

Петров Дмитрий Ильич

доцент

Бородин Андрей Викторович

канд. экон. наук, доцент, заведующий кафедрой

Пауткин Егор Алексеевич

студент

ФГБОУ ВО «Поволжский государственный

технологический университет»

г. Йошкар-Ола, Республика Марий Эл

DOI 10.21661/r-463557

ОБ АРХИТЕКТУРЕ ДОМАШНИХ СЕТЕЙ СЕГМЕНТА ENTERPRISE

***Аннотация:** исследователями разработана онтологическая модель требований к современной мультисервисной домашней сети сегмента Enterprise. На основе этой модели синтезирована архитектура вычислительной сети и выбраны базовые технологии для ее реализации.*

***Ключевые слова:** архитектура вычислительной сети, безопасность, масштабируемость, мультисервисная сеть, онтологическая модель, риск, экономика безопасности, IDEF5.*

Сложность домашних сетей растет. Сегодня никого не удивляет присутствие в IT-инфраструктуре домашнего хозяйства подсистемы видеонаблюдения, службы дистрибуции точного времени, заметного количества различных датчиков и исполнительных устройств, управляемых через сети передачи данных (СПД). И это, не считая множества традиционных сетевых гаджетов, таких, как смартфоны, ноутбуки, телевизоры последних поколений и т. п. Такое многообразие сетевых устройств делает домашнюю сеть плохо управляемой, вызывает определенные сложности при поиске и устранении неисправностей, снижает производительность сети. Резко падает, наконец, безопасность такой сетевой инфраструктуры. См., например, работы [7–10], в которых на основе стохастического моделирования показан рост ущерба в зависимости от количества узлов в

сети при различных стратегиях кооперации атакующих агентов, постановка этой задачи дана в книге [6].

И хотя по количеству узлов, объему трафика такая сеть остается по прежнему относящейся к сегменту SOHO, тем не менее, по количеству потенциально возможных подсистем и связей между ними она, порой, может выходить даже за рамки корпоративного сегмента СПД. Именно в этом смысле в данной статье речь пойдет о домашних сетях сегмента Enterprise.

Целью данной работы является разработка масштабируемой архитектуры домашней сети на основе базовых технологий маршрутизации, списков доступа и VLAN. Сегментация сети при этом должна обеспечивать максимизацию производительности и безопасности при сохранении работоспособности основных сетевых сервисов, востребованных пользователями домашних сетей. При этом должны быть предусмотрены как минимум три категории пользователей: администраторы, доверенные пользователи и гости.

В качестве основного подхода к решению поставленной задачи была использована методология, представленная в работах [1; 3; 12] и использующая нотацию IDEF5 [2].

Онтологическая модель типовой мультисервисной домашней сети в нотации IDEF5 представлена на рисунке 1. Словарь модели представлен в таблице 1.

Особенностью рассматриваемой онтологической модели является построение ее в следующей последовательности:

- 1) классификация хостов сети;
- 2) выявление угроз, характерных для хостов различных классов;
- 3) классификация угроз;
- 4) добавление онтологий, определяющих ограничения на топологию сети.

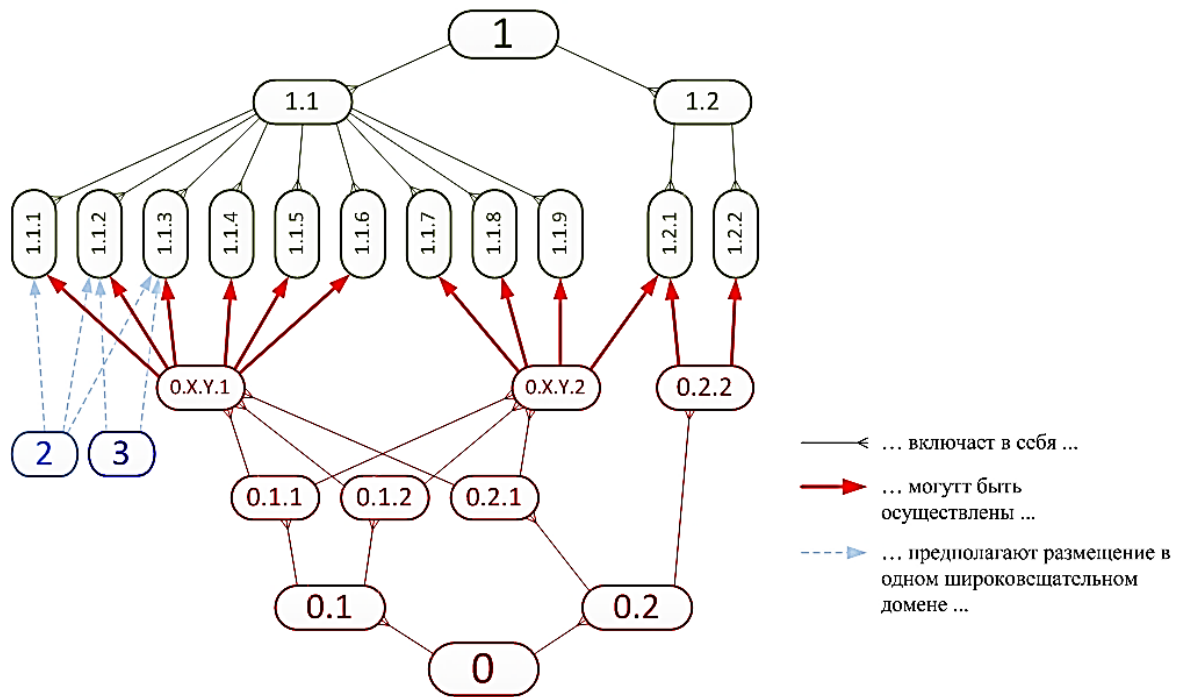


Рис. 1. Онтологическая модель типовой мультисервисной домашней вычислительной сети

Таблица 1

Словарь онтологической модели типовой мультисервисной домашней вычислительной сети

Идентификатор	Описание
1	Домашняя сеть
1.1	Доверенные устройства
1.1.1	Домашние компьютеры
1.1.2	Мобильные устройства (ноутбуки, планшеты, смартфоны и т. п.)
1.1.3	Аудиовизуальные устройства (телевизоры, плееры и т. п.)
1.1.4	IP-телефоны
1.1.5	Сервис печати
1.1.6	Сервера
1.1.7	Устройства Интернета вещей (IoT), критические сервисы
1.1.8	IoT, некритические сервисы
1.1.9	Подсистема видеонаблюдения
1.2	Группа гостевых устройств
1.2.1	Карантинная зона
1.2.2	Гостевые мобильные устройства
0	Угрозы
0.1	Локальные угрозы

0.1.1	Атаки со стороны устройств гостевой зоны
0.1.2	Атаки со стороны доверенных устройств
0.2	Внешние угрозы
0.2.1	Атаки из сети Internet
0.2.2	Несанкционированное взаимодействие с хостами сети Internet
0.X.Y.1	Атаки со стандартной вероятностью успеха
0.X.Y.2	Атаки с повышенной вероятностью успеха
2	Общие требования технологии «jointSPACE» компании PHILIPS [13, 14] и других аналогичных технологий
3	Общие требования технологии «AirPlay» компании Apple [11]

Другими словами, в данной работе онтологическая модель строится по схеме «от оборудования к угрозам» при заданных перечнях противодействий и ограничений.

Заметим, что описанная модель отличается от традиционных моделей, формируемых в рамках методологии [1; 3; 12], например, таких, как модель угроз процесса отчужденной обработки документов [4; 5], в которой принцип построения можно охарактеризовать схемой «от перечня угроз к перечню противодействий» с возможными классификациями угроз и противодействий и с возможным выделением причинно-следственных связей на множествах, как угроз, так и противодействий. Однако отличие схем построения онтологических моделей в разных случаях лишь подчеркивает универсальность используемой методологии.

На основе построенной онтологической модели был осуществлен синтез архитектуры домашней мультисервисной сети. Результат синтеза представлен на рисунке 2.

Решение использует: 1) маршрутизатор, поддерживающий транковые соединения с коммутатором, технологии трансляции IP-адресов и портов, а также входящие и исходящие списки доступа на интерфейсах; 2) управляемый коммутатор второго уровня, поддерживающий технологию VLAN; 3) одну или несколько точек доступа, поддерживающих технологию VAP.

В заключение отметим, что в рамках данной работы была построена онтологическая модель требований к современной мультисервисной домашней сети.

В ходе построения модели были апробированы альтернативные сценарии синтеза онтологических моделей экономики безопасности в рамках методологии, представленной в работах [1; 3; 12]. На основе этой модели была синтезирована масштабируемая архитектура домашней сети сегмента Enterprise.

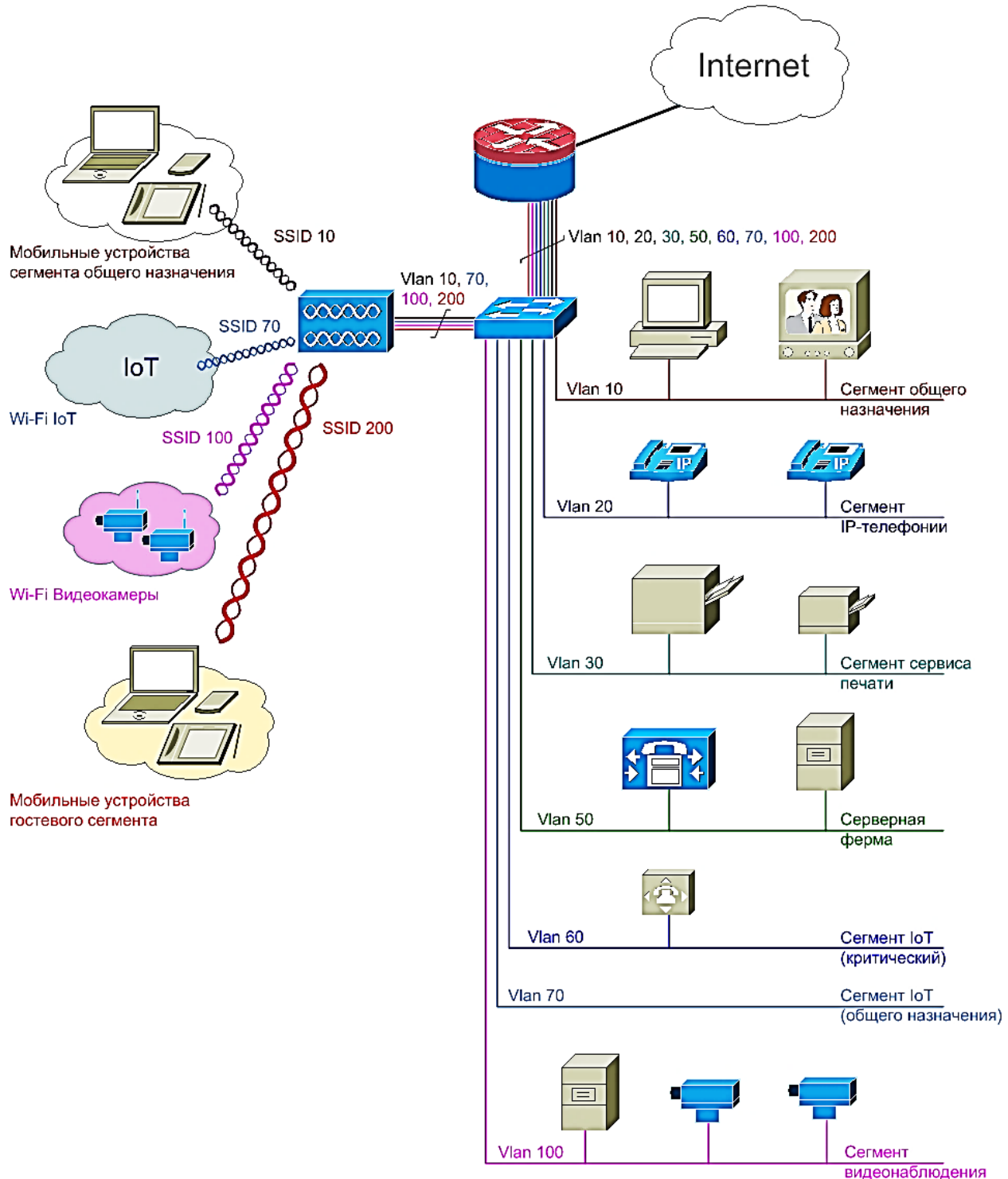


Рис. 2. Архитектура домашней мультисервисной сети

В качестве одного из направлений дальнейших исследований следует указать разработку формального метода синтеза (пригодных для экономической оценки технических решений) событийных моделей на основе онтологических. При этом метод синтеза не должен зависеть от используемой схемы построения онтологий. Отдельного исследования заслуживает экономическая оценка рисков, связанных с эксплуатацией домашней сети предложенной архитектуры.

Список литературы

1. Бородин А.В. Методологические основы моделирования в задачах экономики безопасности / А.В. Бородин // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 217–222.
2. Бородин А.В. Метод онтологического анализа IDEF5 в задачах структурного синтеза динамических моделей угроз / А. В. Бородин // Обзорное прикладной и промышленной математики. – 2006. – Т. 13. – №3. – С. 474–475.
3. Бородин А.В. Онтологические модели в экономике безопасности / А.В. Бородин // Труды Поволжского государственного технологического университета. Серия: Социально-экономическая. – 2014. – №2. – С. 14–19.
4. Бородин А.В. Синтез политики безопасности для процессов отчужденной обработки информации на основе онтологического анализа предметной области / А.В. Бородин // IX Международная научно-практическая конференция «Инновационное развитие российской экономики»: Т. 3: Информационно-коммуникационные технологии. – М.: ФГБОУ ВО «РЭУ им. Г.В. Плеханова», 2016. – С. 14–16.
5. Бородин А.В. Техничко-экономическое обоснование внедрения технологии обеспечения целостности и подлинности информации на бумажном носителе при отчужденной обработке документов / А.В. Бородин // Кибернетика и программирование. – 2017. – №1. – С. 30–47. – DOI: 10.7256/2306–4196.2017.1.22192.

6. Бородин А.В. Феномен компьютерных вирусов: элементы теории и экономика существования / А.В. Бородин. – Йошкар-Ола: Марийский государственный технический университет, 2004. – 144 с.

7. Уразаева Т.А. Инструментальные методы анализа риска в экономике безопасности вычислительных сетей / Т.А. Уразаева // III Международная научно-практическая конференция «Инновационное развитие Российской экономики». Ч. 1. – М.: Московский государственный университет экономики, статистики и информатики, 2010. – С. 246–250.

8. Уразаева Т.А. Модели риска в технико-экономическом обосновании инфраструктурных решений / Т.А. Уразаева // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов: сборник статей. – Йошкар-Ола: Поволжский государственный технологический университет, 2015. – С. 161–164.

9. Уразаева Т.А. Совокупная стоимость владения и риск в задачах инфраструктурной оптимизации вычислительных сетей / Т.А. Уразаева // Моделирование и анализ безопасности и риска в сложных системах: Труды Международной научной школы МАБР-2009. – СПб.: ГУАП, 2009. – С. 315–320.

10. Уразаева Т.А. Стоимостной анализ риска нарушения одной политики безопасности в вычислительных сетях / Т.А. Уразаева // Моделирование и анализ безопасности и риска в сложных системах: Труды Международной научной школы МА БР-2010. – СПб.: ГУАП, 2010. – С. 193–199.

11. AirPlay // Википедия. Свободная энциклопедия [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/AirPlay>

12. Borodin A.V. System of instrumental and mathematical methods of the solution of task of economy of safety / A.V. Borodin // Global Science and Innovation: materials of the III International Scientific Conference (Chicago, October 23–24th, 2014). – Chicago: Publishing office Accent Graphics communications, 2014. – P. 314–317.

13. JointSpace // Ago control wiki [Электронный ресурс]. – Режим доступа: <https://wiki.agocontrol.com/index.php/JointSpace>

14. JointSPACE API Reference Manual. Version 2.2 PHILIPS, 2011 [Электронный ресурс]. – Режим доступа: http://jointspace.sourceforge.net/project-data/jointSPACE_API_Reference_Manual.pdf