РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 640 629**(13) **C1**

(51) МПК
G06F 21/57 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

На основании пункта 1 статьи 1366 части четвертой Гражданского кодекса Российской Федерации патентообладатель обязуется заключить договор об отчуждении патента на условиях, соответствующих установившейся практике, с любым гражданином Российской Федерации или российским юридическим лицом, кто первым изъявил такое желание и уведомил об этом патентообладателя и федеральный орган исполнительной власти по интеллектуальной собственности.

(52) СПК
G06F 21/577 *(2017.08);* ***G05B 17/00*** *(2017.08);* ***G06N 5/00*** *(2017.08);* ***G06F 11/3089*** *(2017.08);* ***G06F 15/16*** *(2017.08);* ***G06Q 10/06*** *(2017.08)*

(21)(22) Заявка: **2017115135, 27.04.2017**

(24) Дата начала отсчета срока действия патента:
27.04.2017

Дата регистрации:
10.01.2018

Приоритет(ы):
(22) Дата подачи заявки: **27.04.2017**

(45) Опубликовано: **10.01.2018** Бюл. № 1

Адрес для переписки:
170012, г. Тверь, ул. Цветочная, 2, кв. 4, Дроботуну Е.Б.

(72) Автор(ы):
Дроботун Евгений Борисович (RU)

(73) Патентообладатель(и):
Дроботун Евгений Борисович (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2338243 C1, 10.11.2008. RU 19942 U1, 10.10.2001. RU 2210112 C2, 10.08.2003. SU 1113807 A, 15.09.1984. WO 2004/038594 A1, 06.05.2004. US 2006/0265750 A1, 23.11.2006. WO 2008/014507 A2, 31.01.2008. US 2008/0271025 A1, 30.10.2008. US 2013/0014263 A1, 10.01.2013.**

(54) СПОСОБ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ

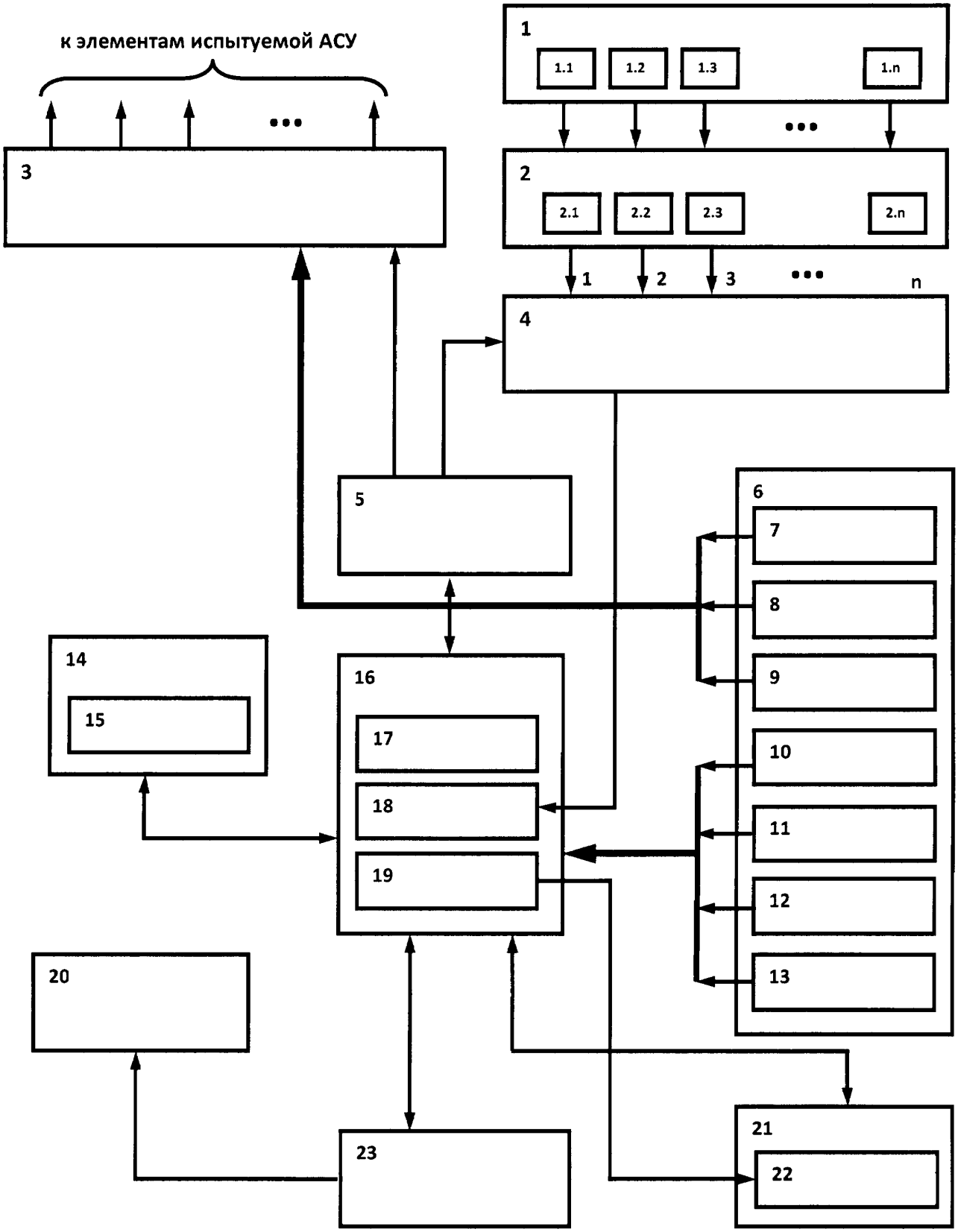
(57) Реферат:

Изобретение относится к способу оценки эффективности функционирования автоматизированных систем управления (АСУ). Технический результат заключается в расширении функциональных возможностей способа оценки эффективности АСУ за счет добавления в него процесса моделирования воздействия вредоносных программ на структурные элементы АСУ. Способ включает в себя выбор стратегии оценки эффективности управления; моделирование воздействие вредоносных программ на структурные элементы (СЭ) АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации, путем внедрения образцов вредоносного кода в память этих СЭ АСУ с помощью устройства моделирования воздействия вредоносных программ, на основе информации об уязвимостях программного и аппаратного обеспечения СЭ АСУ, полученной из запоминающего устройства (ЗУ) уязвимостей, ЗУ весовых коэффициентов, соответствующих критичности каждой уязвимости и ЗУ образцов вредоносного кода; затем автоматически считывают информацию с датчиков через преобразователи и записывают ее в ЗУ считанной информации терминального сервера, в котором преобразуют эту информацию к виду, удобному для текущей оценки, а затем оценивают ее по программе оценки эффективности управления. 1 ил., 1 табл.

RU 2640629 C1

RU 2640629 C1

RU 2640629 C1



Фиг. 1

RU 2640629 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 640 629**(13) **C1**

(51) Int. Cl.
G06F 21/57 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/577 *(2017.08);* ***G05B 17/00*** *(2017.08);* ***G06N 5/00*** *(2017.08);* ***G06F 11/3089*** *(2017.08);* ***G06F 15/16*** *(2017.08);* ***G06Q 10/06*** *(2017.08)*

(21)(22) Application: **2017115135, 27.04.2017**

(24) Effective date for property rights:
27.04.2017

Registration date:
10.01.2018

Priority:
(22) Date of filing: **27.04.2017**

(45) Date of publication: **10.01.2018** Bull. № **1**

Mail address:
170012, g. Tver, ul. Tsvetochnaya, 2, kv. 4, Drobotunu E.B.

(72) Inventor(s):
Drobotun Evgenij Borisovich (RU)

(73) Proprietor(s):
Drobotun Evgenij Borisovich (RU)

(54) METHOD OF FUNCTIONING PERFORMANCE EVALUATION OF AUTOMATED CONTROL SYSTEMS UNDER CONDITIONS OF MALICIOUS PROGRAMS IMPACT

(57) Abstract:

FIELD: information technology.

SUBSTANCE: method includes selecting a strategy for evaluating management effectiveness; modelling the impact of malicious programs on the structural elements (SE) of automated control systems (ACS) that receive, store, process, issue and display information by introducing samples of malicious code into the memory of these SE of automated control systems by using a malicious programs simulation device, based on information on software and hardware vulnerabilities of the SE of automated control systems obtained from a memory device (MD) of vulnerabilities, memory devices of weight coefficients corresponding to the criticality of each vulnerability and malware code memory device; then the information is automatically read from the sensors through the converters and written to the memory of the read out information of the terminal server in which this information is converted to a form convenient for the current evaluation and then evaluated by the program for evaluating the management efficiency.

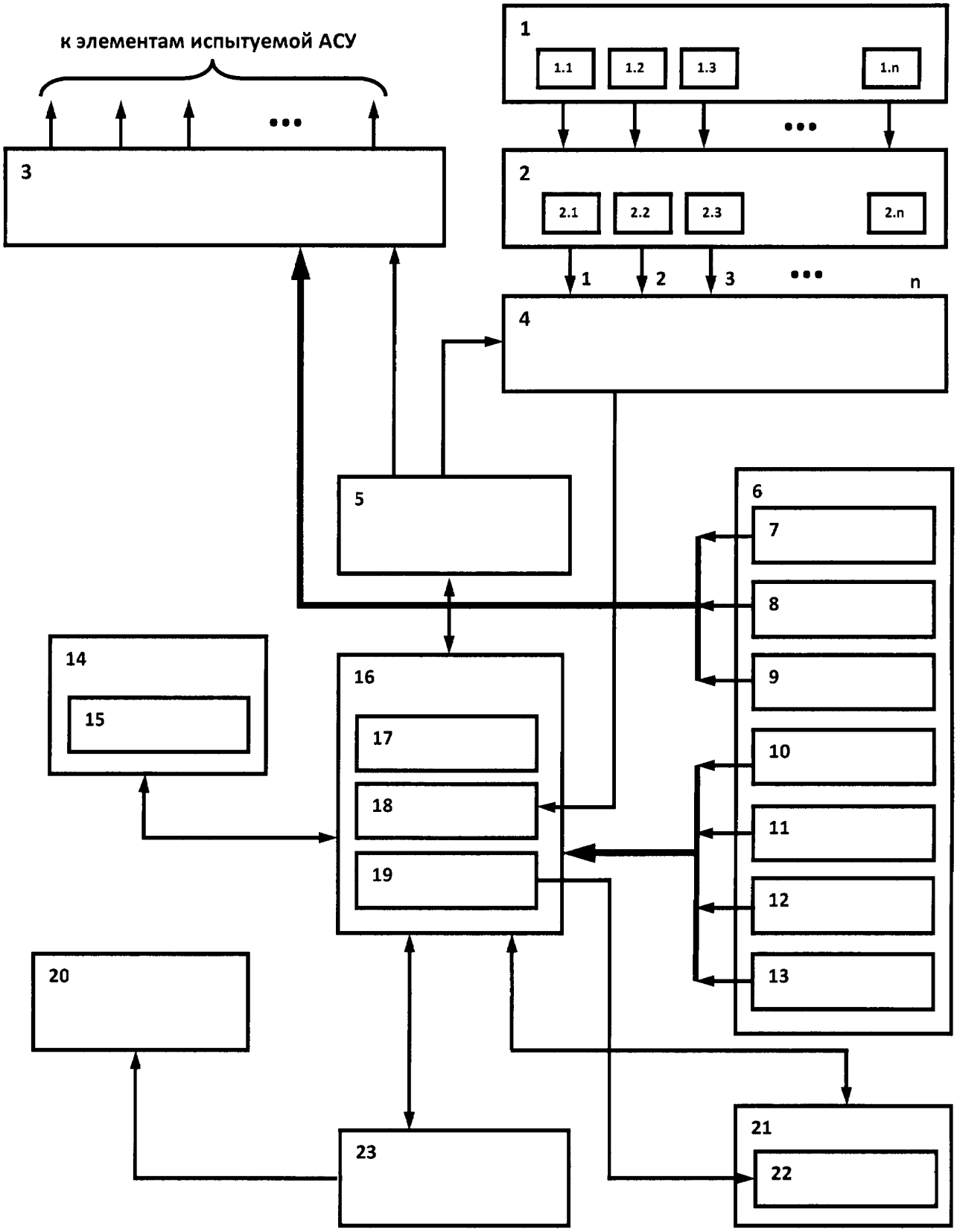
EFFECT: expansion of functioning performance evaluation of automated control systems by adding the process of simulating the malicious programs impact on the structural elements of the automated control systems.

1 dwg,1 tbl

RU 2640629 C1

RU 2640629 C1

RU 2640629 C1



Фиг. 1

RU 2640629 C1

Изобретение относится к области автоматизированных систем управления (АСУ) и может быть использовано для оценки эффективности автоматизированного управления системами широкого класса вне зависимости от их назначения, целей, решаемых задач и сложности.

Из уровня техники известен способ определения работоспособности объектов [см. Мозгалевский А. В., Гаскаров Д. В. Техническая диагностика. - М.: Высшая школа, 1975, с. 38-46], включающий измерение параметров и их сопоставление с соответствующими нормами (эталонами).

Недостатком известного способа является его узкая специализация - диагностика относительно несложных систем, что не позволяет осуществлять оценку эффективности управления сложными большими техническими системами.

Известен также способ [см. Автоматическая аппаратура контроля радиоэлектронного оборудования / Под ред. Н.Н. Пономарева - М.: Сов. радио, 1975, с. 5-10 и с. 293-318], включающий выбор с помощью коммутатора параметров, измерение параметров, преобразование параметров в цифровые данные, удобные для обработки на ЭВМ, регистрацию этих данных и их анализ, а также отображение и документирование результатов анализа.

Недостатком данного известного способа является узкая специализация, ограниченная возможностями контроля, диагностики и прогнозированием технического состояния радиоэлектронного оборудования, что является недостаточным для оценки эффективности управления сложными большими техническими системами, требующей более высокого уровня компьютерного обеспечения с базами данных и знаний, чего нет в аналоге.

Известен также унифицированный способ Чернякова/Петрушина для оценки эффективности больших систем [см. Россия, патент №2210112, G07C 3/08, G06F 17/00, опубл. 10.08.2003 г.], включающий в себя процедуру оценки в реальном масштабе времени, в которой записывают в запоминающее устройство (ЗУ) структурных элементов накопителя базы данных представление конкретной сложной большой технической системы в виде иерархии ее структурных элементов, в ЗУ параметров того же накопителя - частные показатели эффективности, поставленные в соответствие каждому элементу структуры технической системы, в ЗУ нормативов того же накопителя - нормативные значения, соответствующие каждому частному показателю эффективности, а в ЗУ весовых коэффициентов того же накопителя - весовые коэффициенты важности, соответствующие каждому частному показателю эффективности, а также в ЗУ терминального сервера записывают программу оценки эффективности и, наконец, в ЗУ рабочей станции инженера по знаниям загружают сведения, полученные в процессе опроса экспертов данной области знаний, далее с помощью рабочей станции старшего инженера по оценке эффективности осуществляют выбор стратегии оценки, затем с помощью рабочей станции ввода данных, управляя коммутатором, автоматически считывают информацию с датчиков через преобразователи и записывают ее через ЗУ преобразованной считанной информации в терминальном сервере в ЗУ считанной информации в терминальном сервере, в котором преобразуют эту информацию к виду, удобному для текущей оценки, и записывают ее в ЗУ сервера базы данных, а затем оценивают ее по программе оценки эффективности с помощью терминального сервера, при этом результатом оценки является оценка по обобщенному показателю эффективности, представляющему собой свертку частных показателей эффективности, соответствующих результатам анализа измеряемых параметров.

Указанный способ является наиболее близким по технической сущности к заявляемому.

Недостатком данного известного способа оценки эффективности является то, что с помощью этого способа нельзя оценить эффективность функционирования АСУ в условиях воздействия вредоносных программ.

Целью предлагаемого изобретения является расширение функциональных возможностей способа оценки эффективности функционирования АСУ в условиях воздействия вредоносных программ за счет добавления функции моделирования воздействия вредоносных программ на структурные элементы АСУ.

Поставленная задача решается за счет того, что в известном способе оценки эффективности управления, включающем в себя процедуру оценки в реальном масштабе времени, в которой записывают в ЗУ структурных элементов накопителя базы данных представление конкретной АСУ в виде иерархии ее структурных элементов, в ЗУ параметров того же накопителя - частные показатели эффективности управления, в ЗУ нормативов того же накопителя - нормативные значения, соответствующие каждому частному показателю эффективности управления, а в ЗУ весовых коэффициентов того же накопителя - весовые коэффициенты важности, соответствующие каждому частному показателю эффективности управления, а также в ЗУ терминального сервера записывают программу оценки эффективности управления и, наконец, в ЗУ рабочей станции по знаниям загружают сведения, полученные в процессе опроса экспертов данной области знаний, далее с помощью рабочей станции по оценке эффективности управления осуществляют выбор стратегии оценки эффективности управления, затем с помощью рабочей станции ввода данных, управляя коммутатором, автоматически считывают информацию с датчиков через преобразователи и записывают ее через ЗУ преобразованной считанной информации в терминальном сервере в ЗУ считанной информации в терминальном сервере, в котором преобразуют эту информацию к виду, удобному для текущей оценки, и записывают ее в ЗУ сервера базы данных, а затем оценивают ее по программе оценки эффективности управления с помощью терминального сервера, при этом результатом оценки является оценка по обобщенному показателю эффективности управления, представляющему собой свертку частных показателей эффективности управления, соответствующих результатам анализа измеряемых параметров, анализируют, отображают и документируют результаты оценки соответственно на видеомониторе и принтере, новым является то, что после выбора стратегии оценки эффективности непосредственно перед автоматическим считыванием информации с датчиков моделируют воздействие вредоносных программ на структурные элементы АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации, путем внедрения образцов вредоносного кода в память этих структурных элементов АСУ с помощью устройства моделирования воздействия вредоносных программ, на основе информации об уязвимостях программного и аппаратного обеспечения структурных элементов АСУ, полученной из ЗУ уязвимостей, ЗУ весовых коэффициентов, соответствующих критичности каждой уязвимости и ЗУ образцов вредоносного кода.

Необходимость использования частных показателей эффективности управления возникает ввиду сложности оценки эффективности АСУ каким-либо одним показателем, в связи с чем предлагается использование обобщенного показателя эффективности АСУ, который складывается из множества показателей, отражающих отдельные частные свойства АСУ (частных показателей эффективности управления) [см. В.И. Колисниченко. Об оценке эффективности АСУ ВВС // Военная мысль, 2004, №11. - с. 35-40].

При этом, частными показателями эффективности управления, являются показатели эффективности выполнения отдельных функций, возложенных на АСУ и, реализуемые отдельными элементами структуры АСУ.

В качестве частных показателей, характеризующих эффективность выполнения отдельных функций, возложенных на АСУ, возможно использование следующих показателей [см. Е.М. Науменко, Н.С. Козлов. Подход к оценке эффективности автоматизированных систем на ранних стадиях проектирования // Реєстрація, зберігання і обробка даних, 2007, Т. 9, № 4. - с. 132-139] (таблица 1):

- показатели оперативности (быстродействия) при выполнении отдельной функции АСУ;
- показатели устойчивости выполнения отдельной функции АСУ;
- показатели непрерывности выполнения отдельной функции АСУ;
- показатели, характеризующие пропускную способность при реализации отдельной функции АСУ;
- показатели точности выполнения отдельной функции АСУ.

Таблица 1

№	Оцениваемый фактор, характеризующий эффективность выполнения отдельной функции АСУ	Показатели, с помощью которых возможна оценка эффективности выполнения отдельной функции АСУ
1	Оперативность выполнения отдельной функции АСУ	Время на сбор, обработку и выдачу информации
		Время на принятие решения, постановку и доведение задач до исполнителей
2	Устойчивость выполнения отдельной функции АСУ	Средняя продолжительность безотказной работы элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Средняя наработка на один отказ элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Вероятность надежного функционирования элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Вероятности выхода из строя элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Степень (кратность) резервирования элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Время восстановления элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
3	Непрерывность выполнения отдельной функции АСУ	Математическое ожидание времени максимального перерыва в выполнении отдельной функции АСУ
		Математическое ожидание времени минимальной продолжительности бесперебойной работы элементов структуры АСУ, реализующих выполнение отдельной

№	Оцениваемый фактор, характеризующий эффективность выполнения отдельной функции АСУ	Показатели, с помощью которых возможна оценка эффективности выполнения отдельной функции АСУ
		функции АСУ, между двумя перерывами
4	Пропускная способность при выполнении отдельной функции АСУ	Коэффициент информационного наполнения элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
		Коэффициент обработки (переработки) информации
		Коэффициент потребления информации
		Суммарный показатель пропускной способности элементов структуры АСУ, реализующих выполнение отдельной функции АСУ
5	Точность выполнения отдельной функции АСУ	Степень соответствия информации реальным условиям обстановки (точность добывания, формирования, сбора, обработки и выдачи, а также ее давность)
		Суммарный коэффициент искажения информации (время давности информации; время старения информации)
		Среднеквадратические ошибки результатов выполнения отдельных функций АСУ

Более просто сущность предлагаемого способа состоит в том, что для любой по сложности АСУ, которую всегда можно представить иерархической декомпозицией ее структурных элементов и выполняемых ими функций управления, ставят во взаимно однозначное соответствие структуру показателей эффективности управления аналогичной топологии. При этом достаточной мерой оценки эффективности управления, осуществляемого АСУ, является, как минимум, соответствие ее частных показателей требованиям соответствующей проектной документации или действующим стандартам (нормам). Тогда уровень эффективности управления при выполнении всех без исключения норм принимается за достаточный уровень эффективности. Очевидно, что для оценки эффективности управления сложными большими техническими системами необходимы соответствующей мощности вычислительные ресурсы, включающие базу данных, базу знаний, основанную на экспертной системе, организованных в виде локальной вычислительной сети на базе персональных компьютеров, хранящих в своей памяти, с одной стороны, данные о топологии АСУ и ее показателях (параметрах), а с другой стороны, соответствующие им нормы (технические задания, ГОСТ, требования проектной документации и т.п.), а также данные об уязвимостях программного и аппаратного обеспечения использованного при построении оцениваемой системы. Тогда предлагаемый способ оценки эффективности АСУ сводится к подготовке данных перед процедурой оценки эффективности АСУ, включая подготовку данных об уязвимостях программного и аппаратного обеспечения, а затем к самой процедуре, в процессе которой производится моделирование воздействия вредоносных программ и обеспечивается свертка частных показателей эффективности управления, соответствующих составляющим элементам АСУ. В результате получается обобщенный показатель эффективности функционирования АСУ в условиях воздействия вредоносных программ. Аналогичная свертка может выполняться для каждой части АСУ (подсистем и блоков).

Перечисленные отличительные признаки заявленного изобретения позволяют расширить функциональные возможности способа оценки эффективности

функционирования автоматизированных систем управления в условиях воздействия вредоносных программ за счет обеспечения моделирования воздействий вредоносных программ на оцениваемую систему.

Предлагаемые технические решения являются новыми, поскольку из общедоступных сведений не известны предлагаемый способ оценки эффективности функционирования автоматизированных систем управления в условиях воздействия вредоносных программ.

Предлагаемые технические решения имеют изобретательский уровень, поскольку из опубликованных научных данных и известных технических решений явным образом не следует, что заявленная последовательность операций способа приводят к расширению функциональных возможностей способа оценки эффективности функционирования автоматизированных систем управления в условиях воздействия вредоносных программ.

Предлагаемые технические решения промышленно применимы, так как основаны на компьютерной технике и средствах моделирования, широко применяющихся при моделировании процессов управления в автоматизированных системах управления.

Заявляемое изобретение поясняется конкретным примером реализации, который, однако, не является единственно возможным, но наглядно демонстрирует возможность достижения приведенной совокупностью признаков требуемого технического результата.

На фиг. 1 представлена структурная схема устройства для осуществления заявляемого способа, на которой цифрами обозначены:

1 - группа датчиков параметров АСУ;

2 - группа преобразователей параметров информации;

3 - устройство моделирования воздействия вредоносных программ;

4 - коммутатор;

5 - рабочая станция ввода данных;

6 - накопитель базы данных;

7 - ЗУ уязвимостей программного и аппаратного обеспечения;

8 - ЗУ весовых коэффициентов критичности уязвимостей программного и аппаратного обеспечения;

9 - ЗУ образцов вредоносного кода;

10 - ЗУ структурных элементов АСУ;

11 - ЗУ параметров;

12 - ЗУ нормативов;

13 - ЗУ весовых коэффициентов важности показателей эффективности АСУ;

14 - рабочая станция по знаниям;

15 - ЗУ сведений опроса экспертов;

16 - терминальный сервер;

17 - ЗУ программы оценки эффективности управления;

18 - ЗУ считанной информации;

19 - ЗУ преобразованной считанной информации;

20 - устройства отображения и документирования (видеомонитор и принтер);

21 - сервер базы данных;

22 - ЗУ преобразованной информации;

23 - рабочая станция по оценке эффективности управления. Заявленный способ оценки эффективности функционирования автоматизированных систем управления в условиях воздействия вредоносных программ осуществляется следующим образом.

В ЗУ структурных элементов АСУ 10 накопителя базы данных 6 записывают

представление конкретной автоматизированной системы управления в виде иерархии ее структурных элементов, в ЗУ параметров 11 того же накопителя записывают частные показатели эффективности управления, в ЗУ нормативов 12 того же накопителя записывают нормативные значения, соответствующие каждому частному показателю эффективности управления, а в ЗУ весовых коэффициентов важности показателей эффективности 13 того же накопителя записывают весовые коэффициенты важности, соответствующие каждому частному показателю эффективности АСУ, в ЗУ уязвимостей программного и аппаратного обеспечения 7 того же накопителя записывают данные об уязвимостях программного и аппаратного обеспечения структурных элементов АСУ, в ЗУ весовых коэффициентов критичности уязвимостей программного и аппаратного обеспечения 8 того же накопителя записывают весовые коэффициенты критичности уязвимостей, в ЗУ образцов вредоносного кода 9 того же накопителя записывают образцы вредоносного кода, в ЗУ 17 терминального сервера 16 записывают программу оценки эффективности управления, в ЗУ сведений опроса экспертов 15 рабочей станции по знаниям 14 загружают сведения, полученные в процессе опроса экспертов данной области знаний. Далее с помощью рабочей станции по оценке эффективности управления 23 осуществляют выбор стратегии оценки эффективности управления. Затем с помощью рабочей станции ввода данных 5 запускают на моделирование устройство моделирования воздействия вредоносного кода 3. На основе информации из ЗУ уязвимостей программного и аппаратного обеспечения 7, информации о весовых коэффициентах критичности уязвимостей из ЗУ 8, а также с использованием образцов вредоносного кода из ЗУ 9 моделируют воздействие на АСУ вредоносных программ путем внедрения вредоносного кода в память структурных элементов АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации (операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, программируемые логические контроллеры, иные технические средства с установленным программным обеспечением [см. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: утв. пр. ФСТЭК России от 14 марта 2014 г. №31, с. 4]). После этого с помощью рабочей станции ввода данных 5, управляя коммутатором 4, автоматически считывают информацию с датчиков 1.1, 1.2, 1.3, …, 1.n через преобразователи 2.1, 2.1, 2.3, …, 2.n на входы 1, 2, 3, n того же коммутатора 4, записывают ее в ЗУ считанной информации 18 в терминальном сервере 16, в котором преобразуют эту информацию к виду, удобному для текущей оценки, и записывают ее через ЗУ преобразованной считанной информации 19 в терминальном сервере 16 в ЗУ преобразованной информации 22 сервера базы данных 21. Затем оценивают ее по программе оценки эффективности управления с помощью терминального сервера 16, при этом результатом оценки является оценка по обобщенному показателю эффективности управления, представляющему собой свертку частных показателей эффективности управления, соответствующих результатам анализа измеряемых и моделируемых параметров. Анализируют, отображают и документируют результаты оценки с помощью устройств отображения 20.

Датчики 1.1, 1.2, 1.3, …, 1.n производят считывание информации, позволяющей оценить частные показатели эффективности, со структурных элементов АСУ, реализующих выполнение отдельных функций АСУ. При этом для оценки показателей,

характеризующих оперативность, производится измерение и считывание временных характеристик структурных элементов АСУ (время отображения информации на автоматизированных рабочих местах, время реакции системы на управляющее воздействие оператора, произведенного с автоматизированного рабочего места, время выполнения отдельных операций, посредством которых реализуется функция АСУ, в промышленном сервере или в промышленном логическом контроллере, время обработки информации в промышленном сервере или промышленном логическом контроллере); для оценки показателей, характеризующих устойчивость и непрерывность выполнения отдельной функции АСУ производится измерение и считывание временных характеристик структурных элементов АСУ (время работы до выхода какого-либо структурного элемента АСУ из строя, время работы структурных элементов АСУ, реализующих выполнение отдельных функций АСУ, без сбоев, время перезагрузки системы после сбоя), а также считывание информации о техническом состоянии структурных элементов АСУ (количество сбоев и отказов за определенный промежуток времени); для оценки показателей, характеризующих пропускную способность, производится измерение и считывание информации о количестве принятых, переданных и обработанных данных (объем переданных данных по линиям (каналам) связи за определенное время, объем обработанных в промышленном сервере данных за определенное время, объем данных, обрабатываемых в промышленном сервере одновременно); для показателей, характеризующих точность выполнения отдельной функции АСУ, производится измерение и считывание данных с датчиков, которые считывают информацию о состоянии объектов, которые управляются с помощью АСУ и считывание информации о состоянии этих объектах после их обработки в промышленных логических контроллерах или промышленных серверах, либо после отображения информации о состоянии этих объектов на автоматизированных рабочих местах, после чего, путем сравнения и обработки полученных данных, производится оценка точностных показателей выполнения отдельной функции АСУ.

Вредоносный код, внедренный в память структурных элементов АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации нарушает процессы функционирования этих структурных элементов АСУ (вносит ошибки в процесс обработки информации; осуществляет подмену принятых, обрабатываемых или выдаваемых данных; нарушает последовательность операций обработки информации в промышленных серверах и (или) промышленных логических контроллерах; вносит искажения в отображаемую на автоматизированных рабочих местах информацию; загружает процессоры промышленных серверов и промышленных логических контроллеров выполнением ложных (мусорных) команд; снижает пропускную способность линий (каналов) связи путем внедрения в передаваемые данные ложной (мусорной) информации; выводит из строя структурные элементы АСУ путем искажения или уничтожения компонентов общесистемного и специального программного обеспечения; генерирует ложные сообщения об ошибках и сбоях структурных элементов АСУ; вносит изменения в обрабатываемые данные, которые приводят к сбоям структурных элементов АСУ).

Данные нарушения процессов функционирования структурных элементов АСУ приводят к снижению эффективности выполнения как отдельных задач, возложенных на АСУ, так и к снижению эффективности функционирования АСУ в целом, при этом, если снижение эффективности АСУ выходит за допустимые пределы, то необходимо вводить в ее состав дополнительные механизмы (средства) защиты от воздействия вредоносных программ.

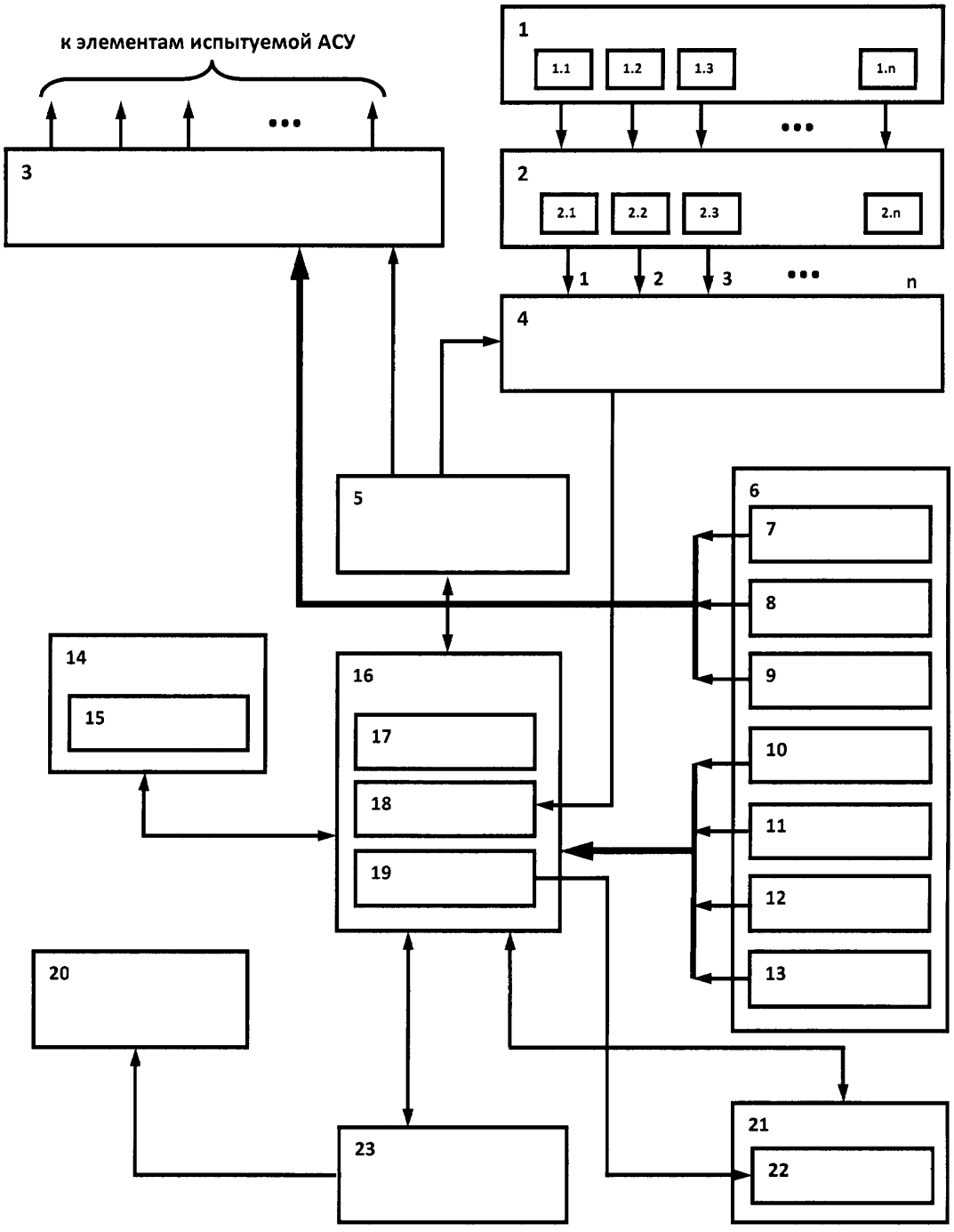
Таким образом, предлагаемый способ позволит производить оценку эффективности автоматизированных систем управления в условиях воздействия на такие системы вредоносных программ и принимать решение о необходимости осуществления дополнительных мер защиты автоматизированных систем управления от вредоносных программ.

(57) Формула изобретения

Способ оценки эффективности функционирования автоматизированных систем управления в условиях воздействия вредоносных программ, включающий в себя процедуру оценки в реальном масштабе времени, в которой записывают в запоминающее устройство (ЗУ) структурных элементов накопителя базы данных представление конкретной автоматизированной системы управления (АСУ) в виде иерархии ее структурных элементов, в ЗУ параметров того же накопителя записывают частные показатели эффективности управления, в ЗУ нормативов того же накопителя записывают нормативные значения, соответствующие каждому частному показателю эффективности управления, а в ЗУ весовых коэффициентов того же накопителя записывают весовые коэффициенты важности, соответствующие каждому частному показателю эффективности управления, а также в ЗУ терминального сервера записывают программу оценки эффективности управления и, наконец, в ЗУ рабочей станции по знаниям загружают сведения, полученные в процессе опроса экспертов данной области знаний, далее с помощью рабочей станции по оценке эффективности управления осуществляют выбор стратегии оценки эффективности управления и затем с помощью рабочей станции ввода данных, управляя коммутатором, автоматически считывают информацию с датчиков через преобразователи и записывают ее в ЗУ считанной информации терминального сервера, в котором преобразуют эту информацию к виду, удобному для текущей оценки, и записывают ее через ЗУ преобразованной считанной информации терминального сервера в ЗУ сервера базы данных, а затем оценивают ее по программе оценки эффективности управления с помощью терминального сервера, при этом результатом оценки является оценка по обобщенному показателю эффективности управления, представляющему собой свертку частных показателей эффективности управления, соответствующих результатам

анализа измеряемых параметров, анализируют, отображают и документируют результаты оценки на видеомониторе и принтере, отличающийся тем, что после выбора стратегии оценки эффективности непосредственно перед автоматическим считыванием информации с датчиков моделируют воздействие вредоносных программ на структурные элементы АСУ, которые осуществляют прием, хранение, обработку, выдачу и отображение информации, путем внедрения образцов вредоносного кода в память этих структурных элементов АСУ с помощью устройства моделирования воздействия вредоносных программ, на основе информации об уязвимостях программного и аппаратного обеспечения структурных элементов АСУ, полученной из ЗУ уязвимостей, ЗУ весовых коэффициентов, соответствующих критичности каждой уязвимости и ЗУ образцов вредоносного кода.

1


к элементам испытуемой АСУ
1
1.1
1.2
1.3
1.n
2
2.1
2.2
2.3
2.n
1
2
3
n
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

Фиг. 1