УДК 004.383.4 ♦ ВАК 05.13.11 ♦ РИНЦ 50.41.00
DOI:

А.М. Черных[1], С.В. Федосеев[2]

[1]Российский государственный университет правосудия, Москва, Россия
[2]Российский экономический университет имени Г.В. Плеханова, Москва, Россия

Реализация концепции ситуационного управления защищённостью информации в автоматизированных системах обучения

Рассмотрены основные подходы к обеспечению защищённости информации в автоматизированных системах обучения, обоснована необходимость применения ситуационного управления защищённостью информации в автоматизированных системах обучения, предложена математическая модель и постановка задачи ситуационного управления, разработана методика ситуационного управления защищенностью информации.

Цель исследования. Целью исследования является обоснование необходимости применения ситуационного управления защищённостью информации подсистемой контроля и защиты информации в автоматизированных системах обучения, а также – разработка методики реализации концепции ситуационного управления.

Материалы и методы. Предполагается, что рассматриваемая автоматизированная система обучения представляет собой фрагмент более масштабной информационной системы, содержащей несколько информационных контуров, в каждом из которых обрабатывается различная по степени защищенности информация: от информации, содержащей сведения, составляющие государственную тайну, до информации открытого доступа.

Принято считать, что технические методы, меры и средства защиты информации в автоматизированных системах обучения реализуют менее половины (около 30%) функций подсистемы контроля и защиты информации. Основную же часть функций этой подсистемы составляют организационные мероприятия по защите информации. Очевидно, что задача обеспечения защищённости информации в автоматизированных системах обучения связана с принятием решения по рациональному выбору и правильному сочетанию технических методов и организационных мероприятий. Условия практического применения автоматизированных систем обучения изменяются во времени и трансформируют ситуацию принятия такого решения, а это с необходимостью приводит к применению методов ситуационного управления.

При реализации ситуационного управления задача защиты информации в автоматизированной системе обучения решается подсистемой контроля и защиты информации путём распределения процессов обеспечения защищённости информации и ресурсов подсистемы элементами автоматизированной системе обучения с учётом изменяющихся условий функционирования.

При регистрации в системе события, связанного с возникновением угрозы защищенности информации, относящегося к одному из элементов ситуационного множества дестабилизирующих факторов, происходит формирование базовых множеств альтернативных управляющих воздействий ситуационного управления, затем - множества допустимых решений вариантов ситуационного управления.

Лучшим признается такое решение, которое обеспечивает экстремум целевой функции ситуационного управления защищенностью информации.

Результаты. Рассмотрены основные подходы к обеспечению защищённости информации в автоматизированных системах обучения, обоснована необходимость применения ситуационного управления защищённостью информации в автоматизированных системах обучения, предложена математическая модель и постановка задачи ситуационного управления, разработана методика ситуационного управления защищенностью информации.

Заключение. Разработанная методика ситуационного управления защищенностью информации в автоматизированных системах обучения предполагает участие оператора в выработке и принятии решений (диалоговые процедуры постановки задачи ситуационного управления, формирования базовых множеств альтернативных управляющих воздействий и т.д.).

Другая важная особенность методики состоит в необходимости использования предварительно разработанных моделей (модели ситуации принятия решений, модели координации и планирования работы подсистемы контроля и защиты информации, модели переработки информации о состоянии этой подсистемы, модели анализа и оценки результатов), а также базы данных, полученной на основе опыта эксплуатации систем защиты информации в автоматизированных системах обучения.

Реализация концепции ситуационного управления защищенностью информации обеспечивает своевременную адаптацию алгоритмов и параметров системы защиты информации к изменениям внешней среды и к характеру решаемых задач внутри систем обучения и на этой основе позволяет улучшить характеристики системы защиты информации в автоматизированных системах обучения.

Ключевые слова: автоматизированная система обучения, подсистема контроля и защиты информации, ситуационное управление защищенностью информации.

Andrew M. Chernih[1], Sergey V. Fedoseev[2]

[1]Russian state university of justice, Moscow, Russia
[2]Russian Economic University named after G.V. Plekhanov, Moscow, Russia

The implementation of the situational control concept of information security in automated training systems

The main approaches to ensuring security of information in the automated training systems are considered, need of application of situational management of security of information for the automated training systems is proved, the mathematical model and a problem definition of situational control is offered, the technique of situational control of security of information is developed.

The purpose of the study. The aim of the study is to base the application of situational control of information security by subsystem of the control and protection of information in automated learning systems and to develop implementation methods of the situational control concept.

Materials and methods. It is assumed that the automated learning system is a fragment of a larger information system that contains several

information paths, each of them treats different information in the protection degree from information, containing constituting state secrets, to open access information.
It is considered that the technical methods, measures and means of information protection in automated learning systems implement less than half (30%) functions of subsystems of control and protection information. The main part of the functions of this subsystem are organizational measures to protect information. It is obvious that the task of ensuring the security of information in automated learning systems associated with the adoption of decisions on rational selection and proper combination of technical methods and institutional arrangements. Conditions of practical application of automated learning systems change over time and transform the situation of such a decision, and this leads to the use of situational control methods.
When situational control is implementing, task of the protection of information in automated learning system is solved by the subsystem control and protection of information by distributing the processes ensuring the security of information and resources of subsystem elements of the automated learning system to meet changing conditions of operation.
When the event, associated with the emergence of threats to the information security related to one of the elements of a situation to a variety of destabilizing factors is checked in the system, the formation of the base of alternative control actions sets of situational management is formed, then the sets of the admissible solutions of the situational control options are formed.
The best solution provides an extremum of the objective function of situational control of information security.
Results. The main approaches to ensuring the information security in automated learning systems are considered, the necessity of the use of situational control of security in automated learning systems is based, mathematical model and problem statement of situational control are offered, the method of situational control of information protection is developed.
Conclusion. Developed method of situational control of information security in automated learning systems, involves the participation of the operator in the development and decision-making (dialogue procedures statement of objectives situational control, the formation of the base of alternative sets of control actions, etc.).
Another important feature of this technique is the necessity of using previously developed models (models of decision-making situation, a model of coordination and planning of operation of a subsystem of the control and protection of information, models of information processing about the status of the subsystem analysis models and evaluation of results) and the database obtained on the basis of operating experience of information protection systems in the automated learning systems.
The implementation of the concept of situational control of information security ensures the timely adaptation of the algorithms and parameters of the information security system to changes in the external environment and the nature of tasks within the education systems and on this basis allows to improve the characteristics of the information protection system in the automated learning systems.

Keywords: *automated training system, subsystem of information control and protection, situational secure information control.*

Введение

Проблема защиты информации в автоматизированных системах обучения (АСО) особенно актуальна в тех случаях, когда используемая для подготовки специалистов АСО является фрагментом другой, более масштабной информационной системы, которая находится в состоянии активного применения и обработки информации. Так, в Российском государственном университете правосудия развёрнут фрагмент Государственной автоматизированной системы РФ «Правосудие», предназначенный для изучения студентами информационной и технологической поддержки судопроизводства, возможностей предоставления информационных и телекоммуникационных услуг работникам судов РФ и населению.

Для обеспечения баланса требований открытости информации и её защиты Государственная автоматизированная система РФ «Правосудие» имеет специальные контуры обработки информации. Защищенный информационный контур для обработки информации, содержащей сведения, составляющие государственную тайну; ведомственный информационный контур для обработки конфиденциальной информации и публичный информационный контур для обработки и предоставления открытой информации [1, 2]. Создание полноценной системы защиты информации для процесса автоматизированного обучения требует системного подхода при решении задач обеспечения сохранности, достоверности и конфиденциальности обрабатываемой информации.

Выбор комбинации методов обеспечения защищённости информации в автоматизированных системах обучения (АСО) определяется формой процесса подготовки специалистов, структурой комплекса средств автоматизации и используемыми моделями безопасности обрабатываемой информации.

Такой выбор не может быть статичным, постоянным во времени ввиду изменяющихся условий функционирования АСО и возможных несанкционированных внешних воздействий на систему.

Реализация концепции ситуационного управления защитой информации позволяет обеспечить своевременную реакцию подсистемы КЗИ на внешние воздействия и достижение, таким образом, высокой эффективности ее функционирования [3, 4, 5].

1. Математическая модель ситуационного управления защищённостью информации

Анализ принципов и методов обеспечения конфиденциальности, достоверности, сохранности учебно-методической информации в АСО показывает, что ни один из способов обеспечения защищённости информации, методов, мер, средств и мероприятий не является абсолютно надежным и что максимальный эффект достигается при объединении всех их в единую целостную подсистему контроля и защиты информации (КЗИ). Подсистема КЗИ создаётся одновременно с разработкой самой АСО, с момента выработки общего замысла ее построения и применения.

Определение набора и содержания мероприятий обеспечения защищённости информации, а также способов их реализации в АСО, осуществляется с учетом имеющихся средств и методов применительно к конкретному комплексу средств автоматизации (КСА). Обобщенная схема подсистемы КЗИ представлена на рис. 1.

В настоящее время для обеспечения защищённости информации в информационных системах широко используются методы:

– аутентификации и идентификации пользователей информационной системы по биометрическим показателям;

– разграничения доступа пользователей к информационным ресурсам системы и авторизации пользователей;

– регистрации и оповещения о событиях, происходящих в информационной системе;

– шифрования хранимых и передаваемых по каналам связи данных и информационных массивов;

– контроля целостности информации, подлинности (аутентичности) данных с использованием электронной подписи;

– выявления и действия по нейтрализации компьютерных вирусов;

– уничтожения отработанной информации на носителях или уничтожения одноразовых носителей информации;

– контроля причин нарушения защищённости информации в информационной системе;

– организационного контроля доступа пользователей к защищённой информации;

– резервного копирования и дублирования информации [1].

Принято считать, что технические методы, меры и средства защиты информации в АСО реализуют менее половины (около 30%) функций подсистемы КЗИ. Основную же часть функций этой подсистемы составляют организационные мероприятия по защите информации. Очевидно, что задача обеспечения защищённости информации в АСО связана с принятием решения по рациональному выбору и правильному сочетанию технических методов и организационных мероприятий [1]. Условия практического применения АСО изменяются во времени и трансформируют ситуацию принятия такого решения, а это с необходимостью приводит к применению методов ситуационного управления.

Использование подсистемой КЗИ алгоритмов ситуационного управления защищённостью информации (СУЗИ) позволяет решить задачу снижения затрат по защите информации на требуемом уровне конфиденциальности, сохранности и достоверности учебно-методической информации.

Основные задачи ситуационного управления защищённостью информации в АСО, решаемые подсистемой КЗИ:

– определение информационных и технических ресурсов, а также объектов информационной среды, подлежащих защите;

– выявление и анализ полного множества потенциально возможных угроз и каналов утечки информации;

– оценка уязвимостей и рисков при нарушении защищённости информации;

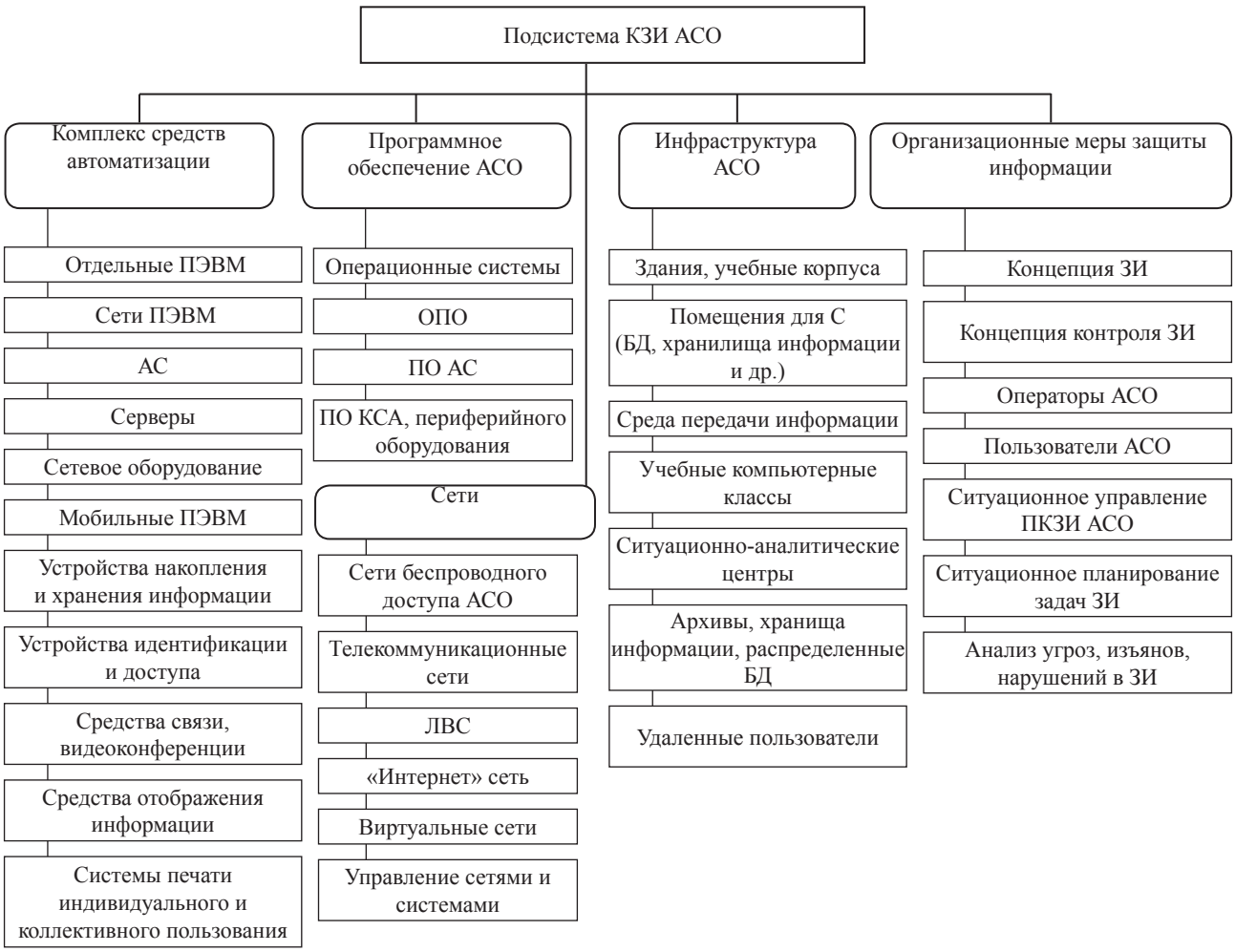

Рис. 1. Обобщенная схема подсистемы КЗИ АСО

– определение общих требований к системе защиты информации с учётом ситуации;

– выбор средств защиты информации с оптимальными характеристиками для данной ситуации;

– обеспечение конфиденциальности, достоверности, сохранности учебно-методической информации выбранными мерами, способами и средствами защиты.

– контроль целостности учебно-методической информации и ситуационное управление подсистемой КЗИ [1, 3, 6].

Математическая модель ситуационного управления защищённостью информации подсистемы КЗИ АСО состоит из трёх основных компонентов:

S – множество средств защиты информации;

R – множество ресурсов, используемых для защиты информации подсистемой КЗИ;

A – множество процессов обеспечения защищённости информации, подлежащих реализации подсистемой КЗИ АСО.

$$\begin{cases} \mathrm{L} = \{\mathrm{S},\ \mathrm{R},\ \mathrm{A}\}; \\ \mathrm{S} = \{s_1,...,s_l,...,s_L\}; \\ \mathrm{R} = \{r_1,...,r_k,...,r_K\}; \\ \mathrm{A} = \{A_1,...,A_p,...,A_P\}. \end{cases}$$

При использовании ситуационного управления процесс обеспечения защищённости учебно-методической информации включает процессы контроля состояния учебно-методической информации, перерабатываемой АСО и состояния средств защиты информации, входящих в состав подсистемы КЗИ (ПКЗИ).

Каждый процесс обеспечения защищённости информации состоит из отдельных фаз, которые рассматриваются как наименьшие составные части такого процесса.

$$A_p = \{a_{p1},\ldots,a_{pi},\ldots,a_{pNp}\}.$$

Подсистема КЗИ реализует каждую такую фазу a_{pi} на временном интервале обучения, определяемом типом проводимого занятия (лекция, семинар, групповое занятие, активные и интерактивные виды занятий, аналитические деловые игры) с использованием имеющегося набора средств защиты информации.

Каждому временному интервалу обучения соответствуют определённые способы обработки учебно-методической информации и определенные формы обучения [4].

Модель процесса подготовки специалистов представляет собой совокупность элементов подготовки специалиста (обучение, контроль, тренировка, тестирование), типов используемой в процессе обучения информации (научная, учебно-методическая, научно-исследовательская, контрольно-тестовая), этапов подготовки специалистов (этап отбора претендентов для обучения, этап обучения слушателей, этап защиты дипломов и сдачи экзаменов).

Задача защиты информации в АСО решается подсистемой КЗИ путём распределения процессов обеспечения защищённости информации и ресурсов подсистемы контроля и защиты информации между элементами АСО с учётом изменяющихся условий функционирования.

Под ресурсами подсистемы контроля и защиты информации следует понимать определенную совокупность специальных технических средств защиты информации, специальное и общее программное обеспечение, организационные меры защиты информации, специалистов по защите информации и др.

В подсистеме КЗИ различают два типа ресурсов, непосредственно расходуемых в процессе обеспечения задач защищённости учебно-методической информации.

К первому типу ресурсов относятся комплекты шифровальных ключей, устройства (карточки, чип – ключи и др.) идентификации, электронные ключи доступа и аутентификации. Ко второму типу – трудовые ресурсы операторов и администраторов защиты информации, КСА, каналы связи и передачи данных, ЭВМ и др. Ресурсы этого типа задаются как функция времени и представляют собой различные расходуемые ресурсы [3, 5].

2. Методика ситуационного управления защищенностью информации

В целом, задача защиты информации в АСО представляется, как совокупность отдельных задач и соответствующих им процессов, выполняемых подсистемой КЗИ. Подсистема КЗИ в ходе выполнения каждой задачи, использует различные ресурсы. Реализация совокупности задач обеспечения защищённости информации рассматривается как процесс, состояние которого непостоянно во времени и может быть целенаправленно изменено воздействиями, выработанными на основе методов ситуационного управления средствами защиты информации.

Требуется рационально использовать имеющиеся в каждой конкретной ситуации функционирования АСО средства защиты информации и ресурсы и оперативно воздействовать на процесс защиты информации таким образом, чтобы при заданных условиях обеспечить его высокую эффективность.

При регистрации в системе события, связанного с возникновением угрозы защищенности информации, относящегося к одному из элементов ситуационного множества дестабилизирующих факторов $W = \{\omega_1,\ldots,\omega_j,\ldots,\omega_J\}$, происходит формирование базовых множеств альтернативных управляющих воздействий ситуационного управления

$$\mathrm{S}_{\delta}(\omega_j) \subseteq \mathrm{S};\ \mathrm{R}_{\delta}(\omega_j) \subseteq \mathrm{R};$$
$$\mathrm{A}_{\delta}(\omega_j) \subseteq \mathrm{A}.$$

Множеством допустимых решений при определении вариантов ситуационного управления в таком случае является кортеж:

$$\mathrm{V}(\omega_j) = <\mathrm{S}_{\delta}(\omega_j), \mathrm{R}_{\delta}(\omega_j), \mathrm{A}_{\delta}(\omega_j)> .$$

Лучшим признается такое решение, которое обеспечивает экстремум целевой функции ситуационного управления защищенностью информации:

$$v^*(s^*, r^*, a^*) : extr\ \mathrm{F}(s, r, a);$$
$$v^*(s^*, r^*, a^*) \in \mathrm{V}(\omega_j).$$
$$s \in \mathrm{S}_{\delta}(\omega_j)$$
$$r \in \mathrm{R}_{\delta}(\omega_j)$$
$$a \in \mathrm{A}_{\delta}(\omega_j)$$

В качестве целевой функции F (.) могут быть использованы, например, затраты на подсистему КЗИ, вероятность предотвращения несанкционированных воздействий на учебно-методическую информацию, ожидаемая величина ущерба от внешних воздействий. Значения целевой функции выбранного варианта для каждого отдельного элемента множества допустимых решений $V(\omega_j)$ выбираются из специального набора, формируемого на основе опыта решения задачи СУЗИ или путем математического моделирования. Для каждого варианта целевой функции назначается сатисфакционное (минимально допустимое, удовлетворительное) значение.

Ограничения при решении задачи ЗИ подсистемой КЗИ могут быть заданы на длительность реализации задач защиты информации при использовании определённого средства автоматизации, вида учебно-методической информации и формы обработки и представления информации; на временные интервалы взаимодействия пользователей с информационными ресурсами АСО; на пропускные способности каналов связи информационно-распределительной сети АСО, уровни достоверности (точности); на вероятность успешного решения задачи АСО; на ожидаемое безопасное время работы КСА АСО. Наиболее важным ограничением является $T_{р\ макс}$ – максимально допустимое время принятия решения подсистемой КЗИ по ситуационному управлению.

Процедура поиска лучшего решения $v^*(s^*, r^*, a^*)$ прекращается либо при определении экстремального значения целевой функции после просмотра всех элементов множества $V(\omega_j)$, либо при нарушении ограничения $T_p \le T_{р\ макс}$. В последнем случае рациональное решение определяется на подмножестве элементов множества $V(\omega_j)$, которые были просмотрены в допустимое время.

Алгоритм ситуационного управления защищенностью информации (рис. 2.) предполагает использование диалоговых процедур выбора целевой функции, оперативной постановки задач ситуационного управления, распределения ресурсов подсистемы КЗИ, формирования базовых множеств альтернативных управляющих воздействий ситуационного управления.

Для определения лучшего решения на множестве допустимых решений $V(\omega_j)$ возможно использование любого математического метода поиска максимального (минимального) элемента множества, включая метод полного перебора.

Методика ситуационного управления защищенностью информации подсистемой КЗИ определяет следующую последовательность действий:

Шаг 1. Определение *F* – цели ситуационного управления защищенностью учебно-методической информации в соответствии с правилами выбора и режимами работы АСО и ПКЗИ, моделями координации и планирования работы ПКЗИ, имеющимися средствами автоматизации, программно-техническими ресурсами, структурно-функциональными ограничениями;

Шаг 2. Сбор информации о текущем состоянии АСО и подсистемы КЗИ на основе сведений о функционировании АСО и ПКЗИ, сведений об угрозах и дестабилизирующих факторах, составе и структуре ПКЗИ, моделях переработки информации о состоянии ПКЗИ;

Шаг 3. Анализ ситуации нарушения защищённости информации в АСО к моменту принятия решения

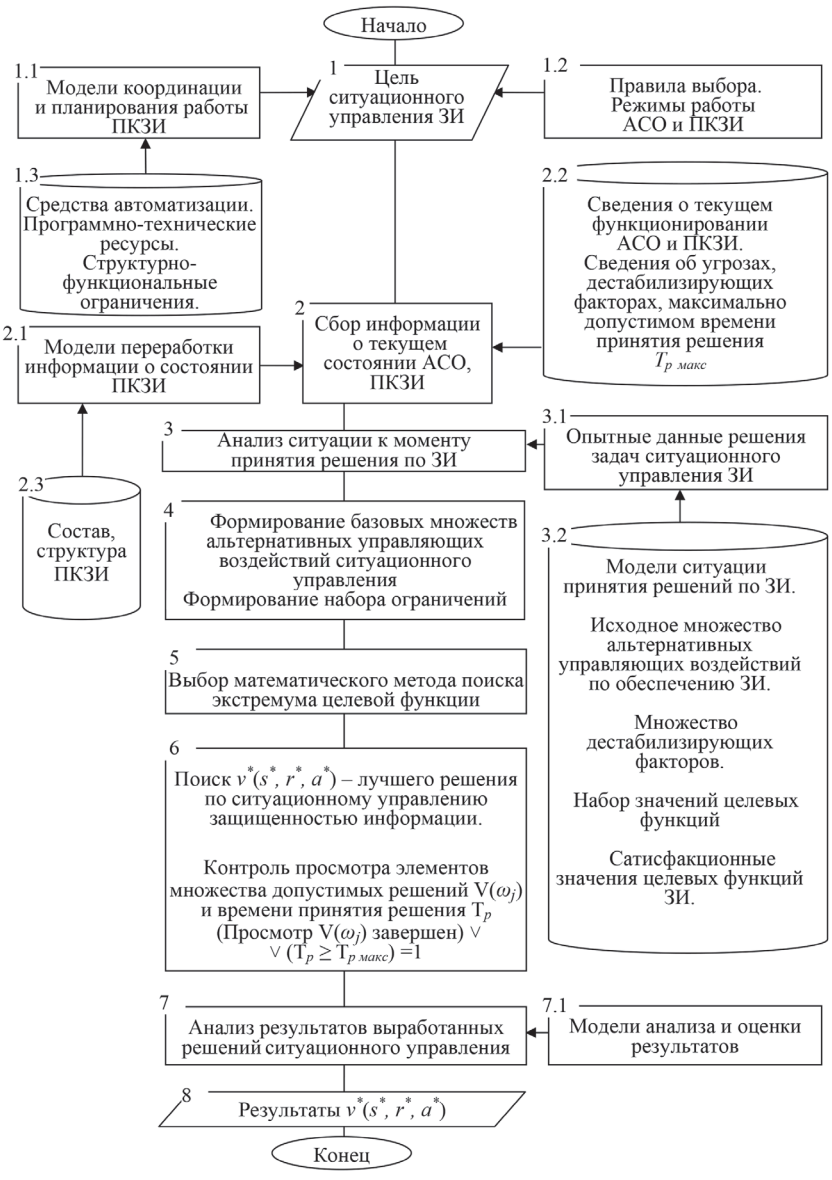

Рис. 2. Алгоритм ситуационного управления защищенностью информации в АСО

подсистемой КЗИ на использование ресурсов защиты информации. При этом используются модели ситуации принятия решений по защите информации (ЗИ), исходное множество альтернативных управляющих воздействий по обеспечению ЗИ, множество дестабилизирующих факторов, набор значений целевых функций, сатисфакционные значения целевых функций;

Шаг 4. Формирование базовых множеств альтернативных управляющих воздействий ситуационного управления $S_б(\omega_j)$, $R_б(\omega_j)$, $A_б(\omega_j)$.

Формирование набора ограничений;

Шаг 5. Выбор математического метода поиска экстремума целевой функции;

Шаг 6. Поиск v*(s*, r*, a*) – лучшего решения по ситуационному управлению защищенностью информации.

Контроль просмотра элементов множества допустимых решений $V(\omega_j)$ и времени принятия решения T_p по выполнению условия: (просмотр $V(\omega_j)$ завершен) $\vee$ $(T_p \geq T_{рмакс}) = 1$;

Шаг 7. Анализ результатов выработанных решений ситуационного управления с использованием разработанных моделей;

Шаг 8. Выдача результатов администратору по защите информации.

Заключение

В представленном виде методика ситуационного управления защищенностью информации в АСО предполагает участие оператора в выработке и принятии решений (диалоговые процедуры постановки задачи ситуационного управления, формирования базовых множеств альтернативных управляющих воздействий и т.д.).

Другая важная особенность методики состоит в необходимости использования предварительно разработанных моделей (модели ситуации принятия решений, модели координации и планирования работы ПКЗИ, модели переработки информации о состоянии ПКЗИ, модели анализа и оценки результатов), а также базы данных, полученной на основе опыта эксплуатации систем защиты информации в АСО.

Реализация концепции ситуационного управления защищенностью информации обеспечивает своевременную адаптацию алгоритмов и параметров системы защиты информации к изменениям внешней среды и к характеру решаемых задач внутри АСО и на этой основе позволяет улучшить характеристики системы защиты информации в АСО

Литература

1. *Черных А.М.* Профессиональная направленность преподавания основ информационной безопасности. В кн. Организация учебной и воспитательной работы в ВУЗе. Выпуск 3. М.: РАП; 2014.

2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

3. *Ловцов Д.А.* Введение в информационную теорию АСУ. М.: ВА им. Ф.Э. Дзержинского; 1996: 435 с.

4. *Ловцов Д.А.* Информационная теория эргасистем. Тезаурус. М.: Наука; 2005: 245 с.

5. *Черных А.М.* Информационная безопасность в автоматизированных системах обучения.//Труды Всероссийской научно-практической конференции «Современное непрерывное образование и инновационное развитие». Серпухов: РАН ИИФ; 2013.

6. *Ловцов Д.А., Сергеев Н.А.* Управление безопасностью эргасистем. М.: РАУ – Университет; 2001: 224 с.

References

1. *Chernykh A.M.* Professional'naya napravlennost' prepodavaniya osnov informatsionnoi bezopasnosti. V kn. Organizatsiya uchebnoi i vospitatel'noi raboty v VUZe. Volume 3. M.: RAP; 2014. (in Russ.)

2. Federal'nyi zakon RF «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» ot 27 iyulya 2006 g. № 149-FZ. (in Russ.)

3. *Lovtsov D.A.* Vvedenie v informatsionnuyu teoriyu ASU. M.: VA im. F.E. Dzerzhinskogo; 1996: 435 P. (in Russ.)

4. *Lovtsov D.A.* Informatsionnaya teoriya ergasistem. Tezaurus. M.: Nauka; 2005: 245 P. (in Russ.)

5. *Chernykh A.M.* Informatsionnaya bezopasnost' v avtomatizirovannykh sistemakh obucheniya.//Trudy Vserossiiskoi nauchno-prakticheskoi konferentsii «Sovremennoe nepreryvnoe obrazovanie i innovatsionnoe razvitie». Serpukhov: RAN IIF; 2013. (in Russ.)

6. *Lovtsov D.A., Sergeev N.A.* Upravlenie bezopasnost'yu ergasistem. M.: RAU – Universitet; 2001: 224 P. (in Russ.)

Сведения об авторах

Андрей Михайлович Черных,
кандидат технических наук, доцент кафедры Информационного права информатики и математики, Российский государственный университет правосудия, Москва, Россия
Эл. почта: kafpi@mail.ru
Тел.: (495) 332-52-67

Сергей Витальевич Федосеев,
кандидат технических наук, доцент кафедры Автоматизированных систем обработки информации и управления, Российский экономический университет имени Г.В. Плеханова, Москва, Россия
Эл. почта: SFedoseev@mesi.ru
Тел.: (985) 970-62-19

Information about the authors

Andrey M. Chernih,
Candidate of Engineering Sciences, Associate Professor of the Department of Information Law, Computer Science and Mathematics, Russian state university of justice, Moscow, Russia
E-mail: kafpi@mail.ru
Tel.: (495) 332-52-67

Sergey V. Fedoseev,
Candidate of Engineering Sciences, Associate Professor of the Department of Automated Systems of Information Processing and Control, Plekhanov Russian University of Economics, Moscow, Russia
E-mail: SFedoseev@mesi.ru
Tel.: (985) 970-62-19