УДК 681.3

Начальник кафедры С.В. Белокуров, адъюнкт О.А. Кондратов,
(ВИ ФСИН России) кафедра МиЕНД. тел. 8 (473) 260–68–20
E-mail: BSVLabs@mail.ru
аспирант А.П. Сидельников,
(Воронеж. гос. технич. ун-т) кафедра СИБ. тел. (8473)274-57-14
доцент Е.В. Белокурова
(Воронеж. гос. унив. инжен. техн.) кафедра сервиса и ресторанного бизнеса.
тел. (473) 255-37-72
E-mail: zvezdamal@mail.ru

Head of the department S.V. Belokurov, graduate O.A. Kondratov,
(Voronezh, VI FPS Russia) Department of math and science disciplines.
phone 8 (473) 260-68-20
E-mail: BSVLabs@mail.ru
graduate A.P. Sidelnikov,
(Voronezh state technical university) Department of information security systems.
phone (8473) 274-57-14
associate professor E.V. Belokurova
(Voronezh state university of engineering technologies) Department of service and restaurant business.
phone (473) 255-37-72.
E-mail: zvezdamal@mail.ru

Управление качеством функционирования механизмов защиты информации в инфокоммуникационных системах

Quality management operation mechanisms for the protection of information in the info-communication systems

Реферат. В статье представлен перечень объектов и необходимых процедур защиты от угроз нарушения доступности информации в условиях воздействия вредоносных программ в инфокоммуникационных системах и принципы концептуального проектирования механизмов антивирусной защиты, реализуемых в виде компонент комплекса программных средств защиты информации. Данная разработка позволяет сформулировать принципы концептуального проектирования механизмов антивирусной защиты, реализуемых в виде компонент комплекса программных средств защиты информации. Особенно ценна эта разработка для реализации процедур управления сложными организационно-техническими системами. Упорядочение обычно преследует одну или в каком-либо сочетании следующие цели (установки): рациональность, эффективность, совершенствование системы. Целью рационального управления (например, противодействие вредоносным программам) является сохранение существующей структуры и параметров системы при некоторых ограничениях (например, ограничениях на вычислительные ресурсы). При невозможности обеспечить управление на рациональной основе, появляется необходимость изменения параметров (параметрический синтез) или поиска и выбора на множестве допустимых структур эффективной по заданным критериям структуры (структурный синтез). Отметим, что в данном случае речь идет об эффективности на определенном временном интервале, так как социальный и научно-технический прогресс объективно ведут к изменению критериев оценок эффективности.

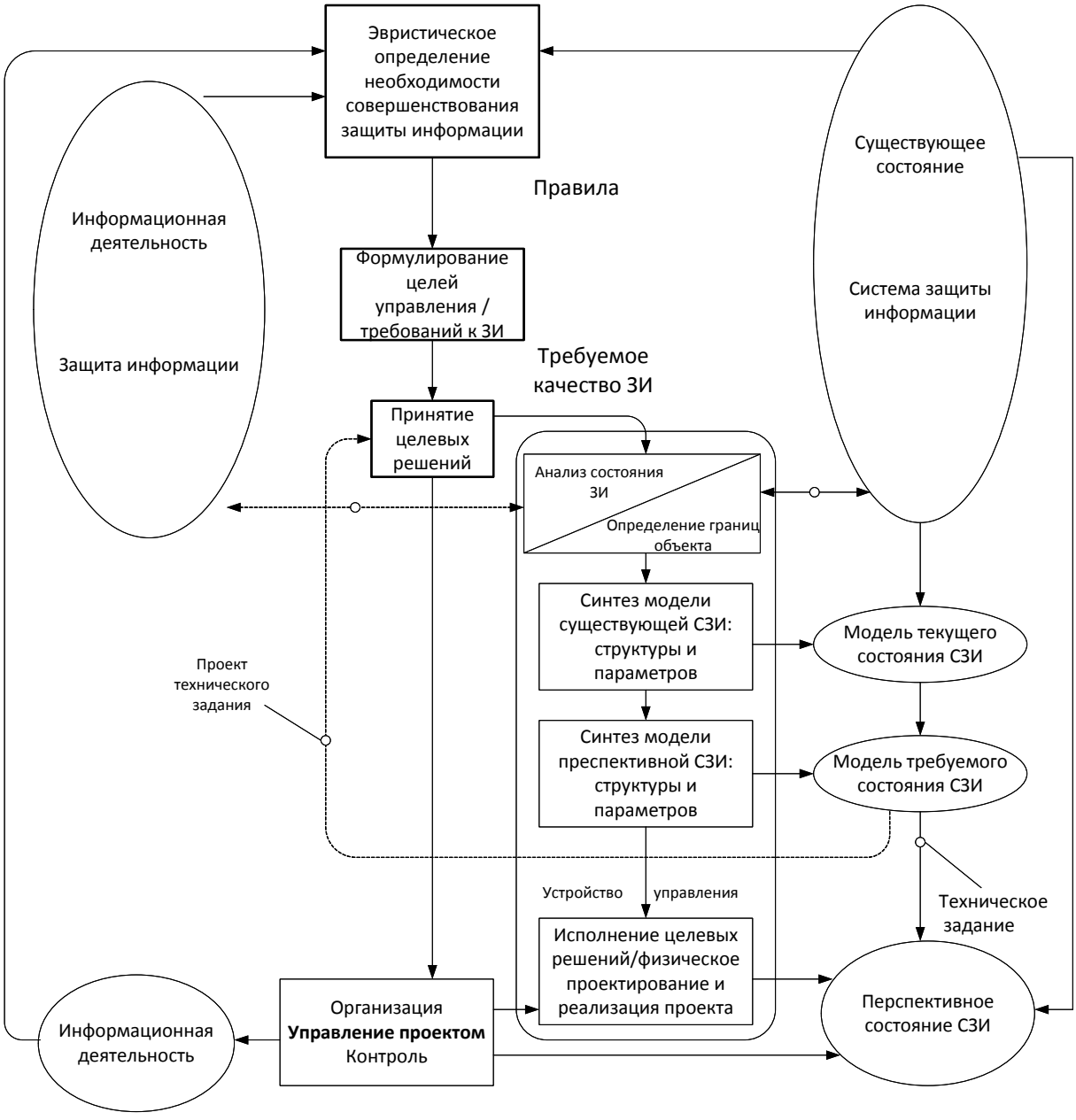
Summary. The article presents the list of facilities and necessary procedures to protect against threats of violation of information availability in terms of exposure to malware in ICT systems and principles conceptual design of mechanisms, antivirus protection, implemented in the form of a component of a software complex for protection of information. This development allows us to formulate the principles of conceptual design of mechanisms, antivirus protection, implemented in the form of a component of a complex of software tools of information security. Special this valuable development for the implementation of procedures for the management of complex organizational-technical systems. Streamlining usually has one or any combination of the following objectives (attitudes): rationality, efficiency, improvement of the system. The aim of good governance (e.g. anti-malware) is the preservation of the existing structure and system parameters under certain constraints (e.g., constraints on computing resources). If you cannot provide the management on a rational basis, it becomes necessary to change the parameters (parametric synthesis) or search for and select the set of admissible structures effective on the criteria of structure (structural synthesis). Note that in this case we are talking about effectiveness for a given period of time, as social and scientific progress inevitably lead to a change of criteria effectiveness evaluation.

Ключевые слова: управление, защита информации, инфокоммуникационная система.

Keywords: management, information security, infocommunication system.

Несмотря на то, что вопросы совершенствования как методов математического моделирования, так и методов теории информационной безопасности являются чрезвычайно актуальными, специальные исследования применительно к проблематике моделирования механизмов антивирусной защиты в инфокоммуникационных системах (ИКС) в интересах их оптимизации носят крайне ограниченный характер.

Сформированный в [1] перечень объектов и необходимых процедур защиты от угроз нарушения доступности информации в условиях воздействия вредоносных программ в ИКС позволяет сформулировать принципы концептуального проектирования механизмов антивирусной защиты, реализуемых в виде компонент комплекса программных средств защиты информации (КПСрЗИ).



Условные обозначения:
ЗИ - защита информации;
СЗИ - система защиты информации

Рисунок 1. Цикл управления системой защиты информации

С системной точки зрения эти компоненты объединены в функционально ориентированные системы защиты информации (СЗИ). Следует отметить, что разработка такого рода мероприятий связана с реализацией процедур управления [2, 3]. Управление такими сложными организационно-техническими системами, как СЗИ, поддержание их динамического равновесия осуществляется в условиях непрерывных изменений их внутреннего состояния, состояния объекта информатизации, подсистемой которой является СЗИ, и внешней среды, обусловливающей угрозы информационной безопасности [2]. При этом управление стабилизирует или повышает эффективность системы, сохраняя неизменной ее целевую функцию [3]. Соотношение этих задач на различных этапах жизненного цикла СЗИ зависит от конкретных условий. Многочисленные авторы, исследовавшие проблемы управления в организационно-технических системах, определяют содержание управления как совокупность функций управления, составляющих управленческий цикл. Реализация управленческого цикла имеет целью упорядочение системы путем перевода ее из одного состояния в другое.

На рисунке 1 показан управленческий цикл, содержание функций управления которого интерпретируется как упорядочение СЗИ. Упорядочение обычно преследует одну или в каком-либо сочетании следующие цели (установки): рациональность, эффективность, совершенствование системы [3].

Рациональность предполагает стабильность как системы в целом, так и входящих в нее подсистем и элементов при воздействии среды.

Целью рационального управления (например, противодействие вредоносным программам) является сохранение существующей структуры и параметров системы при некоторых ограничениях (например, ограничениях на вычислительные ресурсы). При невозможности обеспечить управление на рациональной основе, появляется необходимость изменения параметров (параметрический синтез) или поиска и выбора на множестве допустимых структур эффективной по заданным критериям структуры (структурный синтез). Отметим, что в данном случае речь идет об эффективности на определенном временном интервале, так как социальный и научно-технический прогресс объективно ведут к изменению критериев оценок эффективности.

Управленческая установка совершенствования СЗИ реализуется при изменении целей и условий ее функционирования. Она предполагает создание такого механизма управления, который обеспечивает развитие и совершенствование СЗИ как управляемой системы, изменение ее структуры и параметров в соответствии с динамикой целей и условий функционирования.

Таким образом, для совершенствования механизмов защиты информации система управления должна формировать критерии оценки и осуществлять структурный синтез, сохраняя при этом требования к рациональности и эффективности СЗИ. Желательное сочетание этих требований обеспечивает, с одной стороны, стабильность, а, с другой стороны, гибкость и приспособляемость СЗИ. Однако на практике различные управленческие установки иногда могут вступать в противоречие друг с другом.

Концептуальные позиции, с которых решаются эти противоречия, основываются на принципах системного подхода, сущность которого заключается в следующем [2]:

1) необходимость системного рассмотрения сущности проблемы, заключающегося в определении места проблемы защиты информации в информационном обмене, архитектуры системы защиты, выявлении полного множества значащих факторов, влияющих на эту систему и их взаимосвязь;

2) необходимость исследования или разработки не простых, частных задач, а разработка и обоснование полной и непротиворечивой концепции защиты информации, в рамках которой решение конкретной проблемы или задачи определяется как частный случай;

3) необходимость системного использования методов моделирования систем и процессов защиты информации;

4) для обеспечения надежной защиты должна быть создана регулярная система, важнейшим признаком которой является наличие управления.

В рамках кибернетики общие законы любого управления защитой информации могут быть представлены следующими положениями:

1) всякое управление есть целенаправленный процесс;

2) всякое управление есть информационный процесс, заключающийся в сборе, обработке и передаче информации;

3) всякое управление осуществляется в замкнутом контуре, образованном управляющим и управляемым объектами, объединенными в единую систему прямой и обратной линиями связи.

Фундаментальным достижением кибернетики является доказательство следующих двух положений:

1) перечисленные законы образуют систему, т.е. они должны рассматриваться в совокупности и взаимосвязи;

2) действие системы кибернетических законов носит всеобщий характер, они справедливы для систем любой природы: биологических, технических и организационных.

Рассмотрение процесса управления защитой информации необходимо начинать с анализа условий осуществимости данного управления.

При создании эффективной системы управления защитой информации необходимо выполнить условия, без которых система будет либо малоэффективной, либо управление вообще невозможно.

Условие 1. Система управления должна иметь реальную возможность изменять состояние безопасности информации в соответствии с принимаемыми решениями. Для этого нужны исполнительные органы, реализующие принятые системой управления решения.

Условие 2. Система управления должна располагать ресурсами, обеспечивающими реализацию выбранных управляющих воздействий.

Условие 3. Одним из условий осуществимости принятых решений является тщательный анализ структуры СЗИ, условий ее функционирования, воздействия внешних и внутренних дестабилизирующих факторов, необходимых ресурсов, реальности их получения и использования.

Условие 4. Система управления должна учитывать динамичность СЗИ как управляемой системы. Решение должно быть принято в такой момент времени, чтобы его реализация обеспечила желаемое изменение состояния системы не вообще, а к определенному сроку.

Условие 5. Для правильного выбора характера и интенсивности управляющих воздействий управляющая система должна знать цель — обеспечение требуемого уровня безопасности информации, обрабатываемой на объекте информатизации, а также критерии, по которым оценивается степень и эффективность ее достижения.

Условие 6. Необходимо не только иметь сведения о состоянии СЗИ до и к моменту получения ею управляющих воздействий, но и по возможности и прогнозировать как состояние внешней среды, так и поведение СЗИ под ее влиянием в будущем.

Для этого разработаны соответствующие методы моделирования СЗИ и процессов их функционирования. Процесс сбора данных о состояниях системы защиты информации, принятия решения и выработки управляющих воздействий составляет цикл управления, который можно представить следующей последовательностью этапов:

Этап 1. Накопление системой управления определенного объема данных о состоянии СЗИ, множестве потенциальных угроз и возможных каналов утечки информации, поступающих от запрашиваемых и незапрашиваемых источников.

Этап 2. Формирование множества показателей безопасности информации, анализ на основе данного множества существующего состояния СЗИ и формирование цели, как нового состояния, в которое данной системе желательно перейти.

Этап 3. Формирование множества возможных решений. При этом определяются все возможные способы или пути достижения поставленной цели.

Этап 4. Выбор из множества возможных решений наилучшего в смысле эффективности достижения цели.

Этап 5. Реализация принятого решения, в результате чего изменяется состояние СЗИ как управляемой системы.

Этап 6. Оценка результатов воздействия управляющих решений для возможного уточнения целей, критериев эффективности, множества возможных решений и методов выбора оптимального решения.

Анализ возможностей рассмотренных процедур по обеспечению защиты информации от угроз нарушения ее доступности позволяет выделить два принципиальных способа реализации механизмов защиты:

1) последовательное выполнение всей последовательности процедур с первой по шестую;

2) последовательное выполнение всей последовательности процедур с первой по шестую за исключением третьей процедуры.

В отличие от первого, второй способ является менее ресурсоемким из-за отсутствия в реализуемой последовательности процедуры идентификации угрозы нарушения доступности информации. Однако такое упрощение механизма защиты влечет за собой риск некорректного, из-за отсутствия необходимой идентифицирующей информации, восстановления целостности программного обеспечения, регулирующего доступ к информации в инфокоммуникационных системах.

Таким образом, в статье рассмотрен перечень объектов и необходимых процедур защиты от угроз нарушения доступности информации в условиях воздействия вредоносных программ в инфокоммуникационных системах и принципы концептуального проектирования механизмов антивирусной защиты, реализуемых в виде компонент комплекса программных средств защиты информации.

ЛИТЕРАТУРА

1 Минаев В.А., Скрыль С.В. Основы информационной безопасности: учебник для высших учебных заведений МВД России. Воронеж: Воронежский институт МВД России, 2001. 464 с.

2 Белокуров С.В., Скрыль С.В., Джоган В.К. и др. Методы и средства анализа эффективности систем информационной безопасности при их разработке: монография. Воронеж: Воронежский институт МВД России, 2012. 83 с.

3 Белокуров С.В., Скрыль С.В., Джоган В.К. и др. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах: монография. Воронеж: Воронежский институт МВД России, 2012. 116 с.

4 Мистров Л.Е., Дерканосова А.А. Методы информационного воздействия при синтезе стратегий управления конкурентоустойчивостью социально-экономических организаций // Вестник ВГУИТ. 2013. № 4 (58). С. 282-288.

5 Фролова Л.Н., Василенко В.Н., Копылов М.В., Дерканосова А.А. и др. Оптимизация параметров процесса получения биотоплива методами математического моделирования // Вестник Международной академии холода. 2015. № 3. С. 63-67.

6 Трунова С.Н.Комплексная методика оценки эффективности стратегического управления развитием сельскохозяйственной организации // Технологии пищевой и перерабатывающей промышленности АПК-продукты здорового питания. 2015. № 2 (6). С. 89-96.

REFERENCES

1 Minaev V.A., Skryl' S.V. Osnovy informatsionnoi bezopasnocti [Fundamentals of Information Security: a textbook for higher educational institutions of the Russian Interior Ministry]. Voronezh, Voronezhskii institute MVD Rossii, 2001. 464 p. (In Russ.).

2 Belokurov S.V., Skryl' S.V., Joghan V.K. et al. Metody i sredstva analiza effektivnosti system [Methods and tools for analyzing the effectiveness of information security in their development: a monograph]. Voronezh, Voronezhskii institute MVD Rossii, 2012. 83 p. (In Russ.).

3 Belokurov S.V., Skryl' S.V., Joghan V.K. et al. Model ii algoritmy avtomatizirovannogo kontrolya effektivnosti [The models and algorithms for the automated control of the effectiveness of information security systems in automated systems: monograph]. Voronezh, Voronezhskii institute MVD Rossii, 2012. 116 p. (In Russ.).

4 Mistrov L.E., Derkanosova A.A. Methods of information influence the synthesis of management strategies socio-economic organizations. *Vestnik VGUIT*. [Proceedings of VSUET], 2013, no. 4 (58), pp. 282-288. (In Russ.).

5 Frolova L.N., Vasilenko V.N., Kopylov M.V., Derkanosova A.A. et al. Optimization of the process parameters of biofuel production methods of mathematical modeling. *Vestnik Mezhdunarodnoi akademii kholoda*. [International Academy of Refrigeration], 2015, no. 3, pp. 63-67. (In Russ.).

6 Trunov S.N. Complex method of estimating the efficiency of the strategic management of the development of agricultural organizations. Tekhnologii pishchevoi i pererabatyvayushchei promyshlennosti. [Technology of food processing industry AIC - healthy food], 2015, no. 2 (6), pp. 89-96. (In Russ.).