РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 642 374**(13) **C1**

(51) МПК
G06F 21/57 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/57 (2017.08); G06F 21/577 (2017.08)

(21)(22) Заявка: **2017113170, 17.04.2017**

(24) Дата начала отсчета срока действия патента:
17.04.2017

Дата регистрации:
24.01.2018

Приоритет(ы):
(22) Дата подачи заявки: **17.04.2017**

(45) Опубликовано: **24.01.2018** Бюл. № **3**

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 2331097 C1, 10.08.2008. RU 2558238 C2, 27.07.2015. US 7895659 B1, 22.02.2011. US 2008/0276295 A1, 06.11.2008. US 2008/0072281 A1, 20.03.2008.**

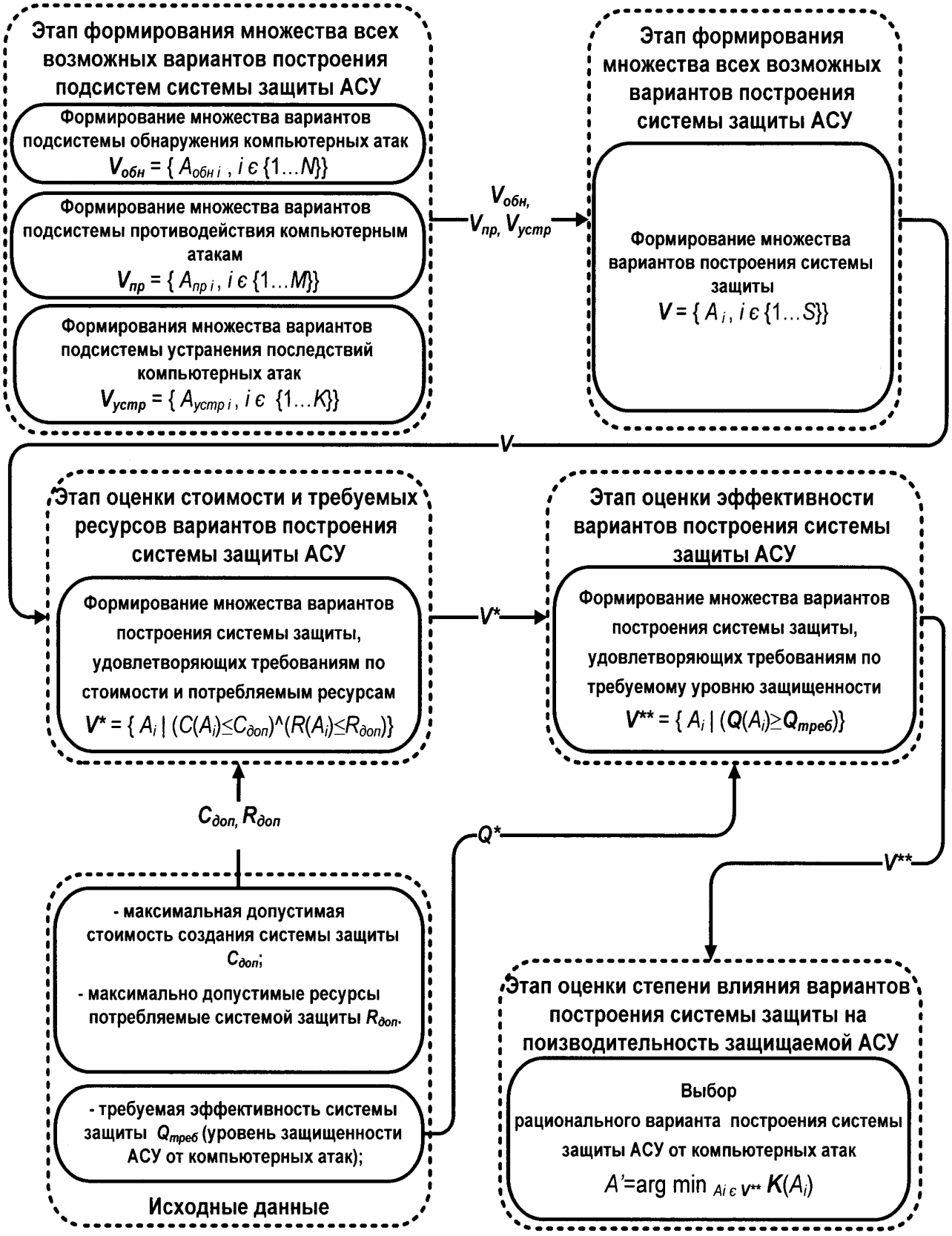
(54) СПОСОБ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

(57) Реферат:

Изобретение относится к области систем защиты автоматизированных систем управления различного назначения от информационно-технических воздействий и может быть использовано для построения систем защиты автоматизированных систем управления (АСУ) от одного из основных видов информационно-технических воздействий - компьютерных атак. Технический результат, заключающийся в получении наиболее эффективного варианта построения системы защиты АСУ от компьютерных атак с наименьшим воздействием на производительность защищаемой АСУ, достигается за счет использования способа построения системы защиты АСУ от компьютерных атак, включающего в себя этап формирования множества всех возможных вариантов построения подсистем системы защиты АСУ от компьютерных атак, этап формирования множества всех возможных вариантов построения системы защиты АСУ от компьютерных атак, этап оценки стоимости и требуемых ресурсов вариантов построения системы защиты АСУ от компьютерных атак, этап оценки эффективности вариантов построения системы защиты АСУ от компьютерных атак и этап оценки степени влияния вариантов построения системы защиты на производительность защищаемой АСУ. 3 ил.

RU 2642374 C1

RU 2642374 C1



Фиг. 3

RU 2642374 C1
RU 2642374 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 642 374**(13) **C1**

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

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/57 (2017.08); G06F 21/577 (2017.08)

(21)(22) Application: **2017113170, 17.04.2017**

(24) Effective date for property rights:
17.04.2017

Registration date:
24.01.2018

Priority:
(22) Date of filing: **17.04.2017**

(45) Date of publication: **24.01.2018** Bull. № **3**

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)

RU 2642374 C1

(54) METHOD FOR CONSTRUCTION OF COMPUTER ATTACK PROTECTION SYSTEM FOR AUTOMATED CONTROL SYSTEMS

(57) Abstract:

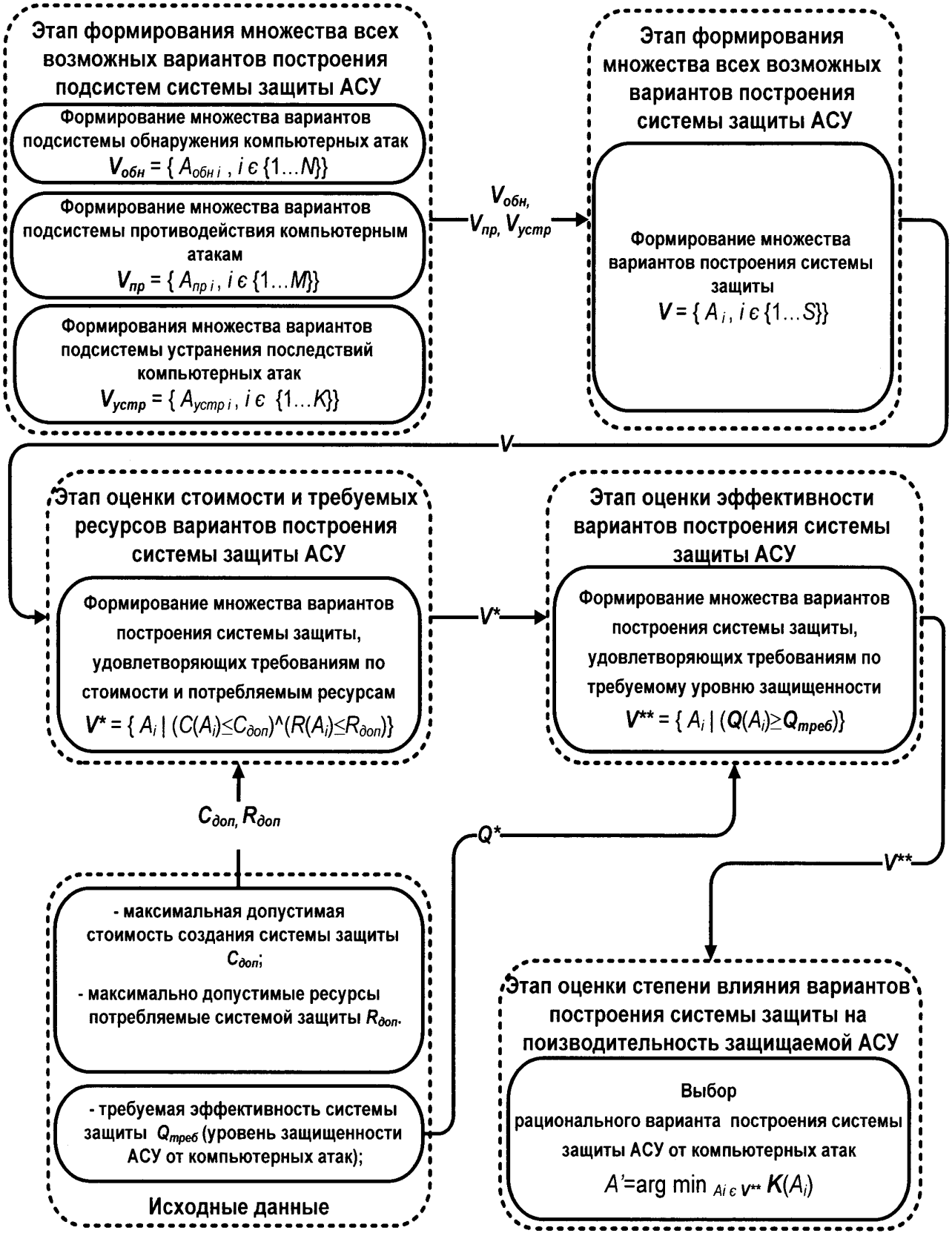
FIELD: information technologies.

SUBSTANCE: invention relates to the field of protection systems for automated control systems for various purposes from information and technical effects and can be used to build systems to protect automated control systems (ACS) from one of the main types of information and technology impacts – computer attacks. Technical result is achieved due to the use of the method of constructing a system for protection of ACS from computer attacks, which includes a step of forming a set of all possible versions of building subsystems of the system for protection of ACS from computer attacks, a step of forming a set of all possible versions for building a system for protecting ACS against computer attacks, a step of estimating the cost and required resources of versions for building a system for protecting ACS against computer attacks, a step of estimating efficiency of versions of building a system for protection of ACS from computer attacks and step of estimating the degree of impact of versions of building the protection system on the performance of the protected ACS.

EFFECT: obtaining the most effective version of building a system for protecting ACS from computer attacks with the least impact on the performance of the protected ACS.

1 cl, 3 dwg

RU 2642374 C1



Фиг. 3

RU 2642374 C1
RU 2642374 C1

Изобретение относится к области систем защиты автоматизированных систем управления различного назначения от информационно-технических воздействий и может быть использовано для построения систем защиты автоматизированных систем управления (АСУ) от одного из основных видов информационно-технических воздействий - компьютерных атак.

Для обеспечения защищенности АСУ от компьютерных атак применяются различные меры технического характера, которые реализуются в виде систем защиты.

Согласно [1] технические меры защиты информации (с точки зрения защиты от компьютерных атак), реализуемые в АСУ в рамках ее системы защиты, должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность автоматизированной системы управления и информации;
- доступность технических средств и информации.

При этом реализация указанных технических мер в рамках системы защиты АСУ от компьютерных атак не должна оказывать отрицательного влияния на штатный режим функционирования АСУ (т.е. не должна снижать производительность АСУ).

Исходя из данных требований задача построения системы защиты АСУ от компьютерных атак сводится к задаче выбора таких структуры и параметров системы защиты АСУ от компьютерных атак, чтобы система защиты, отвечающая выбранным структуре и параметрам, позволяла обеспечить минимальное воздействие на производительность защищаемой АСУ при сохранении требуемого уровня защиты от компьютерных атак и удовлетворяла требованиям по стоимости и потребляемым ресурсам.

Из уровня техники известны способ автоматизированного управления процессом проектирования структуры системы управления техническими системами и устройство для его осуществления [2], которые могут применяться для проектирования многопараметрических объектов.

Недостатком указанных способа и устройства является их узкая специализация - проектирование систем управления техническими системами различного класса, что не позволяет осуществлять построение системы защиты АСУ от компьютерных атак.

Известны также способ и устройство выбора предпочтительного средства защиты информации [3], основанные на использовании оцениваемой выборки, состоящей из нормированных единичных показателей качества, позволяющих создать два эталона $Э_с$ - со среднестатистическим уровнем качества и $Э_л$ - уровнем лучшего качества. На основе использования этих эталонов из всей совокупности оцениваемых средств выбирается предпочтительный объект, обладающий наибольшим комплексным показателем качества.

Недостатком указанных способа и устройства является невозможность их применения при построении системы защиты АСУ от компьютерных атак, состоящей из нескольких взаимосвязанных элементов с учетом их влияния на производительность защищаемой АСУ.

Целью изобретения является получение наиболее эффективного варианта построения системы защиты АСУ от компьютерных атак с наименьшим воздействием на производительность защищаемой АСУ.

Для достижения цели изобретения предлагается использовать способ построения системы защиты от компьютерных атак для автоматизированных систем, основанный на декомпозиции задачи выбора рациональных структуры и параметров системы защиты АСУ от компьютерных атак по последовательности процедур формирования вариантов построения системы защиты и по подсистемам системы защиты (функциональная декомпозиция).

Декомпозиция по подсистемам основывается на том, что систему защиты АСУ от компьютерных атак можно представить в виде множества подсистем, решающих определенные задачи и реализующие определенный перечень функций. Исходя из этого в качестве подсистем, обеспечивающих защищенность АСУ от компьютерных атак в составе системы защиты, можно выделить:

- подсистему обнаружения компьютерных атак;
- подсистему противодействия компьютерным атакам;
- подсистему устранения последствий применения компьютерных атак.

На фиг. 1 показаны декомпозиция системы защиты на подсистемы в соответствии с целями и задачами системы защиты, а также показаны способы решения задач каждой подсистемой.

На фиг. 2 показано соотношение способов решения задач подсистемами системы защиты с техническими мерами защиты от компьютерных атак.

Декомпозиция по последовательности выполнения процедур формирования вариантов построения системы защиты будет иметь следующий вид:

- формирование множеств $V_{обн}$, $V_{пр}$, $V_{устр}$ всех возможных вариантов $A_{обн}$, $A_{пр}$, $A_{устр}$ построения каждой подсистемы:

$$V_{обн} = \{ A_{обн\,i}, i \in \{1 \ldots N\}\},$$

$$V_{пр} = \{ A_{пр\,i}, i \in \{1 \ldots M\}\},$$

$$V_{устр} = \{ A_{устр\,i}, i \in \{1 \ldots K\}\},$$

где $V_{обн}$ - множество всех возможных вариантов построения подсистемы обнаружения компьютерных атак;

$V_{пр}$ - множество всех возможных вариантов построения подсистемы противодействия компьютерным атакам;

$V_{устр}$ - множество всех возможных вариантов построения подсистемы устранения последствий применения компьютерных атак;

N, M и K - количество всех возможных вариантов построения подсистем обнаружения компьютерных атак, противодействия компьютерным атакам и устранения последствий применения компьютерных атак соответственно;

- формирование множества V всех возможных вариантов A построения системы защиты на основе множеств $V_{обн}$, $V_{пр}$, $V_{устр}$ множества вариантов системы защиты:

$$V = \{A_i, i \in \{1 \ldots S\}\},$$

где S - количество всех возможных вариантов построения системы защиты;

- оценка сформированного множества V вариантов A построения системы защиты и выделение из него подмножества V* вариантов A*, удовлетворяющих требованиям по стоимости и потребляемым ресурсам;

• оценка сформированного множества V* вариантов A* построения системы защиты, удовлетворяющих по стоимости и потребляемым ресурсам и выделение из него подмножества V** вариантов A** построения системы защиты, удовлетворяющих требованиям по защищенности;

• оценка сформированного множества V** вариантов A** построения системы защиты, удовлетворяющих требованиям по защищенности, и выбор из рационального варианта A' построения системы защиты, оказывающего минимальное воздействие на производительность защищаемой АСУ.

Общая схема процесса выбора рационального варианта построения системы защиты АСУ от компьютерных атак представлена на фиг. 3.

Исходными данными для построения системы защиты АСУ от компьютерных атак являются:

• требуемая эффективность системы защиты АСУ от компьютерных атак Q* выражаемая совокупностью показателей, характеризующих способность системы защиты обеспечить минимальный риск от компьютерных атак и восстанавливаемость АСУ после применения компьютерных атак;

• максимально допустимая стоимость $C_{доп}$ создания системы защиты от компьютерных атак;

• максимально допустимые требуемые для функционирования системы защиты ресурсы $R_{доп}$.

На этапе формирования множеств всех возможных вариантов построения подсистем производится формирование множества всех возможных вариантов построения подсистемы обнаружения компьютерных атак, множества всех возможных вариантов построения подсистемы противодействия компьютерным атакам и множества всех возможных вариантов построения подсистемы устранения последствий применения компьютерных атак.

Для формирования этих множеств использован метод морфологического анализа [4], преимуществом которого является возможность простой алгоритмизации и компьютерной реализации.

Вариант каждой подсистемы формируется на основе структуры подсистемы, которая представляет собой совокупность элементов L подсистемы, реализующих способы решения задач подсистемы и совокупности параметров F подсистемы, а множество этих вариантов формируется путем перебора всех возможных комбинаций сочетаний элементов подсистемы и их параметров

Для подсистемы обнаружения компьютерных атак все возможные варианты формируются исходя из совокупности множеств $\{L_{обн}, F_{обн}\}$, где $L_{обн}$ - множество всех существующих средств обнаружения компьютерных атак, а $F_{обн}$ - множество совокупностей параметров для каждого средства обнаружения компьютерных атак.

Для подсистемы противодействия компьютерным атакам все возможные варианты формируются исходя из совокупности множеств $\{L_{пр}, F_{пр}\}$, где $L_{пр}$ - множество всех существующих средств противодействия компьютерным атакам, а $F_{пр}$ - множество совокупностей параметров для каждого средства противодействия компьютерным атакам.

Для подсистемы устранения последствий применения компьютерных атак все возможные варианты формируются исходя из совокупности множеств $\{L_{устр}, F_{устр}\}$, где $L_{устр}$ - множество всех существующих средств резервного копирования и

восстановления системы и данных, а $F_{устр}$ - множество совокупностей параметров для каждого средства резервного копирования и восстановления системы и данных.

Для снижения количества всех возможных вариантов построения каждой подсистемы (с целью уменьшения временных затрат), для параметров с плавно изменяющимися значениями принимаются три возможных значения: минимальное значение параметра, среднее значение параметра и максимальное значение параметра.

Далее, на этапе формирования множества всех возможных вариантов построения системы защиты АСУ от компьютерных атак исходя из множеств $V_{обн}$, $V_{пр}$ и $V_{устр}$, полученных на предыдущем этапе, с помощью метода морфологического анализа формируется множество V всех возможных вариантов построения системы защиты путем перебора всех возможных комбинаций сочетаний вариантов построения подсистем.

Далее, на этапе оценки стоимости и требуемых ресурсов, производится формирование множества V* - вариантов построения системы защиты АСУ от компьютерных атак, удовлетворяющих требованиям по стоимости и требуемым для функционирования системы защиты ресурсам:

$$V^* = \{ A_i \mid (C(A_i) \le C_{доп}) \wedge (R(A_i) \le R_{доп}) \},$$

где C и R - стоимость системы защиты и требуемые для функционирования системы защиты ресурсы;

$C_{доп}$ и $R_{доп}$ - максимально допустимые стоимость и требуемые ресурсы.

Стоимость C системы защиты складывается из стоимости подсистем, входящих в ее состав:

$$C=C_{обн}+C_{пр}+C_{устр},$$

где $C_{обн}$, $C_{пр}$, $C_{устр}$ стоимость подсистемы обнаружения компьютерных атак, стоимость подсистемы противодействия компьютерным атакам и стоимость подсистемы устранения последствий применения компьютерных атак соответственно.

Ресурсы R, требуемые для функционирования системы защиты, определяются двумя показателями: $R_{выч}$ - вычислительные ресурсы (требуемый объем памяти, характеристики процессоров и т.п.) и $R_{люд}$ - людские (требуемое количество обслуживающего персонала, необходимого для эксплуатации системы защиты):

$$R = \{R_{выч}, R_{люд}\}.$$

В формируемое на данном этапе множество V* отбираются варианты построения системы защиты, стоимость и требуемые для функционирования ресурсы которых не превышают максимально допустимые $C_{доп}$ и $R_{доп}$.

На этапе оценки эффективности вариантов построения системы защиты из множества V* отбираются варианты построения системы защиты, удовлетворяющие требуемому уровню защищенности, обеспечиваемому системой защиты, и из отобранных вариантов формируется множество V**:

$$V^{**} = \{ A_i \mid (Q(A_i) \ge Q_{треб}) \},$$

где Q - совокупность показателей, характеризующих уровень защищенности АСУ, реализуемый системой защиты;

$Q_{треб}$ - требуемый уровень защищенности АСУ.

В качестве показателей, характеризующих уровень защищенности АСУ от компьютерных атак, используются коэффициент защищенности АСУ Z [5] и время

восстановления работоспособности АСУ после применения компьютерной атаки $T_{восст}$:

$$\boldsymbol{Q} = \{Z,\ T_{восст}\}.$$

Методика определения коэффициента защищенности АСУ Z изложена в [5]. Сущность методики заключается в проведении тестирования АСУ по двум направлениям: локального тестирования и сетевого. Локальное тестирование заключается в проверке состояния защищенности отдельных элементов АСУ от внутреннего нарушителя. Сетевое тестирование заключается в моделировании действий внешнего нарушителя и направлено на проверку защищенности АСУ в целом.

По итогам локального тестирования определяется локальный коэффициент уязвимости L, который определяется следующим образом:

$$L = \sum_{i=1}^{n} \frac{Y_i}{P_i},$$

где P_i - количество открытых портов на i-м элементе АСУ;

Y_i - количество портов i-х элементов АСУ, на которых были найдены уязвимости.

По итогам сетевого тестирования определяется коэффициент уязвимости S вычислительной сети, объединяющей составные элементы АСУ:

$$S = \sum_{i=1}^{n} \frac{R_i}{E_O + A_O},$$

где R_i - количество реализованных сценариев компьютерных атак на i-м элементе АСУ;

E_o - количество основных сценариев моделирования компьютерных атак;

A_o - количество дополнительных сценариев моделирования компьютерных атак.

Далее находится коэффициент общей уязвимости системы W, который определяется следующим образом:

$W=L\cdot S$.

Исходя из того, что уровень защиты АСУ и уровень общей уязвимости АСУ дополняют друг друга до единицы, коэффициент защищенности системы Z можно определить как:

$Z=1-W$.

Время восстановления работоспособности АСУ после компьютерной атаки $T_{восст}$ определяется как сумма общего времени восстановления данных из резервных копий $T_{восстдан}$ и времени восстановления операционной системы из точек восстановления $T_{восст.\ ос}$:

$T_{восст} = T_{восст.\ данн} + T_{восст.\ ос}$.

На заключительном этапе выбора рационального варианта построения системы защиты АСУ от компьютерных атак из множества V**, полученного на предыдущем этапе, выбирается рациональный вариант A' построения системы защиты АСУ от компьютерных атак, который обеспечивает минимальное воздействие на производительность защищаемой АСУ:

$$A' = \arg\min_{A_i \in V^{**}} \boldsymbol{K}(A_i),$$

где K - совокупность показателей снижения производительности АСУ при введении

в ее состав системы защиты от компьютерных атак.

Совокупность показателей снижения производительности АСУ представляет собой два комплексных показателя K_C - комплексный показатель снижения производительности технической компоненты АСУ (совокупности аппаратных, программных и программно-аппаратных средств АСУ) и $K_П$ - комплексный показатель снижения производительности обслуживающего персонала:

$$\boldsymbol{K} = \{\boldsymbol{K_C}, \boldsymbol{K_П}\}.$$

При этом, снижение производительности технической компоненты АСУ оценивается как:

$$\boldsymbol{K_C} = \{K_{ПС}; K_{ПАР}; K_{РЕС}; K_{Тоткл}; K_{ОШ}\},$$

где $K_{ПС}$ - коэффициент снижения пропускной способности (количества операций, выполняемой системой за определенный период времени);

$K_{ПАР}$ - коэффициент снижения параллелизма (количества операций, выполняемых системой одновременно);

$K_{РЕС}$ - коэффициент увеличения запаса ресурса (количества ресурсов, необходимых для обеспечения роста нагрузки);

$K_{Тоткл}$ - коэффициент увеличения времени отклика (времени выполнения одной операции);

$K_{ОШ}$ - коэффициент увеличения частоты ошибок (частоты генерации системой исключений типа «отказ в обслуживании»).

Снижение производительности обслуживающего персонала, в свою очередь оценивается как:

$$\boldsymbol{K_П} = \{K_{Твып}; K_Д\},$$

где: $K_{Твып}$ - коэффициент увеличения времени выполнения операций лицами обслуживающего персонала при выполнении ими функциональных обязанностей;

$K_Д$ - коэффициент повышения дискомфорта при выполнении функциональных обязанностей.

Коэффициент снижения пропускной способности $K_{ПС}$ определяется следующим образом:

$$K_{ПС} = \frac{k_{ПС} - k'_{ПС}}{k_{ПС}}$$

где $k_{ПС}$ - количество операций, выполняемых АСУ за время $T_{исп}$ до введения в состав АСУ системы защиты от компьютерных атак;

$k'_{ПС}$ - количество операций, выполняемых АСУ за время $T_{исп}$ после введения в состав АСУ системы защиты от компьютерных атак, при этом время $T_{исп}$ определяется исходя из предназначения и выполняемых функций защищаемой АСУ.

Коэффициент снижения параллелизма $K_{ПАР}$ определяется по формуле:

$$K_{ПАР} = \frac{k_{ПАР} - k'_{ПАР}}{k_{ПАР}},$$

где $k_{ПАР}$ - количество операций, выполняемых АСУ одновременно до введения в состав АСУ системы защиты компьютерных атак;

$k'_{ПАР}$ - количество операций, выполняемых АСУ одновременно после введения в состав АСУ системы защиты от компьютерных атак.

Коэффициент увеличения запаса ресурса $K_{РЕС}$ определяется по следующей формуле:

$$K_{РЕС} = \frac{k_{РЕС} - k'_{РЕС}}{k_{РЕС}},$$

где $k_{РЕС}$ - вычислительные ресурсы, доступные для обеспечения функциональности АСУ до введения в состав АСУ системы защиты от компьютерных атак;

$k'_{РЕС}$ - вычислительные ресурсы, доступные для обеспечения функциональности АСУ после введения в состав АСУ системы защиты от компьютерных атак.

Коэффициент увеличения времени отклика $K_{Тоткл}$ определяется следующим образом:

$$K_{Тоткл} = \frac{t'_{откл} - t_{откл}}{t'_{откл}},$$

где $t'_{откл}$ - время выполнения одной операции в АСУ после введения в состав АСУ системы защиты от компьютерных атак;

$t_{откл}$ - время выполнения одной операции в АСУ до введения в состав АСУ системы защиты от компьютерных атак.

Коэффициент увеличения частоты ошибок $K_{ОШ}$ определяется по формуле:

$$K_{ОШ} = \frac{k'_{ОШ} - k_{ОШ}}{k'_{ОШ}},$$

где $k'_{ОШ}$– число случаев генерации АСУ исключений типа «отказ в обслуживании» после введения в состав АСУ системы защиты от компьютерных атак;

$k_{ОШ}$– число случаев генерации АСУ исключений типа «отказ в обслуживании» до введения в состав АСУ системы защиты от компьютерных атак.

Исходные данные для расчета вышеприведенных коэффициентов снижения производительности технической компоненты АСУ определяются в ходе пробного тестирования систем защиты, построенных исходя из возможных вариантов построения этой системы с использованием штатных средств оценки производительности, входящих в состав большинства операционных систем.

Коэффициент увеличения времени выполнения операций лицами обслуживающего персонала при выполнении ими функциональных обязанностей $K_{Твып}$ определяется по формуле:

$$K_{Твып} = \frac{t'_{вып} - t_{вып}}{t'_{вып}},$$

где $t'_{вып}$ - время выполнения операции персоналом АСУ после введения в ее состав системы защиты от компьютерных атак;

$t_{вып}$ - время выполнения операции персоналом АСУ до введения в ее состав системы защиты от компьютерных атак.

Исходные данные для определения коэффициента увеличения времени выполнения операций лицами обслуживающего персонала при выполнении ими функциональных обязанностей определяются в ходе пробного тестирования системы путем замера соответствующих отрезков времени.

Коэффициент повышения дискомфорта при выполнении функциональных обязанностей $K_Д$ определяется путем опроса пользователей в процессе пробного тестировании по заранее сформированным опросным листам. Опросные листы формируются группой экспертов на основании информации о структуре и решаемых задачах защищаемой АСУ.

Для обеспечения возможности сравнения вариантов построения по одному обобщенному показателю производится свертка полученных показателей снижения уровня производительности АСУ. Свертка производится с помощью весовых показателей следующим образом:

$$K = r_с K_С + r_п K_П,$$

$$K_С = r_{пс} K_{ПС} + r_{пар} K_{ПАР} + r_{рес} K_{РЕС} + r_{Тоткл} K_{Тоткл} + r_{ош} K_{ОШ},$$

$$K_П = r_{Твып} K_{Твып} + r_д K_Д,$$

где $r_с$, $r_п$, $r_{пс}$, $r_{пар}$, $r_{рес}$, $r_{Тоткл}$, $r_{ош}$, $r_{Твып}$, $r_д$ - весовые коэффициенты значимости при соответствующих коэффициентах снижения производительности, которые определяются группой экспертов исходя из структуры защищаемой АСУ и решаемых ею задач.

Таким образом, предлагаемый способ позволит построить систему защиты АСУ от компьютерных атак, удовлетворяющую требованиям по стоимости, потребляемым ресурсам, эффективности защиты и оказывающей минимальное воздействие на производительность защищаемой АСУ.

Источники информации

1. Методический документ. Меры защиты информации в государственных информационных системах: утв. Директором ФСТЭК 11 февраля 2014 г. // ФСТЭК России. 2014.

2. Пат. 2331097, Российская Федерация, МПК G05B 17/00, G06F 17/50, G06Q 90/00. Способ автоматизированного управления процессом проектирования структуры системы управления техническими системами и устройство для его осуществления / Селифанов В.А., Селифанов В.В., опубл. 10.08.2008.

3. Пат. 2558238, Российская Федерация, МПК G06F 15/16, G06F 17/00. Способ и устройство выбора предпочтительного средства защиты информации / Шемигон Н.Н., Черноскутов А.И., Кукушкин С.С., опубл. 27.07.2015.

4. Одрин В.М. Метод морфологического анализа технических систем. - М.: ВНИИПИ, 1989.

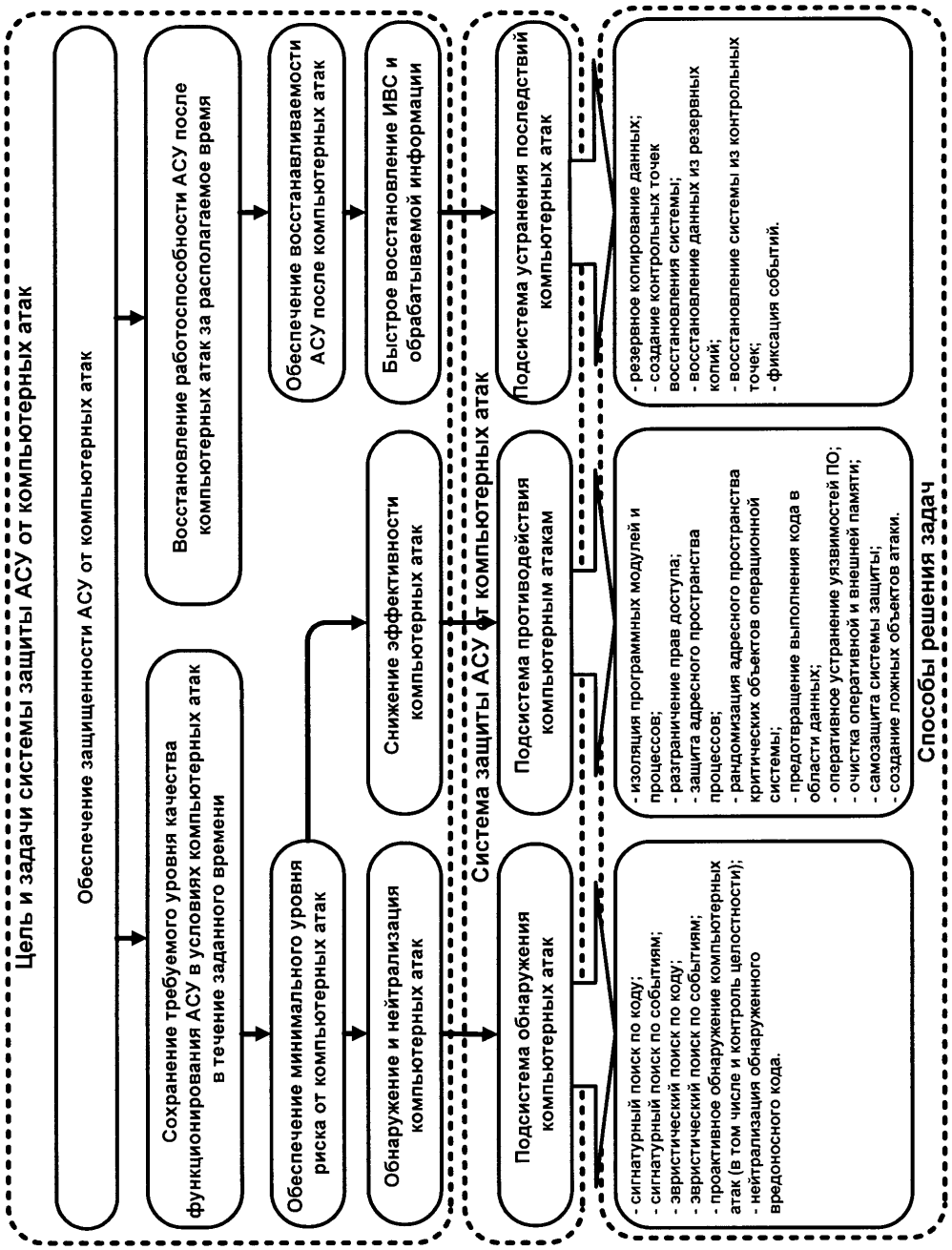
5. Мукминов В.А., Хуцишвили В.М., Лобузько А.В. Методика оценки реального уровня защищенности автоматизированных систем // Программные продукты и системы. 2012. №1(97). С. 39-42.

(57) Формула изобретения

Способ построения системы защиты от компьютерных атак для автоматизированных систем управления, включающий в себя этап формирования множества всех возможных вариантов построения подсистем системы защиты от компьютерных атак, в ходе которого, используя реализуемый с помощью компьютера метод морфологического анализа, формируют множество возможных вариантов построения подсистемы обнаружения компьютерных атак, множество возможных вариантов построения подсистемы противодействия компьютерным атакам и множество возможных вариантов построения подсистемы устранения последствий применения компьютерных атак, при этом для уменьшения количества возможных вариантов построения подсистем для

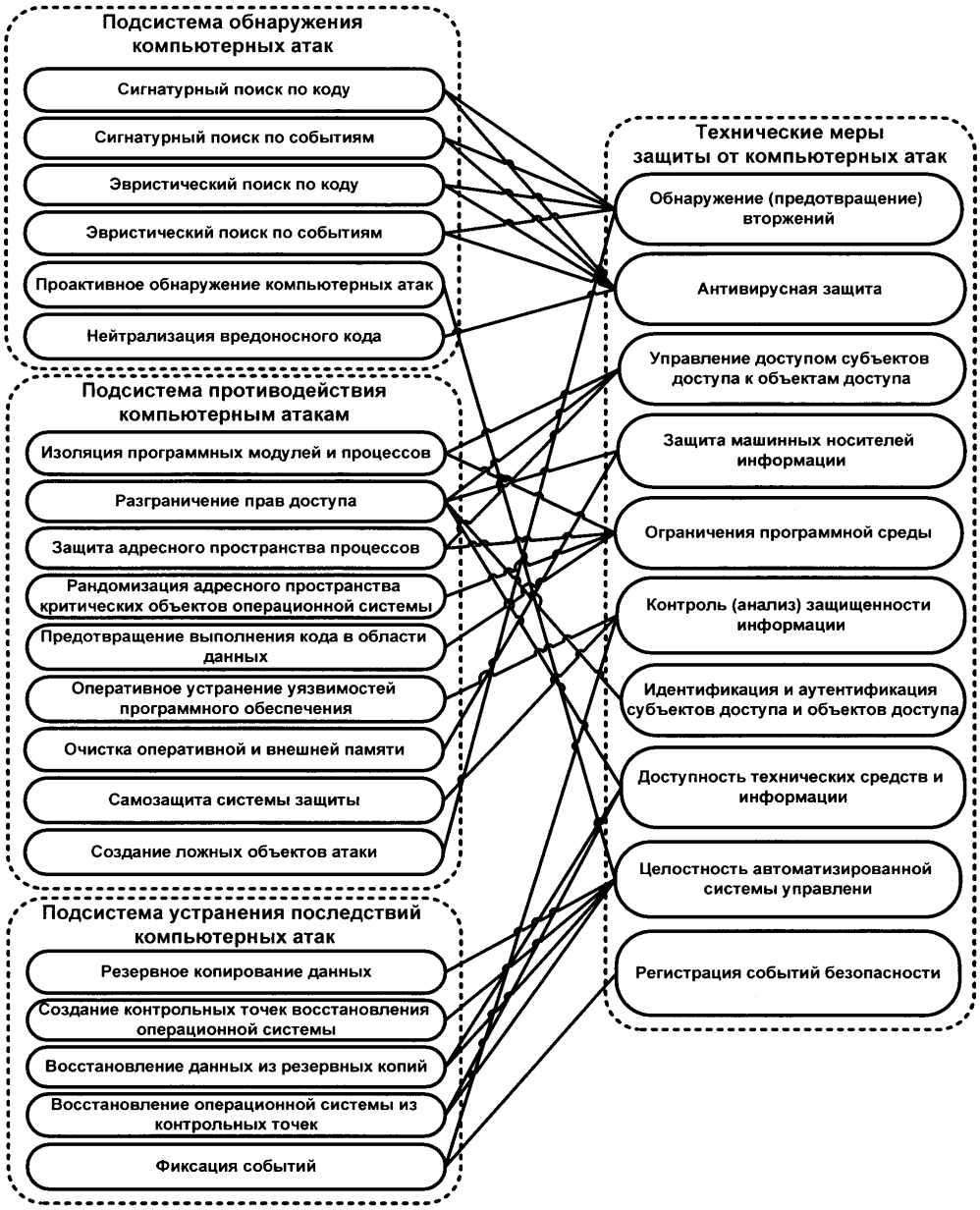
параметров элементов подсистем с плавно изменяющимися значениями принимают минимальное, среднее и максимальное значения; этап формирования множества всех возможных вариантов построения системы защиты от компьютерных атак, в ходе которого, используя реализуемый с помощью компьютера метод морфологического анализа, на основе множеств возможных вариантов построения подсистем, полученных на предыдущем этапе, формируют множество всех возможных вариантов построения системы защиты от компьютерных атак, которое записывают в память компьютера; этап оценки стоимости и требуемых ресурсов вариантов построения системы защиты от компьютерных атак, в ходе которого с помощью компьютера определяют стоимость и требуемые для функционирования ресурсы всех вариантов построения системы из множества вариантов, сформированного на предыдущем этапе, с помощью компьютера, выбирают варианты, стоимость и потребляемые ресурсы которых не превышают заданных, и далее из этих отобранных вариантов формируют множество вариантов построения системы защиты от компьютерных атак, удовлетворяющих требованиям по стоимости и потребляемым ресурсам, которое записывают в память компьютера; этап оценки эффективности вариантов построения системы защиты от компьютерных атак, в ходе которого с помощью тестирования с применением компьютера определяют эффективность вариантов построения системы защиты из множества, сформированного на предыдущем этапе, выбирают варианты, эффективность которых равна или превышает требуемую, и далее из этих отобранных вариантов формируют множество вариантов построения системы защиты от компьютерных атак, удовлетворяющих требованиям по эффективности, при этом в качестве показателей эффективности используют коэффициент защищенности автоматизированной системы управления и время восстановления работоспособности автоматизированной системы управления после применения компьютерных атак; этап оценки степени влияния вариантов построения системы защиты на производительность защищаемой автоматизированной системы управления, в ходе которого оценивают уровень снижения производительности защищаемой автоматизированной системы управления при введении в ее состав вариантов системы защиты от компьютерных атак, удовлетворяющих требованиям по эффективности из множества, сформированного на предыдущем этапе, и выбирают рациональный вариант построения системы защиты от компьютерных атак с минимальным уровнем снижения производительности защищаемой автоматизированной системы управления, при этом в качестве показателя уровня снижения производительности используют комплексный коэффициент снижения производительности, включающий в себя коэффициент снижения производительности технической компоненты защищаемой системы и коэффициент снижения производительности обслуживающего защищаемую систему персонала.

1


Цель и задачи системы защиты АСУ от компьютерных атак
Обеспечение защищенности АСУ от компьютерных атак
Сохранение требуемого уровня качества функционирования АСУ в условиях компьютерных атак в течение заданного времени
Обеспечение минимального уровня риска от компьютерных атак
Обнаружение и нейтрализация компьютерных атак
Восстановление работоспособности АСУ после компьютерных атак за располагаемое время
Обеспечение восстанавливаемости АСУ после компьютерных атак
Быстрое восстановление ИВС и обрабатываемой информации
Снижение эффективности компьютерных атак
Система защиты АСУ от компьютерных атак
Подсистема обнаружения компьютерных атак
Подсистема противодействия компьютерным атакам
Подсистема устранения последствий компьютерных атак
Способы решения задач
- сигнатурный поиск по коду;
- сигнатурный поиск по событиям;
- эвристический поиск по коду;
- эвристический поиск по событиям;
- проактивное обнаружение компьютерных атак (в том числе и контроль целостности);
- нейтрализация обнаруженного вредоносного кода.
- изоляция программных модулей и процессов;
- разграничение прав доступа;
- защита адресного пространства процессов;
- рандомизация адресного пространства критических объектов операционной системы;
- предотвращение выполнения кода в области данных;
- оперативное устранение уязвимостей ПО;
- очистка оперативной и внешней памяти;
- самозащита системы защиты;
- создание ложных объектов атаки.
- резервное копирование данных;
- создание контрольных точек восстановления системы;
- восстановление данных из резервных копий;
- восстановление системы из контрольных точек;
- фиксация событий.

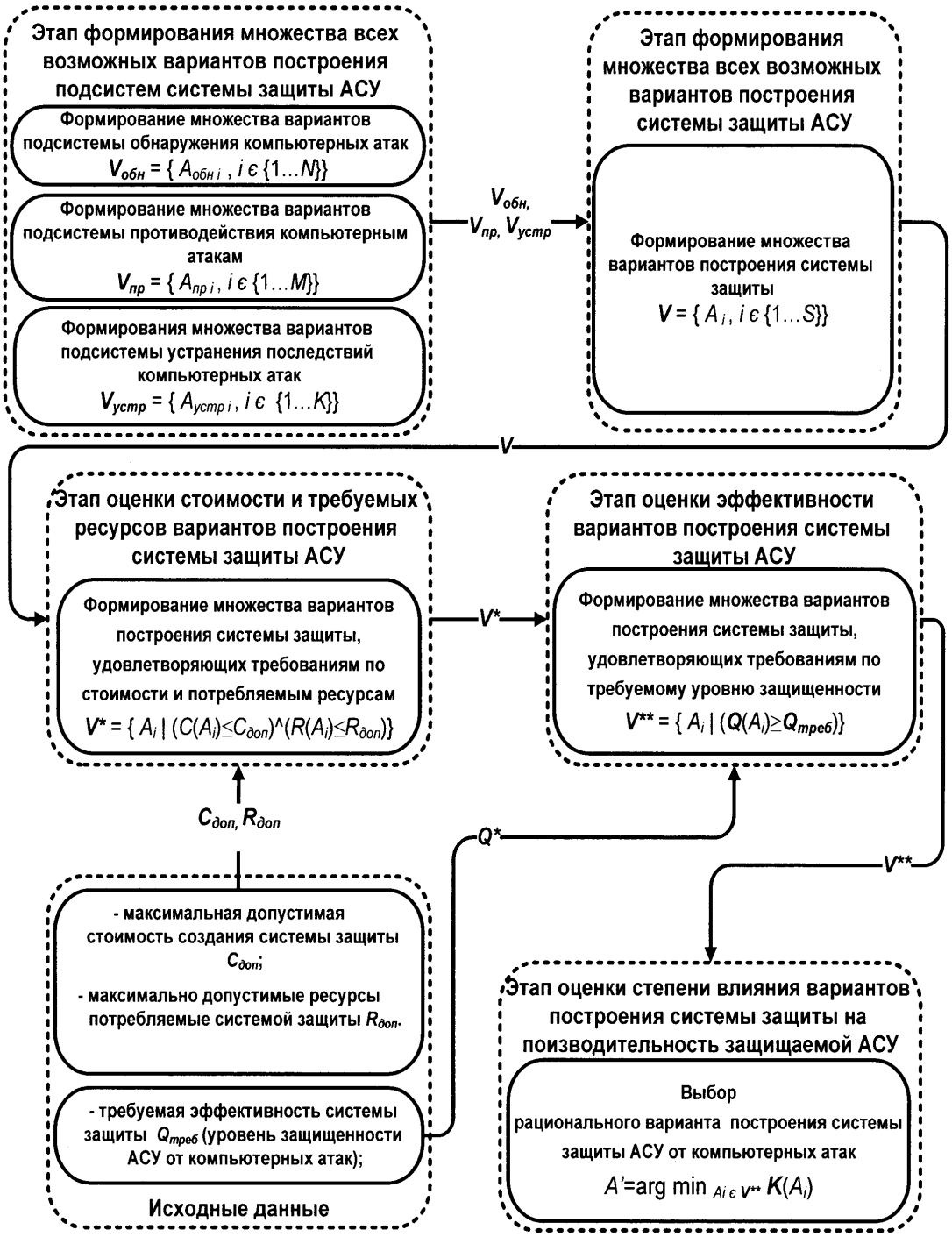
Фиг. 1

2


Подсистема обнаружения компьютерных атак
Сигнатурный поиск по коду
Сигнатурный поиск по событиям
Эвристический поиск по коду
Эвристический поиск по событиям
Проактивное обнаружение компьютерных атак
Нейтрализация вредоносного кода
Подсистема противодействия компьютерным атакам
Изоляция программных модулей и процессов
Разграничение прав доступа
Защита адресного пространства процессов
Рандомизация адресного пространства критических объектов операционной системы
Предотвращение выполнения кода в области данных
Оперативное устранение уязвимостей программного обеспечения
Очистка оперативной и внешней памяти
Самозащита системы защиты
Создание ложных объектов атаки
Подсистема устранения последствий компьютерных атак
Резервное копирование данных
Создание контрольных точек восстановления операционной системы
Восстановление данных из резервных копий
Восстановление операционной системы из контрольных точек
Фиксация событий
Технические меры защиты от компьютерных атак
Обнаружение (предотвращение) вторжений
Антивирусная защита
Управление доступом субъектов доступа к объектам доступа
Защита машинных носителей информации
Ограничения программной среды
Контроль (анализ) защищенности информации
Идентификация и аутентификация субъектов доступа и объектов доступа
Доступность технических средств и информации
Целостность автоматизированной системы управлени
Регистрация событий безопасности

Фиг. 2

3


Этап формирования множества всех возможных вариантов построения подсистем системы защиты АСУ
Формирование множества вариантов подсистемы обнаружения компьютерных атак
$V_{обн} = \{ A_{обн\,i}, i \in \{1...N\}\}$
Формирование множества вариантов подсистемы противодействия компьютерным атакам
$V_{пр} = \{ A_{пр\,i}, i \in \{1...M\}\}$
Формирования множества вариантов подсистемы устранения последствий компьютерных атак
$V_{устр} = \{ A_{устр\,i}, i \in \{1...K\}\}$
$V_{обн}$, $V_{пр}$, $V_{устр}$
Этап формирования множества всех возможных вариантов построения системы защиты АСУ
Формирование множества вариантов построения системы защиты
$V = \{ A_i, i \in \{1...S\}\}$
V
Этап оценки стоимости и требуемых ресурсов вариантов построения системы защиты АСУ
Формирование множества вариантов построения системы защиты, удовлетворяющих требованиям по стоимости и потребляемым ресурсам
$V^* = \{ A_i \mid (C(A_i) \le C_{доп}) \wedge (R(A_i) \le R_{доп})\}$
V*
Этап оценки эффективности вариантов построения системы защиты АСУ
Формирование множества вариантов построения системы защиты, удовлетворяющих требованиям по требуемому уровню защищенности
$V^{**} = \{ A_i \mid (Q(A_i) \ge Q_{треб})\}$
$C_{доп}$, $R_{доп}$
Q*
V**
- максимальная допустимая стоимость создания системы защиты $C_{доп}$;
- максимально допустимые ресурсы потребляемые системой защиты $R_{доп}$.
- требуемая эффективность системы защиты $Q_{треб}$ (уровень защищенности АСУ от компьютерных атак);
Исходные данные
Этап оценки степени влияния вариантов построения системы защиты на поизводительность защищаемой АСУ
Выбор рационального варианта построения системы защиты АСУ от компьютерных атак
$A' = \arg\min_{Ai \in V^{**}} K(A_i)$

Фиг. 3