УДК 004.056.53
DOI: 10.33764/2618-981X-2021-8-332-336

К ВОПРОСУ ФОРМИРОВАНИЯ ЧАСТНОЙ МОДЕЛИ УГРОЗ ДЛЯ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ

Глеб Владимирович Попков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, к.т.н., доцент кафедры информационной безопасности, тел. +7 (953) 868-51-37, e-mail: glebpopkov@inbox.ru

В статье рассмотрены вопросы, связанные с перспективным формированием частных моделей угроз на сети мультисервисных сетей связи (МСС), устойчивых к внешним деструктивным воздействиям (ВДВ). Для формирования модели угроз предложена концепция синтеза моделей жизненного цикла сетей МСС, рекомендаций МСЭ – Т серии Х.800, в частности рекомендации Х.805 [1], восьмиуровневой гиперсетевой G-net модели, позволяющей адекватно сформировать так называемый «профиль атаки» на сети МСС.

Ключевые слова: мультисервисные сети связи, информационная безопасность, модель нарушителя, модель угроз, доступность, целостность информации, внешние деструктивные воздействия

TO THE QUESTION OF FORMING A PARTICULAR THREAT MODEL FOR MULTISERVICE COMMUNICATION NETWORKS

Gleb V. Popkov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, PhD., Associate Professor, Department of Information Security, phone: +7 (913) 478-91-30, e-mail: glebpopkov@inbox.ru

The article deals with the issues related to the prospective formation of particular threat models on the network of multiservice communication networks (MCN) resistant to external destructive influences (EDI). To form a threat model, the concept of synthesis of models of the life cycle of MCN networks, ITU-T recommendations of the X.800 series, in particular X.805 [1], an eight-level hyper MCN networks.

Keywords: multiservice communication networks, information security, intruder model, threat model, availability, information integrity, external destructive influences

Введение

Перспективное формирование модели угроз для устойчивых мультисервисных сетей связи тесно связано с жизненным циклом сети связи, стандартами в области информационной безопасности, теориями надежности и живучести, а также адекватными функциональными и математическими моделями сетей связи.

Рекомендации серии Х.800, в частности рекомендация Х.805 определяют концепцию информационной безопасности по типу «End – to – End» («из конца в конец»). Большой практический интерес представляют рекомендации МСЭ - Т

серии Y.2701, Y.2704, Y.2760, Y.2770 [2–5] в части обеспечения глобальной информационной безопасности сетей следующего поколения.

Концептуальные положения

Для рассмотрения перспективного формирования модели угроз предлагается многопараметрический синтез каскадной модели жизненного цикла (далее, модель ЖЦ) сети связи [6], измеряемых параметров модели стандарта X.805 и восьмиуровневой гиперсетевой модели G-net мультисервисной сети связи.

Концепция связки требований по информационной безопасности сетей связи, серий стандартов МСЭ-Т X.800, подразумевает организацию признакового пространства, образуемого из восьми уровней каскадной модели жизненного цикла сети связи и стандарта X.805 – так называемый End – to – End, QoS стандарт, рекомендуемый операторам связи для выполнения всех требований по информационной безопасности. Восьмиуровневая G-net модель рассматривалась подробно автором здесь [7]. Принцип эффективного формирования моделей угроз зависит от задания необходимых требований и ограничений на проектируемую сеть МСС.

Основной принцип синтеза перечисленных выше моделей состоит в определении вероятности наступления инцидентов безопасности на всех стадиях жизненного цикла сети связи, согласно нарушениям измеряемых параметров рекомендации X.805, а также нахождения этого инцидента на определенном уровне G-net гиперсетевой модели сети МСС.

Учитывая уровни модели жизненного цикла, 72 параметра (измерений защиты) стандарта X.805 и восемь уровней 8-GNet модели, получаем пространство размерностью 4608 возможных точек (состояний) определения инцидента безопасности мультисервисной сети связи (МСС). Синтез – модель устойчивой сети МСС приведена на рис. 1. Для дальнейшего понимания синтеза вышеуказанных моделей введем понятие «профиля атаки», профиль атаки в данном случае – это интегрированный вектор, содержащий множество параметров внешних деструктивных воздействий (ВДВ) на мультисервисные сети связи, обозначим его как P_a.

Множество параметров профиля атаки представляет из себя пространство точек измерения (параметров) инцидента безопасности, лежащих в плоскости модели жизненного цикла сети МСС, точки измерения события согласно рекомендации X.805 и место расположения события на определенном уровне модели 8–GNet. В общем случае профиль атаки содержит в себе адекватные проектируемой МСС модели нарушителя модели угроз сетей МСС [8].

Учитывая вышесказанное, необходимо сформировать описательную модель профиля атаки на сеть МСС.

В общем виде профиль атаки P_a содержит следующие параметры ВДВ:

–источник атаки (антропогенный, не антропогенный характер);

–место (географическая локация), удаленность от объекта, объектов атаки на сети МСС;

–мотивация атакующего объекта;

–цели атаки (вектор атаки) по отношению к объекту атаки;

–пути воздействия ВДВ на объект атаки;

–квалификация атакующего субъекта ВДВ;

–осведомленность, наличие необходимой оперативной информации у субъекта атаки по отношению к объекту атаки;

–время и место реализуемой атаки на модели жизненного цикла сети МСС;

–пространственно-временные характеристики ВДВ, время воздействия (начало воздействия по Гринвичу), длительность воздействия, периодичность воздействия, мощность воздействия;

–тип реализуемого ВДВ согласно классификации стандарта X.805 (нарушение целостности, доступности, конфиденциальности информации и. т. д.);

–тип и место расположения элемента *NE* (объекта атаки) на уровне/уровнях G-net модели сети МСС;

–признак состоявшейся/не состоявшейся атаки на сеть МСС в момент *t*;

–состояние элемента *NE* после состоявшейся атаки (вероятность обеспечения измерений защиты согласно стандарта X.805).

В целом описанная синтез-модель сети МСС, профиль атаки на сеть МСС, позволят адекватно задавать, оценивать угрозы на сеть МСС с точки зрения возможных рисков. Использование вышеописанного подхода позволит анализировать принимаемые решения в области проектируемых устойчивых сетей МСС с точки зрения поддержания уровня безопасности, задаваемого нормами и рекомендациями МСЭ – Т, а также сторонних участников проектирования и эксплуатации устойчивых сетей МСС.

Формализация приведенных моделей представляет собой большую проблему, в первую очередь, это большая размерность пространства состояний элементов, большое количество входных параметров, связанных с динамическими процессами, ограничений, накладываемых на проектируемую сеть МСС. Для проблем, связанных с эффективным проектированием МСС, устойчивых к ВДВ, представляет интерес построение такого рода моделей с использованием стратификации, зачастую применимой для математической логики, теории нечетких множеств, что позволит уменьшать размерность пространства возможных состояний системы (модели) без критического падения адекватности модели для реальных сетей МСС в условиях ВДВ.

Для формирования модели угроз в рамках «профиля атаки» предлагается «сценарный подход», для адекватного описания такой модели угроз применим системно-логический подход при исследовании процессов информационных угроз.

В основу формальных определений положим следующие конструкции:

– набор элементов $A = \{a_a\}, a \in A_A$ – произвольное множество;

– набор отношений $R = \{r_\beta(A_\beta), \beta \in B_A\}$ на множествах $A_\beta \subseteq A$.

– набор свойств $P_r = \left\{ p_\gamma(r_\beta), \gamma \in P_A, \beta \in B_A \right\}$, приписываемых отношениям из R.

В этом случае P_a будет иметь вид:

$$P_a \left\{ \begin{array}{l} A = \left\{ a_a \right\}, a \in A_A \\ R = \left\{ r_\beta(A_\beta), \beta \in B_A \right\} \\ P_r = \left\{ p_\gamma(r_\beta), \gamma \in P_A, \beta \in B_A \right\} \end{array} \right\}$$

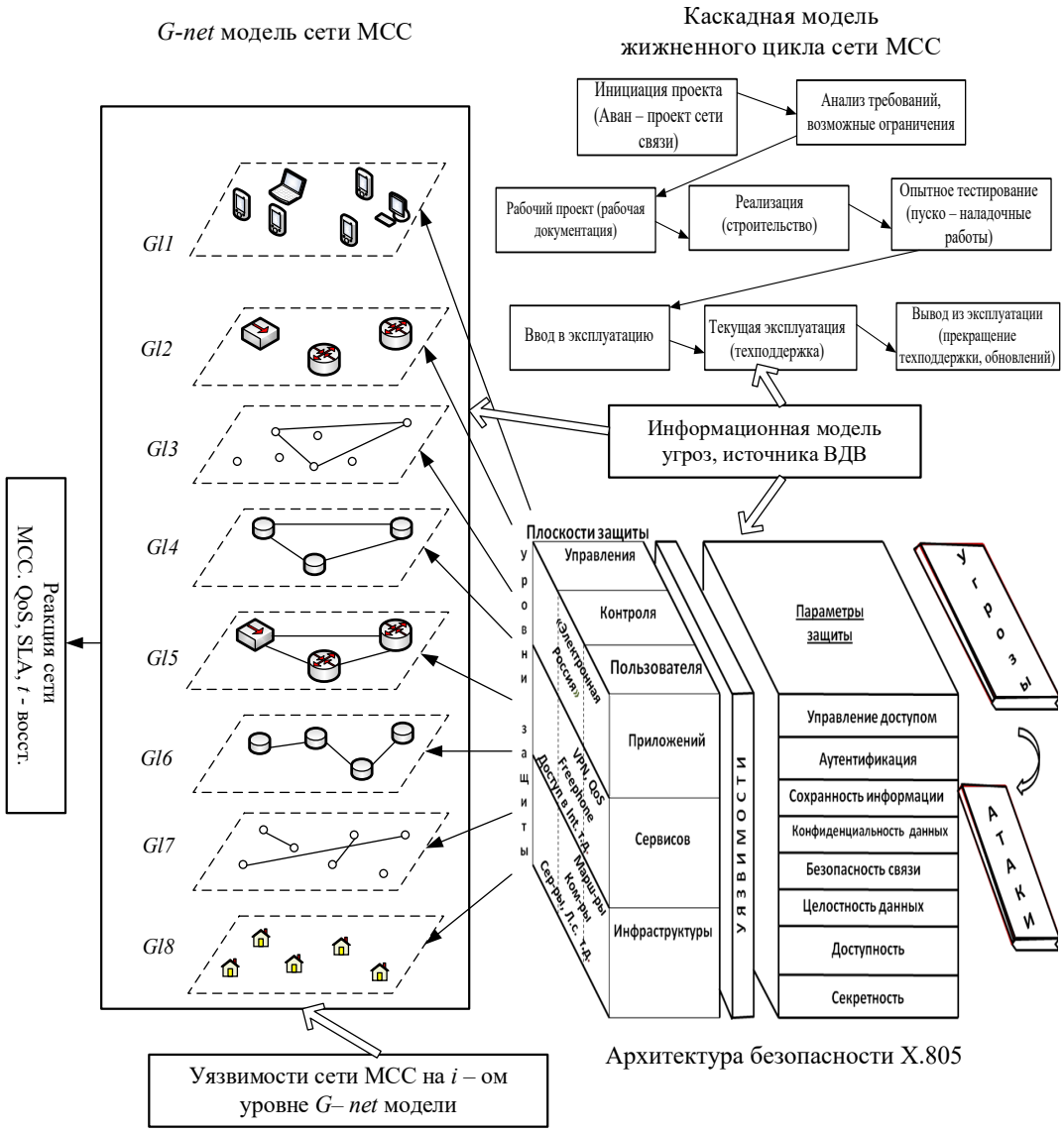

Рис. 1. Синтез-модель МСС, X.805 и G-net.

Вопросы формирования частных моделей угроз на реальные сети МСС в условиях неопределенности остаются актуальными и требуют большого объема дальнейших научных исследований.

Заключение

Формирование частных моделей угроз для мультисервисных сетей связи сопряжено с большими трудностями, зачастую область угроз информационной безопасности формируется в условиях неопределенности, что требует формирования большого количества сценариев прохождения атак на сети МСС. Подход, предложенный в статье, позволит решить ряд задач, в частности, сформировать частную модель угроз таким образом, что элементы этой модели могут быть описаны не только качественными, но и количественными показателями, что позволит поддерживать измерения информационной безопасности на сетях МСС на заданном уровне.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ITU-T X.805: Security architecture for systems providing end-to-end communications, 2003. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=7024.

2. ITU-T Y.2701: Security requirements for NGN release 1, 2007. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8899.

3. ITU-T Y.2704: Security mechanisms and procedures for NGN, 2010. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=10237.

4. ITU-T Y.2760: Mobility security framework in NGN, 2011. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11094.

5. ITU-T Y.2770: Requirements for deep packet inspection in next generation networks, 2012. URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11566.

6. Орлов С. А. Программная инженерия // Изд - во. Питер, 2018. – 640 с., ил.

7. Попков Г. В., Перспективное проектирование сети абонентского доступа с использованием восьмиуровневой модели / Программные продукты и системы. – № 2 (114), 2016. – С. 139 – 145.

8. Бирюков А. А., Информационная безопасность: защита и нападение // М.: Изд – во. ДМК, 2013. – 472 с., ил.

9. Назаров А. Н., Сычев К. И., Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения // Изд – во Поликом, 2011. – 491 с.