УДК 004.5 DOI: 10.17587/it.27.330-336

К. Е. Израилов, канд. техн. наук, e-mail: konstantin.izrailov@mail.ru,
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Обобщенная классификация уязвимостей интерфейсов транспортной инфраструктуры Умного города*

Рассматривается задача классификации уязвимостей, присутствующих в устройствах интерфейсов, которые применяются при взаимодействии людей и составляющих транспортной инфраструктуры Умного города. Вводится концептуальная модель терминологической базы предметной области, на основе которой синтезируется единая классификация уязвимостей. Дается формальная запись классов уязвимостей, а также их примеры.

Ключевые слова: *умный город, транспортная инфраструктура, классификация, уязвимости, информационная безопасность*

Введение

Одной из тенденций развития современного мира является улучшение жизнедеятельности во всех сферах бизнеса, общества и государства. Этой же цели придерживается и концепция "Умного города", стремящаяся связать информационными потоками физические системы с искусственным интеллектом [1, 2]. К достаточно значимой для данной концепции области можно отнести транспортную инфраструктуру, которая обеспечивает комфортное перемещение людей на транспортных средствах — именно она должна обеспечивать высокий уровень интеллектуализации [3].

*Работа выполнена при финансовой поддержке РФФИ (проект № 19-29-06099).

Как и практически любое внедрение новых информационных технологий, помимо очевидных преимуществ оно несет и определенные недостатки, как правило выражающиеся в возникновении угроз информационной безопасности [4]. И если безопасности отдельных подсистем уделено достаточное число исследований [5—8], то вопросы реализации угроз через интерфейсы оставлены практически без внимания. Под последними понимаются вполне определенный набор устройств, обеспечивающий обмен информацией как между частями подсистемы, так и с их окружением (например, с человеком). Следуя классической точке зрения, реализация угроз возникает вследствие наличия уязвимостей в интерфейсах. Следовательно, их изучение с позиции информационной безопасности является актуальной задачей.

Обзор существующих классификаций

Существует достаточно обширное число публикаций, посвященных общим уязвимостям веб-интерфейсов: обобщенное деление на виды [9], выделение классов для веб-сервисов в автоматизированных системах управления [10], изучение проблем обнаружения [11].

В ряде случаев проводится выявление целых уязвимых критических зон инфраструктуры в Умных городах [12]. В работе [13] описываются основы безопасности для Умных городов в целях недопущения неправомерного использования их уязвимостей.

Отдельные работы посвящены именно уязвимостям различных элементов Умного города. Так, в работе [14] выделяются три зоны уязвимостей беспилотного транспортного средства: система управления движением, техническая инфраструктура и информационное взаимодействие субъектов Умного города. Аналогичному вопросу обнаружения уязвимостей беспилотных транспортных средств посвящена монография [15].

Однако научные работы, непосредственно описывающие классификацию уязвимостей в интерфейсах транспортной инфраструктуры Умного города, отсутствуют, хотя отдельные аспекты таких уязвимостей и были изучены. И, следовательно, классификация, сочетающая как общие информационные свойства уязвимостей, так и специфику конкретной инфраструктуры, будет обладать безусловной актуальностью и новизной.

Новый подход к классификации

Для всестороннего исследования безопасности транспортной инфраструктуры Умного города в качестве первого шага может быть востребована задача однозначной классификации (обладающая необходимостью и достаточностью) уязвимостей ее интерфейсов, т. е. тех уязвимостей, которые расположены в средствах обеспечения обмена информацией между подсистемами инфраструктуры, а также ее внешним окружением.

Для классификации уязвимостей необходимо обратиться к современному пониманию данного термина, которое наиболее близко к определению в виде "недостатка в системе, способного привести к реализации угроз". Однако данная трактовка уязвимостей достаточно сложна для создания полноценной их классификации по причине классического научного противоречия: потребности ***vs*** возможности. Так, с одной стороны, следуя практической точке зрения, уязвимость должна отражать некоторую негативную особенность конкретного компонента системы (например, уязвимость в том, что конкретный модуль не обеспечивает защиты шифрованием) — *потребность*. С другой стороны, понятие *недостатка* на уровне целой системы является крайне абстрактным, а точнее усредненным по всем компонентам системы, которые при этом могут быть различным и зависеть от реализации (например, уязвимость в том, что все компоненты не реализуют механизмов шифрования) — *возможность*. Для частичного сглаживания данного противоречия и в интересах классификации уязвимостей, несущей практическую пользу и применимой для любых реализаций транспортных инфраструктур Умного города (и, соответственно, их интерфейсов, искусственных интеллектов, способов взаимодействия с ними человека), воспользуемся подходом, строящимся на следующих предпосылках.

Во-первых, для обозначения процесса взаимодействия в рамках Умного города целесообразно ввести качественно отличные и разноцелевые сущности, обменивающиеся информацией посредством интерфейсов. В случае транспортной инфраструктуры Умного города удачным делением на такие сущности (далее — Сущность) является следующее: 1) инфраструктура — сама реализация концепции (например, умные информационные знаки, пункты оплаты, система мониторинга и парковок и др.); 2) беспилотное транспортное средство (далее — БТС) — средство для перевозки пас-

сажиров и товаров (например, автомобили, автобусы и троллейбусы); 3) окружение — внешние элементы инфраструктуры, не являющиеся частью сети Умного города, но необходимые для выполнения функций последнего (погода, пассажиры, здания, дорожное полотно и др.). В ряде случаев, удобно делить окружение на два элемента: Человек (пассажир, пешеход, водитель) и Пассивный объект (погода, знаки, не беспилотный автомобиль), поскольку первые являются "заказчиками" услуг концепции.

Также будем считать, что каждый из интерфейсов между Сущностями может обеспечиваться целым набором средств (далее — Средство), такими как лидары, радары, камеры, пункты оплаты, микрофоны, светофоры, метеодатчики и т. п.

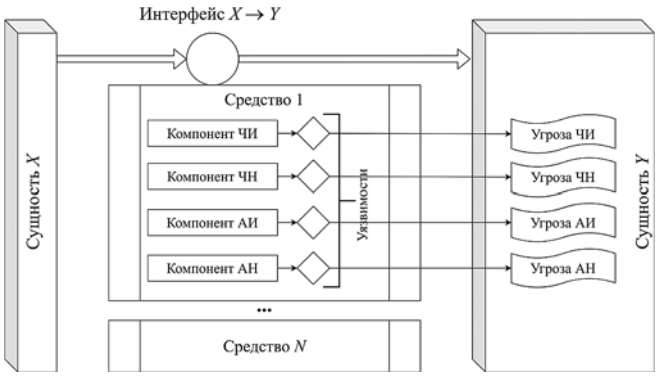
Во-вторых, деление на Сущности позволяет выделить множество классов интерфейсов, каждый из которых ответственен за обмен информацией между парой Сущностей (в том числе между одной и той же). Это приводит к наличию девяти классов следующих интерфейсов (с учетом направления информационного обмена): 1) Инфраструктура ↔ Инфраструктура; 2) Инфраструктура → БТС; 3) Инфраструктура → Окружение; 4) БТС → Инфраструктура; 5) БТС → БТС; 6) БТС → Окружение; 7) Окружение → Инфраструктура; 8) Окружение → БТС; 9) Окружение → Окружение.

В-третьих, каждое из Средств за счет наличия в нем уязвимостей как раз и выводит транспортную инфраструктуру из такого "идеального" состояния. Это можно обосновать тем, что Средство состоит из компонентов, имеющих некоторый функционал по обслуживанию информационных потоков или их логических групп различных типов; нарушение же работы компонента соответственно приведет и к нарушению числа информационных потоков (увеличению или уменьшению).

В-четвертых, поскольку наличие уязвимости так или иначе приводит к некоторой угрозе, то характеристики уязвимостей и угроз должны некоторым образом коррелировать. Для деления последних на классы можно воспользоваться подходом категориального деления, когда сложный объект разбивается на так называемые категориальные пары, элементы которых представляют собой противоположности с некоторой точки зрения [16]. Так, в качестве одной пары удобно выбрать пару *Человек vs Автомат*: первый элемент обладает волей, для него предназначается концепция Умного города, второй же — субъект без воли, реализующий необходимый функционал концепции в интересах первого. В качестве другой пары можно выбрать отражающую некоторый эффект нарушения информационной безопасности с позиции наличия информационных потоков, а именно пару *Избыточность vs Недостаточность*: первый элемент соответствует появлению нового потока (аналог нарушения конфиденциальности, когда информация "утекает" третьим лицам), а второй — исчезновению потока (нарушение доступности, когда информация не достигает законного получателя). Комбинация же элементов пар дает четыре класса, ответственных за нарушения информационных потоков, т. е. классификацию угроз: 1) избыточность информационных потоков, ориентированных на Человека (угроза ЧИ); 2) избыточность информационных потоков, ориентированных на Автомат (угроза АИ); 3) недостаточность информационных потоков, ориентированных на Человека (угроза ЧН); 4) недостаточность информационных потоков, ориентированных на Автомат (угроза АН).

В-пятых, существует состояние транспортной инфраструктуры, условно называемое "идеальным" (как правило, достижимое лишь теоретически), в котором Средства не имеют уязвимостей (и, следовательно, отсутствует возможность реализации угроз), а все информационные потоки считаются корректными. Иными словами, такая система находится в некотором локальном максимуме (с позиции безопасности), а появление любой уязвимости приводит к отклонению от этого экстремума вследствие появления новых или исчезновения существующих информационных потоков (что соответствует элементам категориальной пары).

В-шестых, исходя из связи функционала уязвимостей с угрозами, поделенными ранее на четыре подкласса, можно предположить и наличие в Средстве такого же числа групп компонентов (или меньшего для Средств без соответствующего функционала), каждый из которых несет соответствующий информационно-деструктивный эффект. Для простоты и без потери корректности будущей классификации будем считать, что в каждой группе находится лишь один компонент, т. е. Средство состоит из четырех компонентов, наличие уязвимости в каждом из которых приводит к одному из нарушений информации в Сущности (выбираемой согласно направлению информационного обмена через интерфейс, реализуемый Средством). Можно дать следующую, более встречаемую в практике, интерпретацию эффекта от наличия уязвимостей в каждом из таких компонент Средства: в первом произойдет утечка пользовательских



Концептуальная модель терминологической базы предметной области

данных или несанкционированный доступ (появится новый поток Человека); во втором пользователь не получит запрашиваемую информацию или не сможет ее отправить получающей стороне (исчезнет старый поток Человека); в третьем будут передаваться излишние или некорректные служебные данные (появится новый поток Автомата); в четвертом система не сможет корректно функционировать из-за отсутствия или нарушения обмена служебной информацией (исчезнет старый поток Автомата).

Концептуальная модель описанной выше терминологической базы предметной области — Сущностей, интерфейсов, Средств и их компонентов, уязвимостей, угроз — представлена на рисунке.

Так, на рисунке показано взаимодействие Сущности X с Сущностью Y через Интерфейс $X \to Y$, который может реализовываться множеством Средств (Средство 1, ..., Средство N). При этом в Средстве 1 присутствуют четыре Компонента с функционалом, нарушения в работе которого (при наличии уязвимости) приводит к нарушению информационных потоков, ведущих к соответствующим Угрозам в Сущности Y.

Таким образом, с одной стороны, уязвимости расположены в достаточно конкретных компонентах средств, реализующих интерфейсы между Сущностями, а с другой стороны, уязвимости обобщены негативным эффектом влияния на компоненты, приводящим к угрозам определенного класса. Это позволяет перейти к классификации уязвимостей интерфейсов, которая сглаживает выявленное ранее противоречие.

Формализация классов уязвимостей

Исходя из предложенной концептуальной модели терминологической базы предметной области (см. рисунок) синтезируем единую классификацию уязвимостей, используя выделенные ранее Сущности, а также классификации интерфейсов и угроз.

Каждому из классов уязвимостей может быть дано следующее достаточно формальное, хотя и хорошо понятное человеку, определение:

«Уязвимость класса расположена в Компоненте ZW Средства M, которое реализует Интерфейс $X \to Y$ (т. е. для передачи информации от Сущности X к Сущности Y)", при этом

$$\begin{cases} Z \in \{\text{Человек, Автомат}\}; \\ W \in \{\text{Избыточность, Недостаточность}\}; \\ M \in \text{Implement Interface}\,(X \to Y); \\ X, Y \in \{\text{Инфраструктура, БТС, Окружение}\}; \\ \text{Компонент} \in \text{Composition}\,(M), \end{cases}$$

где Z, W — элементы категориальных пар, определяющие также функционал компонентов Средства; M — одно из средств, реализующих интерфейс (ImplementInterface) $X \to Y$; X и Y — ранее введенные Сущности транспортной инфраструктуры Умного города; Компонент — компонент из состава (Composition) реализующего средства M.

Важной особенностью такой классификации является ее гибкость: она не является однозначной для любой модели транспортной инфраструктуры и учитывает ее конкретные особенности, поскольку зависит от состава средств, реализующих интерфейс, которые могут отличаться как для разных интерфейсов в рамках одной модели инфраструктуры, так и для разных моделей.

Гипотетический пример классификации

Приведем простейший пример предложенной классификации для модели следующей транспортной инфраструктуры. Предположим, что Окружение состоит только из пассажиров, пользующихся услугами такси в виде БТС. Инфраструктура же предоставляет возможность пассажирам заказывать такси непосредственно на остановках путем голосового задания конечного пункта маршрута; при этом для идентификации и авторизации пассажира используется сам голос. Также логично ввести в Инфраструктуру оператора, представляющего собой службу поддержки пассажиров БТС, для чего в средства интерфейсов Инфраструктуры внедрен соответ-

ствующий функционал (запрос помощи, сигнализация о чрезвычайных ситуация с БТС и т. п.). Таким образом, существует интерфейс для связи Окружения (и его элемента — Человека) и Инфраструктуры в виде системы распознавания голоса (аппаратный микрофон + программное обеспечение) и кнопки экстренного вызова оператора. Как следствие, будет существовать интерфейс между Инфраструктурой и БТС, обеспечивающий выдачу задания последнему на доставку пассажира, его контроля и т. п.; однако для простоты классификации уязвимостей ограничимся лишь первым.

После идентификации пассажира и доставки его на указанное место Инфраструктура автоматически проводит расчет путем взимания с пользователя необходимой денежной суммы.

Теперь исходя из предложенной классификации опишем каждую из возможных уязвимостей. Согласно формальному определению классов между Инфраструктурой и БТС возможно по одной уязвимости в каждом из четырех компонентов средства, реализующего интерфейс системы распознавания голоса и экстренного вызова оператора:

1) компонент ЧИ, уязвимость в котором приводит к новому информационному потоку данных человека; например, недостатки в алгоритмах работы системы взаимодействия со службой поддержки БТС может привести к тому, что конфиденциальная информация, передаваемая от пользователя оператору, окажется у третьих лиц (например, пассажир на другой остановке узнает о местоположении первого);

2) компонент ЧН, уязвимость в котором приводит к пропаже существующего информационного потока; например, из-за неэффективной балансировки голосового трафика в час пик пассажир не сможет экстренно сообщить оператору Инфраструктуры, о том, что БТС неисправно или попало в ДТП;

3) компонент АИ, уязвимость в котором приводит к новому информационному потоку данных автомата; например, система распознавания голоса некорректно распознала неизвестного пользователя, приняв его за существующего пассажира, что привело к бесплатному проезду первого за счет второго;

4) компонент АН, уязвимость в котором приводит к пропаже существующего информационного потока данных автомата; например, система избавления от шумов привела к тому, что голос пользователя не был распознан из-за низкого качества, что привело к невозможности пассажира доехать до пункта назначения.

Выводы

Приведенная классификация позволяет отнести любую уязвимость в интерфейсах транспортной инфраструктуры Умного города, использование которой прямо или косвенно приводит к соответствующим угрозам, к одному из классов, зависящих от конкретной модели инфраструктуры — числа Сущностей и интерфейсов их взаимодействий, средств реализации интерфейсов, функционала их компонентов. Отличительными особенностями по сравнению с множеством других классификаций являются следующие. Во-первых, в основу каждого класса уязвимостей заложена как ее "заточенность" под конкретный интерфейс (за счет его реализации средствами), так и обобщающие факторы (влияние на абстрактные информационные потоки). Во-вторых, любая из уязвимостей будет обязательно относиться к одному из классов, при этом невозможна ситуация отнесения уязвимости сразу к двум классам.

Если же какая-либо уязвимость не поддается корректной классификации, то значит, что она расположена не в рассматриваемом интерфейсе или ведет не к информационным угрозам, и, следовательно, ее выявление рассматривается в соответствующей отдельной предметной области, выходящей за рамки данной области уязвимостей в интерфейсах транспортной инфраструктуры Умного города.

Направлением дальнейшего исследования должна стать разработка методов обнаружения уязвимостей интерфейсов, что частично является продолжением предыдущих авторских работ, посвященных поиску уязвимостей в программном коде телекоммуникационных устройств, в особенности при отсутствии исходного кода [17—25].

Список литературы

1. **Глебова И. С., Ясницкая Я. С.** Возможности реализации концепции "умного города": практика российских городов // Экономика и предпринимательство. 2014. № 1-3 (42). С. 232—235.

2. **Ярош Н. Н.** Городское хозяйство: от "города солнца" к умному городу // Экономический журнал. 2013. № 2 (30). С. 72—88.

3. **Buinevich M., Izrailov K., Stolyarova E., Vladyko A.** Combine method of forecasting VANET cybersecurity for application of high priority way // 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, South Korea. 2018. P. 266—271.

4. **Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A.** Software defined internet of things: cyber antifragility and vulnerability forecast // Application of information and communication technologies (AICT). 2017. P. 293—297.

5. **Буйневич М. В., Щербаков О. В., Владыко А. Г., Израилов К. Е.** Архитектурные уязвимости моделей телекоммуникационных сетей // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2015. № 4. С. 86—93.

6. **Вебб С.** Безопасность умных городов // Технологии и средства связи. 2015. № 3 (108). С. 30—32.

7. **Красильников А. А.** Угрозы информационной безопасности в развитии умных городов // Форум молодых ученых. 2019. № 2 (30). С. 839—844.

8. **Ефременко И. П., Колодезная Г. В.** Безопасность и конфиденциальность "умного города" в сетях 5G // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. 2020. Т. 1. С. 114—118.

9. **Бессольцев В. Е., Марков П. Н., Сазонов К. В.** Уязвимости интерфейса пользователя веб-приложения // Труды Военно-космической академии имени А. Ф. Можайского. 2018. № 660. С. 100—110.

10. **Бессольцев В. Е., Марков П. Н.** Уязвимости веб сервисов, используемых в автоматизированных системах управления // I-methods. 2018. Т. 10, № 3. С. 23—35.

11. **Раздобаров А. В., Петухов А. А., Гамаюнов Д. Ю.** Проблемы обнаружения уязвимостей в современных Веб-приложениях // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 64—69.

12. **Alqahtani A., Tipper D., Kelly-Pitou K., Babay A.** Identifying Vulnerable Critical Infrastructure Zones in Smart Cities // 16th International Conference on the Design of Reliable Communication Networks DRCN, Milano, Italy. 2020. P. 1—7.

13. **Tubaishat A., Jouhi M. A.** Building a Security Framework for Smart Cities: A Case Study from UAE // 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China. 2020. P. 477—481.

14. **Моисеев Д. В., Брюховецкий А. А., Скатков А. В.** Адаптивное обнаружение уязвимостей интерфейсов БТС // Modern Science. 2020. № 8-1. С. 375—378.

15. **Скатков А. В., Брюховецкий А. А., Доронина Ю. В., Моисеев Д. В., Скатков И. А., Ченгарь О. В.** Адаптивное обнаружение уязвимостей интерфейсов беспилотных транспортных средств. Симферополь: Издательство Типография "Ариал", 2020. 352 с.

16. **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.

17. **Израилов К. Е., Покусов В. В.** Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура [Электронный ресурс] // Информационные технологии и телекоммуникации. 2016. Т. 4, № 4. С. 104—121.

18. **Буйневич М. В., Израилов К. Е.** Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 1. Функциональная архитектура [Электронный ресурс] // Информационные технологии и телекоммуникации. 2016. Т. 4, № 1. С. 115—130.

19. **Израилов К. Е.** Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 2. Информационная архитектура [Электронный ресурс] // Информационные технологии и телекоммуникации. 2016. Т. 4, № 2. С. 86—104.

20. **Израилов К. Е.** Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах: дис.... канд. техн. наук: 05.13.19. СПб., 2017. 261 с.

21. **Buinevich M., Izrailov K.** Method and utility for recovering code algorithms of telecommunication devices for vulnerability search // 16th International Conference on Advanced Communication Technology (ICACT). 2014. P. 172—176.

22. **Buinevich M., Izrailov K., Vladyko A.** Method for partial recovering source code of telecommunication devices for vulnerability search // 17th International Conference On Advanced Communications Technology (ICACT). 2015. P. 76—80.

23. **Buinevich M., Izrailov K., Vladyko A.** Method and prototype of utility for partial recovering source code for low-level and medium-level vulnerability search // 18th International Conference on Advanced Communication Technology (ICACT). 2016. P. 700—707.

24. **Buinevich M., Izrailov K., Vladyko A.** Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices // 19th International Conference on Advanced Communication Technology (ICACT). 2017. P. 408—414.

25. **Buinevich M., Izrailov K., Vladyko A.** Metric of vulnerability at the base of the life cycle of software representations // 20th International Conference on Advanced Communication Technology (ICACT). 2018. P. 1—8.

K. E. Izrailov, PhD, e-mail: konstantin.izrailov@mail.ru,
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg Federal Research Center of the Russian Academy of Sciences

Generalized Classification of Vulnerabilities of Interfaces to the Transport Infrastructure of the Smart City

We consider the problem of classifying the vulnerabilities present in interface devices that are used in the interaction of people and components of the transport infrastructure of the Smart City. A conceptual model of the terminological base of the subject area is introduced, on the basis of which a unified classification of vulnerabilities is synthesized. A formal record of vulnerability classes is given, as well as their examples.

Keywords: *smart city, transport infrastructure, classification, vulnerabilities, information security*

Acknowlegements: This work was financially supported by the Russian Foundation for Basic Research (project No. 19-29-06099).

DOI: 10.17587/it.27.330-336

References

1. **Glebova I. S., Yasnitskaya Ya. S.** Possibilities of implementing the concept of "smart city": the practice of Russian cities, *Ekonomika i predprinimatel'stvo,* 2014, no. 1—3 (42), pp. 232—235 (in Russian).

2. **Yarosh N. N.** Urban economy: from the "city of the sun" to the smart city, *Ekonomicheskiy zhurnal,* 2013, no. 2 (30), pp. 72—88 (in Russian).

3. **Buinevich M., Izrailov K., Stolyarova E., Vladyko A.** Combine method of forecasting VANET cybersecurity for application of high priority way, *20th International Conference on Advanced Communication Technology (ICACT),* Chuncheon, South Korea, 2018, pp. 266—271.

4. **Buinevich M., Izrailov K., Stolyarova E., Vladyko A.** Software defined internet of things: cyber antifragility and vulnerability forecast, *Application of information and communication technologies (AICT)*, 2017, pp. 293—297.

5. **Buynevich M. V., Shcherbakov O. V., Vladyko A. G., Izrailov K. Ye.** Architectural vulnerabilities of telecommunication network models, *Nauchno-analiticheskiy zhurnal Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoy protivopozharnoy sluzhby MCHS Rossii*, 2015, no. 4, pp. 86—93 (in Russian).

6. **Vebb S.** Smart city safety, *Tekhnologii i sredstva svyaz,* 2015, no. 3 (108), pp. 30—32 (in Russian).

7. **Krasilnikov A. A.** Information security threats in the development of smart cities, *Forum molodykh uchenykh*, 2019, no. 2 (30), pp. 839—844 (in Russian).

8. **Yefremenko I. P., Kolodeznaya G. V.** 5G Smart City Security and Privacy, *Nauchno-tekhnicheskoye i ekonomicheskoye sotrudnichestvo stran ATR v XXI veke*, 2020, vol. 1, pp. 114—118 (in Russian).

9. **Bessol'tsev V. Ye., Markov P. N., Sazonov K. V.** Web Application User Interface Vulnerabilities, *Trudy Voyenno-kosmicheskoy akademii imeni A. F. Mozhayskogo*, 2018, no. 660, pp. 100—110 (in Russian).

10. **Bessol'tsev V. Ye., Markov P. N.** Vulnerabilities of web services used in automated control systems*, I-methods*, 2018, vol. 10, no. 3, pp. 23—35 (in Russian).

11. **Razdobarov A. V., Petukhov A. A., Gamayunov D. Yu.** Vulnerability detection issues in modern web applications, *Problemy informatsionnoy bezopasnosti. Komp'yuternyye sistemy*, 2015, no. 4, pp. 64—69 (in Russian).

12. **Alqahtani A., Tipper D., Kelly-Pitou K., Babay A.** Identifying Vulnerable Critical Infrastructure Zones in Smart Cities, *16th International Conference on the Design of Reliable Communication Networks DRCN*, Milano, Italy, 2020, pp. 1—7.

13. **Tubaishat A., Jouhi M. A.** Building a Security Framework for Smart Cities: A Case Study from UAE, *5th International Conference on Computer and Communication Systems (ICCCS),* Shanghai, China, 2020, pp. 477—481.

14. **Moiseyev D. V., Bryukhovetskiy A. A., Skatkov A. V.** Adaptive Vulnerability Detection for BTS Interfaces, *Modern Science*, 2020, no. 8-1, pp. 375—378 (in Russian).

15. **Skatkov A. V., Bryukhovetskiy A. A., Doronina Yu. V., Moiseyev D. V., Skatkov I. A., Chengar' O. V.** Adaptive Vulnerability Discovery of Unmanned Vehicle Interfaces: A Monograph, Simferopol', Publishing house Tipografiya "Arial", 2020, 352 p. (in Russian).

16. **Buynevich M. V., Izrailov K. Ye.** Categorical synthesis and technological analysis of options for safe import substitution of software for telecommunications devices, *Informatsionnyye tekhnologii i telekommunikatsii*, 2016. vol. 4, no. 3, pp. 95—106 (in Russian).

17. **Izrailov K. Ye., Pokusov V. V.** A utility for searching for vulnerabilities in the software of telecommunication devices using machine code algorithms. Part 3. Modular-algorithmic architecture [Electronic resource], *Informatsionnyye tekhnologii i telekommunikatsii*, 2016, vol. 4, no 4, pp. 104—121 (in Russian).

18. **Buynevich M. V., Izrailov K. Ye.** A utility for searching for vulnerabilities in the software of telecommunication devices using machine code algorithms. Part 1. Functional architecture [Electronic resource], *Informatsionnyye tekhnologii i telekommunikatsii*, 2016, vol. 4, no. 1, pp. 115-130 (in Russian).

19. **Izrailov K. Ye.** A utility for searching for vulnerabilities in the software of telecommunication devices using machine code algorithms. Part 2. Information architecture [Electronic resource], *Informatsionnyye tekhnologii i telekommunikatsii*, 2016, vol. 4, no. 2, pp. 86—104 (in Russian).

20. **Izrailov K. Ye.** Algorithmization method for machine code to find vulnerabilities in telecommunication devices: dis. ... Cand. tech. sciences: 05.13.19, SPb., 2017, 261 p (in Russian).

21. **Buinevich M., Izrailov K.** Method and utility for recovering code algorithms of telecommunication devices for vulnerability search, *16th International Conference on Advanced Communication Technology (ICACT),* 2014, pp. 172—176.

22. **Buinevich M., Izrailov K., Vladyko A.** Method for partial recovering source code of telecommunication devices for vulnerability search, *17th International Conference On Advanced Communications Technology (ICACT)*, 2015, pp. 76—80.

23. **Buinevich M., Izrailov K., Vladyko A.** Method and prototype of utility for partial recovering source code for low-level and medium-level vulnerability search, *18th International Conference on Advanced Communication Technology (ICACT),* 2016, pp. 700—707.

24. **Buinevich M., Izrailov K., Vladyko A.** Testing of Utilities for Finding Vulnerabilities in the Machine Code of Telecommunication Devices, *19th International Conference on Advanced Communication Technology (ICACT),* 2017, pp. 408—414.

25. **Buinevich M., Izrailov K., Vladyko A. M.** Metric of vulnerability at the base of the life cycle of software representations, *20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 1—8.

Адрес редакции:

107076, Москва, Стромынский пер., 4

Телефон редакции журнала **(499) 269-5510**

E-mail: it@novtex.ru

Технический редактор *Е. В. Конова*.
Корректор *М. Ю. Безменова*.
Сдано в набор 10.04.2021. Подписано в печать 25.05.2021. Формат 60×88 1/8. Бумага офсетная.
Усл. печ. л. 8,86. Заказ IT621. Цена договорная.

Журнал зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-15565 от 02 июня 2003 г.

Оригинал-макет ООО "Адвансед солюшнз". Отпечатано в ООО "Адвансед солюшнз".
119071, г. Москва, Ленинский пр-т, д. 19, стр. 1. Сайт: **www.aov.ru**