На правах рукописи

КОЗЛОВ Андрей Олегович

МЕТОДЫ ИНТЕГРИРОВАННОЙ ЗАЩИТЫ ИНФОРМАЦИОННОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АСУ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ

Специальность 05.13.06 – Автоматизация и управление технологическими процессами и производствами (образование)

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Москва – 2011

Работа выполнена в Учреждении Российской академии образования «Институт информатизации образования», в лаборатории проектирования автоматизированных систем научных исследований в области образования

Научный руководитель: доктор технических наук, профессор
Надеждин Евгений Николаевич

Официальные оппоненты: доктор технических наук, профессор
Жиров Михаил Вениаминович

кандидат технических наук, профессор
Малюк Анатолий Александрович

Ведущее учреждение: **ГОУ ВПО «Тамбовский Государственный технический университет»**

Защита состоится «3» июня 2011 г. в 15.00 час. на заседании диссертационного совета ДМ 008.004.02 при Учреждении Российской академии образования «Институт информатизации образования» по адресу:
119121, г. Москва, ул. Погодинская, д.8

С диссертацией можно ознакомиться в библиотеке Учреждения Российской академии образования «Институт информатизации образования», автореферат размещён на сайте http://www.iiorao.ru.

Автореферат разослан «29» апреля 2011 г.

Ученый секретарь диссертационного совета
доктор педагогических наук,
кандидат технических наук, профессор ***О.А. Козлов***

ОБЩАЯ ХАРАКТЕРИСТИКА ИССЛЕДОВАНИЯ

Актуальность исследования. Достижение конечных целей государственного курса на инновационное развитие экономики России в значительной степени зависит от результатов модернизации отечественного образования на основе внедрения новейших достижений в области педагогики и средств информационных и коммуникационных технологий (ИКТ). Успешная реализация государственной программы создания единой информационной образовательной среды (ИОС) позволила выйти на новый уровень информатизации образовании, дало толчок к освоению новейших достижений в области ИКТ и одновременно обозначило ряд проблем, связанных с созданием и обеспечением эффективного доступа к распределённому образовательному ресурсу. Техническую основу региональной ИОС составляют автоматизированные системы управления (АСУ) деятельностью образовательных учреждений (ОУ) и средства сетевой коммуникации. Развитие АСУ ОУ в составе региональных ИОС в настоящее время ограничивается отсутствием продуктивных научно-методических подходов к обеспечению сетевой и корпоративной безопасности.

Методам обработки и защиты данных в АСУ посвящены многочисленные работы отечественных и зарубежных ученых: В.А. Балыбердина, В.А. Герасименко, А.А. Малюка, В.Д. Киселёва, В.В. Кульбы, А.Г. Мамиконова, Д. Сяо, Л.Дж. Хоффмана, Б.Дж. Уолкера и др. В этих исследованиях получили также развитие теоретические положения и методы обеспечения ИБ в системах управления в сферах науки, производства и бизнеса. В меньшей степени изучены вопросы создания защищённой сетевой инфраструктуры АСУ ОУ ВПО.

Анализ отечественного и зарубежного опыта позволил сделать вывод, что попытки решить проблему информационной безопасности за счёт прямого наращивания средств и организационных мер защиты во всех компонентах региональной ИОС являются малопродуктивными и, в принципе, не решают обострившейся проблемы защиты информационного и программного обеспечения АСУ ОУ. В условиях явного доминирования гетерогенных АСУ ОУ следует признать обоснованным переход к использованию адаптивных методов и средств защиты сетевых ресурсов. В этой связи научное исследование, направленное на создание гибких механизмов защиты информационного и программного обеспечения (ИО и ПО) АСУ ОУ в составе региональной ИОС, представляется актуальным и своевременным**.**

С точки зрения современных взглядов на проблему построения защищённой сетевой инфраструктуры АСУ ОУ представляется перспективным дальнейшее развитие известной концепции комплексной защиты информации (В.А. Герасименко, А.А. Малюк) в аспектах мониторинга состояния информационной безопасности, в частности: анализа уязвимостей, аудита действий пользователей и адаптивного управления механизмами защиты ИО и ПО.

Под *комплексной защитой ресурсов* АСУ ОУ понимается целенаправленное применение совокупности программно-аппаратных методов и средств и организационных мер с интересах поддержания заданного уровня защищенности ИО и ПО по всей совокупности показателей и условий, являющихся существенно значимыми с точки зрения обеспечения установленных требований политики ИБ вуза.

На этапе эксплуатации АСУ ОУ в составе региональной ИОС актуализируется задача интеграции методов и средств защиты информационных и вычислительных ресурсов и оперативного управления событиями ИБ. При этом оптимальность интегрированной защиты ресурсов (ИЗР) в нашем исследовании понимается как достижение заданного уровня защищенности ИО и ПО АСУ при минимальных затратах. В настоящее время наименее изученным остаётся вопрос выбора рациональной стратегии управления механизмами ИЗР, что обусловлено: гетерогенностью и многофункциональностью АСУ ОУ, распределённостью её ресурсов и неопределённостью условий работы. Последнее в значительной степени обусловлено природой человеческого фактора.

Таким образом, на этапе активного развития региональных ИОС обострилась проблема защиты ресурсов АСУ ОУ, что объясняется относительно низкими темпами внедрения инновационных методов и сервисов ИБ и способов оперативного управления механизмами защиты (МЗ).

Проблемная ситуация, определяющая актуальность исследования, заключается в противоречии между возросшими требованиями к защищённости ресурсов и стабильности функционирования региональной ИОС, с одной стороны, и ограниченными возможностями используемых на практике способов обеспечения защиты информационного и программного обеспечения АСУ ОУ, с другой стороны.

Целью диссертационного исследования является повышение устойчивости функционирования АСУ ОУ в составе региональной ИОС на основе разработки научно-методического подхода к организации и обеспечению адаптивного ситуационного управления механизмами интегрированной защиты информационного и программного обеспечения от несанкционированных действий пользователей.

Объект исследования – интегрированная система защиты информационного и программного обеспечения АСУ ОУ в составе единой региональной ИОС.

Предмет исследования – методы и алгоритмы адаптивного ситуационного управления механизмами интегрированной защиты информационного и программного обеспечения АСУ ОУ в условиях вариативности угроз несанкционированного доступа к информационным и вычислительным ресурсам.

В диссертации решается **научная задача –** разработка методов, моделей и алгоритмов, реализующих стратегию адаптивного ситуационного управления механизмами интегрированной защиты информационного и программного обеспечения АСУ ОУ, используемой в составе региональной ИОС.

В соответствии с целью и научной задачей определены следующие основные под**задачи исследования**:

1) проанализировать тенденции развития коммуникационной инфраструктуры АСУ ОУ и оценить требования к обеспечению защиты её ресурсов;

2) разработать теоретико-множественную модель адаптивного ситуационного управления механизмами ИЗР АСУ ОУ в составе единой региональной ИОС;

3) разработать алгоритм обнаружения и статистической идентификации профиля нарушителя политики ИБ вуза на основе интеллектуальной обработки и анализа уязвимостей критических ресурсов и учетных записей пользователей;

4) разработать методику оценки и прогнозирования показателей ИЗР на основе процедур статистической идентификации профиля нарушителя, имитационной модели механизма адаптивного ролевого управления доступом, вероятностной модели управления МЗ и игровой модели функционирования ИЗР в условиях нарушения пользователями АСУ требований корпоративной политики ИБ вуза;

5) обосновать предложения по организации мониторинга событий информационной безопасности и аудита действий пользователей при функционировании АСУ ОУ; подготовить методические рекомендации по обучению системных программистов и администраторов баз данных на курсах повышения квалификации.

Методологическую основу диссертационных исследований составили фундаментальные и прикладные работы:

- по методологии проектирования автоматизированных систем и АСУ ОУ: Изотова В.Н., Колина К.К., Кульбы В.В., Мамиконова А.Г., Мачкина П.И., Павлова А.А., Романова В.П., Черненького В.М., Скурихина В.И., Шахгельдян К.И.;
- по теории адаптивных систем управления: Данилюка С.Г., Ильичёва А.В., Назина А.В., Надеждина Е.Н., Растригина Л.А, Саридиса Дж., Фрадкова А.Л., Цыпкина Я.З., Ядыкина И.Б.;
- по моделированию процессов управления и исследованию эффективности методов и средств защиты информации в АСУ: Герасименко В.А., Есикова О.В., Киселёва В.Д., Малюка А.А., Романова В.П., Сердюкова В.И., Советова Б.Я.

Для решения подзадач исследования в диссертации использован ***математический аппарат***, основу которого составили: общие положения и принципы системного анализа; теория и методы исследования операций; методы теории адаптивных систем; методы организации и проектирования автоматизированных систем; методы моделирования информационных процессов в АСУ.

Научная новизна и теоретическая значимость исследования:

1. Дана теоретико-множественная интерпретация задачи адаптивного ситуационного управления механизмами ИЗР в терминах методологии адаптивного выбора вариантов, развивающая концепцию комплексной защиты информации для сервисно-ориентированной архитектуры АСУ ОУ в аспектах: а) интеграции функций защиты ИО и ПО; б) адаптивного управления механизмами защиты ИО и ПО на основе рекуррентных стохастических алгоритмов;

2. Разработана имитационная модель адаптивного ролевого управления правами доступа к информационным ресурсам АСУ ОУ, отличающаяся применением аппарата модифицированных временных сетей Петри и позволяющая адекватно отразить информационные процессы, протекающие в многоуровневой системе интегрированной защиты распределённых ресурсов;

3. Разработана методика прогностической оценки устойчивости интегрированной защиты ИО и ПО в условиях несанкционированных действий пользователей АСУ ОУ, основанная на применении комплекса математических моделей и алгоритмов, включающего: настраиваемую модель профиля потенциального нарушителя, игровую модель функционирования динамической системы «Система ИЗР – нарушитель политики ИБ», вероятностную модель управления механизмом ИЗР и имита-

ционную модель адаптивного ролевого управления правами доступа (РУД). Модели и алгоритмы в совокупности позволяют выявлять и оценивать потенциальные уязвимости и осуществлять выбор параметров для оперативной настройки механизмов интегрированной системы защиты ИО и ПО при эксплуатации АСУ ОУ.

Практическая значимость исследования заключается в реализации разработанных диссертантом моделей, алгоритмов и программных продуктов при создании интегрированной защиты ИО и ПО АСУ образовательным учреждением:

1. Разработанная подсистема администрирования ИБ АСУ, обеспечивающая автоматизированный контроль, сопровождение и изменение учётных записей пользователей и корректировку уровня доступа к ресурсам, использована при модернизации системы защиты информационного и программного обеспечения АСУ ГОУ ВПО «Шуйский государственный педагогический университет».
2. Вероятностная модель управления механизмом защиты ресурсов и имитационная модель адаптивного РУД используются на практических занятиях по дисциплинам «Комплексная система защиты информации на предприятии» и «Моделирование систем» при обучении студентов по специальности 090103.65 «Организация и технология защиты информации» в Тульском филиале Московского института комплексной безопасности.
3. Разработана учебная программа и методические рекомендации по обучению системных программистов и администраторов баз данных на курсах повышения квалификации, в которых нашли отражение особенности организационного обеспечения и оперативного управления механизмами защиты ИО и ПО АСУ ОУ.

Достоверность и обоснованность сформулированных в диссертации положений и полученных научных результатов определяются:

1. Опорой на фундаментальные положения и принципы информатизации образования в аспектах автоматизации процессов управления деятельностью образовательных учреждений (И.В. Роберт);
2. Общим методологическим подходом к обоснованию теоретических положений и к решению задач исследования, отвечающих положениям известной концепции комплексной защиты информации в автоматизированных системах (В.А. Герасименко, А.А. Малюк);
3. Корректным использованием комплекса апробированных методов анализа и операционного моделирования процесса управления механизмами защиты информации, соответствующих предмету и подзадачам исследования;
4. Положительными результатами апробации разработанных математических моделей и алгоритмов управления механизмами защиты ИО и ПО АСУ в ГОУ ВПО «Шуйский государственный педагогический университет».

Апробация результатов исследования. Основные положения и результаты исследования докладывались и обсуждались: на XXII Международной НТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникации» (Рязань, 2004); на I Всероссийской НПК «Развитие творческого наследия С.Я. Батышева в системе непрерывного профессионального образования» (Н.Новгород, ВГИПУ, 2006); на V Всероссийской НПК «Проблемы информатизации образования: регио-

нальный аспект» (Чебоксары, 2007); на Всероссийской НПК студентов, аспирантов, специалистов и молодых ученых «Современные проблемы науки, образования и производства» (Н. Новгород, НФ УРАО, 2007); на IX Международной научно-методической конференции преподавателей вузов, ученых и специалистов «Инновации в системе непрерывного профессионального образования» (Н. Новгород, 2008, 2010); на II Межвузовской НМК «Шуйская сессия студентов, аспирантов, молодых ученых» (Москва – Шуя, 2009); на XVII Межвузовской НТК «Пути совершенствования ракетно-артиллерийских комплексов, средств управления войсками и оружием, их эксплуатации и ремонта» (Тула, 2010); на Международной НПК «Современные достижения в науке и образовании: математика и информатика» (Архангельск, 2010); на Всероссийской научно-практической конференции с международным участием «Информационные технологии на базе свободного программного обеспечения» (Елец, 2010); на Всероссийской с международным участием НПК, посвящённой 80-летию Чувашского ГПУ им. И.Я. Яковлева (Чебоксары, 2010) на теоретических семинарах и научно-практических конференциях ИИО РАО, г. Москва (2007-2010 гг.).

Внедрение результатов. Авторские модели и алгоритмы реализованы в учебном процессе Московского института комплексной безопасности (Тульский филиал) при обучении студентов по специальности «Организация и технология защиты информации» и на кафедре автоматики и телемеханики Тульского государственного университета при обучении студентов по специальности «Программное обеспечение вычислительной техники и автоматизированных систем»; использованы при разработке программы подготовки системных программистов и администраторов баз данных АСУ ОУ на специализированных курсах повышения квалификации.

Основные результаты, выносимые на защиту:

1. Теоретико-множественная модель адаптивного ситуационного управления механизмами интегрированной защиты, развивающая концепцию комплексной защиты информации для сервисно-ориентированной архитектуры АСУ ОУ с учётом особенностей интеграции функций защиты и адаптивной настройки механизмов защиты ИО и ПО на основе рекуррентных стохастических алгоритмов адаптивного выбора вариантов;
2. Имитационная модель адаптивного ролевого управления правами доступа к информационным ресурсам, отличающаяся применением аппарата модифицированных временных сетей Петри и позволяющая адекватно отразить информационные процессы, протекающие в АСУ ОУ;
3. Методика оценки устойчивости интегрированной защиты ИО и ПО АСУ ОУ в условиях несанкционированных действий пользователей, основанная на применении настраиваемой модели профиля потенциального нарушителя, вероятностной модели механизма управления ИЗР, имитационной модели адаптивного ролевого управления правами доступа и игровой модели функционирования динамической системы «СИЗР – нарушитель политики ИБ», которые в совокупности позволяют выявлять потенциальные уязвимости и осуществлять настройку механизмов интегрированной защиты ИО и ПО.

Структура работы - диссертация состоит из введения, трех глав, заключения, списка литературы, включающего 140 источников, и трёх приложений. Общий объём диссертации без списка литературы и приложений – 146 с.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность темы диссертации, определяется цель, объект и предмет исследования, раскрыта методологическая основа и описаны этапы исследования, показана научная новизна, теоретическая и практическая значимость диссертации, определены основные положения, выносимые на защиту, указаны сведения об апробации работы.

В **первой главе** «Теоретические основы обеспечения защиты ресурсов АСУ образовательных учреждений» проведён анализ перспективных технологий построения автоматизированных систем организационного управления, выполнена декомпозиция структуры АСУ ОУ в виде совокупности типовых функциональных подсистем, определены особенности функционирования АСУ ОУ в составе региональной ИОС, изучено состояние вопроса по материалам отечественной и зарубежной литературы и сформулирована задача исследования.

В процессе исследования установлено, что наибольшее внимание в ведущих ОУ ВПО уделяется автоматизации следующих видов деятельности: работа библиотек (27,1 %), организация и обеспечение учебного процесса (20,5 %), управление персоналом (18,4 %), дистанционное обучение (18,1 %), экономика и финансы (16,0 %). По данным аналитических исследований (Д.Ю. Столяров, 2009 г.), 54% вузов РФ используют автоматизированные информационные системы поддержки организации и управления учебным процессом с разной степенью автоматизации. При этом 25 % ОУ ВПО внедрили АСУ собственной разработки. Установлено, что в условиях интеграции гетерогенных корпоративных вычислительных сетей (КВС) и АСУ ОУ в составе региональных ИОС обострилась проблема защиты ИО и ПО от внешних и внутренних угроз. Повышение гибкости защиты сетевой инфраструктуры АСУ ОУ в региональной ИОС может быть достигнуто через внедрение новых способов оперативного управления механизмами интегрированной защиты ресурсов.

На основе изучения опыта инновационных вузов РФ определены принципы автоматизации процессов организационного управления и предложена гипотетическая модель ИТ-инфраструктуры АСУ ОУ. Базовыми компонентами АСУ ОУ являются: коммуникационная сеть; информационные комплексы структурных подразделений; информирующая система; система документооборота; комплекс системных сервисов. Архитектура АСУ ОУ характеризуется: единой коммуникационной системой, распределённостью ресурсов, многообразием способов программно-аппаратной реализации функциональных подсистем, унифицированным информационным интерфейсом, регламентированным использованием Интернета. В качестве платформы создания АСУ ОУ рассматривается кустовая архитектура на базе унифицированного портального решения, а методологическую основу АСУ составляют принципы концепции сервисно-ориентированной архитектуры SOA (Service-Oriented Architecture).

В интересах исследования за основу принята типовая структура АСУ ОУ

(рис.1), допускающая линейную декомпозицию на линейные автоматизированные системы (АС) и (или) информационные системы (ИС) $АС_k$ (*k=1,…,N)*, структурных подразделений ОУ и линейные функциональные подсистемы: ЕСВИФ, ЕТС, ЕИАС, ЕСК. Каждая из функциональных подсистем состоит из совокупности типовых комплексов средств автоматизации (КСА), реализующих однотипные процессы и процедуры обработки информации в составе линейных АС и ИС изучаемой АСУ ОУ. В структуре всех функциональных подсистем предусматриваются центры координации функционирования (ЦКФ), что соответствует тенденции выхода на новый уровень унификации и типизации программно-аппаратных решений и создания инвариантных механизмов интегрированной защиты ресурсов АСУ ОУ.

Изучение функциональных задач АСУ ОУ, а также потенциальных возможностей автоматизированных систем с элементами адаптации и обучения позволило определить перспективу реализации возросших требований ИБ через создание системы ИЗР, оснащённой адаптивной дискретной системой управления. Наиболее полно механизм адаптивного дискретного управления ИЗР может быть осуществлён при оперативно-диспетчерском управлении (ОДУ) механизмами защиты (рис. 2).

В нашей работе предложена теоретико-множественная модель ИЗР АСУ ОУ, основанной на принципах адаптивного ситуационного управления и учитывающей топологические особенности единой региональной ИОС. Для формального отображения процесса согласованного управления механизмами ИСЗ использована методология адаптивного выбора вариантов (АВВ) в базовой схеме «диагонально-выпуклая игра» (А.В. Назин и А.С. Позняк). Рабочее правило выбора рационального варианта защиты в соответствии методом стохастической аппроксимации представляется в виде рекуррентной процедуры:

$$p_{n+1}^k = \pi_{\varepsilon n}^{Nk}\{p_n^k - \nu_k \cdot \nabla_{pk} V_\delta^k\}. \qquad (1)$$

Здесь p_n^k - условная вероятность выбора на n-м шаге k-го варианта; $\pi_{\varepsilon_{n+1}}^{N_k}$ - оператор проектирования на ε_n- симплекс, используемый для нормировки потерь ξ_n; $\nabla_{p^k} V_\delta^k$ - градиент целевой функции.

С использованием аппарата АВВ предложена модель системы адаптивного ситуационного управления механизмами ИЗР (рис.2). Задача построения модели сведена к определению рациональной стратегии управления или, иначе, алгоритма формирования такой последовательности вариантов (управляющих воздействий), которая в определенном вероятностном смысле обеспечивает минимум предельных средних потерь, характеризующих качество осуществляемого процесса управления.

В задачах АВВ имеет место следующая общая ситуация, возникающая при синтезе систем с дискретным управлением. В каждый из последовательных моментов времени t_n $(n = 1,2,,3,...)$ необходимо выбирать вариант x_n из конечного множества возможных вариантов (управлений) $x_n \in X$. Возникающие в результате произведенного выбора x_n^k $(k = \overline{1,l})$ потери системы ξ_n представляют собой случайную величину (функцию элементарного исхода ω) и зависят от x_n и от состояний системы:

$$\xi_n^k = (\eta_n^{вх} - \eta_n^{вых}) + \alpha_k \cdot (T - \tau_n), \;\; n = 1,2,3,... \qquad (2)$$

Здесь n - номер текущего интервала времени длительности T; $\eta_n^{вх}$ *и* $\eta_n^{вых}$ - количество поступивших на обработку и обслуженных в системе ИЗР на этот интервал времени вызовов; α_k - весовые положительные постоянные; τ_n - оценка времени обслуживания вызовов, вычисляемая на основе априорных сведений о времени работы средств защиты

$$\tau_n = \sum_{i=1}^{m} \varsigma_n^i \cdot (\tau_i^R + \sum_{j=1}^{l} x_n^j \cdot \tau_j^r), \qquad (3)$$

где ς_n^i - количество вызовов i-го вида, обслуженных в течение n-го интервала времени; τ_i^R - среднее суммарное время выполнения рабочих программ (обязательных для каждых вызова) при обслуживании одного вызова i-го вида; τ_i^r - среднее время выполнения программы контроля r_j; $(\eta_n^{вх} - \eta_n^{вых})$ - показывает, как система ИЗР справляется с обслуживанием поступающих на обработку вызовов; $(T - \tau_n)$ – представляет собой ту часть n-го интервала времени T, в течение которой система защиты простаивает.

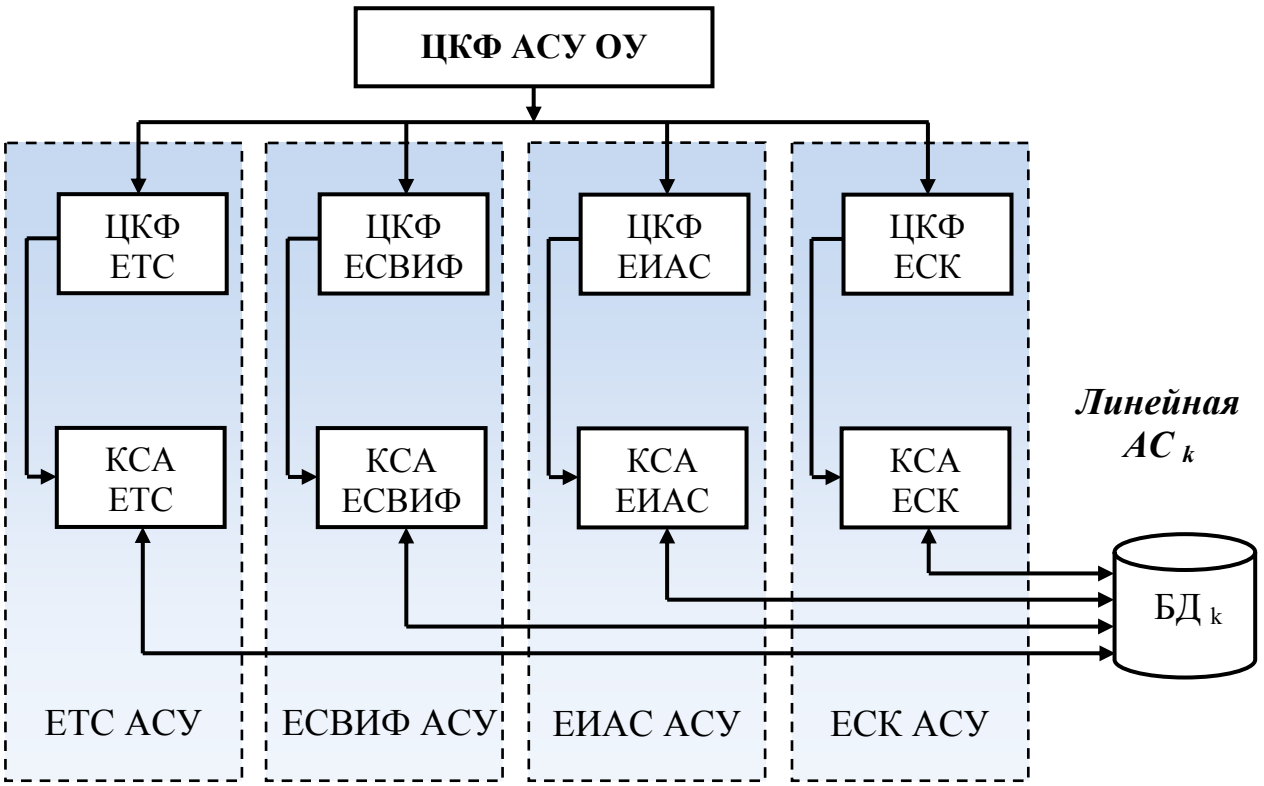

Рисунок 1. - Декомпозиция типовой структуры АСУ ОУ на линейные автоматизированные и информационные системы и линейные функциональные подсистемы: ЕТС - единая информационная технологическая система; ЕСВИФ – единая информационная система формирования и поддержания единого информационного фонда АСУ ОУ; ЕСК – единая система контроля; ЕИАС – единая информационная аналитическая система.

Реализуемая при этом последовательность вариантов (управлений) $\{x_n\}$ назначается такой, чтобы при выборе конкретного варианта достигалась заданная цель,

формулируемая в терминах предельных значений текущих средних потерь. Последовательность вариантов $\{x_n^k\}$ выбирают таким образом, чтобы с ростом номера интервала n значение показателя средних потерь снижалось

$$\Phi_n^k = \frac{1}{n} \cdot \sum_{i=1}^{n} \xi_i^k , \ k = \overline{1, l} . \tag{4}$$

Рекуррентный алгоритм выбора оптимального варианта на n-м шаге, синтезированный с учётом введённых положений, имеет вид:

$$p_{n+1}^k = \pi_{\varepsilon_n}^{N_k} \left\{ p_n^k - \nu_n \left(\frac{\xi_n^k}{e^T(x_n) \cdot p_n^k} + \delta_n \right) \cdot e(x_n^k) \right\}, \tag{5}$$

где $\pi_{\varepsilon_{n+1}}^{N_k}$ - оператор проектирования на ε- симплекс, который используется для нормировки потерь ξ_n; $e(x_n^k)$ - оптимум (экстремум) показателя ξ_n^k, соответствующий выбранному варианту $x_n^k \in X_k$; ν_n и δ_n - детерминированные убывающие функции, зависящие от шага n.

Рисунок 2 .- Структура системы ИЗР с адаптивным дискретным управлением

Предложенная модель в достаточной мере отражает сущность адаптивного ситуационного управления - поддержание на заданном уровне качества управления МЗ в условиях нарушений пользователями политики ИБ. Конкретизация и учёт особенностей функционирования ИЗР достигаются на основе выбора параметров рекуррентного алгоритма АВВ в рамках базовой схемы диагонально-выпуклой игры. На рис.3 показана блок-схема, поясняющая механизм адаптивного ситуационного управ-ления механизмами ИЗР АСУ. Система управления содержит основной и дополнительный контуры управления. На вход системы через функциональный преобразователь (ФП) поступает поток вызовов пользователей. В основном контуре выделены: информационно-измерительная система (ИИС), многоканальное управляющее устройство (МУУ) и обобщённый объект управления (ООУ) – механизмы ИЗР АСУ. Дополнительный контур включает: имитационную прогнозирующую модель (ИПМ),

алгоритм принятия решения (ПР), идентификатор и алгоритм расчёта коэффициентов эффективности (АРКЭ).

Во **второй главе** «Разработка алгоритмов управления адаптивными механизмами интегрированной защиты ИО и ПО АСУ» дано обоснование инструментария для разработки моделей и алгоритмов поддержки ситуационного управления механизмами ИСЗ, дана классификация нарушений политики ИБ, связанных с получением несанкционированного доступа (НСД) к ресурсам АСУ, предложена формальная модель нарушителя и алгоритм идентификации и корректировки его профиля, дана типизация способов нейтрализации угроз НСД, разработана вероятностная модель управления механизмом ИЗР, синтезирован рекуррентный алгоритм адаптивного ситуационного управления ИСЗ в терминах АВВ.

Содержательная постановка *задачи управления* правами доступа имеет вид: для заданной архитектуры и системных характеристик АСУ ОУ необходимо построить модель разграничения доступа и определить её управляемые параметры, при которых механизм разграничения доступа будет оптимален в смысле критерия минимума риска от НСД. Представим формальную математическую постановку задачи на оптимизацию схемы разграничения доступа в АСУ. Исходными данными являются: $Q = \{q_i\},\ i = \overline{1,I}$ - множество объектов доступа (ОД); $S = \{s_j\},\ j = \overline{1,J}$ - множество субъектов доступа (СД); $U = \{u_k\},\ k = \overline{1,K}$ - множество узлов связи (УС); $G^0 = \{g^0_{i,j}\}$, $i = \overline{1,I},\ j = \overline{1,J}$ - оптимальный механизм, отвечающий критериям безопасности, где

$$g_{i,j} = \begin{cases} 1, \ \textit{если}\ \ q_i \ \ \textit{размещён в узле}\ \ u_k; \\ 0, \ \textit{в противном случае.} \end{cases}$$

$Z = \{z_{m,n}\},\ m,n = \overline{1,K}$ - матрица организации АСУ, элементы которой

$$z_{m,n} = \begin{cases} 1, \ \textit{если}\ \ u_m \in Z_r \ \textit{и}\ \ u_n \in Z_r,\ Z_r - \textit{локальная сеть подразделения}; \\ 0, \ \textit{в противном случае.} \end{cases}$$

$C^0 = \{c^0_{i,j}\},\ i = \overline{1,I},\ j = \overline{1,J}$ - матрица ущерба, обусловленного возможностью НСД к ресурсам; элементы $\{c^0_{i,j}\}$ определяются степенью конфиденциальности информации в ОД и моделью СД (профилем пользователя).

Управляемыми переменными задачи являются:

$D^1 = [d^1{}_{i,k}]$ - матрица размещения ОД на узлах АСУ, элементы которой

$$d^1{}_{i,k} = \begin{cases} 1, \ \textit{если}\ \ q_i \in u_k; \\ 0, \ \textit{в противном случае.} \end{cases}$$

$D^2 = [d^2{}_{j,k}]$ - матрица распределения СД по узлам АСУ, в которой элементы

$$d^1{}_{j,k} = \begin{cases} 1, \ \textit{если}\ \ s_j \in u_k; \\ 0, \ \textit{в противном случае.} \end{cases}$$

$V = \{v_i\}$ - вектор признаков общего доступа к ресурсам, в котором элементы

$$v_i = \begin{cases} 1, \ \textit{если к}\ \ v_i \ \ \textit{разрешён общий доступ}; \\ 0, \ \textit{в противном случае.} \end{cases}$$

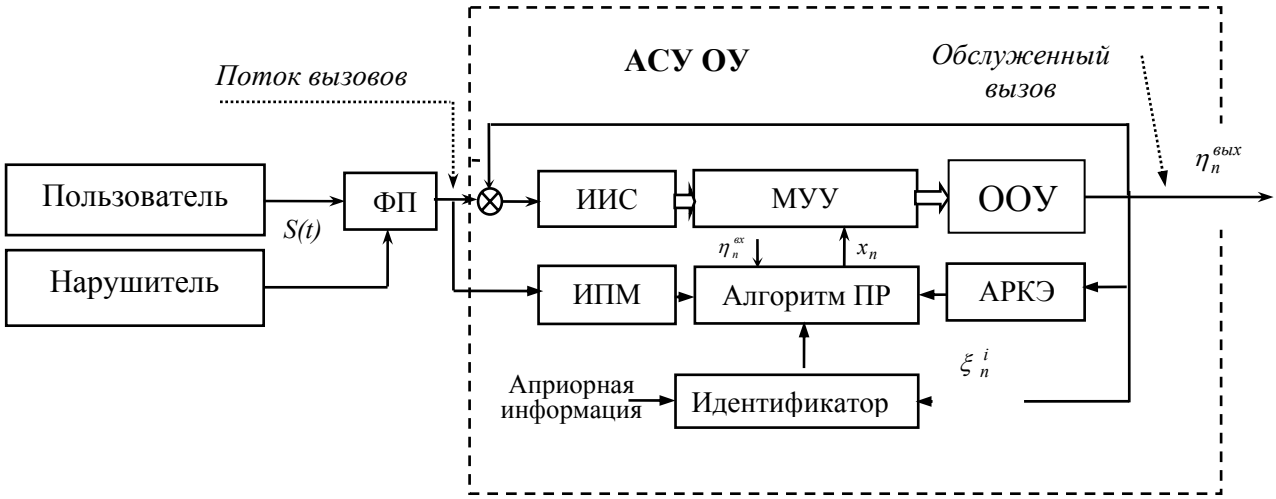

Рисунок 3. - Блок-схема концептуальной модели адаптивного управления ИЗР

В качестве целевой функции принята величина ожидаемого ущерба от НСД, определяемая через меру расхождения между реальным и оптимальным механизмами разграничения доступа

$$W = \sum_{i=1}^{I} \sum_{j=1}^{J} c_{i,j}^{0} \cdot \left| g_{i,j} - g_{i,j}^{0} \right|. \qquad (6)$$

Здесь $\{g_{i,j}\}$ - элементы прямоугольной матрицы $G(\cdot)$, отражающие реализованные правила доступа; элементы вычисляются с помощью выражений:

$$g_{i,j} = \sum_{k=1}^{K} z_{i,k} \cdot r_{k,j}^{0}\ ; \quad r_{i,j}^{0} = r_{i,j}^{1} + v_i \cdot (1 - r_{i,j}^{1})\ ; \quad r_{i,j}^{1} = \sum_{k=1}^{K} (d^{2}{}_{i,k} \cdot d^{1}{}_{k,j})\,. \qquad (7)$$

В результате преобразований получим формулировки задачи разграничения прав доступа как задачи нелинейной оптимизации вектора управляемых параметров $X = (D^1, D^2, F)$ в булевых переменных:

$$X^{*} = \min \sum_{i=1}^{I} \sum_{j=1}^{J} c_{i,j}^{0} \cdot \left| g_{i,j} - g_{i,j}^{0} \right| \qquad (8)$$

при ограничениях $\sum_{k=1}^{K} d^{1}{}_{i,k} \le 1$ и $\sum_{k=1}^{K} d^{2}{}_{j,k} \le 1$. (9)

Формальную модель пользователя представим в виде кортежа

$$P = \{F, H, V, D, Q\}, \qquad (10)$$

где F - цель пользователя; H - априорные знания; V - предпочтения; D - уровень подготовки и наличие опыта; Q - установленный статус.

Введём формальное понятие «профиль пользователя»:

$$\mathrm{Pr}_i = \left\{ (C_j, W_j, \alpha_j)_i, j = \overline{1,k} \right\}, \qquad (11)$$

где i - текущий интервал времени; C_j - категория; W_j - текущий вес; α_j - уровень изменчивости; при этом $\mathrm{Pr}_i = \mathrm{Pr}\,R_i \cup \mathrm{Pr}\,L_i$, где $\mathrm{Pr}\,R_i = \left\{ (C_j, W_j, \alpha_j)_i \middle| \forall W_j \ge 0,\ j = 1, k \right\}$- крат-косрочный профиль, $\mathrm{Pr}\,R_i = \left\{ (C_j, W_j, \alpha_j)_i \middle| \forall W_j \prec 0,\ j = 1, k \right\}$ - долгосрочный профиль.

Для непрерывной корректировки профиля активного пользователя использован итерационный алгоритм, который основан на неявной обратной связи сервера с пользователем, реализуемой через учёт статистики запросов. Полученная оценка текущего профиля пользователя используется для ранжирования пользователей на группы по степени опасности для ресурсов АСУ: а) пользователь; б) потенциально опасный пользователь; в) опасный пользователь; г) нарушитель. Для синтеза процедуры автоматической классификации применен аппарат нечётких множеств.

В случае реализации РУД логическая обработка запросов и настройка МЗ существенно усложняются из-за учёта вложенности правил регулирования доступа. На рис. 4 показана схема адаптивного управления, в которой реализована РУД. Алгоритм допуска представлен в виде совокупности вложенных процедур: допуск к работе (в составе проекта), допуск к функциональному компоненту (ФК) и допуск к информационным ресурсам. На схеме (рис.4) выделено два замкнутых контура: контур управления правами доступа и контур адаптации алгоритма управления доступом.

Введение контура дискретной адаптации механизма управления доступом существенно повышает гибкость и расширяет функционал системы ИЗР АСУ, работающей в многопользовательском режиме. Выполненная декомпозиция задачи многоуровневого логического управления доступом упрощает формальное описание и исследование ИЗР с использованием инструментария дискретных потоковых систем. Для количественного анализа ИЗР с ролевой моделью доступа применен аппарат модифицированных временных сетей (МВС) Петри.

Разработана модель адаптивного ролевого управления доступом к ресурсам в базисе МВС Петри, позволяющего корректно описать конфликтные ситуации и особенности обработки запросов в многопользовательском режиме работы. Синтезирована операционная схема информационного взаимодействия, определен функционально полный набор позиций, сформулированы условия срабатывания переходов и определена начальная разметка МВС.

На рис. 5 представлена схема, отражающая логическую структуру операционной модели системы трёхступенчатого управления правами доступа, построенной с использованием формализма МВС Петри. Сетевая модель в базисе МВС Петри содержит два множества элементов – позиции и переходы, связь между которыми отражает логическую структуру принятой схемы управления доступом.

Позиции $p_1,...,p_9$ отражают функциональные состояния системы управления доступом: p_1 - активное состояние пользователя; p_2 - пользователь допущен к работе в проекте; p_3 - пользователь допущен к работе с функциональными компонентами; p_4 - пользователь допущен к файлам информационного ресурса; p_5 - проверка прав пользователя в проекте; p_6 - проверка прав доступа пользователя к функциональным компонентам; p_7 - проверка прав пользователя к файлам; p_8 - восстановление исходного состояния системы управления доступом; p_9 - ограничение активности пользователя во времени, связанного с разработкой или корректировкой информационного проекта. Переходы $t_1,...,t_8$ - отображают совокупность условий перехода (и модифи-

кации) маркеров из одной позиции сети в другие, что определяется набором априорных данных – функционала множества переходов.

Формализм МВС Петри обладает широким спектром функциональных возможностей для вероятностно-временного описания процессов, протекающих в системе РУД с адаптацией процедур регулирования прав доступа. Статистические данные о динамике маркеров в МВС Петри дают основание для определения характеристик системы управления доступом по результатам имитационного моделирования.

Для оценки статистических характеристик системы управления доступом и определения перспективных способы снижения риска инсайдеровских утечек предложена вероятностная модель механизма управления доступом. Предположим, что на заданном отрезке времени $t \in [t_0, t_N]$ выделены характерные состояния $S_1,...,S_n$ системы управления доступом. Переход системы из состояния S_i в состояние S_j осуществляется в случайные моменты времени t с интенсивностью $\lambda_{i,j}$ в соответствии с размеченным графом переходов. Математическая модель представляет собой систему линейных дифференциальных уравнений, которые составляются в соответствии с рекомендациями теории Марковских процессов. В качестве переменных в уравнениях выступают вероятности $P_i(t)$ нахождения системы в состояниях $S_i(t)$, $i = \overline{1,n}$.

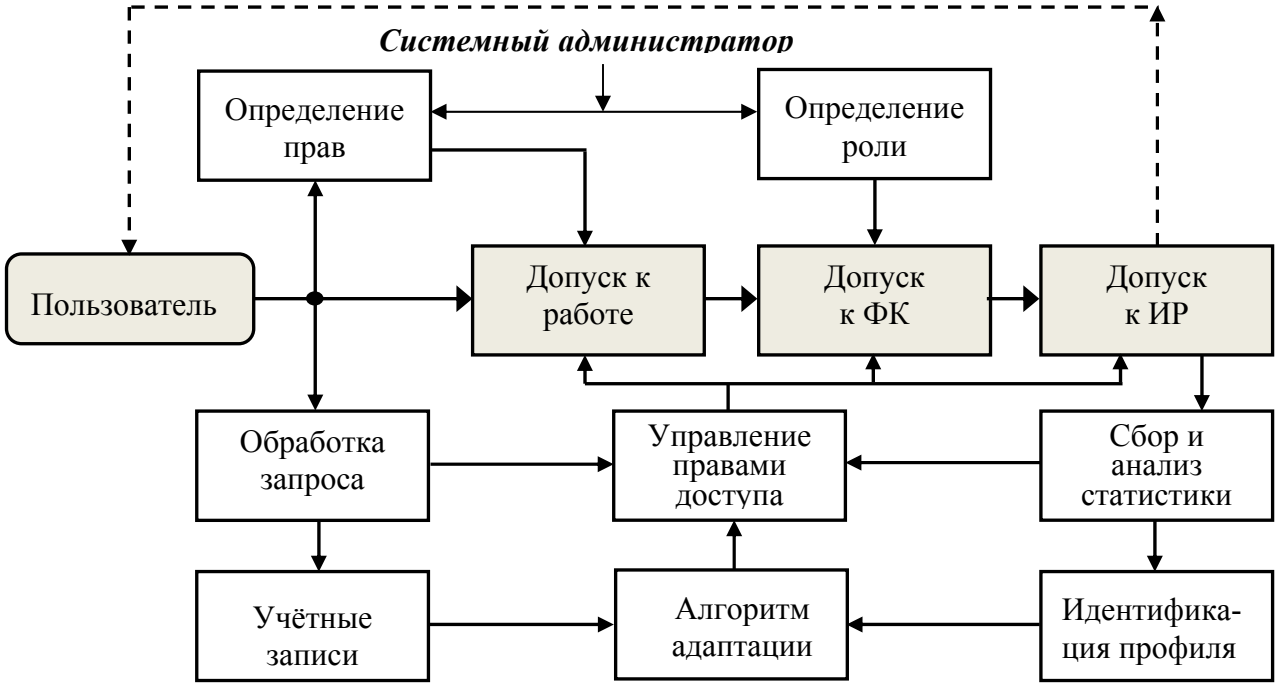

Рисунок 4 - Схема адаптивного управления правами доступа с базовой моделью РУД

На рис. 6 представлен размеченный граф переходов СУД: S_1- готовность к обслуживанию запроса; S_2 и S_3 - идентификация и аутентификация пользователя соответственно; S_4 - выполнение запроса пользователя на обслуживание; S_5 - выдача информации из базы данных по запросу; S_6 - обнаружение превышения полномочий пользователя, игнорирование его запроса; S_7 - обнаружение попытки нарушения конфиденциальности информации, игнорирование запроса пользователя; S_8 - выяв-

ление факта нарушения целостности данных, связанного с некорректной работой пользователя, аутентификация пользователя; S_9 - фиксация нарушения и блокирование доступа, восстановление повреждённого информационного элемента.

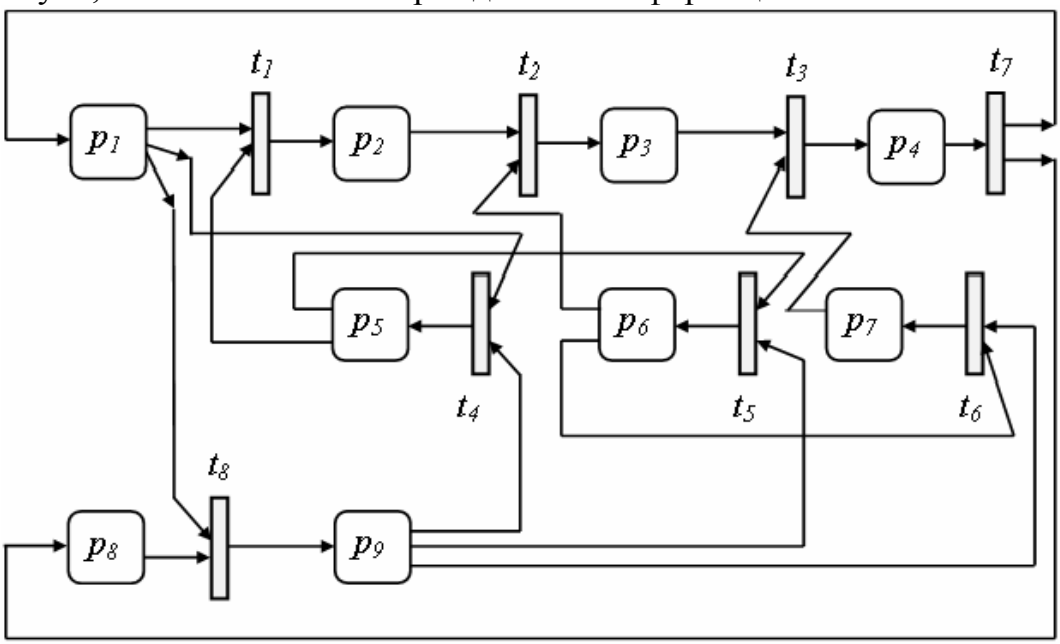

Рисунок 5. - Схема имитационной модели адаптивного управления с базовой моделью РУД в терминах МВС Петри

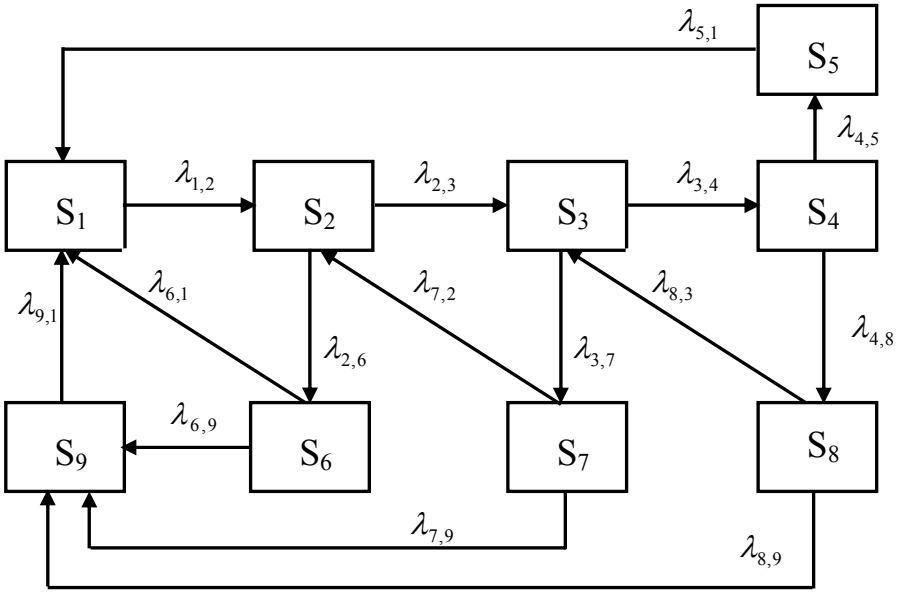

Рисунок 6. - Размеченный граф состояний модели СУД

Система однородных уравнений Колмогорова представлена выражением:

$$\frac{dP_i(t)}{dt} = -A_{i,k} \cdot P_i(t) + \sum_{k=1}^{n} B_{k,i} \cdot P_k(t), \quad i = \overline{1,n}, \tag{13}$$

где $A_{i,k}$ и $B_{k,i}$ - коэффициенты дифференциальных уравнений, полученные по известной методике и выраженные через интенсивности переходов (рис.6). Решение систе-

мы уравнений (13) осуществляют численным методом для заданных начальных условий: $P_1(t_0)=1, P_i(t_0)=0\ \forall i=\overline{2,\ n}$. Результаты решения представляются в виде таблиц и графиков, на основе которых определяют значения вероятностей нахождения СУД в выделенных состояниях на отрезке времени $t\in[t_0,t_N]$. Результаты моделирования используются для анализа результативности действий нарушителя и, следовательно, для косвенной оценки эффективности механизмов защиты ресурсов АСУ. Для определения оптимальных настроек процедур управления доступом осуществляют:

а) параметризацию интенсивностей переходов $\lambda_{i,j}(t)$ в виде регрессионных моделей $\lambda_{i,j}(t)=a+b_1\cdot t+b_2\cdot t^2$, где a, b_1, b_2 - коэффициенты регрессии; t - время;

б) разделение множества возможных состояний $S=(S_1,...,S_n)$ на два подмножества S^A и S^B, которые соответствуют работоспособному или неработоспособному состояниям системы; при этом вероятность $P_r(t^*)=\sum_{i\in B}P_i(t^*)$, где B - множество неработоспособных состояний, определяющее оценку риска.

в) параметризацию риска $P_r(t^*)$ нарушения конфиденциальности информации в виде многофакторной регрессионной модели 2-го порядка:

$$P_r(t^*)=c_0+\sum_{k=1}^{m}c_k\cdot v_k+\sum_{q=1}^{m}c_{q,q}\cdot v_q{}^2+\sum_{i,\,j=1}^{m}c_{i,j}\cdot v_i\cdot v_j\ ,\quad i\neq j\ ,$$

где $v=(v_1,...,v_m)^T$ - вектор управляемых параметров, регламентирующих используемое правило разграничения прав доступа пользователей.

В **третьей главе** «Методика прогностической оценки устойчивости интегрированной защиты ресурсов АСУ ОУ» разработан методический подход к определению количественных оценок показателей эффективности защиты ИО и ПО. Методика основана на применении имитационной модели адаптивного РУД с использованием инструментария модифицированных временных сетей Петри, вероятностной модели механизма управления доступом и игровой модели функционирования динамической системы (ДС) «Система ИЗР – нарушитель политики ИБ» («СИЗР-Н»).

Оценка показателей ИСЗ базируется на операционном моделировании процесса изменения состояния ДС «СИЗР-Н» и сводится к определению численностей состояния компонентов модели в момент времени t^* завершения информационного конфликта. Для оценки эффективности защиты ресурсов АСУ введен векторный показатель потерь $W=\{W_i(t^*)\}$, под которыми понимают величину относительного ущерба, нанесенного средствам $z=\{z_i, i=1,...,n\}$ в результате целенаправленных информационных атак противоположного игрока. Показатель относительного ущерба $W_i(t^*)$ по переменной z_i вычисляют по формуле:

$$W_i(t^*)=\frac{z_i(t_0)-z_i(t^*)}{z_i(t_0)}\cdot 100\%,\quad i=\overline{1,n}\ , \qquad (14)$$

где t_0 - момент начала информационного противоборства; t^* - момент выхода из цикла моделирования; $z_i(t_0)$ - исходный потенциал средства z_i в момент времени t_0; $z_i(t^*)$ - сохранившийся потенциал средства z_i в момент времени t^*.

На рис. 7 представлена операционная схема информационного взаимодействия элементов динамической системы «СИЗР-Н». При этом введены следующие обозначения: игрок А – СИЗР; игрок В - нарушитель, стремящийся получить доступ к ресурсам АСУ ОУ. В составе модели игрока А выделены элементы: средства программного обеспечения (СПО), база данных (БД), средства пассивной защиты (восстановления ресурсов) (СПЗ) и средства активной защиты (САЗ). В модели игрока В выделены: средства активного нападения 1-го и 2-го типов ($САН_1$ и $САН_2$) и система управления ими. СПЗ используются для обнаружения, локализации и восстановления повреждённых информационных элементов и программных модулей.

Для формализованного представления ДС «СИЗР-Н» введены переменные $z_i, i = 1,...,n$ $(n = 6)$, под которыми соответственно понимают численности состояний средств ПО, ИО и средств активной защиты игрока А, средств активного нападения 1-го типа, системы управления и средств активного нападения 2-го типа игрока В. Состояние динамической системы «СИЗР-ЗЛ» в целом в текущий момент времени $t \in [t_0, t_N]$ характеризуется вектором состояния $z(t) = [z_1(t), ..., z_n(t)]^T$.

Результаты цифрового моделирования информационного взаимодействия игроков А и В, представленные в табличной и графической формах, позволяют проследить фазовую траекторию ДС $z_i(t), i = \overline{1,6}$, и через расчёт показателей $W_i(t^*)$ по формуле (16) косвенно оценить эффективность механизма ИЗР АСУ ОУ.

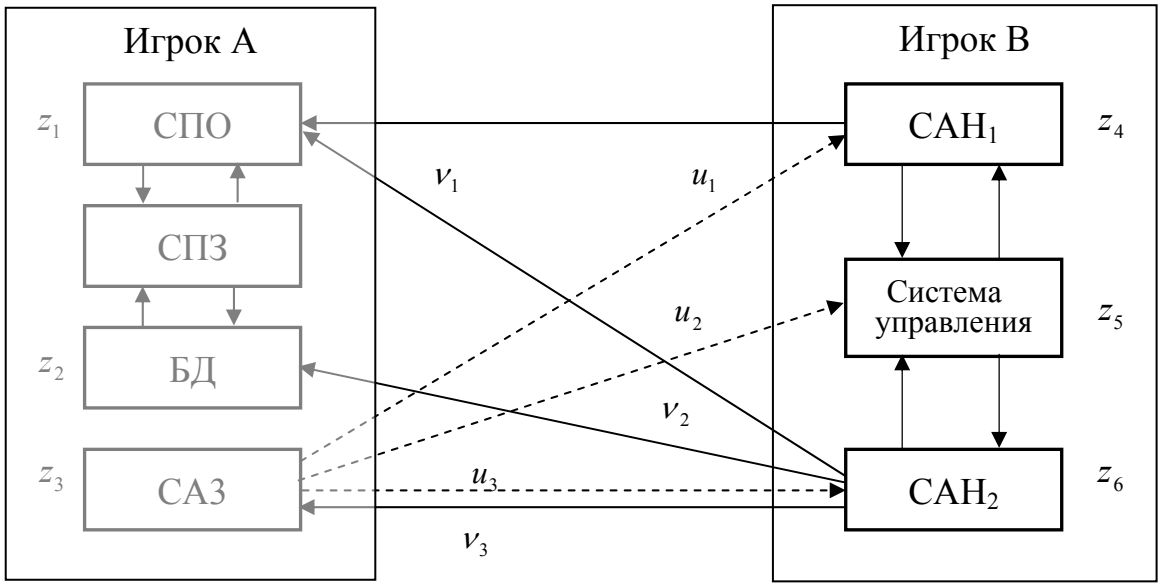

Рисунок 7. - Операционная схема конфликтной ситуации в ДС «ИЗР-Н».

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

В диссертации сформулирована и решена **научная задача -** разработка методов, моделей и алгоритмов, реализующих стратегию адаптивного ситуационного управ-

ления механизмами интегрированной защиты информационного и программного обеспечения АСУ ОУ, используемой в составе региональной ИОС.

1. На основе обобщения и систематизации опыта инновационных вузов России в решении задач автоматизации процессов управления проведён анализ тенденций развития коммуникационной инфраструктуры АСУ ОУ и определены основные требования к обеспечению защиты её ресурсов. Установлено, что перспективы АСУ ОУ связаны с переходом к сервисно-ориентированной архитектуре, а для защиты её ресурсов продуктивным является технологический подход, в котором реализуются принципы комплексности защиты и гибкости управления.

2. С использованием аппарата адаптивного выбора вариантов разработана теоретико-множественная модель адаптивного ситуационного управления механизмами интегрированной защиты ресурсов АСУ ОУ в составе единой региональной ИОС. Предложенный подход заключается в определении последовательности рациональных механизмов защиты ресурсов, которая в определенном вероятностном смысле обеспечивает минимум предельных средних потерь в условиях варьирования угроз. Это соответствует общей задаче управления рисками информационной безопасности в региональной ИОС и создаёт концептуальную основу для осуществления согласованного управления комплексом средств ИЗР в многоуровневой структуре АСУ ОУ. Синтезированный в соответствии с методом стохастической аппроксимации рекуррентный алгоритм определяет решающее правило рандомизированного выбора рационального варианта механизма защиты.

3. Разработан алгоритм обнаружения и статистической идентификации профиля нарушителя политики ИБ вуза на основе интеллектуальной обработки и анализа уязвимостей критических ресурсов и учетных записей пользователей. Алгоритм отличается комплексным использованием анализа учётных записей и результатов мониторинга ресурсов и позволяет осуществлять гибкую настройку базовой модели профиля пользователя с последующей идентификацией потенциального нарушителя.

4. Разработана методика оценки и прогнозирования показателей ИЗР на основе процедур статистической идентификации профиля нарушителя, имитационной модели механизма адаптивного ролевого управления доступом, вероятностной модели управления механизмами защиты и игровой модели функционирования ИЗР в условиях нарушения пользователями АСУ требований корпоративной политики ИБ вуза. Разработана имитационная модель адаптивного ролевого управления правами доступа к информационным ресурсам АСУ ОУ, отличающаяся применением аппарата модифицированных временных сетей Петри и позволяющая адекватно отразить определяющие логико-вероятностные связи и информационные процессы, протекающие в контурах системы управления. Предложенные модели в совокупности позволяют выявлять потенциальные уязвимости и осуществлять автоматическую настройку механизмов интегрированной защиты ИО и ПО АСУ ОУ.

5. Обоснованы предложения по организации мониторинга событий информационной безопасности и аудита действий пользователей при функционировании АСУ ОУ. Подготовлены методические рекомендации по обучению системных программистов и администраторов баз данных на курсах повышения квалификации. В инте-

ресах высокого уровня организационного обеспечения функционирования системы ИЗР внесены изменения в программу переподготовки и повышения квалификации системных программистов и администраторов баз данных. В учебную программу дополнительно введены дисциплины, обеспечивающие формирование у штатных сотрудников системы управления ОУ специальных умений и навыков мониторинга ресурсов АСУ ОУ, решения задач выявления уязвимостей и оперативного управления механизмами ИСЗ с использованием авторских моделей и алгоритмов адаптивного ситуационного управления.

В результате теоретических исследований, цифрового моделирования и опытно-экспериментальной проверки разработанных положений, моделей и алгоритмов подтверждён существенный синергетический эффект, который обусловлен переходом к адаптивному ситуационному управлению механизмами интегрированной защиты информационного и программного обеспечения и проявляется в приращении устойчивости функционирования АСУ ОУ к проявлению угроз.

РАБОТЫ, ОПУБЛИКОВАННЫЕ ПО ТЕМЕ ДИССЕРТАЦИИ:

Статьи, опубликованные в периодических изданиях, рекомендуемых ВАК

1. Надеждин Е.Н., Козлов А.О. Вероятностная модель системы управления доступом в корпоративной вычислительной сети образовательного учреждения // Известия Института инженерной физики, 2010. - Т.2. - №16. - С. 39-43.

Другие публикации результатов исследования

2. Козлов А.О. К вопросу о защищённости операционных систем от утечки информации // Сб. трудов 12-й Международной НТК «Проблемы передачи и обработки информации в сетях и системах телекоммуникации». - Рязань: Изд-во ГОУ ВПО «Рязанская государственная радиотехническая академия», 2004. - С. 131-133.

3. Козлов А.О. Проблемы обеспечения информационной безопасности в информационно-образовательной среде // Материалы I Всероссийской НПК «Развитие творческого наследия С.Я. Батышева в системе непрерывного профессионального образования». Том 4. – Н.Новгород: ГОУ ВПО «Волжский государственный инженерно-педагогический университет», 2006. – С. 51-53.

4. Козлов А.О., Поляков В.П. Аспекты защиты информации при проектировании корпоративных сетей учебного назначения // Материалы V Всероссийской научно-практической конференции «Проблемы информатизации образования: региональный аспект». – Чебоксары, 2007. – С. 9-11.

5. Козлов А.О. Проблемы защиты информации в корпоративных сетях учебного назначения // Сборник материалов Всероссийской НПК студентов, аспирантов, специалистов и молодых ученых «Современные проблемы науки, образования и производства». Том 1. – Н. Новгород: НОУ ВПО «Нижегородский филиал Университета Российской академии образования», 2007. - С. 174-176.

6. Козлов А.О. Обеспечение информационной безопасности в информационно-образовательной среде // Материалы IX международной научно-методической конференции преподавателей вузов, ученых и специалистов «Инновации в системе непрерывного профессионального образования», Т. 2. – Н. Новгород: ГОУ ВПО

«Волжский государственный инженерно-педагогический университет», 2008. – С. 158-161.

7. Надеждин Е.Н., Смирнова Е.Е., Козлов А.О. Модели информационного противоборства в задачах оценки безопасности вычислительных сетей // Информатизация образования и науки. - 2009. - № 2. - С.45-50.

8. Козлов А.О. Оптимизация системы защиты информации методом вектора спада // Сборник трудов II Межвузовской научно-методической конференции «Шуйская сессия студентов, аспирантов, молодых учёных». - Москва – Шуя: Изд-во ГОУ ВПО «Шуйский государственный педагогический университет», 2009. - С. 63-66.

9. Надеждин Е.Н., Козлов А.О., Соколов И.Н. Проблемные вопросы адаптации механизма интегрированной защиты ресурсов корпоративной вычислительной сети // Труды XVII Межвузовской НТК «Пути совершенствования ракетно-артиллерийских комплексов, средств управления войсками и оружием, их эксплуатации и ремонта». - Тула: Издательство ГОУ ВПО «Тульский артиллерийский институт», 2010. - С.49.

10. Козлов А.О. Проблемы эффективной организации и обеспечения интегрированной защиты информационного и программного обеспечения вычислительных сетей образовательных учреждений // Материалы Международной НПК «Современные достижения в науке и образовании: математика и информатика». - Архангельск: ГОУ ВПО «Поморский государственный университет им. М.В. Ломоносова», 2010. - С. 554-557.

11. Козлов А.О. Упрощение и удешевление администрирования компьютерного парка школьных образовательных учреждений в масштабах района с помощью применения единой компьютерной среды на основе технологии «виртуальный компьютер» и «тонкий клиент» // Материалы Всероссийской с международным участием НПК, посвящённой 80-летию Чувашского ГПУ им. И.Я. Яковлева.- Чебоксары: Изд-во ГОУ ВПО «Чувашский государственный педагогический университет им. И.Я. Яковлева», 2010. - С. 61-64.

12. Козлов А.О. Разработка и анализ компонентов системы управления интегрированной системы защиты сетевых ресурсов // Сборник статей по материалам XI Международной научно-методической конференции преподавателей вузов, учёных и специалистов «Инновации в системе непрерывного профессионального образования». – Н. Новгород: ГОУ ВПО «Волжский государственный инженерно-педагогический университет», 2010. - С. 78-85.

13. Козлов А.О. Проблемы администрирования компьютерного парка школьных образовательных учреждений на основе технологий "виртуальный компьютер", "тонкий клиент", "бездисковая рабочая станция" // Материалы Всероссийской научно-практической конференции с международным участием «Информационные технологии на базе свободного программного обеспечения». - Елец: ГОУ ВПО «Елецкий государственный университет им. И.А. Бунина», 2010. - С.100-104.