К. Е. ИЗРАИЛОВ
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича; Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук, Санкт-Петербург
П. А. КУРТА
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича**,** Санкт-Петербург

МОДЕЛИРОВАНИЕ УЯЗВИМОСТЕЙ В ИНТЕРФЕЙСАХ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ УМНОГО ГОРОДА

Доклад посвящен вопросу безопасности Умного города в части ее транспортной инфраструктуры. В результате проведенного исследования предлагается модель обобщенной классификации уязвимостей в интерфейсах инфраструктуры, заданная в аналитическом виде. Для этого вводятся 8 подсистем транспортной инфраструктуры (с применением аппарата категориального деления), выявляются существующие между ними взаимодействия и выделяются необходимые для этого интерфейсы. Определение основных элементов последних позволяет разделить уязвимости всей транспортной инфраструктуры Умного города на классы, соответствующие их расположению в устройствах интерфейсов.

Введение. Информационные технологии стали неотъемлемой частью жизни любого современного общества, переведя процессы его функционирования на качественно новый уровень. Это дало существенный толчок к развитию новых направлений, одним из которых стала концепция Умного города (далее – УГ) [1]. И, несмотря на то, что целью создания УГ является улучшение качества жизни, оно может также иметь и негативные для жителей последствия. Так, поскольку в данную концепцию включается другая – Интернет вещей, обеспечивающая взаимодействие между объектами реального мира, то нарушение информационной безопасности (далее – ИБ) может напрямую приводить и к физическим угрозам [2]. Одной из наиболее подверженных этому областей является транспортная инфраструктура (далее – ТИ) УГ, поскольку она предназначена для физического перемещения людей и грузов. Нарушения же в работе ТИ УГ могут приводить не только к задержкам доставки грузов, но и к травмам пассажиров или же летальным исходам [3]. Например, ошибка в распознавании максимально разрешенной скорости движения беспилотным транспортным средством на аварийно-опасном участке движения неуклонно приведет к аварии с человеческими жертвами.

Поскольку в принципы функционирования ТИ УГ вложена необходимость сосуществования разнородных участников с недетерминированным поведением (пассажиры, водители, автомобили, шлагбаумы и пр.) в условиях изменяющихся внешних условий (погода, время суток, катаклизмы), то для их взаимодействия требуется соответствующий механизм обмена информацией – *интерфейс* [4]. При этом под последним будем понимать не теоретическое понятие – как границу между функциональными объектам, а практическую реализацию – как программно-аппаратное устройство, передающее (с необходимым преобразованием) информацию от одного объекта к другому.

Одной из основных причин нарушения ИБ считается наличие уязвимостей (или ошибок) в работе соответствующих средств. И если поиску и нейтрализации уязвимостей в отдельно стоящих устройствах от «безопасников» уделяется достаточное количество внимания, то вопросы безопасности интерфейсов, соединяющих такие устройства в единую информационную систему, оставлены практически без внимания. Причиной этого в аспекте УГ в том числе можно считать относительную новизну концепции УГ, не всегда доведенной до практической реализации и не позволяющей провести натурные эксперименты и испытания «в бою». При этом, риск ошибки в случае внедрения в ТИ небезопасных решений, будет иметь критические последствия.

Подытоживая указанные факторы, первоначально требуется теоретическое исследование потенциально опасных последствий применения интерфейсов ТИ УГ. Первым же этапом этого, в условиях общей слабой теоретической проработанности данного вопроса, должно стать выявление уязвимостей интерфейсов и их обобщенная классификация в виде аналитической модели – что является *задачей текущего исследования*. Для этого должны быть выполнены следующие шаги: 1) введение классов подсистем ТИ УГ; 2) определение возможных взаимодействий подсистем и классов интерфейсов между ними; 3) выявление элементов интерфейсов взаимодействий; 4) классификация уязвимости интерфейсов в виде модели. Предлагаемый доклад посвящен выполнению указанных шагов, что позволит создать обобщенную классификацию уязвимостей ТИ УГ и представить ее в аналитическом виде.

Подсистемы инфраструктуры. На 1-м шаге исследования необходимо разбить достаточно разнородную область ТИ УГ на классы подсистем, имеющие собственное функциональное предназначение. Типичной проблемой такого рода разбиений является сложность выделения областей, которые как не перекрывались бы с другими, так и целиком покрывали всю исходную область. В интересах применим достаточно хорошо себя зарекомендовавший аппарат категориального деления, суть которого заключается в постепенном делении некоторой области (т.е. множества входящих в нее элементов) на две примерно одинаковые подобласти, являющиеся противоположностями по некоторому критерию. Для этого выбирается соответствующая пара категорий-антагонистов (самым ярким примером которой может быть следующая – «положительный» vs «отрицательный»).

Такое деление ТИ УГ на классы подсистем ранее уже производилось авторами путем выбора следующих пар категорий-антагонистов [5]:

- «человек» vs «автомат», поскольку назначение УГ заключается в повышении качества жизни людей за счет (в том числе) автоматизации процессов;
- «эксперт» vs «интеллект», исходя из наличия в УГ возможностей искусственного интеллекта [6];
- «статика» vs «динамика», отражая тем самым применение деления именно к ТИ, состоящей из множества объектов, перемещающихся в среде неподвижных.

Очевидно, что полная комбинация 3-х пар даст 8 классов подсистем ТИ УГ, каждая из которых обладает своими особенностями. Так, например, класс подсистемы, соответствующий элементам «человек + эксперт + динамика» отвечает группе штурманов беспилотного транспортного средства, контролирующей корректность его работы; в противоположность этому класс подсистемы для комбинации «автомат + интеллект + статика» соответствует всем возможным интеллектуальным средствам управления дорожным движением, таким, как умные светофор или пешеходный переход с датчиком пешехода [7].

Взаимодействие подсистем. На 2-м шаге исследования необходимо определить все возможности взаимодействий между классами подсистем ТИ УГ, выделенными на 1-м шаге. В общем случае, каждая из подсистем может взаимодействовать с любой другой. Например, подсистема пассажир потока (комбинация элементов «человек + интеллект + динамика») обменивается информацией (посредством интерфейсов) с подсистемой беспилотных транспортных средств (комбинация элементов «автомат + интеллект + динамика») [8]. Также, поскольку подсистема определяет целый набор входящих в нее устройств, которые взаимодействуют и друг с другом, то информационные потоки могут идти от отдельно взятой подсистемы к ней самой. Например, датчики света передают сигнал к лампам освещения в случае наступления темноты в рамках соответствующей подсистемы (комбинация «автомат + эксперт + статика»).

Общее же количество комбинаций направлений обмена информацией между подсистемами с учетом их направленности составляет $8 \times 8 = 64$ класса взаимодействия. Очевидно, существует такое же количество классов интерфейсов, каждый из которых предназначен для передачи информации от одного класса подсистемы ТИ УГ к другому (или же к самому себе).

Элементы интерфейса. На 3-м шаге необходимо выделить основные элементы интерфейса (или обосновать их отсутствие, если интерфейс неделим) [9]. Согласно описанной ранее логике, интерфейс предназначен для обеспечения обмена информацией между разнородными классами подсистем ТИ УГ. Следовательно, в интерфейсе должно обеспечиваться преобразование данных, выходящих из одной подсистемы в данные, входящие в другую систему. Таким образом, в любом интерфейсе логично выделить 3 следующих элемента, имеющих последовательно вы-

полняемый функционал: *анализатор*, распознающий форму входного потока данных (от подсистемы-отправителя); *обработчик* – преобразующий содержимое данных (согласно смысловому предназначению интерфейса); *синтезатор* – генерирующий выходной поток данных в нужной форме (к подсистеме-получателя). Например, камера распознавания автомобильных номеров вначале преобразует графическое изображение номерного знака к набору графических точек, затем с применением машинного обучения (как правило) переводит их во внутреннее представление записи номера, после чего передает итоговую запись в текстовом виде на сервер управления автоматическим поднятием шлагбаума.

Поскольку устройство интерфейса было разделено на 3 элемента, то общее количество классов таких элементов для всех классов интерфейсов (полученных на 2-м шаге) равно $64 \times 3 = 192$.

Важно отметить, что каждый элемент в каждом классе интерфейсов будет отличаться от аналогичного элемента в другом классе, поскольку он входит в интерфейс, имеющий собственное предназначение. Впрочем, элементы, примыкающие к одинаковым подсистемам, будут все-таки близки. Например, анализаторы подсистемы пассажир потока, так или иначе, ориентируются на распознавании различных особенностей человека (лицо, голос, движение); синтезаторы же информации для всех подсистем, связанных с автоматизированными устройствами, будут производить данные в формализованной (т. е. машинно-ориентированной) форме и т. д.

Уязвимости интерфейса. На 4-м шаге необходимо определить основные места в интерфейсах ТИ, где возможно появление уязвимостей, нарушающих общую ИБ УГ. Исходя из этого, можно утверждать, что наличие уязвимости в каждом таком элементе будет приводить к нарушению функционирования интерфейса, за которым последует некорректная передача информации между подсистемами и, значит, общее нарушение функционирования системы (в данном случае – ТИ УГ). Следовательно, можно выделить 192 класса уязвимостей (каждая из которых по месту нахождения соответствует одному из 192 классов элементов интерфейсов). А исходя из принципа введения уязвимостей, можно ввести их формальную классификацию в виде следующей аналитической модели:

$$\begin{cases} \text{У} \equiv \text{С}_{xyz} \overset{\text{Э}}{\rightarrow} \text{С}_{xyz} \\ x, y, z \in \{\text{П}_1, \text{П}_2, \text{П}_3\} \\ \text{П}_1 \in \{\text{Человек}, \text{Автомат}\} \\ \text{П}_2 \in \{\text{Эксперт}, \text{Интеллект}\} \\ \text{П}_3 \in \{\text{Статика}, \text{Динамика}\} \\ \text{Э} \in \{\text{Анализатор}, \text{Обработчик}, \text{Синтезатор}\} \end{cases}, \quad (1)$$

где У – класс уязвимости; С_{xyz} – подсистема ТИ УГ, соответствующая элементам категориальных пар x, y, z; П_1, П_2 и П_3 – категориальные пары; Э – элемент интерфейса ТИ УГ.

Заключение. Статья описывает теоретическое исследование информационной безопасности транспортной инфраструктуры умного города. Для этого оценивается возможность нарушения информационных потоков между ее подсистемами вследствие уязвимостей в обеспечивающих это интерфейсах. Как результат, предлагается модель обобщённой классификации уязвимостей, состоящей из 192 элементов. Новизна такой классификации заключается в ее абсолютной корректности с позиции необходимости (классы не пересекаются) и достаточности (классы перекрывают все возможные уязвимости). Значимость исследования заключается в том, что превентивное теоретическое предсказание уязвимостей уменьшит их появление в практических решениях концепции умного города [10]. Также необходимо подчеркнуть общее слабое развитие методологического аппарата данной предметной области, что говорит о важности получения любых новых знаний в ней.

Продолжением исследования должно стать создание подхода для прогнозирования конкретных уязвимостей, связанных как с каждым из введенных классов, так и с оцениваемой инфраструктурой.

Исследование выполнено при финансовой поддержке РФФИ
в рамках научного проекта № 19-29-06099

ЛИТЕРАТУРА

1. **Хузмиев И.К., Гассиева О.И.** О «цифровой экономике» и «Умном – Smart» городе. А*втоматизация и IT в энергетике*. 2019. № 4 (117). С. 44-50.
2. **Izrailov K., Chechulin A., Vitkova L.** Threats Classification Method for the Transport Infrastructure of a Smart City. *The proceedings of 14th International Conference on Application of Information and Communication Technologies* (Tashkent, Uzbekistan, 7-9 october 2020). IEEE, 2020. PP. 1-6.
3. **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.). 2020. С. 253-258
4. **Вострых А.В.** Анализ интерфейсов специализированных мобильных приложений для вызова экстренных служб. *Пожарная и техносферная безопасность: проблемы и пути совершенствования*. 2021. № 2 (9). С. 78-82.
5. **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
6. **Котякова В.А., Мурашкина Е.Н.** Алгоритм взаимодействия пользователя и интеллектуальной транспортной системы «Умного города». *Современные информационные технологии*. 2013. № 17. С. 257-261.
7. **Зюрина О.А.** Инновационные методы построения городской логистической системы. *Наука и образование транспорту*. 2018. № 1. С. 143-145.
8. **Загидулина А.Д., Николаева Р.В.** Беспилотный транспорт – транспорт будущего. Тех*ника и технология транспорта*. 2017. № 4 (5). С. 12.
9. **Хрусталев В.И.** Сравнительный анализ структуры технологий человеко-машинного интерфейса. *Известия Тульского государственного университета. Технические науки*. 2019. № 9. С. 275-279.
10. **Израилов К.Е.** Обобщенная классификация уязвимостей интерфейсов транспортной инфраструктуры Умного города. *Информационные технологии*. 2021. Т. 27. № 6. С. 330-336. DOI: 10.17587/it.27.330-336.

K.E.Izrailov (The Bonch-Bruevich Saint-Petersburg state university of telecommunications, Saint-Petersburg; St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg), P.A.Kurta (The Bonch-Bruevich Saint-Petersburg state university of telecommunications, Saint-Petersburg)

Vulnerability Modeling in Smart City Transport Infrastructure Interfaces

The report is devoted to the security of the Smart City in terms of its transport infrastructure. As a result of the study, a model for a generalized classification of vulnerabilities in infrastructure interfaces, specified in an analytical form, is proposed. To do this, 8 subsystems of the transport infrastructure are introduced (using the categorical division apparatus), the interactions between them are identified and the interfaces necessary for this are identified. The definition of the main elements of the latter allows us to divide the vulnerabilities of the entire transport infrastructure of the Smart City into classes corresponding to their location in the interface devices.

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus