БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 3 (114). – 53–62

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2024-3-53-62

К ВОПРОСУ РЕАЛИЗАЦИИ АЛГОРИТМОВ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ*

Г.В. ПОПКОВ

630102, РФ, г. Новосибирск, ул. Кирова, 86, Сибирский государственный университет телекоммуникаций и информатики, кандидат технических наук, заведующий кафедрой защиты информации в социальных системах. E-mail: glebpopkov@inbox.ru

Существующие подходы проектирования защищенных сетей передачи данных (ЗСПД) зачастую базируются на руководящих документах для проектирования сетей связи в широком смысле, в настоящий момент отсутствуют четкие регламенты для проектирования сетей связи в защищенном исполнении с точки зрения информационной безопасности. В процессе перспективного проектирования ЗСПД возникают проблемы поиска эффективных решений построения такого рода сетей связи и обеспечения информационной безопасности ЗСПД в части средств защиты информации (СЗИ) в заданных границах, определяемых измерениями информационной безопасности, таких как целостность, доступность, секретность информации, циркулирующей в ЗСПД. В статье предлагаются алгоритмы, базирующиеся на параметрах нестационарных гиперсетевых моделей, позволяющие реализовывать анализ и синтез ЗСПД, а также учитывать исходные данные по предполагаемым пользователям, сервисам / приложениям, реализуемым на ЗСПД в условиях внешних деструктивных воздействий (ВДВ).

Ключевые слова: сети передачи данных, информационная безопасность, целостность, доступность информации, гиперсетевые модели, устойчивость сетей передачи данных

ВВЕДЕНИЕ

Исходя из парадигмы проектирования защищенных сетей передачи данных (ЗСПД), устойчивых к внешним деструктивным воздействиям (ВДВ), в рамках систем принятия и поддержки решений (СППР) предлагаются алгоритмы, позволяющие использовать перспективные подходы для проектирования ЗСПД, работающих в условиях ВДВ.

* Статья получена 14 августа 2024 г.

1. ОПИСАНИЕ ЗАДАЧИ

Исходными данными при проектировании являются:

1) количество потребителей услуг ЗСПД;

2) набор и тип телекоммуникационных услуг, соответствующих потребителям;

3) территория, охватываемая ЗСПД (топооснова);

4) набор и типы систем связи, предполагаемых для создания ЗСПД;

5) типы нарушителей ИБ;

6) виды актуальных угроз на ЗСПД;

7) онтологии уязвимостей программно-аппаратного обеспечения предполагаемых систем связи;

8) риски, связанные с нарушением режима ИБ ЗСПД.

Для реализации анализа и синтеза ЗСПД автором была предложена нестационарная гиперсетевая [6, 7] модель *G-Net* в статье [1], используемая в системе проектирования (рис. 1), уровни модели задают параметры ЗСПД, соответствующие нижним четырем уровням модели *OSI* (open interconnect model) [2].

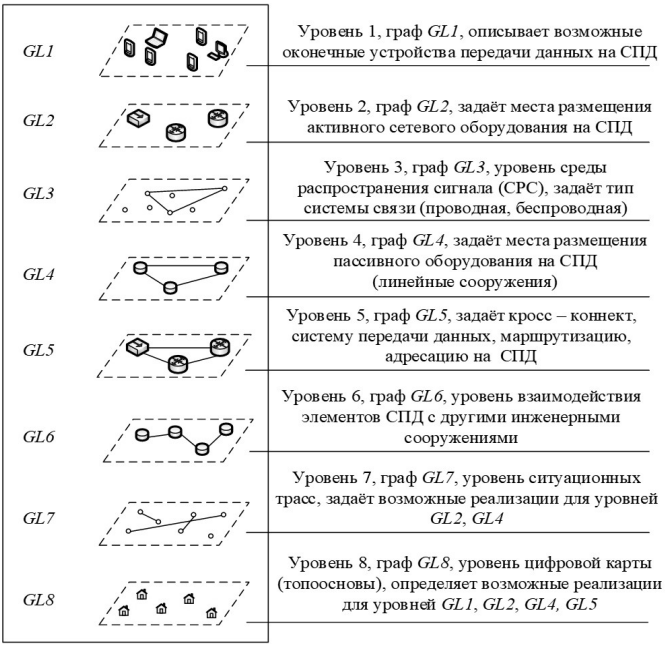

Рис. 1. Уровни нестационарной гиперсетевой модели *G-Net* СПД

2. АЛГОРИТМЫ D11, D12

На рис. 2 приведен укрупненный алгоритм D11, позволяющий проектировать защищенные СПД, устойчивые к ВДВ с ограничениями.

Шаг 1. Формирование структуры абонентов ЗСПД с учетом типа предполагаемых услуг $U_i[n..m]Gl_1$, теоретически количество пользователей ничем не ограничено либо ограничено параметрами уровня Gl_5.

Шаг 2. Определение границ предоставления услуг ЗСПД, ввод данных о местоположении пользователей на предполагаемой территории обслуживания сети ЗСПД вида $U_i[n..m]Gl_8$.

Шаг 3. Формирование структуры услуг ЗСПД, ввод данных о структуре и типе услуг на ЗСПД. Вывод промежуточных результатов по границам районов оказания услуг и необходимым потребностям в *i*-х услугах. Если результаты по услугам меньше требуемых, то переход на шаг 1.

Шаг 4. Формирование требований к заданному уровню измерений ИБ, целостности, доступности, структурной надежности, живучести элементов ЗСПД (программного обеспечения, коммутационных узлов, линейных сооружений) [8–10].

Шаг 5. Формирование профиля атаки с учетом модели нарушителя, модели угроз на сегменты ЗСПД с использованием баз *MITRE*, *CVSS*, ФСТЭК РФ.

Шаг 6. Задание узловой основы для транспортного сегмента ЗСПД с учетом уровней Gl_1, Gl_3, Gl_8.

Шаг 7. Решение о выборе системы связи с учетом вектора атаки на основании решений, принятых на уровнях Gl_2, Gl_4, Gl_5, Gl_6.

Шаг 8. Ранжирование критически значимых элементов ЗСПД согласно уровням модели *G-NET*, ввод данных о критически важных элементах *NE*.

Шаг 9. Формирование структуры проектируемой ЗСПД (кластера сети) с учетом выбранной системы связи и данных с уровней Gl_2, Gl_4, Gl_5, Gl_6.

Шаг 10. Решение задач маршрутизации на ЗСПД, ввод актуальных данных об известных угрозах на уровень маршрутизации (уровень Gl_5).

Шаг 11. Расчет значений устойчивости, проектируемой ЗСПД с учетом шага 7 (задание параметров надежности, живучести элементов ЗСПД).

Шаг 12. Определение показателей защищенности элементов ЗСПД с учетом выбранной системы связи, вектора атаки, применяемых методов избыточности (резервирования элементов ЗСПД), информации об уровнях Gl_2, Gl_4, Gl_5, Gl_6.

Шаг 13. Формирование структуры ЗСПД с учетом выбранной системы связи, вектора атаки, вывода результатов. Если результат удовлетворяет требованиям, то завершение работы алгоритма, если результат и условия не удовлетворяют шагу 4, то переход на шаг 5.

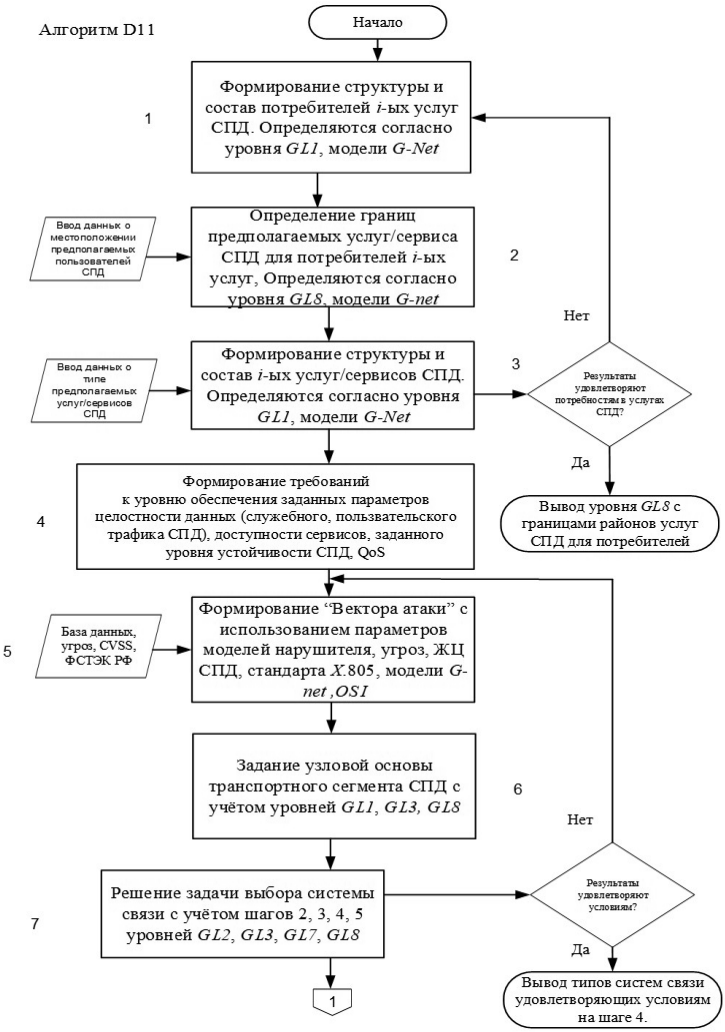

Рис. 2. Алгоритм D11

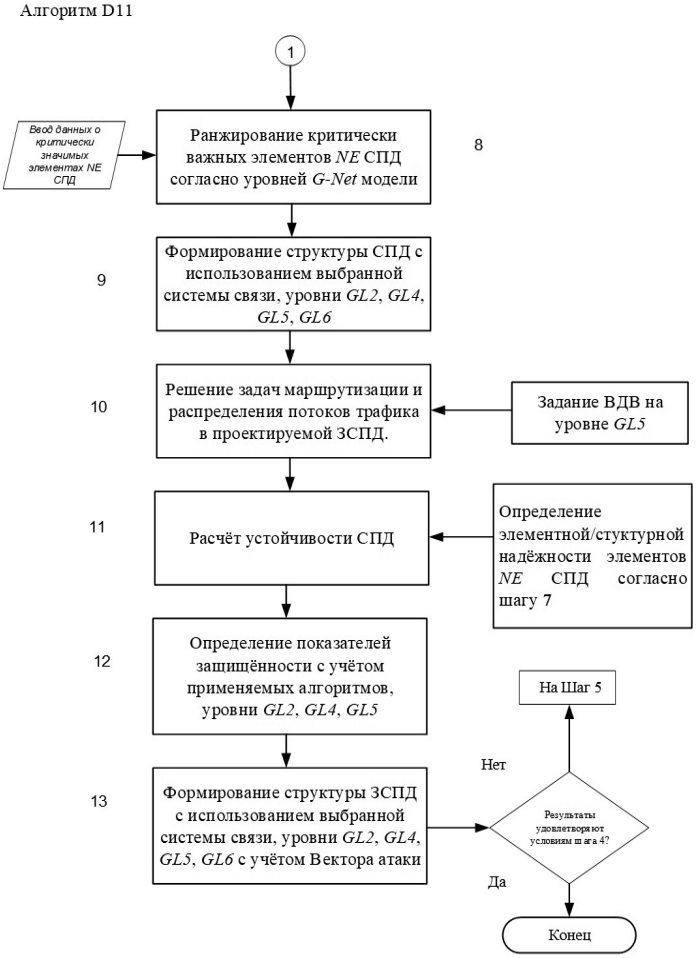

Рис. 2. Окончание

Рассмотренные алгоритмы являются частью системы СППР, основанной на задачном подходе [3, 4].

Очевидно, что предложенные алгоритмы являются частным случаем методики проектирования защищенных автоматизированных систем [5] и не противоречат нормативным документам, принятым в Российской Федерации.

Важнейшим этапом проектирования ЗСПД является выбор сертифицированных средств защиты информации, удовлетворяющих требованиям ФСТЭК Российской Федерации, по типу защищаемой информации. Выбор средств криптозащиты информации (СКЗИ) определяется на основании регулятивных документов ФСБ Российской Федерации.

На рис. 3 приведен укрупненный алгоритм D12 выбора эффективных средств защиты информации (СЗИ, СКЗИ), проектируемых ЗСПД в широком смысле.

Шаг 1. Анализ проектируемой ЗСПД по заданным параметрам (пропускная способность, система управления, система мониторинга инцидентов безопасности и т. д.).

Шаг 2. Определение критически важной информации, циркулирующей в ЗСПД.

Шаг 3. По итогам анализа определяется, требуется ли создание защищенной СПД.

Шаг 4. Определение класса защищенности.

Шаг 5. Выявление (определение) актуальных угроз для проектируемой ЗСПД.

Шаг 6. Разработка частных моделей нарушителя, частных моделей угроз.

Шаг 7. Формирование требований к средствам СЗИ, СКЗИ.

Шаг 8. Оценка возможности реализации требований по выбранным СЗИ.

Шаг 9. Анализ возможных уязвимостей сетевых элементов ЗСПД.

Шаг 10. Выбор сертифицированных средств СЗИ для проектируемой ЗСПД.

Шаг 11. Определяется, существует ли необходимый комплекс СЗИ. Если да, то переход на шаг 15; если нет, то переход на шаг 12.

Шаг 12. Формирование перечня сертифицированных СЗИ (СрСЗИ) для включения в систему защиты ЗСПД.

Шаг 13. Анализ эффективности выбранных средств СрСЗИ согласно выбранным критериям.

Шаг 14. Формирование / выбор оптимального состава СрСЗИ для комплекса мер защиты ЗСПД по заданным критериям.

Шаг 15. Формирование комплекса защитных средств с выбранными СрСЗИ.

Шаг 16. Анализ эффективности выбранных СрСЗИ.

Шаг 17. Формирование выбранных СрСЗИ для дальнейших проектов по планированию защищенных СПД.

Шаг 18. Определяется, удовлетворяют ли требованиям значения показателей СЗИ, СКЗИ. Если да, то переход на шаг 22; если нет, то переход на шаг 19.

Шаг 19. Оптимизация СЗИ, СКЗИ для проектируемой ЗСПД.

Шаг 20. Определяется, выполняются ли требования к СЗИ. Если да, то переход на шаг 21; если нет, то переход на шаг 10.

Шаг 21. Внедрение / тестирование СЗИ, СКЗИ на ЗСПД.

Шаг 22. Техническая эксплуатация комплексов СЗИ, СКЗИ ЗСПД.

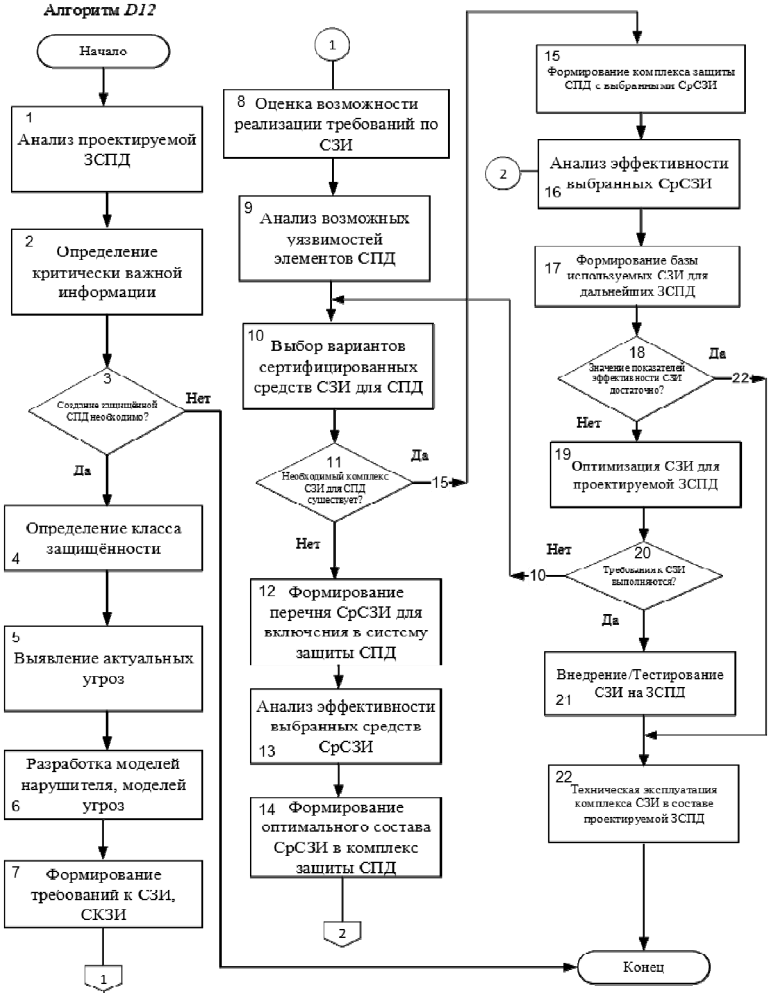

Рис. 3. Укрупненный алгоритм D12

ЗАКЛЮЧЕНИЕ

В статье рассмотрены два алгоритма проектирования защищенных сетей передачи данных, функционирующих в условиях внешних деструктивных воздействий. Эти алгоритмы являются составной частью системы принятия и поддержки решений, в конечном итоге определяющей состав, структуру, функционал защищенной сети связи, а также состав средств защиты информации, реализуемых на ЗСПД. В результате исследования был сделан вывод, что реализация нестационарных гиперсетевых моделей в части формирования задания ЗСПД позволяет проводить эффективный анализ и синтез ЗСПД в условиях ВДВ.

СПИСОК ЛИТЕРАТУРЫ

1. *Попков Г.В.* Перспективное проектирование сети абонентского доступа с использованием восьмиуровневой модели // Программные продукты и системы. – 2016. – № 2. – С. 139–145. – DOI: 10.15827/0236-235X.114.139-145.

2. Open System Interconnection model. CCITT X.200 (ITU-T X.200).

3. *Витяев Е.Е., Гончаров С.С., Свириденко Д.И.* О задачном подходе в искусственном интеллекте // Сибирский философский журнал. – 2019. – Т. 17, № 4. – С. 5–25. – DOI: 10.25205/2541-7517-2019-17-4-5-25.

4. *Витяев Е.Е., Гончаров С.С., Свириденко Д.И.* О задачном подходе в искусственном интеллекте и когнитивных науках // Сибирский философский журнал. – 2020. – Т. 18, № 2. – С. 5–29. – DOI: 10.25205/2541-7517-2020-18-2-5-29.

5. ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – М.: Стандартинформ, 2014.

6. *Попков В.К.* Математические модели связности. – Новосибирск: Изд-во ИВМиМГ СО РАН, 2006. – 490 с.

7. *Свами М., Тхуласираман К.* Графы, сети и алгоритмы. – М.: Мир, 1984. – 455 с.

8. *Назаров А.Н., Сычёв К.И.* Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. – Красноярск: Поликом, 2011. – 491 с.

9. ITU-T Recommendation X.800. Security Architecture for Open Systems Interconnection for CCITT Applications. – ITU, 1991.

10. ITU-T Recommendation X.805. Security Architecture for Systems providing end-to-end Communications. – ITU, 2003.

Попков Глеб Владимирович, кандидат технических наук, заведующий кафедрой защиты информации в социальных системах Сибирского государственного университета телекоммуникаций и информатики Область научных интересов – информационная безопасность. E-mail: glebpopkov@inbox.ru

DOI: 10.17212/2782-2230-2024-3-53-62

On the issue of implementing algorithms for designing secure transmission networks*

G.V. Popkov

Siberian state university of telecommunications and information science, 86 Kirova street, Novosibirsk, 630102, Russian Federation, head of the Department of Information Protection in Social Systems. E-mail: glebpopkov@inbox.ru

Existing approaches to the design of secure data transmission networks (DRN) are often based on guidelines for the design of communication networks in a broad sense, at the moment there are no clear regulations for the design of communication networks in a secure version from the point of view of information security. In the process of advanced design of the SPDS, problems arise in finding effective solutions for the construction of such communication networks and ensuring the information security of the SPDS in terms of information security tools (SIS) in given areas determined by information security measurements, such as the availability, accessibility, secrecy of information circulating in the SPDS. The article proposes algorithms based on the parameters of non-stationary hyper-network models, which make it possible to implement the analysis and synthesis of ZSPD, as well as take into account the initial data on the intended users, services/applications implemented on ZSPD under conditions of external destructive effects (VDV).

Keywords: data transmission networks, information security, integrity, information availability, hypernetwork models, stability of data transmission networks

REFERENCES

1. Popkov G.V. Perspektivnoe proektirovanie seti abonentskogo dostupa s ispol'zovaniem vos'miurovnevoi modeli [Advansed design of a customer access network using an 8-tier model]. *Programmnye produkty i sistemy = Software and Systems*, 2016, no. 2, pp. 139–145. DOI: 10.15827/0236-235X.114.139-145.

2. CCITT X.200. Standard (ITU-T X.200).*Open System Interconnection model*.

3. Vityaev E.E., Goncharov S.S., Sviridenko D.I. O zadachnom podkhode v iskusstvennom intellekte [On the task approach to artificial intelligence]. *Sibirskii*

* *Received 14 August 2024.*

filosofskii zhurnal = Siberian Journal of Philosophy, 2019, vol. 17 (4), pp. 5–25. DOI: 10.25205/2541-7517-2019-17-4-5-25.

4. Vityaev E.E., Goncharov S.S., Sviridenko D.I. O zadachnom podkhode v iskusstvennom intellekte i kognitivnykh naukakh [On the Task Approachin Artificial Intelligenceand Cognitive Sciences]. *Sibirskii filosofskii zhurnal = Siberian Journal of Philosophy*, 2020, vol. 18 (2), pp. 5–29. DOI: 10.25205/2541-7517-2020-18-2-5-29.

5. GOST R 51583–2014. *Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya* [State standard R 51583–2014. Information protection. Sequence of protected operational system formation. General]. Moscow, Standartinform Publ., 2014.

6. Popkov V.K. *Matematicheskie modeli svyaznosti* [Mathematical models of connectivity]. Novosibirsk, IVMiMG SO RAN Publ., 2006. 490 p.

7. Swamy M.N.S., Thulasiraman K. *Grafy, seti i algoritmy* [Graphs, networks and algorithms]. Moscow, Mir Publ., 1984. 455 p. (In Russian).

8. Nazarov A.N., Sychev K.I. *Modeli i metody rascheta pokazatelei kachestva funk-tsionirovaniya uzlovogo oborudovaniya i strukturno-setevykh parametrov setei svyazi sleduyushchego pokoleniya* [Models and methods for calculating performance indicators of nodal equipment and structural and network parameters of next-generation communication networks]. Krasnoyarsk, Polikom Publ., 2011. 491 p.

9. ITU-T Recommendation X.800. *Security Architecture for Open Systems Interconnection for CCITT Applications*. ITU, 1991.

10. ITU-T Recommendation X.805. *Security Architecture for Systems providing end-to-end Communications*. ITU, 2003.

Для цитирования:

Попков Г.В. К вопросу реализации алгоритмов проектирования защищённых сетей передачи данных // Безопасность цифровых технологий. – 2024. – № 3 (114). – С. 53–62. – DOI: 10.17212/2782-2230-2024-3-53-62.

For citation:

Popkov G.V. K voprosu realizatsii algoritmov proektirovaniya zashchishchennykh setei peredachi dannykh [On the issue of implementing algorithms for designing secure transmission networks]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 3 (114), pp. 53–62. DOI: 10.17212/2782-2230-2024-3-53-62.