РАЗРАБОТКА МОДЕЛИ РАСПРОСТРАНЕНИЯ САМОМОДИФИЦИРУЮЩЕГОСЯ КОДА В ЗАЩИЩАЕМОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

DEVELOPMENT OF SELF-MODIFYING CODE PROPAGATION MODELS IN THE PROTECTED INFORMATION SYSTEM

A. Gelfand
I. Pestov
A. Katasonov
K. Ryazantsev

Summary. Recently, in the field of managing data networks, there is a problem in ensuring the security of data confidentiality and integrity. In this article, we consider an example of one of the information systems in which a public data network is supported. For example, given an information system where it is provided and used by software developers, they actively exchange data, and also store their developments on a protected database. To protect the information system, special software packages are used that are responsible for the imposition of a digital watermark, the addition of licensed special symbols, as well as various properties of non-repudiation and authenticity for «fresh» programs. Purpose: Since there is a risk in the information system that protected special characters can be intercepted and copied for illegal actions. Therefore, the goal is to develop software that effectively extends to the protected information system, namely the self-modifying code (hereinafter referred to as SMS) developed during the distribution model implementation. Task: Development of the SMS distribution model in the protected information system. Research hypothesis: It is assumed that if we develop software that implements the SMS and efficiently distributes it, then the information system can be considered safe from attacks on intercepting protected special symbols for illegal actions. Method: This article looks at an example of an information system, and this example developed software, which implements the SMS. Result Achieved: A software model has been designed that most extensively distributes self-modifying code over the IS.

Keywords: EIGRP, Model Predictive Control, State-Space Model Predictive Control, self-modifying code, data network.

Гельфанд Артем Максимович
Ассистент, СПбГУТ им. проф. Бонч-Бруевича
amgelfand@mail.ru
Пестов Игорь Евгеньевич
Старший преподаватель, СПбГУТ им. проф. Бонч-Бруевича
pestovie@outlook.com
Катасонов Александр Игоревич
Техник, СПбГУТ им. проф. Бонч-Бруевича
ksasha716@yandex.ru
Рязанцев Кирилл Сергеевич
Инструктор-консультант, FastLane RCIS
kirikkryazancev1995@yandex.ru

Аннотация. В последнее время в области управления сетями передачи данных (далее — СПД) существует проблема по обеспечению безопасности конфиденциальности и целостности данных. В данной статье рассматривается пример одной из информационной систем, в которой поддерживается публичная СПД. К примеру, дана информационная система, где обеспечивается и используется разработчиками программного обеспечения, они активно обмениваются данными, а также хранят свои разработки на защищенной базе данных. Для защиты информационной системы (далее — ИС) используются пакеты специального программного обеспечения, которое отвечает за наложение цифрового водяного знака, добавление лицензионных спецсимволов, а также различных свойств неотрекаемости и подлинности для «свежих» программ. Цель: Так как в информационной системе существует риск того, что защищенные спецсимволы могут быть перехвачены и скопированы для незаконных действий. Потому цель состоит в разработке программного обеспечения, которое эффективно распространяется по защищаемой ИС, а именно разрабатываемый в ходе реализации модели распространения самомодифицирующийся код (далее — СМК). Задача: Разработка модели распространения СМК в защищаемой информационной системе. Гипотеза исследования: Предполагается, что если осуществить разработку программного обеспечения, которое реализует СМК и эффективно его распространяет, то ИС можно считать обезопашенной от атак по перехвату защищенных спецсимволов для незаконных действий Метод: В данной статье рассмотрен пример ИС и по этому примеру разработано программное обеспечение, которое реализует СМК. Достигнутые результаты: Спроектирована модель программного обеспечения, которое наиболее результативно распространяет по ИС самомодифицирующийся код.

Ключевые слова: EIGRP, Model Predictive Control, State-Space Model Predictive Control, самомодифицирующийся код, сети передачи данных.

Ранее опубликованных работах [1–3] идет речь о развитии СМК, о построении данного кода, а также внедрения цифровых водяных знаков (далее — ЦВЗ) в программные приложения. В работе [3–5] имелась ввиду некая ИС, в которой проходил анализ распространения СМК. Общие результаты возможных действий СМК сравнивались по аналогии с компьютерными вирусами и всегда имели приблизительные коэффициенты доли пребывания в ИС предприятия. Из действительно верных решений можно будет вывести только одну фор-

Рис. 1. Алгоритм распространения СМК

мулировку, а именно, возможно существование девяти различных пар узлов, однако, исключив симметрию, вводится следующее дифференциальное управление для описания состояния распространения СМК в ЛВС:

$$[ABC] \approx \frac{(n-1)N}{n^2}\frac{[AB][BC][AC]}{[A][B][C]} \quad (1)$$

Распространение СМК на узлы и персональные компьютеры ЛВС можно разделить на три этапа:

Сравнительно медленное (но тем не менее экспоненциальное) нарастание присутствия СМК (коэффициента СМК) до порогового уровня 0,05, определяемого как

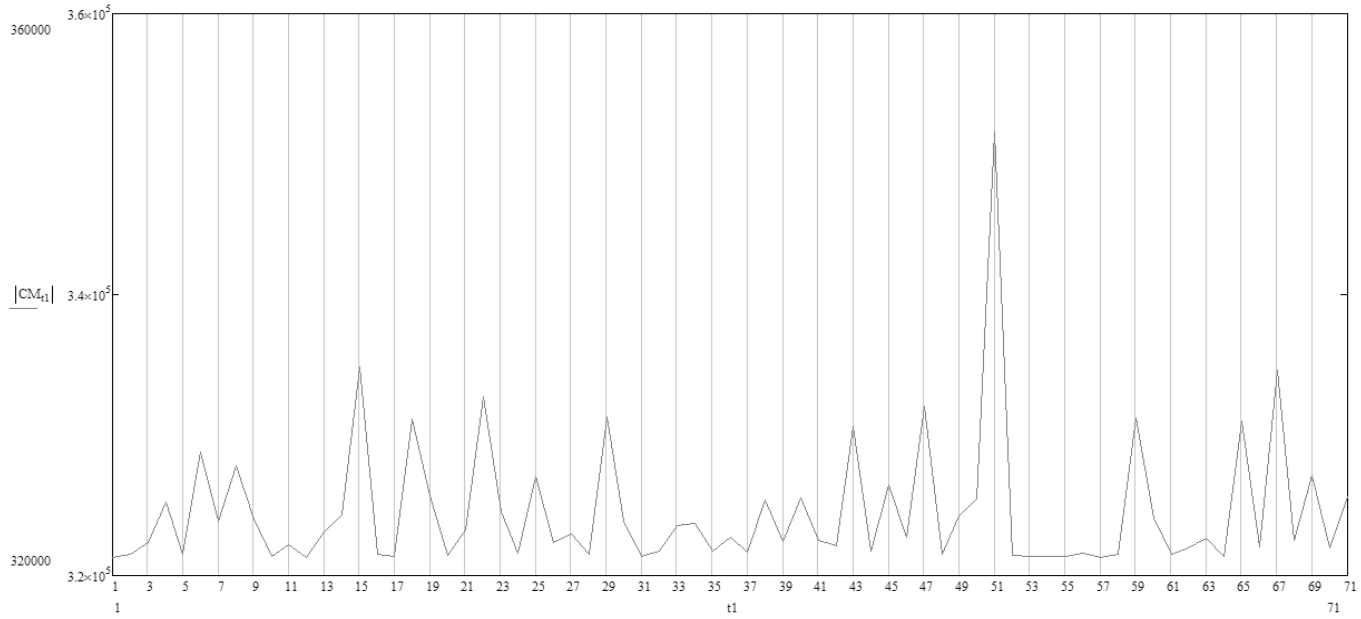

Рис. 2. Метрика нагрузок

$$k_{смк} = \frac{I}{N}.$$

Скорость удвоения доли пораженных машин равна $\ln(2)/\beta$.

Фаза максимального распространения в диапазоне 0,05 < $k_{смк.}$< 0,95. Продолжительность определяется приблизительно равна $5,89/\beta$.

Насыщение, $k_{смк.}$ > 0,95. На этом участке при случайном сканировании адресного пространства зараженные узлы контактируют преимущественно друг с другом, поэтому уцелевшие узлы могут оставаться «чистыми» неопределенно продолжительное время.

Для достижения порога насыщения $k_{смк.}$ = 0,95 требуется время

$$\frac{1}{\beta}\ln\left[19\left(\frac{1}{k_{смк.\ нач.}}\right)-1\right], \quad (2)$$

где $k_{смк.\ нач.}$ — распространение СМК в ЛВС в начальный момент времени t_0.

В данной статье необходимой задачей ставится разработка модели распространения СМК в защищаемой информационной системе. Суть модели — имитация распространения СМК в информационной системе, но при помощи нового алгоритм распространения СМК. Поскольку известны коэффициент порога насыщения и этапы распространения СМК, имеет место наличие первостепенного алгоритма, принимающего во внимание значение нагрузки сети.

Приведенный алгоритм (рис. 1) должен выполняться на контроллере, содержащем в себе топологию сети, представленную в виде графа. При восстановлении маршрута после обхода, складываются стоимости каналов связи. Эта сумма является метрикой маршрута. В контексте терминологии EIGRP на каждой итерации цикла происходит сложение Reported Distance родителя (длина маршрута от старта до родителя) для текущей вершины и стоимости канала между родителем и текущей вершиной. Данная величина — это Computed Distance.

Для проведения исследования были выбраны следующие значения:

- $BW_1 = 100\ \text{Mbps} = 100000\ \text{Kbps}$;
- $Del_1 = 100\ \text{msec} = 0.0001\ \text{sec}$;
- $Rel = 255$
- $BW_2 = 8\ \text{Mbps} = 8000\ \text{Kbps}$;
- $Del_2 = 5000\ \text{msec} = 0.005\ \text{sec}$;

В качестве значений нагрузки $Load$ выбираются значения функции равномерного распределения.

Значения коэффициентов, используемые в исследовании:

- $K_1 = K_2 = K_3 = 1$;
- $K_4 = K_5 = 0$.

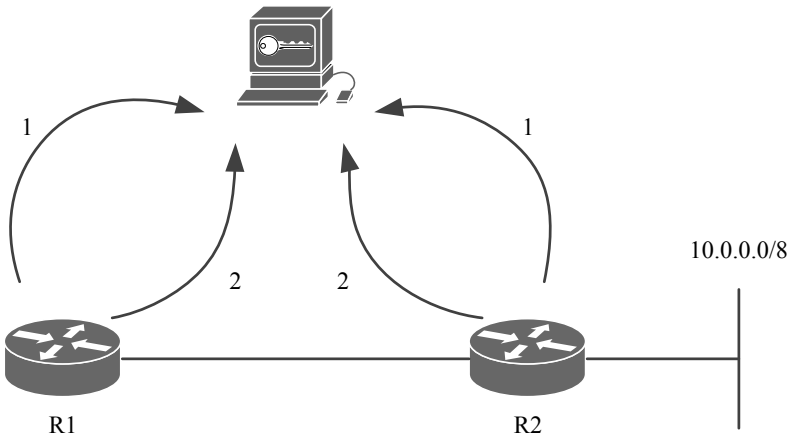

Рис. 3. Межсетевое взаимодействие

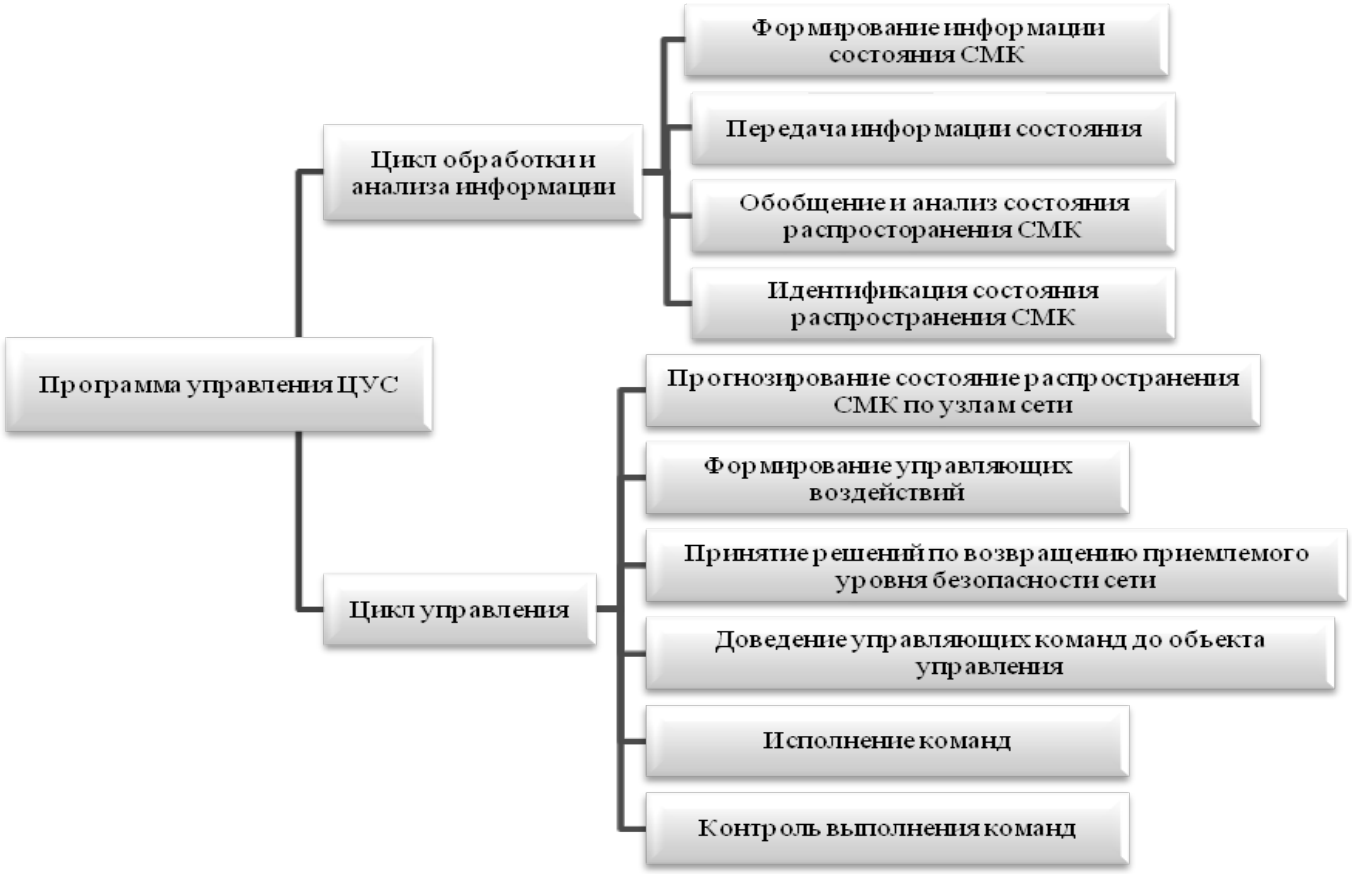

Рис. 4. State-Space Model Predictive Control

Таким образом, формула (1) принимает вид:

$$CM = (K_1 * \left(\frac{256*10^7}{BW_2}\right) + K_2 * \left(\frac{\left(\frac{256*10^7}{BW_2}\right)}{256-Load}\right) + + K_3 * (256 * (\frac{Del_1}{10} + \frac{Del_2}{10}))) \quad (3)$$

Без учёта предыдущих нагрузок метрика будет выглядеть так, как показано на рисунке (Рис. 2).

Как видно из графика, в некоторые моменты времени значения метрики значительно увеличиваются, образовывая «пик». Это может негативно сказаться

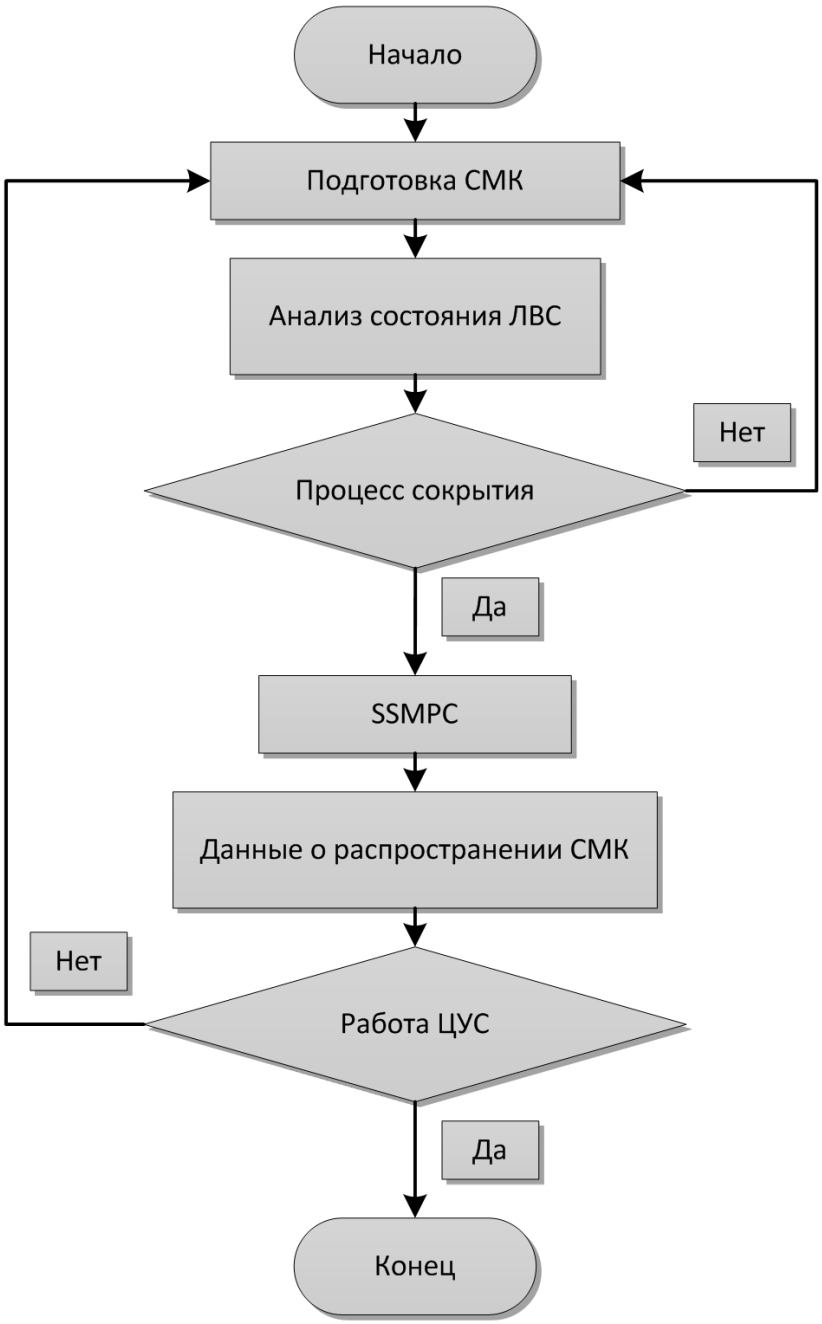

Рис. 5 Алгоритм управления сетью

на работе программного обеспечения ИС, где функционирует СМК.

Основной проблемой EIGRP при работе с параметрами нагрузки, из-за её вероятностной природы является нестабильность маршрутов. Для того, чтобы обойти эти ограничения, СМК можно использовать адаптивный алгоритм реагирования на изменения нагрузки [6,7], который задается разностным уравнением:

$$\mathrm{Load_i} = \\ = \alpha * \mathrm{Loa4d_{i-1}} + (1-\alpha) * \mathrm{Load_{new}},\ 0 \le \alpha \le 1 \quad (4)$$

На уровне контроллера [6,7] задается пороговое значение (формула 2) для СМК, которое обеспечивает условие реакции на изменения в нагрузке, совместно с заданием коэффициента α определяется общая реакция алгоритма на изменения нагрузки в сети.

Поскольку при вычислении метрики для маршрута маршрутизатором используются целые значения параметров (пропускной способности, задержки, нагрузки, надежности), то и вычисления на уровне контроллера имеет смысл производить с целыми числами

Поскольку маршрутизатору известны текущие значения параметра нагрузки, то эти параметры не будем передавать. После получения решения о перерасчете маршрутов маршрутизатор вычисляет метрики всех маршрутов, или для тех, которые затрагиваются изменившимся значением метрики (рис. 3). Предложенный алгоритм (рис. 1) вместе со всеми вычислениями развертывается на контроллере, в роли которого может выступать любая платформа [7] с поддержкой соответствующих программных интерфейсов.

Для прогнозирования распространения СМК было принято решение использовать способ методологии управления на основе прогнозирующих моделей: Model Predictive Control (MPC).

Процесс разработки способа управления ИС на основе краткосрочного прогнозирования распространения СМК можно разделить на следующие этапы: описание модели распространения СМК в ЛВС, составление критерия безопасного состояния ЛВС, расчет закона управления [8,9]. Одно из преимуществ методологии управления с использованием прогнозирующих моделей — возможность исследования многофакторного процесса в опережающем режиме. В связи с чем, на основе анализа, выбран метод прогнозирования на основе модели пространства состояний: State-Space Model Predictive Control (SSMPC) (см. рис. 4).

Для применения метода SSMPC необходимо составить математическую модель объекта управления, в последствии использующуюся для предсказания выходных данных ИС (формула 4). Эти воздействия вычисляются оптимизатором, который учитывает критерий качества (где принимаются во внимание ошибки в будущем) и ограничения, накладываемые на переменные процесса, описывающего объект управления (формула 2).

Безопасное состояние для СМК то, в котором доля наличия СМК в компьютерах или узлов сети не превышает 5%. Из приведенных данных в формулах 2 и 4, возможно сформировать простой общий алгоритм (рис. 5) управления сетью на основе краткосрочного прогнозирования распространения СМК.

Как видно из простого алгоритма, данные о распространении СМК должны последовать за методом SSMPC и передать основное управление ЦУС. Предложенная модель должна охватывать динамику процесса для точного предсказания будущих выходных значений, быть простой для внедрения и понимания, в чем ее и принципиальная разница от предыдущих моделей стеганографических систем, где не демонстрировались до этого примеры внедрения программ-закладок (чем и может быть СМК) на контроллеры передаваемых устройств.

ЛИТЕРАТУРА

1. Штеренберг С.И., Виткова Л. А., Андрианов В. И. Методы использования пустых секций исполнимого файла для стеговложения саморазвивающегося кода в распределенной системе однозначного отождествления // Системы управления и информационные технологии. 2015. Т. 59. № 1.1. С. 189–194.
2. Штеренберг С.И., Виткова Л. А. Анализ возможностей вложения скрытого самомодифицирующегося кода в формат исполнимых файлов.exe // В сборнике: Современные тенденции в науке и образовании Сборник научных трудов по материалам Международной научно-практической конференции: в 5 частях. ООО «АР-Консалт». 2015. С. 109–113.
3. Штеренберг С. И. Методика применения в адаптивной системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии. 2016. Т. 63. № 1. С. 51–54.
4. Штеренберг С. И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применение стеговложения // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 2. С. 86–90.
5. Штеренберг С.И., Кафланов Р. И., Дружин А. С., Марченко С. С. Методика применения самомодификации файлов для скрытой передачи данных в экспертной системе // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 1. С. 71–75.
6. Красов А.В., Левин М. В. Возможности управления тра-фиком в рамках концепции SDN // IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. Актуальные проблемы инфотелекоммуникаций в науке и образовании, Санкт-Петербург, 03–04 марта 2015. Санкт-Петербург: Санкт-Петербургский государственный университет телекомму-никаций им. проф. М. А. Бонч-Бруевича, 2015. С. 350–354.
7. Красов А.В., Левин М. В., Цветков А. Ю. Управление се-тями передачи данных с изменяющейся нагрузкой // Все-российская научная конференция по проблемам управле-ния в технических системах, Санкт-Петербург, 28–30 ок-тября 2015. Санкт-Петербург: Санкт-Петербургский гос-ударственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), 2015. № 1. С. 141–146.
8. Душин С.Е., Красов А. В., Кузьмин Н. Н. Моделирование систем управления // учебное пособие для студентов высших учебных заведений, обучающихся по направлению 220400 «Управление в технических системах» / С. Е. Душин, А. В. Красов, Н. Н. Кузьмин; под ред. С. Е. Душина. Москва, 2012.

9. Душин С.Е., Красов А. В., Кузьмин Н. Н., Пошехонов Л. Б. Численное моделирование систем управления // Учеб. пособие для студентов вузов, обучающихся по направлениям 550200, 651900 «Автоматизация и упр.» подгот. бакалавров, магистров и дипломир. специалистов / М-во образования РФ. С.-Петерб. гос. электротехн. ун-т «ЛЭТИ»; [С. Е. Душин и др.]. СПб., 2003.
10. Shterenberg SI, Vitkova LA, Andrianov VI Methods of using empty sections of an executable file for stegovlozheniya self-developing code in a distributed system of unambiguous identification / / Control Systems and Information Technology. 2015. Vol. 59. № 1.1. Pp. 189–194.
11. Shterenberg SI, Vitkova L. A. Analysis of the possibilities of embedding hidden self-modifying code in the format of executable files.exe // In the collection: Modern trends in science and education. Collection of scientific papers on the materials of the International Scientific and Practical Conference: in 5 parts. LLC «AR-Consult». 2015. pp. 109–113.
12. Shterenberg, SI Method of application in the adaptive system of local computer networks stegovleniya in executable files based on self-modifying code // Control Systems and Information Technology. 2016. Vol. 63. No. 1. P. 51–54.
13. Shterenberg, SI Analysis of the operation of information protection algorithms based on self-modifying code with the use of stegovlozheniya / / High technology in space exploration of the Earth. 2016. T. 8. № 2. P. 86–90.
14. Shterenberg SI, Kaflanov RI, Druzhin AS, Marchenko SS Method of application of self-modification of files for hidden data transmission in the expert system. // High technology in space exploration of the Earth. 2016. T. 8. No. 1. P. 71–75.
15. Krasov AV, Levin M. V. Possibilities of trafic control within SDN concept // IV International scientific-technical and scientific-methodical conference: a collection of scientific articles in 2 volumes. Actual problems of information telecommunications in science and education, St. Petersburg, March 03–04, 2015. St. Petersburg: St. Petersburg State University of Telecommunications. prof. M. A. Bonch-Bruevich, 2015. P. 350–354.
16. Krasov AV, Levin MV, Tsvetkov A. Yu. Management of data transmission networks with variable load // All-Russian scientific conference on control problems in technical systems, St. Petersburg, 28–30 October, 2015. St. Petersburg: St. Petersburg State Electrotechnical University « LETI «them. IN AND. Ulyanov (Lenin), 2015. № 1. P. 141–146.
17. Dushin SE, Krasov AV, Kuzmin NN Modeling of the management system // a textbook for students of higher educational institutions studying in the direction 220400 «Management in technical systems» / SE Dushin, AV Krasov, NN Kuzmin; Ed. S. E. Dushina. Moscow, 2012.
18. Dushin SE, Krasov AV, Kuzmin NN, Poshekhonov LB Numerical modeling of control systems // Proc. manual for university students studying in directions 550200, 651900 «Automation and management.» preparation. bachelors, masters and diplomas. specialists / Ministry of Education of the Russian Federation. S.-Petersburg. state. electrotechnical. un-t «LETI»; [FROM. E. Dushin, etc.]. SPb., 2003.

СПбГУТ им. проф. Бонч-Бруевича