УДК 004.5

Модель классификации уязвимостей интерфейсов транспортной инфраструктуры «умного города»

Израилов К. Е., Левшун Д. С., Чечулин А. А.

Постановка задачи: *внедрение концепции «умного города» помимо очевидных достоинств несет в себе и ряд существенным недостатков, одними из которых считаются угрозы информационной безопасности, являющиеся в том числе следствием наличия уязвимостей в программно-аппаратных модулях, реализующих данную концепцию. Ситуация становится критичной для таких инфраструктур, как транспортная, нарушение функционирования которых потенциально ведет к человеческим жертвам. Существующие исследования посвящены в основном безопасности модулей, обеспечивающих функционирование подсистем «умного города», вместе с тем безопасность интерфейсов, поддерживающих взаимодействие модулей, оставлено практически без внимания. Таким образом, требуется более глубокое исследование уязвимостей интерфейсов транспортной инфраструктуры «умного города» с целью их последующего поиска и нейтрализации.* ***Целью работы*** *является систематизация уязвимостей интерфейсов транспортной инфраструктуры «умного города» в виде обобщающей модели классификации. Предлагается разделять уязвимости исходя из классов интерфейсов, к которым они относятся; интерфейсы же делятся на подклассы согласно используемым их компонентам транспортной инфраструктуры, а также смысловой ориентированности взаимодействий.* ***Используемые методы****: Для получения подклассов интерфейсов «умного города» использовался аппарат категориального деления: для элементов транспортной инфраструктуры применялись пары – человек vs автомат, экспертный vs интеллектуальный и статика vs динамика; а для взаимодействий – человекоориентированность vs машиноориентированность. Для формализации взаимосвязей между транспортной инфраструктурой «умного города» и уязвимостями ее интерфейсов применялся аппарат категориального деления.* ***Новизна:*** *элементом новизны представленного решения является учет в модели классификации требования «необходимости и достаточности», заключающегося в том, что любая, даже гипотетическая уязвимость гарантированно будет отнесена к одному и только к одному классу. Также в представленную модель заложена вариативность классификации путем возможности ее расширения и детализации за счет добавления новых пар категориального деления.* ***Результат****: Выделение различных элементов транспортной инфраструктуры «умного города», а также вариантов взаимодействий между ними позволило перейти к классификации соответствующих интерфейсов, обеспечивающих такие взаимодействия, и, как следствие, к классификации уязвимостей последних. Применение аппарата категориального деления обосновывает корректность полученной классификации.* ***Практическая значимость****: представленное решение предлагается реализовать в виде программного прототипа. Также на базе модели классификации и прототипа планируется разработка непосредственного метода поиска уязвимостей в транспортной инфраструктуре «умного города».*

Ключевые слова: *умный город, транспортная инфраструктура, уязвимость, классификация, модель, поиск уязвимостей.*

Библиографическая ссылка на статью:
Израилов К. Е., Левшун Д. С., Чечулин А. А. Модель классификации уязвимостей интерфейсов транспортной инфраструктуры «умного города» // Системы управления, связи и безопасности. 2021. № 5. С. 199-223. DOI: 10.24412/2410-9916-2021-5-199-223

Reference for citation:
Izrailov K. E., Levshun D. S., Chechulin A. A. Vulnerability classification model for Smart City transport infrastructure interfaces. *Systems of Control, Communication and Security*, 2021, no. 5, pp. 199-223 (in Russian). DOI: 10.24412/2410-9916-2021-5-199-223

Введение

Важнейшим показателем развития современного общества можно считать его практически полный переход на информационные технологии, что безусловно является существенным достижением человеческой мысли, повысившим, как следствие, качества жизни людей [1]. Тем не менее, одной из возникающих при этом проблем считается появление в создаваемых технологиях и реализующих их устройствах таких сущностей, как уязвимости, приводящим к нарушениям информационной безопасности. Как следствие, в ряде случаев это является причиной не только экономических ущербов или политических поражений, но даже и человеческих жертв. Последнее особо актуально для областей, непосредственно связанных с жизнедеятельностью людей, одной из которых считается транспортная инфраструктура «умного города» (ТИУГ). Необходимо особо отметить, что ТИУГ является не просто объектом критической информационной инфраструктуры [2], но и имеет стратегическое значение для безопасности государства, особенно при нарастании военной угрозы. Это обусловлено тем, что подходы, применяемые в рамках ТИУГ, могут быть успешно использованы для создания интеллектуальной системы тылового обеспечения в масштабах вооруженных сил и всей страны, в том числе, в условиях военного времени. И если устройства, обеспечивающие функционирование основных подсистем можно считать стандартными и достаточно хорошо изученными с позиции безопасности (так, например, существуют обширные базы данных уязвимостей операционных систем, телекоммуникационного оборудования, сетевых протоколов и пр.), то такое узкое место, как интерфейсы взаимодействия между элементами системы на данный момент оставлены практически без внимания [3-5], при том, что они могут оказаться «объектами ударов» сил информационных операций (кибервойск) недружественных стран. При этом под интерфейсами понимается не абстрактная сущность, означающая разделение двух сред, а реальная часть инфраструктуры ТИУГ, обеспечивающая физический обмен данными между двумя элементами; так, например, взаимодействие пассажира с беспилотным транспортным средством будет осуществляться через средства коммуникации (микрофон, динамик, клавиатура и т.п.). Как следствие, отсутствует достаточное количество информации и об уязвимостях таких интерфейсов, что ставит под вопрос как безопасность уже существующих интерфейсных средств, так и не позволяет уделять должного внимания этому в еще только разрабатываемых. Таким образом, задача поиска уязвимостей интерфейсов, применимого для ТИУГ, является особенно актуальной. Первым шагом на пути ее решения может стать анализ предметной области и создание модели классификации уязвимостей интерфейсов [6, 7], чему и посвящено текущее исследование. В особенностях такой модели необходимо указать то, что она подходит не только для поиска уже известных уязвимостей (т.е. существующих на практике), но и позволяет прогнозировать еще не обнаруженные (предполагаемые в теории).

1. Обозначения

Для формализации решения задачи поиска и классификации уязвимостей интерфейсов ТИУГ введены обозначения, представленные в табл. 1.

Таблица 1 – Используемые обозначения

Символ	Физический смысл
M	множество компонент, составляющих ТИУГ
m_i	i-й компонент ТИУГ
$\leftrightarrow$	взаимно однозначное соответствие двух элементов друг другу
C_i^M	i-й класс для множества компонентов ТИУГ; может быть одним из $\{К_{ЧЭС}, К_{ЧЭД}, К_{ЧИС}, К_{ЧИД}, К_{АЭС}, К_{АЭД}, К_{АИС}, К_{АИД}\}$
T	множество взаимодействий между компонентами ТИУГ
$\langle m_i \vert m_j \rangle$	взаимодействие между i-м и j-м компонентами ТИУГ
C_k^T	k-й класс для множества взаимодействий компонентов ТИУГ; может быть одним из набора 64 элементов
G	множество групп компонентов
g_i	i-я группа компонентов; может быть одной из набора следующих групп компонентов: g_I (интеллектуальных), g_U (пользовательских), g_P (прогностических), g_O (устаревших)
TO	множество взаимодействий со смысловой ориентированностью между компонентами ТИУГ
$\langle m_i \vert m_j \rangle_o$	взаимодействие с o-й смысловой ориентированностью между i-м и j-м компонентами ТИУГ; ориентированность может быть одной из $\{О_Ч, О_М\}$
C_k^{TO}	k-й класс для множества взаимодействий со смысловой ориентированностью компонентов ТИУГ; может быть одним из набора 128 элементов
F	множество интерфейсов, обеспечивающих взаимодействие со смысловой ориентированностью компонентов ТИУГ
f_i	i-й интерфейс, обеспечивающий взаимодействие ТИУГ; может быть одним из набора 128 элементов
C_k^F	k-й класс для множества интерфейсов взаимодействия со смысловой ориентированностью между компонентами ТИУГ; может быть одним из набора 128 элементов
$\rightarrow$	соответствие одного элемента другому
V	множество уязвимостей всех интерфейсов ТИУГ
v_i	i-я уязвимость интерфейса ТИУГ
B	множество модулей, реализующих все интерфейсы ТИУГ
b_i	i-й модуль, реализующий интерфейсы ТИУГ
$\{v_l\}_m$	m-е подмножество l-х уязвимостей модулей, реализующий интерфейсы ТИУГ
$\{b_m\}_n$	n-е подмножество m-х модулей, реализующих интерфейсы ТИУГ
$\{\{v_l\}_m\}_n$	m-е подмножество l-х уязвимостей, содержащихся в n-м подмножестве модулей, реализующий интерфейсы ТИУГ
y_{max}	общее число классов уязвимостей; должно быть не более 128
$\{v_x\}_y$	y-е подмножество x-х уязвимостей, содержащихся в модулях, реализующий интерфейсы ТИУГ; может быть одним из набора, не превышающего 128 элементов

Символ	Физический смысл
C_y^V	*y*-й класс уязвимостей интерфейсов; может быть одним из набора, не превышающего 128 элементов
P	множество признаков интерфейса ТИУГ, для которого производится поиск уязвимостей
p_i	*i*-й признак интерфейса ТИУГ
$\{v_z\}'$	множество искомых уязвимостей для заданного интерфейса ТИУГ
$D()$	операция поиска уязвимостей по модели классификации уязвимостей ТИУГ и признакам интерфейса

2. Обзор работ в предметной области исследования

Произведем обзор научных работ, посвященных различным способам и моделям классификации интерфейсов сложных информационных систем и их уязвимостей в аспекте применения к текущей задаче исследования.

В работе [8] пользовательские интерфейсы разделяют на программные, аппаратные и смешанные. При этом программные интерфейсы могут быть классифицированы по их целевому назначению человека в человеко-машинном взаимодействии, по виду средства взаимодействия, по продолжительности работы человека с интерфейсом, а также по количеству технических средств, с которыми взаимодействует человек. Аппаратные же интерфейсы с позиции влияния на органы чувств оператора относятся к визуальным, звуковым и тактильным классам.

Автор в [9] предлагает деление интерфейсов по способу взаимодействия с пользователем на следующие классы: текстовые, графические, тактильные, жестовые, голосовые, материальные и сенситивные интерфейсы.

В исследовании [7] приводится классификация интерфейсов ТИУГ на основе взаимодействия выделенной триады элементов: инфраструктуры, беспилотных транспортных средств и окружения. Всего авторы выделяют 9 классов интерфейсов на основе взаимодействия этих элементов.

Классификация интерфейсов оператора по способу представления и принципу отбора информации приведена в [10]. Согласно первому, выделяют приборные, схематические, экологические, функциональные и иммерсивные интерфейсы; а второму – системные, обзорные и задачные интерфейсы.

Авторы в [11] предлагают классифицировать интерфейсы на основе особенностей языка задания его синтаксиса (декларативные, объектно-ориентированные, языки событий и т.д.), задействованных средств визуализации, предоставляемых средств взаимодействия с объектами интерфейса, а также по решаемой интерфейсом задаче.

В работе авторами [12] описана классификация интерфейсов, применяемых в индустриальном интернете вещей, с целью анализа их предрасположенности к кибератакам. Классификация приводится в соответствии с компонентами систем, при этом систему разделяют на следующие элементы: производственное оборудование; датчики и исполнительные механизмы; контроллеры и распределенные системы управления; производственные операционные системы; а также сторонние услуги.

В статье [13] предлагается классифицировать интерфейсы следующим образом: по способу реализации, использованию среды передачи, диапазону частот, типу связи и способу представления информации.

Исследование [14] разделяет интерфейсы на естественные и опосредованные. Так, естественные интерфейсы бывают простыми (голосовой, жестовый) и комплексными (материальный, социальный, невидимый, диалоговый). В качестве же примера опосредованных приводятся такие устройства, как мышь, клавиатура и консоль.

Статья [15] посвящена классификации интерфейсов многокомпонентной системы на основе алгебраического подхода. При этом их систематизация и классификация основана на операциях вложения, сопряжения и фильтрации.

Автор работы [16] производит классификацию интерфейсов по структуре связей, способу подключения и передачи данных, принципу управления и синхронизации. Также выделены внутримашинный, внешний и пользовательский интерфейсы. В свою очередь, пользовательский интерфейс разделен на командный, WIMP (window, image, menu, pointer) и SILK (speech, image, language, knowledge).

В исследовании [17] приводится классификация нейрокомпьютерных интерфейсов по разнообразию входных сигналов, стратегии использования, модальности стимулирующего воздействия, сигнатуре сигнала мозга, способу взаимодействия и режиму работы.

Исследование [18], проведенное целым коллективом авторов, производит классификацию внешних человеко-машинных интерфейсов автоматизированных транспортных средств на основе сложности реализации, процесса работы с участниками дорожного движения, дальности, диапазона и способа связи, возможных состояний, характера передаваемых данных, способа связи, а также типа транспортного средства.

В статье [19] представлена классификация нейрокомпьютерных интерфейсов по следующим критериям: степень инвазивности, тип, число и расположение электродов, скорость передачи данных, тип выходных данных, тип батареи и ценовой сегмент.

Результаты сделанного обзора позволяют сделать следующие выводы. Во-первых, задача единой классификации интерфейсов сложных информационных систем все также остается не до конца решенной. Во-вторых, при классификации интерфейсов аспекты информационной безопасности, как правило, не учитываются. И, в-третьих, хотя и существуют отдельные работы, учитывающие специфику ТИУГ, предлагаемые в них классификации имеют существенные недостатки, что не позволяет говорить о завершенности исследований. Таким образом, несмотря на достаточное количество исследований в области классификации интерфейсов и уязвимостей, все они имеют применение для решения частных задач и плохо применимы для масштабных и разнородных подсистем, входящих в состав «умного города» (УГ); в частности, для его транспортной инфраструктуры. При этом, уязвимости именно интерфейсов взаимодействия компонентов подсистем изучены недостаточно. Как следствие,

требуется разработка собственной модели (далее – модель), подходящей для решения поставленной задачи.

3. Модель классификации

Произведем анализ предметной области и построение соответствующей модели, в терминах которой в дальнейшем можно будет задать метод поиска уязвимостей в ТИУГ.

Исходя из того, что какая-то единая классификация уязвимостей интерфейсов отсутствует, целесообразно предложить собственную, основанную на следующем принципе.

Во-первых, поскольку каждый интерфейс является частью ТИУГ, обеспечивающей информационный обмен, то уязвимости интерфейса представляют собой некоторую слабость, приводящую к нарушениям такого обмена. Следовательно, уязвимость неразрывно связана с программно-аппаратным средством, реализующим интерфейс, и значит классификацию уязвимостей можно сопоставить с классификацией интерфейсов.

Во-вторых, транспортная инфраструктура имеет определенные цели (обусловленные общей концепцией УГ), и, следовательно, ее интерфейсы решают некоторые специализированные задачи по обмену информацией между заранее известными компонентами инфраструктуры. Таким образом, возможно произвести классификацию интерфейсов на основании связанных с ними компонентов ТИУГ. Как следствие, классификация интерфейсов отразится и на классификации их уязвимостей.

В-третьих, взаимодействие может гипотетически (т.к. не только в настоящий момент, но и в будущем) происходить между любой парой компонентов (получая тем самым топологию полносвязного графа), что приводит к существованию такого же количества интерфейсов и их классов.

В-четвертых, особенности информационного обмена связаны не только с конечными компонентами, но и с назначением передаваемых данных, что добавит еще один «подуровень» классификации.

И, в-пятых, поскольку реализация интерфейсов представляет собой некоторые относительно стандартные программно-аппаратные решения (устройства пользовательского ввода/вывода, детектирования окружающей обстановки, сетевого обмена с инфраструктурой и т.п.), сами обладающие уже известными уязвимостями, то с каждым классом интерфейса может быть сопоставлена некоторая группа уязвимостей.

Суммируя вышесказанное, идея модели состоит из классов уязвимостей, тождественных классам содержащих их интерфейсов, которые определяются по связываемым ими классами компонентов ТИУГ и назначению передаваемых данных. Каждый же такой класс (уязвимости или интерфейса) содержит определенное и заранее известное множество уязвимостей; например, в российских базах ФСТЭК России или международных NVD (National Vulnerability Database), CVE (Common Vulnerabilities and Exposures) и пр.

Прогностические особенности предложенной модели заключаются в том, что еще только при проектировании некоторого интерфейса можно будет опре-

делить его класс и предсказать возможные актуальные уязвимости, предотвращение которых будет произведено на ранних стадиях – при создании концептуальной модели устройства или его архитектуры.

Опишем далее более подробно основные элементы модели, созданную с учетом указанных выше принципов.

3.1. Классы компонентов

Одной из основных проблем любой классификации является ее несоответствие требованиям, названным авторами, как «условия необходимости и достаточности деления». Суть первой части заключается в том, что любой элемент должен быть отнесен не более чем к одному классу, а второй – что для любого элемента существует хотя бы один класс. Таким образом, одновременное выполнение условий позволит однозначно проклассифицировать все элементы.

Достаточно работоспособным подходом, многократно доказавшим свою состоятельность [20, 21], является применение категориального деления путем выделения пар категорий, являющихся с некоторой позиции (философской) антагонистами, с последующим их комбинированием. Как результат, все множество элементов будет «разнесено» по разные стороны от условного начала отсчета N-мерного пространства признаков элементов.

Выделим далее категориальные пары, используя ключевые особенности ТИУГ, что позволит поделить последнего на множество равноценных классов компонентов. При этом, помимо указанных требований, на удачность классификации будут влиять мощности каждого из классов. Так, чем ближе количество элементов в классах, тем более равномерно произведено деление и, следовательно, полученная классификация более результативна. И, наоборот, если в одном из классов количество элементов аномально низкое, то, следовательно, некоторая категориальная пара выбрана неудачно, что снижает результативность классификации. Например, деление ТИУГ по паре Внешняя *vs* Внутренняя сторона по отношению к концепции УГ бессмысленно, поскольку абсолютно все элементы транспортной инфраструктуры будут относится к Внутренней стороне, т.к. являются образующей частью концепции.

Именно исходя из приведенных выше размышлений, последующий выбор пар категорий должен быть основан на ключевых особенностях ТИУГ, обладающих внутренним взаимодействием и противоборством. Каждая же пара категорий будет разделять компоненты на 2 качественно разных подмножества. Таким образом, категория в данном случае тождественна одному из классов в бинарной классификации.

Во-первых, поскольку основной концепцией УГ [22–24] является предоставление услуг [25] пользователям со стороны автоматизированных подсистем [26], то 1-я пара классификатора компонентов ТИУГ будет состоять из следующих категорий-антагонистов:

1) категория «человек» ($КП_ч$), соответствующая подмножеству человеческих компонентов, обладающих сознанием и умеющих ставить цель для ее решения (например, пассажир или водитель);

2) категория «автомат» ($КП_А$), соответствующая подмножеству автоматических компонентов, не обладающих сознанием и не умеющих ставить цель (примером автомата является дорожный знак или пункт оплаты).

Таким образом, все компоненты ТИУГ могут быть проклассифицированы на те, функционирование в которых основано на людях или автоматах.

Во-вторых, внедрение искусственного интеллекта [27–29] в функционирование УГ означает то, что часть алгоритмов «стремится» заменять человека и его творческие решения; тогда 2-я пара классификатора компонентов ТИУГ будет состоять из следующих категорий-антагонистов:

1) категория «эксперт» ($КП_Э$), соответствующая подмножеству экспертных компонентов, функционирующих по заданным правилам (например, пассажир, переезжающий из точки А в точку Б, или служба помощи терминалов);
2) категория «интеллект» ($КП_И$), соответствующая подмножеству интеллектуальных компонентов, обучающихся и создающих правила (например, менеджер по перевозке грузов посредством услуг ТИУГ или интеллектуальная система предупреждения об аварии на дороге).

Таким образом, все компоненты ТИУГ могут быть проклассифицированы на экспертные и интеллектуальные.

И, в-третьих, сама суть транспортной инфраструктуры [30-32] означает наличие в УГ подвижных механизмов, предоставляющих услуги транспортировки (как людей, так и грузов), что дает 3-ю пару классификатора компонентов ТИУГ в виде следующих категорий-антагонистов:

1) категория «статика» ($КП_С$), соответствующая подмножеству статических компонентов, неподвижных в инфраструктуре (например, оператор пункта оплаты, шлагбаум);
2) категория «динамика» ($КП_Д$), соответствующая подмножеству динамических компонентов, движущихся в инфраструктуре (например, пассажир или беспилотное транспортное средство).

Таким образом, все компоненты ТИУГ могут быть проклассифицированы на статические и динамические.

Каждое категориальное деление представляет собой классификацию всех компонентов ТИУГ на 2 класса по качественно разным признакам. Применение же сразу всех 3 указанных делений на категориальные пары позволит выделить 8 классов для компонентов ТИУГ. Каждый из таких классов будет определяться комбинацией одного из элементов каждой категориальной пары. Приведем интерпретацию каждого класса (с примером), обозначив их с помощью символа «*К*» и нижнего индекса в виде последовательности первых букв образующих их категорий:

1) $К_{ЧЭС}$ – неподвижные люди, работающие по определенным правилам (например, персонал технического обслуживания);

2) $К_{ЧЭД}$ – перемещающиеся люди, работающие по определенным правилам (например, «штурманы» беспилотного транспорта, которые не управляют движением, а лишь контролируют корректность и безопасность процесса);
3) $К_{ЧИС}$ – неподвижные люди, использующие интеллектуальные правила поведения (например, непосредственно служба поддержки пассажиров или ситуационный центр);
4) $К_{ЧИД}$ – перемещающиеся люди, использующие интеллектуальные правила поведения (например, непосредственно пассажир транспортного средства);
5) $К_{АЭС}$ – неподвижные автоматические механизмы, работающие по заложенным человеком правилам (например, электронный знак ограничения скорости движения);
6) $К_{АЭД}$ – перемещающиеся автоматические механизмы, работающие по заложенным человеком правилам (например, управляемый водителем транспорт);
7) $К_{АИС}$ – неподвижные автоматические механизмы, работающие по интеллектуальным правилам (например, светофор, регулирующий движение, исходя из текущей загруженности дорог);
8) $К_{АИД}$ – перемещающиеся автоматические механизмы, работающие по интеллектуальным правилам (например, беспилотный транспорт).

В приведенной интерпретации класс компонентов для категории «человек» по уровню творчества делится на две составляющие:

- экспертная – означающая выполнение действий, не требующих творческой деятельности (т.е. некоторая замена автомата по причине невозможности функционирования последних в окружающих условиях);
- интеллектуальная – в результате которой требуется синтез определенных задач или их решений.

Таким образом, приведенная интерпретация может считаться вполне обоснованной. Также часть интерпретации, как «неподвижные люди» означает живых субъектов, которые перемещаются в рамках своей группы, а сама группа при этом остается топологически неподвижной.

В формализованном виде деление ТИУГ на компоненты (m_i из множества M) и их классы (C_i^M из состава 8, выделенные ранее) может быть записано следующим образом:

$$\begin{cases} M = \bigcup\limits_{i=1..8} m_i; \\ \forall i = 1..8 \mid m_i \leftrightarrow C_i^M; \\ \forall i = 1..8 \mid \left\{C_i^M\right\} \equiv \left\{К_{ЧЭС}, К_{ЧЭД}, К_{ЧИС}, К_{ЧИД}, К_{АЭС}, К_{АЭД}, К_{АИС}, К_{АИД}\right\}. \end{cases}$$

Таким образом, с каждым компонентом m_i связан свой класс C_i^M и наоборот.

Важной особенностью данных классов является различность их целеориентированности, поскольку пары категорий выбирались исходя из особенностей, отражающих ТИУГ. Как следствие, между всеми классами компонентов возможны различные взаимодействия (в рамках решаемой задачи – информационные взаимодействия), имеющие определенные направления передачи данных. При этом возможны взаимодействия компонентов каждого класса с компонентами того же класса, поскольку входящие в его состав задачеориентированные модули (в отличие от целеориентированности всего компонента) могут передавать данные друг другу.

Эти 8 полносвязных классов компонентов образуют $8 \times 8 = 64$ вариантов взаимодействия между классами (упорядоченные пары $\langle m_i | m_j \rangle$ из множества T), связанных с соответствующими классами (C_k^T из набора 64 классов), что может быть записано в формализованном виде следующим образом:

$$\begin{cases} T = \bigcup\limits_{\substack{i=1..8 \\ j=1..8}} \langle m_i | m_j \rangle; \\ \forall i = 1..8,\ j = 1..8, k = 1..64 \mid \langle m_i | m_j \rangle \leftrightarrow C_k^T. \end{cases}$$

Таким образом, с каждым взаимодействием между двумя компонентами $\langle m_i | m_j \rangle$ связан свой класс C_k^T и наоборот.

3.2. Группы компонентов

Поскольку новой тенденцией в информационных системах является наделение их способностями, заменяющими творческую деятельность человека, то целесообразно отдельно отметить те компоненты ТИУГ, которые имеют непосредственное отношение к искусственному интеллекту – группа g_I (от англ. intellectual group, перев. на рус. интеллектуальная группа). Экспертный анализ позволяет выделить следующие подгруппы согласно их функциональному назначению:

1) компоненты, реализующие работу искусственного интеллекта ТИУГ:
   - $К_{АИС}$ (например, средство управления сетью светофоров, исходя из общей загрузки дорог);
   - $К_{АИД}$ (например, средство контроля за состоянием водителя в транспортном средстве);
2) компоненты, поддерживающие работу искусственного интеллекта ТИУГ:
   - $К_{ЧИС}$ (например, разработчик и отладчик моделей машинного обучения).

Также среди компонентов можно выделить группу g_U (от англ. user group, перев. на рус. пользовательская группа), которая содержит потребительскую составляющую всех услуг ТИУГ:

- $К_{ЧИД}$ (например, водитель управляемого транспортного средства);

– $К_{АЭД}$ (например, груз, перевозка которого осуществляется посредством сервисов ТИУГ).

Достаточно интересным компонентом можно считать $К_{ЧЭД}$, поскольку на первый взгляд в современном мире отсутствуют какие-либо близкие его аналоги. По сути, компонент соответствует людям, которые передвигаются (при помощи автоматизированных средств или самостоятельно) по ТИУГ, при этом не совершая какие-либо творческие действия, а действуя в рамках строго заданных правил. Наиболее близким аналогом этого компонента (что и было указано в примере ранее) может быть контроль за работой автоматических передвижных механизмов (как интеллектуальных, так и использующих отлаженные правила) [33-34]. Причиной же появления данного компонента является пока еще недостаточное понимание, прогнозирование и отладка инновационно новой концепции УГ. Исходя из этого, данный компонент можно отнести к прогностической группе g_P (от англ. prognostic group, перев. на рус. прогностическая группа).

Схематично, все выделенные ранее компоненты ТИУГ отображены на рис. 1 (серым фоном отмечены элементы образующих категориальных пар, синим – интеллектуальная группа компонентов, зеленым – потребительская группа, желтая – прогностическая группа).

	КПЭ		КПИ	
	КПС	КПД	КПС	КПД
КПЧ	КЧЭС	КЧЭД	КЧИС	КЧИД
КПА	КАЭС	КАЭД	КАИС	КАИД

Рис. 1. Графическое отображение категориального деления транспортной инфраструктуры УГ на компоненты (с группировкой)

Компоненты, не отнесенных ни к одной группе – $К_{ЧЭС}$ и $К_{АЭС}$ (представлены на рис. 1 как элементы с белым фоном), соответствуют неподвижным людям и механизмам, работающим по заданным правилам, что, по сути, относит их в некотором роде к устаревающим внутренним функциям ТИУГ, а в перспективе – постепенно заменяемым на полностью динамические интеллектуальные сущности (например, на полностью самовосстанавливающийся и самообучающийся беспилотный транспорт с роевым интеллектом). Таким образом, для компонентов можно ввести отдельную группу – g_O (от англ. obsoleted group, перев. на рус. устаревшая группа).

Группы компонентов имеют следующую формализованную запись:

$$\begin{cases} G = \bigcup\limits_{i\in\{I,U,P,O\}} \mathrm{g_i}; \\ \left\{C_i^M\right\} \equiv \left\{\mathrm{К_{ЧИС}},\ \mathrm{К_{АИС}},\ \mathrm{К_{АИД}}\right\}, m_i \to C_i^M \ | m_i \in \mathrm{g_I}; \\ \left\{C_i^M\right\} \equiv \left\{\mathrm{К_{ЧИД}},\ \mathrm{К_{АЭД}}\right\}, m_i \to C_i^M \ | m_i \in \mathrm{g_U}; \\ \left\{C_i^M\right\} \equiv \left\{\mathrm{К_{ЧЭД}}\right\}, m_i \to C_i^M \ | m_i \in \mathrm{g_P}; \\ \left\{C_i^M\right\} \equiv \left\{\mathrm{К_{ЧЭС}}, \mathrm{К_{АЭС}}\right\}, m_i \to C_i^M \ | m_i \in \mathrm{g_O}. \end{cases}$$

Таким образом, каждым компонент m_i может быть отнесен к одной из 4-х введенных групп g_i.

3.3. Классы взаимодействий

Помимо источника и получателя информации при взаимодействии между компонентами, также важной характеристикой можно считать смысловую ориентированность взаимодействий – т.е. то, для кого предназначены передаваемые данные; в рамках ТИУГ ориентированность означает направленность на человека или автоматическое средство. Так, применяя аппарат категориального деления с этой позиции, можно выделить следующие классификационные категории-антагонисты для взаимодействий компонентов ТИУГ (подобные первой категориальной паре, используемой при классификации компонентов ТИУГ):

1) категория «человек» ($\mathrm{O_ч}$), соответствующая подмножеству человеко-ориентированных взаимодействий, необходимых людям, поскольку последние являются основными потребителями услуг ТИУГ (например, информацией может быть текстовая стоимость оплаты поездки на автомобиле);
2) категория «машина» ($\mathrm{O_М}$), соответствующая подмножеству машино-ориентированных взаимодействий, необходимых автоматам, поскольку работа ТИУГ основана на автоматическом (или машинном) предоставлении услуг потребителям (например, в информации могут содержаться сведения в бинарном виде о загрузке автомобильных дорог, текущих погодных условиях, стоимостях тарифов и т.п.).

Таким образом, все взаимодействия между компонентами ТИУГ могут быть проклассифицированы на предназначенные для человека и для машины.

Смысловая ориентированность позволит увеличить детализированность классификации взаимодействия между компонентами в 2 раза (т.е. довести их число до $64\times 2 = 128$). Такие новые ориентированные взаимодействия ($\left\langle m_i | m_j \right\rangle_o$ из множества TO) и их классы (C_k^{TO} из набора 128 классов) могут быть записаны в формализованном виде следующим образом:

$$\begin{cases} TO = \bigcup\limits_{\substack{i=1..8 \\ j=1..8 \\ o\in\{\mathrm{O_ч},\ \mathrm{O_М}\}}} \left\langle m_i | m_j \right\rangle_o; \\ \forall i = 1..8,\ j = 1..8, o \in \left\{\mathrm{O_ч},\ \mathrm{O_М}\right\}, k = 1..128 \ | \left\langle m_i | m_j \right\rangle_o \leftrightarrow C_k^{TO}. \end{cases}$$

Таким образом, с каждым взаимодействием со смысловой ориентированностью между двумя компонентами $\langle m_i | m_j \rangle_o$ связан свой класс C_i^{TO} и наоборот.

3.4. Классы интерфейсов

Как было сказано изначально, интерфейс представляет собой средство обеспечения информационного обмена между элементами системы (в данном случае, ТИУГ). Исходя из того, что все классы взаимодействий между компонентами ТИУГ являются качественно различными (поскольку процесс их получения основан на аппарате категориального деления), то за процесс информационного обмена ответственны такие же различные классы интерфейсов. В ином случае, один интерфейс содержал бы в себе слишком разнородный функционал и логически его было бы целесообразно поделить на несколько; сам он в этом случае являлся бы «комплексным интерфейсом». Например, хотя пропускной барьер, открывающий проход в транспортное средство по отпечатку пальцев, визуально и выглядит как законченное устройство с единым интерфейсным функционалом, логически он состоит из нескольких интерфейсов: человекоориентированный интерфейс со сканером отпечатков для передачи в центр интеллектуальной обработки; человекоориентированный интерфейс с переговорным устройством с оператором; машиноориентированный интерфейс для получения информации о достижении пункта назначения и пр. Следовательно, каждое такое взаимодействие, качественно отличное от других, может быть сопоставлено с определенным интерфейсом, что позволяет связать и их классы.

В формализованном виде, деление интерфейсов (f_i из множества F) ТИУГ на классы (C_i^F из набора 128 классов) может быть записано следующим образом:

$$\begin{cases} F = \bigcup\limits_{i=1..128} f_i \ ; \\ \forall i = 1..128 \mid f_i \leftrightarrow C_i^F \leftrightarrow C_i^{TO}. \end{cases}$$

Таким образом, с каждым интерфейсом f_i связан свой класс C_i^F, сопоставленный с классом взаимодействия со смысловой ориентированностью C_i^{TO} и наоборот.

3.5. Классы уязвимостей

Поскольку интерфейс фактически представляет собой программно-аппаратное решение – «интерфейсное средство», реализующее некоторый обмен информацией через себя, то ошибки такого обмена могут происходить исключительно по причине уязвимостей в средстве (естественно, полагаясь на то, что данные, создаваемые самими компонентами ТИУГ абсолютно корректны, а инсайдерская деятельность полностью пресечена [35-38]). Следовательно, с каждым интерфейсом может быть связан некоторый набор уязвимостей [39-40]. А поскольку современное программное обеспечение строится на базовых наборах модулей (например, библиотеках программ) и уязвимости находятся имен-

но в них, то одна и та же уязвимость может присутствовать в различных классах интерфейсов. Такое утверждение правомерно, поскольку классы интерфейсов решают задачи обмена качественно различной информацией, для которой в большинстве случаев применяются специализированные шаблоны проектирования, алгоритмы и наборы данных, как раз и содержащие определенные уязвимости.

В формализованном виде уязвимости (v_i из множества V), находящиеся в модулях интерфейсов (b_j из множества B), могут быть записаны следующим образом:

$$\begin{cases} V = \bigcup\limits_{i} \mathrm{v_i}; \\ B = \bigcup\limits_{j} \mathrm{b_j}; \\ \{v_l\}_m \to b_m; \\ \{b_m\}_n \to f_n; \\ \forall l \ge 1, m \ge 1, x \ge 1, n = 1..128, y = 1..y_{max}, y_{max} < 128; \\ C_n^F \to \{b_m\}_n \to \{\{v_l\}_m\}_n \equiv \{v_x\}_y \to C_y^V. \end{cases}$$

Таким образом, каждый интерфейс определенного класса C_n^F реализуется подмножеством программно-аппаратных модулей $\{b_m\}_n$, каждый из которых содержит подмножество уязвимостей $\{v_l\}_m$; подмножество же всех уязвимостей $\{v_x\}_y$ определенного интерфейса соответствует классу C_y^V. В данном случае, C_y^V является основным результатом, для получения которого построена и используется модель классификации. При этом, поскольку, различные интерфейсы могут реализовываться одинаковыми модулями, потенциально содержащими одинаковые уязвимости, то множества уязвимостей двух интерфейсов могут не только перекрываться, но и совпадать и, следовательно, количество классов уязвимостей интерфейсов должно быть не более количества классов интерфейсов ($n = 1..128$ *vs* $y = 1..y_{max}, y_{max} < 128$).

3.6. Представление модели

Искомая модель классификации уязвимостей ТИУГ (*Model*) в формализованном виде может быть записана следующим образом:

$$Model = \langle M, T, G, TO, F, V, B \rangle.$$

Таким образом, в модель входят все введенные ранее множества – компонентов M, взаимодействий T, групп G, взаимодействий со смысловой ориентированностью TO, интерфейсов F, уязвимостей V и модулей B.

В графическом виде обобщенная модель имеет следующую схему (см. рис. 2).

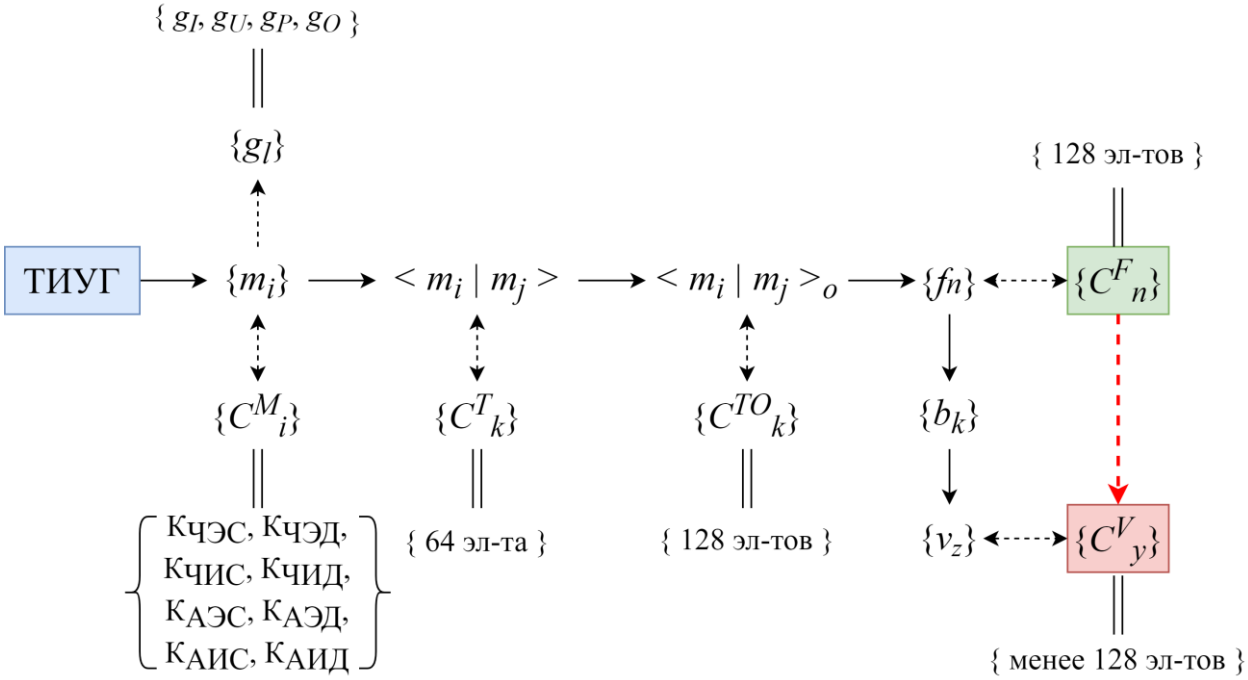

Рис. 2. Схема обобщенной модели классификации уязвимостей ТИУГ[1]

Введем операцию поиска уязвимостей ТИУГ – $D()$, которая, используя данную модель и признаки интерфейса P, позволяет определять классы уязвимостей и может лежать в основе будущего метода:

$$\begin{cases} \{\mathrm{v}_z\}' = D(\mathrm{Model},\ P); \\ P = \bigcup_j p_j; \\ D := P \to \mathrm{C}_n^{\mathrm{F}} \to \{b_m\}_n \to \{\{v_l\}_m\}_n \to \{v_x\}_y \equiv \{\mathrm{v}_z\}'. \end{cases}$$

Таким образом, операция поиска уязвимостей $D()$ в качестве аргументов принимает модель *Model* и признаки интерфейса P, по которым затем определяется сам интерфейс $\mathrm{C}_n^{\mathrm{F}}$, по составу модулей $\{b_m\}_n$ которого, а также их уязвимостям $\{\{v_l\}_m\}_n$ и вычисляется искомое множество уязвимостей интерфейса $\{\mathrm{v}_z\}'$.

Для работы операции поиска уязвимостей открытым вопросом остаются признаки интерфейсов и метод получения по ним самого класса интерфейса, однако, данный вопрос выходит за рамки предметной области, рассматриваемой в текущей статье, и попытка его решения будет предпринята авторами в продолжении исследования.

[1] Примечание: на схеме модели используются следующие обозначения: синий фон – исходная точка исследования (т.е. ТИУГ), зеленый фон – вводимые в модель данные (класс интерфейса), красный фон – искомые по модели данные (класс уязвимостей для интерфейса), «непрерывная стрелка» – получение нового элемента, «пунктирная стрелка» – соответствие одного элемента другому (как однонаправленное, так и двунаправленное), «двойная линия» – указание элементов из состава множества.

Заключение

В интересах первого шага по решению задачи поиска уязвимостей интерфейсов ТИУГ был произведен обзор существующих решений по классификации интерфейсов и их уязвимостей. На основании произведенного анализа была предложена формализация модели классификации уязвимостей компонентов ТИУГ, новизной которой является впервые установленная формальная взаимосвязь между ТИУГ, ее компонентами, их взаимодействиями, интерфейсами, модулями, реализующими функционал интерфейсов, и уязвимостями последних. Так, вся ТИУГ была поделена на 8 компонентов (с выделением интеллектуальной, потребительской и прогностической групп), которые в сумме дали 128 классов взаимодействий, обеспечиваемых таким же количеством интерфейсов, каждый из которых может содержать некоторый набор модулей с уязвимостями. Особенностью полученной классификации является удовлетворение требованиям необходимости и достаточности классов, что обосновывается корректным применением научно-методического аппарата категориального деления.

Продолжение исследования авторы видят в следующем. Во-первых, на базе модели необходимо создать прототип программного средства классификации интерфейсов, обладающего низкими значениями ошибок I и II рода, высокой оперативностью и не требующего высокого уровня подготовки от эксперта-пользователя. Во-вторых, используя представленную модель и прототип, возможно будет синтезировать сам метод поиска уязвимостей интерфейсов ТИУГ, предложив тем самым решение поставленной изначально задачи. И, в-третьих, потребуется произвести оценку поиска уязвимостей созданным методом, что будет основанием для подтверждения успешности всего проведенного исследования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-29-06099 и при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Литература

1. Волщуков Ю. Н., Волщуков М. Ю., Израилов К. Е., Романенко А. В. Визуализация информационного обмена в условиях концепции Industry 4.0 // Автоматизация в промышленности. 2020. № 8. С. 23-29.

2. Смирнов Г. Е., Макаренко С. И. Использование тестовых информационно-технических воздействий для аудита защищенности информационных систем железнодорожного транспорта // Интеллектуальные технологии на транспорте. 2020. № 3 (23). С. 20-29.

3. Курта П. А. Взаимодействие пользователя с информационной системой. Часть 1. Схема взаимодействия и классификация недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 8-9. С. 35-45.

4. Курта П. А. Взаимодействие пользователя с информационной системой. Часть 2. Алгоритмы обнаружения недостатков // Известия СПбГЭТУ ЛЭТИ. 2020. № 10. С. 34-44.

5. Курта П. А. Взаимодействие пользователя с информационной системой. Часть 3. Оценка эффективности // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 58-72.

6. Виткова Л. А., Израилов К. Е., Чечулин А. А. Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020): сборник научных статей IX Международной научно-технической и научно-методической конференции (Санкт-Петербург, 26-27 февраля 2020 г.). Санкт-Петербург, 2020. С. 253-258

7. Курта П. А., Коломеец М. В. Обобщенная классификация интерфейсов транспортной инфраструктуры «Умного города» // Вестник кибернетики. 2020. № 4 (40). С. 6-13.

8. Семенов С. С., Федоров В. Г., Федорова С. В. Классификация пользовательских интерфейсов программно-аппаратных комплексов связи и автоматизированных систем управления военного назначения // Проблемы технического обеспечения войск в современных условиях: труды III Межвузовской научно-практической конференции (Санкт-Петербург, 16 февраля 2018 г.). Санкт-Петербург, 2018. С. 360-366.

9. Суранова Д. А. Структура стенда для исследования человеко-машинного интерфейса на естественном языке // Известия Алтайского государственного университета. 2013. № 1-2 (77). С. 114-117.

10. Анохин А. Н., Ивкин А. С. Человеко-машинный интерфейс для поддержки когнитивной деятельности операторов АС // Ядерные измерительно-информационные технологии. 2012. № 1. С. 41.

11. Федечкин Р. С., Французова Ю. В. Разработка интерфейса пользователя для автоматизированной системы // Известия Тульского государственного университета. Технические науки. 2016. № 2. С. 287-290.

12. Дойникова Е. В., Федорченко А. В. Классификация интерфейсов и типов событий, применяемых в индустриальном интернете вещей для анализа их предрасположенности к кибератакам // Перспективные направления развития отечественных информационных технологий: материалы V межрегиональной научно-практической конференции (Севастополь, 24-28 сентября 2019 г.). Севастополь, 2019. С. 306-308.

13. Кривоногов В. М. Тенденции развития интерфейсов терминалов сетей связи общего пользования // T-Comm: Телекоммуникации и Транспорт. 2010. № 7. С. 180-181.

14. Зильберман Н. Н., Алексеев С. А. Категория «естественность» в классификации пользовательских интерфейсов // Гуманитарная информатика. 2018. № 14. С. 6-17.

15. Кулясов П. С. Классификация интерфейсов многокомпонентной системы на основе алгебраического подхода // Информационные системы и технологии (ИСТ-2020): сборник материалов XXVI Международной научно-технической конференции (Нижний Новгород, 24–28 апреля 2020 г.). Нижний Новгород, 2020. С. 419-423.

16. Любчикова О. В. Типы интерфейсов и виды элементов // Новая наука: От идеи к результату. 2016. № 12-3. С. 121-124.

17. Choi I., Nam C. S., Rhiu I., Lee Y., Yun M. H. A systematic review of hybrid brain-computer interfaces: Taxonomy and usability perspectives // PloS one. 2017. Vol. 12. No. 4. P. e0176674.

18. Dey D., Habibovic A., Löcken A., Wintersberger P., Pfleging B., Riener A., Martens M., Terken J. Taming the eHMI jungle: A classification taxonomy to guide, compare, and assess the design principles of automated vehicles' external human-machine interfaces // Transportation Research Interdisciplinary Perspectives. 2020. Vol. 7. P. 100174.

19. Prpa M., Pasquier P. Brain-computer interfaces in contemporary art: a state of the art and taxonomy // Brain art. 2019. P. 65-115.

20. Буйневич М. В., Израилов К. Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 95-106.

21. Израилов К. Е., Татарникова И. М. Подход к анализу безопасности программного кода с позиции его формы и содержания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2019): сборник научных статей VIII Международной научно-технической и научно-методической конференции (Санкт-Петербург, 27–28 февраля 2019 г). Санкт-Петербург, 2019. С. 462-467.

22. Федотова А. А. Будущее за умными городами: теория и практика создания Умного города // Интеграция современных научных исследований в развитие общества: сборник материалов IV Международной научно-практической конференции (Кемерово, 26 декабря 2017 г). Кемерово, 2017. С. 217-220.

23. Низамов Р. К. Умный город. Стратегии умного города // Цифровая документалистика для всех: сборник статей победителей и участников студенческого конкурса научно-исследовательских работ. Тюмень, 2018. С. 77-98.

24. Грибков Р. В., Мухин М. А. Умный город: концептуальный подход к созданию платформы умного города на муниципальном уровне // Развитие менеджмента в Индустрии 4.0: переход к киберфизическим организациям и формирование их систем управления: материалы XI Российской научно-практической конференции (с международным участием) (Пермь, 29 ноября 2018 г). Пермь, 2018. С. 49-51.

25. Курта П. А., Буйневич М. В. Онтологическая модель взаимодействия пользователя с информационной системой в рамках получения услуги информационного сервиса // Вестник кибернетики. 2021. № 2 (42). С. 17-23.

26. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software defined internet of things: cyber antifragility and vulnerability forecast // The proceedings of 11th IEEE International Conference on Application of Information and Communication Technologies (Moscow, Russia, 2017). IEEE, 2017. P. 293-297.

27. Вотенцев А. С. Революция искусственного интеллекта // Язык в сфере профессиональной коммуникации: сборник трудов международной научно-практической конференции преподавателей, аспирантов и студентов (Екатеринбург, 29 апреля 2021 г.). Екатеринбург, 2021. С. 395-401.

28. Федулова Е. К. Искусственный интеллект как средство создания музыки // Язык в сфере профессиональной коммуникации: сборник трудов международной научно-практической конференции преподавателей, аспирантов и студентов (Екатеринбург, 29 апреля 2021 г.). Екатеринбург, 2021. С. 606-611.

29. Терехина Е. А., Селюкова Г. П. Об искусственном интеллекте // Актуальные вопросы науки и хозяйства: новые вызовы и решения: сборник материалов LV Студенческой научно-практической конференции (Тюмень, 17-19 марта 2021 г.). Тюмень, 2021. С. 581-584.

30. Тихонова В. Умный транспорт будущего // Саморегулирование и бизнес. 2015. № 64 (09). С. 38-41.

31. Матвеева А. А. Транспорт в «Умном городе» // Экономика и социум. 2017. № 1-2 (32). С. 1115-1118.

32. Васильева Е. Ю., Полякова И. С. Умному городу – умный транспорт // Транспортное дело России. 2019. № 3. С. 161-163.

33. Скуратова А. Ю., Королькова Е. Е. Смертоносные автономные системы вооружений: проблемы международно-правового регулирования // Российский юридический журнал. 2019. № 1 (124). С. 22-30.

34. Даречкин В. М. Использование искусственного интеллекта в автомобильной промышленности: социально-экономические аспекты // Фундаментальные исследования. 2018. № 12-2. С. 245-249.

35. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders // ACM International Conference Proceeding Series. 4. The proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS, Санкт-Петербург, 2020). 2020. P. 3442619.

36. Буйневич М. В., Власов Д. С. Аналитическим обзор моделей инсайдеров информационных систем // Информатизация и связь. 2020. № 6. С. 92-98.

37. Буйневич М. В., Власов Д. С. Сравнительный обзор способов выявления инсайдеров в информационных системах // Информатизация и связь. 2019. № 2. С. 83-91.

38. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPV6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51.

39. Федорченко А. В., Чечулин А. А., Котенко И. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С.72-79.

40. Kotenko I., Fedorchenko A., Chechulin A. Integrated repository of security information for network security evaluation // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). 2015. Vol. 6. № 2. P. 41-57.

References

1. Volshhukov Ju. N., Volshhukov M. Ju., Izrailov K. E., Romanenko A. V. Vizualizacija informacionnogo obmena v uslovijah koncepcii Industry 4.0 [Visualization of information exchange in the context of the Industry 4.0 concept]. *Automation in Industry*, 2020, no. 8, pp. 23-29 (in Russian).

2. Smirnov G. E., Makarenko S. I. Ispol'zovanie testovykh informatsionno-tekhnicheskikh vozdeistvii dlia audita zashchishchennosti informatsionnykh sistem zheleznodorozhnogo transporta [The use of test information and technical influences to audit the security of information systems of railway transport]. *Intellectual Technologieson Transport*, 2020, no. 3 (23), pp. 20-29 (in Russian).

3. Kurta P. A. Vzaimodejstvie pol'zovatelja s informacionnoj sistemoj. Chast' 1. Shema vzaimodejstvija i klassifikacija nedostatkov [User interaction with the information system. Part 1. Scheme of interaction and classification of shortcomings]. *Izvestiya SPbGETU «LETI»*, 2020, no. 8-9, pp. 35-45 (in Russian).

4. Kurta P. A. Vzaimodejstvie pol'zovatelja s informacionnoj sistemoj. Chast' 2. Algoritmy obnaruzhenija nedostatkov [User interaction with the information system. Part 2. Algorithms for flaw detection]. *Izvestiya SPbGETU «LETI»*, 2020, no. 10, pp. 34-44 (in Russian).

5. Kurta P. A. Vzaimodejstvie pol'zovatelja s informacionnoj sistemoj. Chast' 3. Ocenka jeffektivnosti [User interaction with the information system. Part 3. Evaluation of effectiveness]. *Izvestiya SPbGETU «LETI»*, 2021, no. 4, pp. 58-72 (in Russian).

6. Vitkova L. A., Izrailov K. E., Chechulin A. A. Klassifikacija ujazvimostej interfejsov transportnoj infrastruktury umnogo goroda [Classification of Vulnerabilities of Smart City Transport Infrastructure Interfaces]. *Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO-2020): sbornik nauchnyh statej IX Mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii* [Actual problems of infotelecommunications in science and education (APINO-2020): collection of scientific articles of the IX International scientific-technical and scientific-methodological conference], Saint-Petersburg, 2020, pp. 253-258 (in Russian).

7. Kurta P. A., Kolomeec M. V. Obobshhennaja klassifikacija interfejsov transportnoj infrastruktury «Umnogo goroda» [Generalized classification of interfaces of the transport infrastructure of the «Smart City»]. *Proceedings in Cybernetics*, 2020, no. 4 (40), pp. 6-13 (in Russian).

8. Cemenov S. S., Fedorov V. G., Fedorova S. V. Klassifikacija pol'zovatel'skih interfejsov programmno-apparatnyh kompleksov svjazi i avtomatizirovannyh sistem upravlenija voennogo naznachenija [Classification of user interfaces of software and hardware communication systems and automated control systems for military purposes]. *Problemy tehnicheskogo obespechenija vojsk v sovremennyh uslovijah: trudy III Mezhvuzovskoj nauchno-prakticheskoj konferencii* [Problems of technical support of troops in modern conditions: proceedings of the III Interuniversity Scientific and Practical Conference], Saint-Petersburg, 2018, pp. 360-366 (in Russian).

9. Suranova D. A. Struktura stenda dlja issledovanija cheloveko-mashinnogo interfejsa na estestvennom jazyke [The structure of the stand for the study of the

human-machine interface in natural language]. *Izvestiya of Altai State University*, 2013, no. 1-2 (77), pp. 114-117 (in Russian).

10. Anohin A. N., Ivkin A. S. Cheloveko-mashinnyj interfejs dlja podderzhki kognitivnoj dejatel'nosti operatorov AS [Human-machine interface to support the cognitive activity of the AS operators]. *Nuclear measurement and information technologies*, 2012, no. 1, pp. 41 (in Russian).

11. Fedechkin R. S., Francuzova Ju. V. Razrabotka interfejsa pol'zovatelja dlja avtomatizirovannoj sistemy [Development of a user interface for an automated system]. *Izvestiya Tula State University*, 2016, no. 2, pp. 287-290 (in Russian).

12. Dojnikova E. V., Fedorchenko A. V. Klassifikacija interfejsov i tipov sobytij, primenjaemyh v industrial'nom internete veshhej dlja analiza ih predraspolozhennosti k kiberatakam [Classification of interfaces and types of events used in the industrial Internet of things to analyze their susceptibility to cyber attacks]. *Perspektivnye napravlenija razvitija otechestvennyh informacionnyh tehnologij: materialy V mezhregional'noj nauchno-prakticheskoj konferencii* [Promising directions for the development of domestic information technologies: materials of the V interregional scientific and practical conference], Sevastopol, 2019, pp. 306-308 (in Russian).

13. Krivonogov V. M. Tendencii razvitija interfejsov terminalov setej svjazi obshhego pol'zovanija [Development trends of interfaces of terminals of public communication networks]. *T-Comm – Telecommunications and Transport*, 2010, no. 7, pp. 180-181 (in Russian).

14. Zil'berman N. N., Alekseev S. A. Kategorija «estestvennost'» v klassifikacii pol'zovatel'skih interfejsov [Category «naturalness» in the classification of user interfaces]. *Humanitarian Informatics*, 2018, no. 14, pp. 6-17 (in Russian).

15. Kuljasov P. S. Klassifikacija interfejsov mnogokomponentnoj sistemy na osnove algebraicheskogo podhoda [Classification of interfaces of a multicomponent system based on an algebraic approach]. *Informacionnye sistemy i tehnologii (IST-2020): cbornik materialov XXVI Mezhdunarodnoj nauchno-tehnicheskoj konferencii* [Information systems and technologies (IST-2020): collection of materials of the KSVA International Scientific and Technical Conference], Nizhny Novgorod, 2020, pp. 419-423 (in Russian).

16. Ljubchikova O. V. Tipy interfejsov i vidy jelementov [Interface types and element types]. *Novaja nauka: Ot idei k rezul'tatu* [New Science: From Idea to Results], 2016, no. 12-3, pp. 121-124 (in Russian).

17. Choi I., Nam C. S., Rhiu I., Lee Y., Yun M. H. A systematic review of hybrid brain-computer interfaces: Taxonomy and usability perspectives. *PloS one*, 2017, vol. 12, no. 4, pp. e0176674.

18. Dey D., Habibovic A., Löcken A., Wintersberger P., Pfleging B., Riener A., Martens M., Terken J. Taming the eHMI jungle: A classification taxonomy to guide, compare, and assess the design principles of automated vehicles' external human-machine interfaces. *Transportation Research Interdisciplinary Perspectives*, 2020, vol. 7, pp. 100174.

19. Prpa M., Pasquier P. Brain-computer interfaces in contemporary art: a state of the art and taxonomy. *Brain art*, 2019, pp. 65-115.

20. Bujnevich M. V., Izrailov K. E. Kategorial'nyj sintez i tehnologicheskij analiz variantov bezopasnogo importozameshhenija programmnogo obespechenija

telekommunikacionnyh ustrojstv [Categorical synthesis and technological analysis of options for safe import substitution of software for telecommunication devices]. *Telecom IT*, 2016, vol. 4, no. 3, pp. 95-106 (in Russian).

21. Izrailov K. E., Tatarnikova I. M. Podhod k analizu bezopasnosti programmnogo koda s pozicii ego formy i soderzhanija [An approach to the analysis of the security of program code from the point of view of its form and content]. *Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO-2019): sbornik nauchnyh statej VIII Mezhdunarodnoj nauchno-tehnicheskoj i nauchno-metodicheskoj konferencii* [Actual problems of infotelecommunications in science and education (APINO-2019): collection of scientific articles of the VIII International scientific-technical and scientific-methodological conference], Saint-Petersburg, 2019, pp. 462-467 (in Russian).

22. Fedotova A. A. Budushhee za umnymi gorodami: teorija i praktika sozdanija Umnogo goroda [The future belongs to smart cities: theory and practice of creating a Smart city]. *Integracija sovremennyh nauchnyh issledovanij v razvitie obshhestva: sbornik materialov IV Mezhdunarodnoj nauchno-prakticheskoj konferencii* [Integration of modern scientific research into the development of society: a collection of materials of the IV International Scientific and Practical Conference], Kemerovo, 2017, pp. 217-220 (in Russian).

23. Nizamov R. K. Umnyj gorod. Strategii umnogo goroda [Smart city. Smart city strategies]. *Cifrovaja dokumentalistika dlja vseh: sbornik statej pobeditelej i uchastnikov studencheskogo konkursa nauchno-issledovatel'skih rabot* [Digital Documentary for All: A Collection of Articles by Winners and Participants of the Student Research Paper Competition], Tyumen, 2018, pp. 77-98 (in Russian).

24. Gribkov R. V., Muhin M. A. Umnyj gorod: konceptual'nyj podhod k sozdaniju platformy umnogo goroda na municipal'nom urovne [Smart city: a conceptual approach to creating a smart city platform at the municipal level]. *Razvitie menedzhmenta v Industrii 4.0: perehod k kiberfizicheskim organizacijam i formirovanie ih sistem upravlenija: materialy XI Rossijskoj nauchno-prakticheskoj konferencii (s mezhdunarodnym uchastiem)* [Development of management in Industry 4.0: the transition to cyber-physical organizations and the formation of their management systems: materials of the XI Russian scientific-practical conference (with international participation)], Permian, 2018, pp. 49-51 (in Russian).

25. Kurta P. A., Bujnevich M. V. Ontologicheskaja model' vzaimodejstvija pol'zovatelja s informacionnoj sistemoj v ramkah poluchenija uslugi informacionnogo servisa [Ontological model of user interaction with an information system within the framework of receiving an information service]. *Proceedings in Cybernetics*, 2021, no. 2 (42), pp. 17-23 (in Russian).

26. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software defined internet of things: cyber antifragility and vulnerability forecast. *The proceedings of 11th IEEE International Conference on Application of Information and Communication Technologies*, Moscow, 2017, pp. 293-297.

27. Votencev A. S. Artificial intelligence revolution. *Iazyk v sfere professional'noi kommunikatsii: sbornik trudov mezhdunarodnoi nauchno-prakticheskoi konferentsii prepodavatelei, aspirantov i studentov* [Language in the field of professional communication: a collection of works of the international

scientific-practical conference of teachers, graduate students and students], Ekaterinburg, 2021, pp. 395-401.

28. Fedulova E. K. Artificial intelligence as a means of creating music. *Iazyk v sfere professional'noi kommunikatsii: sbornik trudov mezhdunarodnoi nauchno-prakticheskoi konferentsii prepodavatelei, aspirantov i studentov* [Language in the field of professional communication: a collection of works of the international scientific-practical conference of teachers, graduate students and students], Ekaterinburg, 2021, pp. 606-611.

29. Terehina E. A., Seljukova G. P. Ob iskusstvennom intellekte [About artificial intelligence]. *Aktual'nye voprosy nauki i hozjajstva: novye vyzovy i reshenija: sbornik materialov LV Studencheskoj nauchno-prakticheskoj konferencii* [Topical issues of science and economy: new challenges and solutions: collection of materials LV Student scientific and practical conference], Tyumen, 2021, pp. 581-584 (in Russian).

30. Tihonova V. Umnyj transport budushhego [Smart transport of the future]. *Samoregulirovanie i biznes* [Self-regulation and business], 2015, no. 64 (09), pp. 38-41 (in Russian).

31. Matveeva A. A. Transport v «Umnom gorode» [Transport in the «Smart City»]. *Jekonomika i socium* [Economy and society], 2017, no. 1-2 (32), pp. 1115-1118 (in Russian).

32. Vasil'eva E. Ju., Poljakova I. S. Umnomu gorodu - umnyj transport [Smart city – smart transport]. *Transport business of Russia*, 2019, no. 3, pp. 161-163 (in Russian).

33. Skuratova A. Ju., Korol'kova E. E. Smertonosnye avtonomnye sistemy vooruzhenij: problemy mezhdunarodno-pravovogo regulirovanija [Lethal autonomous weapons systems: problems of international legal regulation]. *Russian juridical journal*, 2019, no. 1 (124), pp. 22-30 (in Russian).

34. Darechkin V. M. Ispol'zovanie iskusstvennogo intellekta v avtomobil'noj promyshlennosti: social'no-jekonomicheskie aspekty [The use of artificial intelligence in the automotive industry: socio-economic aspects]. *Fundamental Research*, 2018, no. 12-2, pp. 245-249 (in Russian).

35. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders. *ACM International Conference Proceeding Series. 4. The proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, Saint-Petersburg, 2020, pp. 3442619.

36. Bujnevich M. V., Vlasov D. S. Analiticheskim obzor modelej insajderov informacionnyh sistem [Analytical overview of information systems insider models]. *Informatization and communication*, 2020, no. 6, pp. 92-98 (in Russian).

37. Bujnevich M. V., Vlasov D. S. Sravnitel'nyj obzor sposobov vyjavlenija insajderov v informacionnyh sistemah [Comparative review of ways to identify insiders in information systems]. *Informatization and communication*, 2019, no. 2, pp. 83-91 (in Russian).

38. Saharov D. V., Krasov A. V., Ushakov I. A., Birih Je. V. Modelirovanie zashhishhennoj masshtabiruemoj seti predprijatija s dinamicheskoj marshrutizaciej na osnove IPV6 [Modeling a secure scalable enterprise network with dynamic routing based on IPV6]. *Zasita informacii. Inside*, 2020, no. 1 (91), pp. 51 (in Russian).

39. Fedorchenko A. V., Chechulin A. A., Kotenko I. V. Issledovanie otkrytyh baz ujazvimostej i ocenka vozmozhnosti ih primenenija v sistemah analiza zashhishhennosti komp'juternyh setej [Research of open databases of vulnerabilities and assessment of the possibility of their application in security analysis systems of computer networks]. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 5, pp. 72-79 (in Russian).

40. Kotenko I., Fedorchenko A., Chechulin A. Integrated repository of security information for network security evaluation. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 2015, vol. 6, no. 2, pp. 41-57.

Статья поступила 27 сентября 2021 г.

Информация об авторах

Израилов Константин Евгеньевич – кандидат технических наук. Доцент кафедры защищенных систем связи. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Старший научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: информационная безопасность; безопасность киберфизических систем; реверс инжиниринг программного кода; умный город; машинное обучение. E–mail: konstantin.izrailov@mail.ru

Левшун Дмитрий Сергеевич – соискатель ученой степени кандидата технических наук. Младший научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: безопасность в соответствии с проектом; проектирование, моделирование и верификация киберфизических систем. E–mail: levshun@comsec.spb.ru

Чечулин Андрей Алексеевич – кандидат технических наук, доцент. Ведущий научный сотрудник лаборатории проблем компьютерной безопасности. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук. Область научных интересов: информационная безопасность; защита от информации; визуализация безопасности; безопасность киберфизических устройств; цифровая криминалистика. E–mail: chechulin@comsec.spb.ru

Адрес: 199178, Россия, г. Санкт-Петербург, 14 линия В.О., д. 39.

Vulnerability classification model for Smart City transport infrastructure interfaces

K. E. Izrailov, D. S. Levshun, A. A. Chechulin

Problem. *In addition to obvious advantages, the implementation of the Smart City concept carries a number of significant disadvantages, one of which is information security threats, which are, among other things, a consequence of the presence of vulnerabilities in software-hardware modules that implement this concept. The situation is becoming critical for such infrastructures as transport, the disruption of which po-*

tentially leads to human casualties. Existing studies are devoted mainly to the security of modules that ensure the functioning of the Smart City subsystems, although the security of interfaces that support the interaction of modules has been largely neglected. Thus, a deeper study of the vulnerabilities of the interfaces of the transport infrastructure of the Smart City is required for their subsequent search and neutralization. ***The purpose*** *of the work is to systematize the vulnerabilities of the interfaces of the transport infrastructure of the Smart City in the form of a generalizing classification model. It is proposed to separate vulnerabilities based on the classes of interfaces to which they belong; while interfaces are divided into subclasses according to the components of the transport infrastructure used by them, as well as the semantic orientation of interactions.* ***Methods****. To distinguish subclasses of the Smart City interfaces, the apparatus of categorical division was used: for the elements of transport infrastructure, pairs were used –- Human vs Automaton, Expert vs Intellectual, and Static vs Dynamics; and for interactions – Human Oriented vs Machine Oriented. Analytical modelling was used to build relationships between the transport infrastructure of the Smart City and the vulnerabilities of its interfaces.* ***Novelty****. The element of novelty of the presented solution is the inclusion in the classification model of the requirement of "necessity and sufficiency", which is that any, even hypothetical, vulnerability is guaranteed to be attributed to one and only one class. Also, the presented model includes the variability of the classification by the possibility of its expansion and detailing by adding new pairs of categorical division.* ***Result****. The identification of various elements of the transport infrastructure of the Smart City, as well as the options for interactions between them, made it possible to move to the classification of the corresponding interfaces that provide such interactions, and, as a consequence, to the classification of the vulnerabilities of the latter. The use of the apparatus of categorical division confirms the correctness of the classification obtained.* ***Practical relevance****. The presented solution is proposed to be implemented in the form of a software prototype. Also, based on the classification model and the prototype, it is planned to develop a direct method for searching for vulnerabilities in the transport infrastructure of the Smart City.*

Key words: *smart city, transport infrastructure, vulnerability, classification, model, search vulnerabilities.*

Information about Authors

Konstantin Evgenievich Izrailov – Ph.D. of Engineering Sciences. Associate Professor at the Department of Secure Communication Systems. The Bonch-Bruevich Saint-Petersburg state university of telecommunications. Senior Researcher at the Computer Security Problems Laboratory. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: information security; cyber physical devices security; reverse engineering of program code; smart city; machine learning. E–mail: konstantin.izrailov@mail.ru

Dmitry Sergeevich Levshun – Ph.D student. Junior Researcher at the Computer Security Problems Laboratory. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: security by design; design, modeling and verification of cyber-physical systems. E–mail: levshun@comsec.spb.ru

Andrey Alekseyevich Chechulin – Ph.D. of Engineering Sciences, Associate Professor. Leading Researcher at the Computer Security Problems Laboratory. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Field of research: information security; protection against information; security visualization; cyber physical devices security; digital forensics. E–mail: chechulin@comsec.spb.ru

Address: 199178, Russia, Saint-Petersburg, 14 line V.O., 39.