способом.

Запись $a \rightharpoonup b$ означает, что информация от актива a передается активу b безопасным способом.

Определение 3. Будем называть операции чтения $\left(\frac{r}{\mapsto}\right)$ и записи $\left(\frac{w}{\mapsto}\right)$ антисимметричными, если $a \left(\frac{w/r}{\mapsto}\right) b \not\Rightarrow b \left(\frac{r/w}{\mapsto}\right) a$, иными словами, если операция записи/чтения из a в b не приводит к возможности чтения/записи из b в a.

Определение 4. Назовем передачу информации безопасной, если из отношения $a \rightharpoonup b \not\Rightarrow a \mapsto b$, т. е.

Таблица 2

Сопоставление активов и связей между активами в системе с БТС с компонентами модели (типы активов и отношения)

Актив	Вид связи между активами	Тип актива	Возможные типы отношений в модели
Оператор	Доступ к управлению и информации. Передача управления другому оператору	Субъект	t, g
БТС	Доступ к управлению и информации	Субъект	r
Облачная инфраструктура	Доступ к информации/удаленное управление	Субъект	r, w
Пассивный элемент облачной инфраструктуры (базы данных и пр.)	Доступ к информации	Объект	r, w
GPS	Доступ к информации	Объект	r
Дорожная инфраструктура («умные» светофоры, знаки и др.)	Доступ к информации	Объект	r

передача информации не нарушает целостности актива *b*. ♦

В определении 4 необходимо конкретизировать смысл термина «целостность». Исторически, наиболее часто употребляемое определение целостности в контексте промышленных систем управления приведено в ГОСТ [7]: «Целостность — свойство, гарантирующее, что данные не были изменены, уничтожены или потеряны из-за несанкционированных действий или случайно на протяжении жизненного цикла.» Это определение, аналогично подходу стандарта ИСО [21], сужает проблему ИБ до вопроса целостности данных в информационных системах. Такое допущение оправдано для систем, основные функции которых состоят в хранении и обработке данных. Для систем управления физическими объектами основная функция — это управление собственно объектом. Целесообразно расширить понятие целостности на оборудование и методы. В таком виде этот термин трактуется в ГОСТ [22]: «Свойство защиты корректности и полноты имущественных объектов». В отличие от первого определения [7], такое определение расширяет понятие целостности на материальные средства, в том числе на их защитные механизмы и методы, которые в отличие от самих данных являются внутренними свойствами защищаемой системы, что позволяет собственнику реализовать эффективные меры по сохранению целостности методов. В этом контексте нарушение целостности данных не критично, если оно не приводит к нарушению критических свойств объекта. Например, если система получит неправильные данные от скомпрометированного источника, но в результате не сформируется неверная команда управления и система останется в физически безопасном состоянии, то зачастую можно пренебречь нарушением целостности информации. «Безопасная передача» трактуется как отсутствие нарушений безопасности функционирования объекта.

Примером безопасной передачи может служить замена записи информации активом *a* в актив *b* на операцию чтения активом *b* из актива *a* при условии, что приняты меры, обеспечивающие нарушение симметричности операций *r* и *w* по отношению к требуемому свойству кибербезопасности.

Расширение модели «take-grant» несимметричными отношениями типа «де факто» позволяет описывать случаи безопасной передачи информации при условии приоритета сохранения целостности, например, в реальной системе, принадлежащие, кроме основного «прямого» потока команд между активами на разных уровнях в направлении «сверху вниз», существуют дополнительные «обратные» потоки данных в виде диагностической информации, сигналов квитирования и др.

1.2. Характеристики информационной безопасности

Рассмотрим ИБ системы с БТС как задачу поддержания в заданных пределах значений рисков, связанных с возможным нарушением доступности, целостности или конфиденциальности. Набор характеристик для описания каждого из свойств ИБ может варьироваться в зависимости от свойств анализируемой системы.

В работе [14] предложен набор характеристик активов с учетом их функциональных, информационных, технологических и других свойств. Далее мы ограничимся рассмотрением только информационных свойств активов, т. е. характеристик, отражающих связи актива с другими активами в системе и возможные пути распространения атаки при нарушении конфиденциальности, целостности и доступности информации, ассоциированной с активом.

Определим множество Q_j информационных свойств актива $a_j \in A$ как $Q_j = \{C_j, I_j, T_j\}$, где C_j, I_j и T_j, – множества характеристик конфиденциальности, целостности и доступности. В рамках нашей (упрощенной) модели ИБ далее не рассматриваются свойства, связанные с конфиденциальностью и доступностью, т. е. $Q_j = \{I_j\}$.

Исходя из модели Биба, примем, что более важными в смысле организации защиты считаются активы системы, имеющие доступ к большему числу других активов по отношению *w*. Тогда задача нахождения важных активов во многом аналогична, например, задаче нахождения лидера (наиболее влиятельного лица) в социальных графах (см., например, работу [23]) или применению метрик цикломатической сложности (точек ветвления) для программного обеспечения при оценке его надежности, когда наиболее критичным модулем программы считается модуль с наивысшей цикломатической сложностью [24].

Для системы, описываемой графом безопасности G_0, определим количественную характеристику I_j информационных свойств актива для целостности как степень вершины по исходящим ребрам для транзитивного замыкания графа G_0 по выбранному отношению доступа *w*.

В общем случае, при учете функциональных и иных свойств актива, а также среды передачи информации в характеристике I_j могут учитываться веса активов (вершин графа) и связей между ними (ребер графа).

Однако отметим, что при рассмотрении характеристик конфиденциальности в ИБ можно учесть, что в моделях Биба и Белла — Лападуллы разрешенные потоки информации противоположны друг другу, что позволяет выразить характеристику C_j через характеристику I_j [25, *гл. 5*].

2. ПРИМЕРЫ ОПИСАНИЯ И АНАЛИЗА АРХИТЕКТУРЫ БЕЗОПАСНОСТИ В РАМКАХ ДИСКРЕЦИОННОЙ МОДЕЛИ

Данный параграф носит прикладной характер и демонстрирует читателю применение комплексной модели на практике. Его содержание может быть полезно проектировщикам систем управления с БТС, у которых нет опыта описания систем с помощью дискреционных моделей ИБ.

Приведем два простых примера моделей систем БТС в среде «умного города», где рассматривается проблема синтеза архитектуры кибербезопасности. Первый из них — базовый и демонстрирует особенности трансформации отношений и активов при описании реальной системы дискреционной моделью. Второй пример иллюстрирует применение безопасных связей в процессе разделения системы на информационные зоны.

2.1. Пример модели с разделением доступа при управлении беспилотными транспортными средствами из локальных пунктов управления

Пусть необходимо описать двухуровневую систему удаленного управления БТС с центральным и двумя локальными пунктами управления (ПУ), причем центральный ПУ может при необходимости вмешиваться в работу всех БТС системы, а локальный — только в работу тех БТС, управление которыми ему делегировано.

Покажем, как при моделировании реальных систем с БТС следует учитывать наличие неявных связей между субъектами (см. п. 1.1). Рассмотрим модель с графом безопасности (рис. 1, *а*) с вершинами: *CC* — центральный ПУ, *C*1 и *C*2 — два локальных ПУ, которым центральный ПУ делегировал полномочия (отношения типа «де юре») на управление БТС *AV*1 и *AV*2 соответственно. Отношения, на рисунке относящиеся к разным типам, здесь и далее обозначены разными линиями: *g*, *w* и *r* — штриховыми, пунктирными и сплошными соответственно. В изображенном графе субъекты *C*1, *C*2 и *CC* объединены в единый сегмент (остров) отношениями «де юре» [15], поэтому каждый из локальных ПУ имеет доступ ко всем ресурсам системы. В таком графе безопасности обособленное управление БТС из локальных ПУ осуществляться не может, а значит, что либо модель неверно описывает архитектуру кибербезопасности системы, либо архитектура кибербезопасности (когда локальные пункты управления разделяют полномочия от общего центра) изначально одноуровневая.

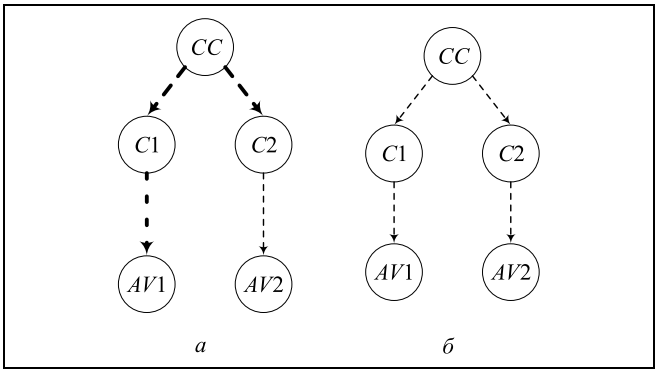

Рис. 1. Граф безопасности для системы управления с двумя БТС *AV*1 и *AV*2: *а* — с общим доступом из локальных пунктов управления *C*1 и *C*2; *б* — с раздельным доступом из локальных пунктов управления и с сохранением управления из общего центра. Полужирным выделен путь, по которому локальный пункт управления *C*2 может получить управление БТС *AV*1

Один из возможных вариантов графа безопасности, моделирующего обособленное управление с общим центром, приведен на рис. 1, *б*. По сравнению с графом безопасности (см. рис. 1, *а*) отношения «де юре» заменены отношениями «де факто». Замена отношений отражает характер управления, при котором полномочия заменяются директивами от центрального ПУ к локальному. Этот простой пример показывает, что прямая трансляция отношений реального мира в модель без учета смысловой составляющей языка модели может привести к созданию систем управления с изначально уязвимой архитектурой безопасности.

2.1. Пример модели системы с обособленным управлением и единым информационным пространством

Рассмотрим систему с БТС, содержащую все активы, указанные в табл. 2, но ограничимся случаем, когда в системе есть только два БТС и минимальное число других активов. Пусть каждое БТС (рис. 2) получает информацию от дорожных сенсоров *RS*, системы позиционирования GPS и облачной структуры, где выделена облачная среда выполнения программ *CL* и база данных *DB*. Внешнее управление БТС осуществляют программы, функционирующие в облачной структуре, или операторы. Мы полагаем, что данный пример может иллюстрировать подход к описанию архитектуры безопасности централизованного/облачного управления БТС на территории «умного предприятия». Каждое из БТС через облачное хранилище получает информацию от другого БТС, операторы имеют равные права на управление каждым из БТС.

Анализ графа безопасности для БТС показывает, что каждое из БТС может не только получать информацию о состоянии другого БТС в системе, но и непосредственно влиять на второе БТС, передавая информацию о дорожной обстановке оператору или в хранилище данных. Представленная архитектура безопасности одноуровневая, где все БТС находятся в одной зоне безопасности. Комп-

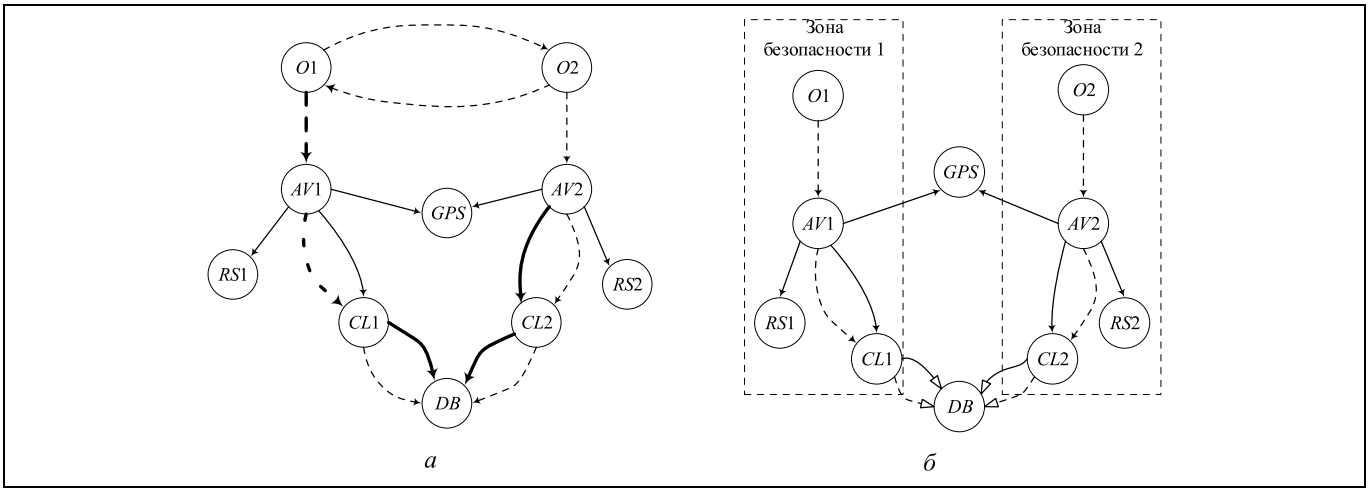

Рис. 2. Граф безопасности системы «умного предприятия»: *а* — с единой зоной по управлению БТС *AV*1 и *AV*2; *б* — с раздельным управлением операторами *O*1 и *O*2 для БТС *AV*1 и *AV*2 и единым информационным пространством. «Безопасные» отношения выделены незакрашенными стрелками. Утолщенными линиями выделены пути передачи информации от *O*1 к *AV*2 в незащищенной системе

рометация любого актива-субъекта (например, потеря целостности в результате записи в него ложной информации) дает потенциальную возможность скомпрометировать все остальные активы. Атака, направленная из одного БТС на другой БТС, может проводиться двумя способами: либо через общее облачное хранилище, либо через оператора, когда БТС представляет для него ложную информацию, по которой оператор принимает ложное решение по управлению другим транспортным средством. Пример возможного пути нарушения целостности в результате посылки команды управления оператором БТС *AV*1 для БТС *AV*2 без согласия второго оператора приведен на рис. 2, *а*. Всего же в данном графе есть более 20 путей нарушения целостности между БТС.

Предположим, что необходимо обеспечить обособленное управление для обоих БТС от своих операторов (аналогично предыдущему примеру), но сохранив у БТС возможность обмениваться информацией (чтением) в режиме единого информационного пространства для всей системы. Для этого есть несколько решений. Так, аналогично предыдущему примеру, можно обеспечить независимость по отношениям «де юре» операторов, а также сделать безопасным доступ к базе данных с применением несимметричных отношений, введенных в п. 1.1.

Один из практических способов реализации несимметричного доступа к базе данных — это изоляция данных с разграничением прав доступа, когда каждому БТС в хранилище доступны только «собственные» данные, а данные других БТС не доступны. Модифицированный таким образом граф безопасности с указанием зон безопасности по отношению *w* приведен на рис. 2, *б*.

3. ПОДХОДЫ К АНАЛИЗУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДИНАМИЧЕСКИХ СИСТЕМАХ НА ПРИМЕРЕ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Рассмотрим проблему анализа ИБ для БТС в структуре «умного города». Среда «умного города», в которой функционирует БТС, постоянно изменяется. Из динамического характера транспортных систем очевидно, что граф безопасности такой системы зависит от времени и сам тоже динамический. В графе меняется как число БТС в системе, так и связи БТС с другими активами, и его можно рассматривать как пример динамической сети [9].

Соответственно, для сохранения референтности модели граф безопасности должен обновляться по любому событию, связанному со значимым изменением реальной системы, а его свойства ИБ должны пересчитываться. Наличие в моделируемой системе множества активов и отношений приводит к построению графа, решение задач ИБ для которого требует большого объема расчетов. Например, как показывает проведенный нами анализ реальных данных системы БТС компании «Waymo» [26], в каждый момент времени на «близком» расстоянии от БТС в «интенсивной» городской среде находится около десятка объектов, а в пределах «видимости» — более сотен. Для уменьшения вычислительной сложности предлагается для конкретного БТС проводить анализ не на общем графе безопасности, а на некотором его индуцированном подграфе, который назовем актуальным графом безопасности для данного БТС. При этом вершины (активы) в общем графе безопасности исключаются из рассмотрения, если они находят-

ся на большом «расстоянии» от актива, для которого проводится анализ.

Пусть $V(G)$ — множество вершин, а $E(G)$ — множество ребер общего графа безопасности G. Для оценки «расстояния» между активами введем характеристику, основанную на физической и информационной «удаленности» вершин графа друг от друга.

Определение 5. Назовём отклонением $d(v_i, v_j) = d_{ij}$ между вершинами v_i и v_j графа $G = \{V, U\}$ характеристику кратчайшего пути, соединяющего вершины по заданному отношению ИБ, рассчитываемую по формуле:

$$d_{ij} = k_1 \sum_{l=1}^{M} w_l^{ij} + k_2 S_{ij},$$

где w_l^{ij} — вес l-го ребра, входящего в кратчайший путь между активами i и j, $w_l^{ij} \sim \tau$, τ — задержка прохождения сигнала между активами (один из способов оценки задержки см. в работе [27]); S_{ij} — длина минимальной физически реализуемой траектории между активами i и j, если оба актива — физические, и ноль — если хотя бы один из активов чисто информационный; k_1, k_2 — размерные нормировочные коэффициенты. ♦

Подчеркнем отличия введенного нами отклонения на графе безопасности от «обычного» геометрического расстояния. Первое отличие связано с информационной составляющей отклонения. При исследовании информационной зависимости допускается наличие петель в графе и полагается, что расстояние между вершинами v_i и v_j равно длине кратчайшего цикла, проходящего через вершину, т. е. в общем случае $d(v_i, v_j) \neq 0$.

Второе отличие связано с тем, что кратчайшая траектория между БТС, находящимися в точках v_1 и v_2, в общем случае не является отрезком прямой (v_1, v_2), так как два БТС могут находиться на изолированных проезжих частях и быть разделены рельефом, зданиями, объектами инфраструктуры и т. п.

Третье отличие состоит в том, что в транспортной системе путь между точками v_1 и v_2 в прямом и обратном направлении также может быть различен: $d(v_i, v_j) \neq d(v_j, v_i)$.

Поэтому только в специальных случаях введенное нами отклонение может обладать теми же свойствами, что и метрика в топологическом смысле этого слова.

Таблица 3

Формулы расчета отклонения в зависимости от цели атаки

Цель атаки	Формула расчета отклонения
Нанесение физического вреда БТС со стороны другого актива	Для БТС i: $d_{ij} = k_2 S_{ij}$, $k_1 = 0$. При этом БТС i в некий момент времени будет находиться в безопасном состоянии по отношению к данной угрозе со стороны актива j, если если $S_{ij} \geq L_i > 0$, где L_i — длина траектории между физическими объектами, при которой БТС i способно осуществить маневр, предотвращающий столкновение. Значение L_i зависит от многих факторов, например, от плотности потока, средней скорости, типа транспортного средства, погоды и пр. Очевидно, что физический актив j, для которого в данный момент времени выполняется данное условие, можно удалить из графа безопасности
Получение конфиденциальной информации о БТС	В данном случае мы имеем дело с чисто информационным воздействием, когда $k_2 = 0$. Пусть - существует W_i — длина информационного пути, при которой возможны гарантированное детектирование кибератаки на актив и изоляция атакующего. Тогда все активы j графа безопасности, для которых $\sum_{l=1}^{M} w_l^{ij} > W_{i,\,ij}$, где l — номер ребра в пути, можно исключить из рассмотрения и построить таким образом актуальный граф безопасности
Срыв задания БТС	Под срывом задания БТС мы имеем в виду недопущение прибытия БТС в конечную точку маршрута. Причиной срыва задания может быть как физической, так и информационная атака (например, передача ложной информации о ситуации на маршруте, ложных координат и т. п.). Возможность проведения такой информационной атаки простыми средствами была недавно продемонстрирована [28]. Пусть существуют L_i — длина пути между физическими объектами, при которой БТС способно осуществить маневр, предотвращающий физическое повреждение, и W_i — длина информационного пути, при которой возможно гарантированное детектирование кибератаки и изоляция атакующего. Тогда в актуальный граф безопасности для рассматриваемой задачи войдут вершины v_i и b_j, удовлетворяющие условиям $\begin{cases} \sum_{l=1}^{M} w_l^{ij} \leq W_i \\ S_{ij} \leq L_i \end{cases}$

Определение 6. Назовем $\mathcal{G}_i^{\Sigma}(t)$ актуальным графом безопасности для БТС i, если $\forall t > 0$ $\mathcal{G}_i^{\Sigma}(t) \subset G_0(t)$, $v_i \subset \mathcal{G}_i^{\Sigma}(t)$, а также:

$$\begin{cases} \forall v_j \subset \mathcal{G}_i^{\Sigma}(t)\colon\ d_{ij} \le D = \text{const}, \\ \forall v_j \not\subset \mathcal{G}_i^{\Sigma}(t)\colon\ d_{ij} > D. \end{cases} \blacklozenge$$

Иными словами, актуальный граф безопасности получается из общего графа безопасности удалением вершин $v_j \subset V$ и инцидентных этим вершинам ребер, для которых отклонение от вершины v_i больше заданного порогового значения, определяемого видом решаемой задачи. Возможные формулы расчета отклонения между активами для отдельных задач приведены в табл. 3.

Итак, мы предлагаем такой подход к анализу ИБ БТС в динамической среде «умного города»:

1) построение графа безопасности системы с БТС с помощью табл. 2;

2) переход от общего графа безопасности к актуальному графу безопасности для конкретного БТС в соответствии с областью и целью анализа ИБ (см. табл. 3);

3) анализ информационной безопасности БТС на актуальном графе с помощью дискреционной модели.

ЗАКЛЮЧЕНИЕ

Рассмотрена проблема оценки информационной и кибербезопасности (ИБ) для беспилотных транспортных средств (БТС). Для решения этой проблемы предложен метод моделирования архитектуры ИБ с применением дискреционных моделей. Основное внимание при моделировании уделено свойству ИБ «целостность», которое имеет более высокую значимость для промышленных систем управления по сравнению с другими свойствами безопасности [7, 20]. Для анализа целостности рассмотрен подход, учитывающий информационные характеристики актива, т. е. его связи с другими активами в системе и возможные пути распространения атаки при нарушении конфиденциальности, целостности и доступности информации, ассоциированной с активом. В качестве количественной характеристики информационных свойств актива для целостности введена степень вершины по исходящим ребрам для результата транзитивного замыкания графа безопасности по отношению доступа по записи.

Рассмотрена проблема уменьшения пространства поиска при анализе путей в графе безопасности путем перехода от «общего» графа безопасности к индуцированному подграфу — «актуальному» графу безопасности. Для построения актуального графа безопасности введена характеристика, основанная на физической и информационной удаленности вершин графа друг от друга. Для некоторых практических случаев предложены формулы расчета этой характеристики.

ЛИТЕРАТУРА

1. *The United* Nations Economic Commission for Europe (UNECE). — URL: http://www.unece.org/trans/theme_its.html
2. *Паспорт* федерального проекта «Общесистемные меры развития дорожного хозяйства». — URL: https://sudact.ru/law/pasport-federalnogo-proekta-obshchesistemnye-mery-razvitiia-dorozhnogo/ [*Passport* of the Federal Project «System-wide Measures for Road Development» (In Russian)]
3. *Коробеев А.И.*, *Чучаев А.И.* Беспилотные транспортные средства: новые вызовы общественной безопасности // Lex Russica. — 2019. — Т. 2. [*Korobeev, A.I., Chuchaev, A.I.* Unmanned Vehicles: New Challenges to Public Safety // Lex Russica. — 2019. — Vol. 2. (In Russian)]
4. *Басан Е.С.*, *Басан А.С.*, *Макаревич О.Б.*, *Бабенко Л.К.* Исследование влияния активных сетевых атак на группу мобильных роботов // Вопросы кибербезопасности. — 2019. — № 1 (29). — С. 35—44. — URL: https://cyberleninka.ru/article/n/issledovanie-vliyaniya-aktivnyh-setevyh-atak-na-gruppu-mobilnyh-robotov [*Basan, E.S., Basan, A.S., Makarevich, O.B., Babenko, L.K.* Studying the Impact of Active Network Attacks on a Mobile Robots Group // Voprosy Kiberbezopasnosti. — 2019. — No. 1 (29). — S. 35—44.]
5. *URL:* https://www.marketsandmarkets.com/Market-Reports/connected-car-market-102580117.html?gclid=EAIaIQobChMIh6mR9e-C5gIVysqyCh0k4QiTEAAYASAAEgIs6_D_BwE
6. *URL:* https://www.leslivresblancs.fr/livre/filieres-specialisees/automobile/vehicules-autonomes-et-connectes
7. *ГОСТ Р* МЭК 62443-1-1—2009. Ч. 1-1. Терминология, концептуальные положения и модели. — М.: Стандартинформ 2013. [*GOST* R IEC 62443-1-1—2009. Part 1-1. Terminology, Conceptual Provisions and Models. — Moscow: Standartinform, 2013. (In Russian)]
8. *Алпеев А.С.* Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. — 2014 — № 5. — С. 39—42. [*Alpeev, A.* Terminology of Isecurity: Cybersecurity, Information Security. — 2014. — No. 5. — P. 39—42. (In Russian)]
9. *Fok*, *E.* An Introduction to Cybersecurity Issues in Modern Transportation Systems // Inst. Transportation Engineers J. — 2013. — Vol. 83, no. 7. — P. 18—21.
10. *Bhattacharjee*, *D.* Unmanned Aerial Vehicles and Counter Terrorism Operations // SSRN Electronic Journal. — 2015. — 10.2139/ssrn.2608969.
11. *Hamida*, *E.B.*, *Noura*, *H.*, *Znaidi*, *W.* Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures // Electronics. — 2015. — Vol. 4. — P. 380—423, doi: 10.3390/electronics4030380
12. *Security* Cyber Security and Resilience of Intelligent Public Transport Good practices and recommendations. — ENISA (European Union Agency for Network and Information Security), December 2015.
13. *Hong*, *J.* Cyber Security Issues in Connected Vehicle of Intelligent Transport System // Indian Journal of Science and Technology. — June 2016. — Vol. 9 (24), doi: 10.17485/ijst/2016/v9i24/96027
14. *Промыслов В.Г.*, *Семенков К.В.*, *Шумов А.С.* // Синтез архитектуры кибербезопасности для систем управления атомных электростанций. — Проблемы управления. — 2019. — № 3. — С. 61—71. [*Promyslov, V.G, Semenkov, K.V., Shumov, A.S.* Security Model for Instrumentation and Control Systems for Nuclear Power Plants // Control Sciences. — 2019. — No. 3. — P. 61—71. (In Russian)]

15. *Bishop*, *M.* Computer Security: Art and Science. — Boston: Addison Wesley, 2003. — 1136 p.
16. *Denning*, *E.* A Lattice Model of Secure Information Flow // Communications of the ACM. — 1976. — Vol. 19, iss. 5. — P. 236—243.
17. *Lockman*, *A.*, *Minsky*, *N.* Unidirectional Transport of Rights and Take-Grant Control // IEEE Trans. on Software Engineering. — November 1982. — Vol. 8, no. 6. — P. 597—604, doi: 10.1109/TSE.1982.236020
18. *Biba*, *K.J.* Integrity Considerations for Secure Computer Systems / MTR-3153, The Mitre Corporation, April 1977.
19. *Bell*, *D.E.*, *La Padula*, *L.J.* Secure Computer System: Mathematical Foundations // MITRE Technical Report MTR-2547, vol. 1. — MITRE Corporation, Bedford, Mass, 1973.
20. *Бабаев Д.И.*, *Полетыкин А.Г.*, *Промыслов В.Г.*, *Тимофеев М.Ю.* Управление архитектурой кибербезопасности АСУТП АЭС // Проблемы управления. — 2018. — № 3. — С. 47—55. [*Babaev, D.I., Poletikin, A.G., Promyslov, V.G., Timofeev, M.Yu.* Managing the Cybersecurity Architecture of Automated Process Control Systems of Nuclear Power Plants // Control sciences. — 2018. — No. 3. — P. 47—55. (In Russian)]
21. *ISO/IEC* 27000. Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary. — 2018.
22. *ГОСТ Р* МЭК 62443-3-3. Сети промышленной коммуникации. Безопасность сетей и систем. Ч. 3-3. Требования к системной безопасности и уровни безопасности. — 2016. [*GOST* R IEC 62443-3-3. Industrial Communication Networks. Security of Networks and Systems. Part 3-3. System Security Requirements and Security Levels. — 2016. (In Russian)]
23. *Newman*, *M.E.J.* The Structure and Formation of Complex Networks // SIAM Review. — 2003. — Vol. 45, no. 2. — P. 167—256.
24. *Антонов А.В.*, *Жарко Е.Ф.*, *Промыслов В.Г.* Проблемы оценки надежности и качества программного обеспечения в автоматизированных системах управления технологическими процессами // Надежность. — 2015. — № 4 (55). — С. 82—96. [*Antonov, A.V., Zharko, E.F., Promyslov, V.G.* Problems of Evaluation of Software Dependability and Quality in Industrial Automation and Control Systems // Reliability. — 2015. — No. 4 (55). — P. 92—96.
25. *Jaeger*, *T.* Operating System Security (Synthesis Lectures on Information Security, Privacy, and Trust). — Morgan and Claypool Publishers, 2008. — 218 p.
26. *URL:* https://waymo.com/open/data/
27. *Байбулатов А.А.*, *Промыслов В.Г.* Аппроксимация огибающей в приложениях «Network calculus» // Проблемы управления. — 2016. — № 6. — С. 59—64. [*Baybulatov, A.A., Promyslov, V.G.* The Approximation of Envelope in «Network Calculus» Applications // Control Sciences. — 2016. — No. 6. — P. 59—64. (In Russian)]
28. *Hern*, *A.* Berlin Artist Uses 99 Phones to Trick Google into Traffic Jam Alert // The Guardian, 03 Feb 2020. — URL: https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert

Статья представлена к публикации членом редколлегии В.В. Кульбой.

Поступила в редакцию 22.01.2020, после доработки 17.02.2020. Принята к публикации 23.03.2020.

Промыслов Виталий Георгиевич — канд. физ.-мат. наук, ✉ v1925@mail.ru,

Семенков Кирилл Валерьевич — канд. физ.-мат. наук, ✉ semenkovk@mail.ru,

Жарко Елена Филипповна — канд. тех. наук, ✉ zharko@ipu.ru,

Институт проблем управления им. В.А. Трапезникова РАН, г. Москва.

SECURITY THREAT ASSESSMENT METHODS FOR UNMANNED VEHICLES IN A SMART CITY

V.G. Promyslov[1], K.V. Semenkov[2], E.Ph. Jharko[3]

V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

[1]✉ v1925@mail.ru, [2]✉ semenkovk@mail.ru, [3]✉ zharko@ipu.ru

Abstract. This paper presents a comprehensive cybersecurity model for autonomous vehicles (AV) system in framework of the smart city. We consider a problem of information flow description for a real AV system in the frame of discretional security models. The definition of safe data transfer for some types of information exchange between the system assets is presented. Some techniques for asset classification in frame of Biba and Bell-LaPadula models taking into account information links between the assets are introduced. We discuss the complexity and ambiguousness of the «integrity» definitions in relation to cybersecurity provision and emphasize the significance of its extension to the equipment and data processing methods. This approach is considered to shift the focus to the system analysis and system vulnerability removal and to develop the protection upon the system internal properties. Dynamical methods of cybersecurity architecture synthesis for transport systems with AVs are considered. The methods are shown to lessen computational complexity of system modelling. Instead of analyzing the complete security graph, one may analyze an induced subgraph for a given AV. The vertices (assets) of full security graph are excluded from the consideration if they are at a great «distance» from the analyzed AV. Formulae for the distance calculation are provided for some cases. Some examples of cybersecurity architecture analysis and synthesis for autonomous vehicles are presented.

Keywords: cybersecurity, autonomous vehicles, smart city, security architecture, classification, clustering, security graph, take-grant model.

Funding. The study (Sections 3 and 4) was performed with partial financial support of Russian Foundation of Basic Research, project no. 19-29-06044.