Динамическая модель управления функционированием легальных пользователей информационной системы

А.В. Калач[1], А.С. Кравченко[1], А.А. Зенин[1]

[1]Воронежский институт ФСИН России, Иркутская 1а, Воронеж, Россия, 394072

Аннотация. В настоящее время наблюдается тенденция роста числа компьютерных преступлений, состоящих в хищении информации ограниченного распространения и, как следствие, в значительных материальных потерях. Поэтому сейчас важную роль играет обеспечение информационной безопасности, защиты информации и объектов информатизации. Исследование посвящено разработке модели аудита компьютерных систем с точки зрения обеспечения их информационной безопасности. Создана динамическая модель контроля работы пользователей в интересах Федеральной службы исполнения наказаний России.

1. Введение

Динамическая модель управления функционированием легальных пользователей информационных систем, очевидно, может быть построена правильно только на базе понимания общих принципов и этапов построения автоматизированных систем.

Процесс создания автоматизированной информационной системы в основе которой лежит динамическая модель управления функционированием легальных пользователей проходит несколько этапов:

– исследование экономических показателей разрабатываемой информационной системы (ответ на вопрос о выгодах от разработки системы автоматизации управления);

– создание модели, имитирующей штатную работу информационной системы и возможные изменения ее управляемых параметров;

– разработка методов принятия решений и схемы взаимосвязей между устройствами управления;

– создание работоспособного экземпляра информационной системы.

Последовательность указанных этапов итерационно повторяется с изменением детализации структуры информационной системы с подсистемой управления легальными пользователями и точности постановки целевых параметров ее работы.

Естественный ход этапов процесса создания автоматизированной информационной системы (АИС) в основе которой лежит динамическая модель управления функционированием легальных пользователей накладывает требование учета сложных и достаточно сложно формализуемых особенностей входов системы управления и порождаемых ими изменений конечного состояния системы управления, содержательные особенности входного потока сведений, вероятностные характеристики возможностей изменения состояния системы управления и объекта управления.

В существующей системе ограничений наилучшим выбором построения модели управления работой информационной системы является применение имитационного динамического моделирования, способного описать модель, которую можно применить для исследования функционирования АИС в основе которой лежит динамическая модель управления функционированием легальных пользователей.

При выборе структурной схемы и алгоритма управления автоматизированной информационной системой существенной является информация о состоянии исследуемого режима функционирования с учетом его динамических свойств. Что касается учета отклонений измерений состояния объекта управления и определения меры достоверности результатов работы алгоритма управления в обстановке большого информационного потока, то такой расчет должен опираться на адекватную имитационную динамическую модель.

Принятие структурной схемы внутреннего строения АИС обуславливает необходимость идентификации и характеристики информационных ресурсов, которые являются исходными данными для устройства управления легальным пользователем с целью изменения выходных характеристик АИС при угрозе нарушения безопасности сведений.

Разработка управленческого решения основывается на хорошо зарекомендовавших себя методах принятия решений [1-3].

Разработка управленческого решения должна опираться на аппарат, способный принять во внимание возмущения, отклоняющие оцениваемый режим от нормальных условий функционирования АИС и подсистемы управления, которые могут быть как внутрисистемными, так и внешними.

Внешние по отношению к подсистеме управления легальными пользователями возмущающие факторы:

- возможные отклонения внешних процессов и средств технологического характера;
- возможные внешние отклонения организационного характера
- возможные внешние отклонения социального характера.

Внутренние по отношению к подсистеме управления легальными пользователями возмущающие факторы

- возможные внутренние возмущения процесса управления, выражающихся во взаимовлиянии управляющих воздействий одного управляемого параметра на другой;
- возможные внутренние возмущения выражающихся во взаимовлиянии состояния одного управляемого параметра на другой.

Динамическое моделирование управления автоматизированной системой и функционированием ее легальных пользователей, по существу, представляется в форме описания ее деятельности как информационной системы с обратной связью. На вход модели поступают массивы информации извне, на выходе – прогнозируемый результат.

Критериями оценки качества управления могут выступать эффективность, надежность, защищенность, быстродействие, качество продукции и т.д.

Наиболее важные функции устройства управления и всей подсистемы управления можно охарактеризовать следующим образом:

- получение информации о текущем состоянии объекта управления с системных датчиков;
- анализ сведений о текущем состоянии объекта управления;
- выработка оптимального в заданной системе ограничений управляющих воздействий на объект управления, которые приводят его в целевое состояние.

Необходимо отметить важные отличительные черты процесса разработки моделей АИС с подсистемами управления сложными объектами:

- модель определения качества выработанных управляющих воздействий одновременно является моделью АИС в целом, содержащей целостное представление о ее функционировании, интерфейсах объектов управления;
- отсутствие стандартизированных моделей обработки информационных ресурсов АИС с подсистемой управления легальными пользователями и как следствие необходимость их разработки.

Автоматизированная информационная система – это совокупность взаимосвязанных систем передачи информации с централизованным управлением. Каждым режимом функционирования управляет автомат принятия решения, входными сведениями для которого являются данные датчиков объектов информационной системы.
Все возможные режимы работы автомата управления («решение», «действие», «отклик») поведение системы управления характеризуется наличием пауз для выполнения действий и принятия решений, разногласиями между входными и выходными параметрами системы управления, наличием непроизвольных модификаций в системе управления.

2. Контекст безопасности информационных технологий при динамическом моделировании автоматизированной информационной системы

В рамках решения комплексной задачи разработки модели управления работой легальных пользователей информационной системы значение имеет предварительная оценка таких систем с точки зрения их безопасности.
Всякая система управления, в том числе автоматизированная информационная система, выполняет три основные функции, упомянутые ранее.
Существенно, чтобы требования, предъявляемые к разработке АИС, эффективно содействовали достижению целей безопасности.
Суть динамического моделирования заключается в том, что система или отдельные ее элементы заменяются такой моделью, которая имеет сходные с оригиналом динамические свойства самых широких границах.
Динамическое моделирование рассматривает переходные процессы. Для этих целей на исследуемую схему в заданных точках подаются типовые воздействия.
Процесс разработки динамической модели функционирования АИС также имеет целью уточнение требований безопасности, причем каждое приближение в итерационном процессе уточнения представляет собой декомпозицию проекта с его дополнительной детализацией.
Требования безопасности функционирования АИС в предлагаемой структуре динамической модели содержат описание штатных (нормальных) для АИС режимов работы, так могут быть заявлены требования отсутствия нештатных способов функционирования системы.
Наличие штатного (нормального) режима, очевидно, доказывается в процессе эксплуатации АИС по ее назначению, и тогда достаточно будет описать объектную модель, описывающую предметную область для которой разрабатывается система в виде неизменной во времени структуры взаимодействия объектов. В то время как уменьшение риска наличия нежелательного режима в значительной мере определяется последовательно:

– моделированием поведения АИС, предоставляющим оценку влияния на него массива внешних воздействий;
– испытаниями (тестированием) АИС;
– экспертизой проекта;
– окончательной реализацией АИС.

Такой подход в уменьшении рисков позволяет, судить, во-первых, об отсутствии нежелательного режима, во-вторых, об адекватности применяемой модели функционирования АИС.

3. Оценка возможных сценариев и развития событий

Для возможности исследования функционирования АИС в режиме функционирования нужно предусмотреть конечное множество сценарием ее работы, в которых в явном виде проявляются наиболее стандартные варианты применения АИС легальным пользователем.
С помощью динамического моделирования создается единая структурная схема АИС, в которой интегрируются внутренние функциональные взаимодействия управления. При этом реализуются количественный и экспериментальный методы решения задачи приведения логической структуры и способов такого взаимодействия в соответствие требованиям к устойчивости функционирования.

Следует отметить, что построенная статическая структурная схема взаимосвязей компонентов и потоков данных между ними не в полной мере способна отразить работу информационной системы в целом. Чтобы дополнить картину и построить модель наиболее верно повторяющую суть информационных процессов нужно иметь возможность описание динамики изменения состояния информационной системы в процессе ее штатной работы, а также в исключительных ситуациях.

Основные компоненты модели функционирования любой АИС включают в себя структурные элементы, которые содержат параметры, дающие возможность разработчику специфицировать совокупность характеристик, включаемых в техническое задание на разработку конкретной АИС для выполнения требований безопасности информации.

Структурные элементы, внедренные для обеспечения безопасности информации способны однозначно определять значения указанных параметров, ограничения на значения которые он принимает. Значения могут рассматриваться как дискретное измерение параметра, а также как правило, описывающее допустимые значения параметра.

Использование такого универсального метода позволяет получить динамическую модель функционирования любой конкретной АИС.

Практическая ценность модели всегда определяется:

– проявлением системных свойств в выбранной архитектуре модели;
– полнотой и содержанием требований заказчика;
– компетентностью разработчика модели;
– квалификацией приглашаемых экспертов.

Причем ее полнота и адекватность будет определяться:

– набором и предполагаемой структурой взаимодействия элементов и их параметров в рамках модели;
– полнотой и непротиворечивостью массива исходных данных для модели и массива ожидаемых результатов.

В этом плане цель разработчика модели состоит в том, чтобы:

– разработать выверенное по всем аспектам работы информационной системы представление о соответствии ее функций решаемой задаче;
– обосновать указанное соответствие разработав систему тестирования и оценки адекватности модели предъявляемым требованиям.

4. Методика создания модели функционирования автоматизированной информационной системы

Оценка режима функционирования АИС проводится по выбранным критериям с использованием динамической модели и преследует две цели:

– во-первых, продемонстрировать, что описание режима функционирования АИС является полным, непротиворечивым, технически правильным и, следовательно, пригодным для использования в качестве основы для оценки соответствующего объекта;
– во-вторых, в случае, если в задании имеется утверждение о соответствии какому-либо условию (требованию), продемонстрировать, что данная АИС должным образом отвечает этим требованиям.

Как правило, динамическая модель представляет собой совокупность разработанных на основе описания структуры информационной системы диаграмм состояний ее объектов, которые в полной мере описывают интерфейсные связи ее объектов, управляемые параметры и возможные состояния системы управления. Такое представление решает задачу описания практического взаимодействия объектов управления информационной системы.

Для построения диаграмм состояний нужно решить ряд задач:

– подготовка сценариев взаимодействия легальных пользователей с АИС;
– определений интерфейсов взаимодействия с убавляемыми параметрами АИС;
– построение диаграммы состояний каждого объекта информационной системы, отражающие типовые события как внешние, так и внутренние по отношению к информационной системе;

– доказательство непротиворечивости постоянных диаграмм состояний каждого объекта информационной системы.

На этапе аттестации АИС необходимо сначала построить (выбрать) общую структуру (архитектуру) системы.

После принятия решения о структуре системы в целом следует производить ее разбиение на относительно независимые в реализации подсистемы (модули), то есть необходимо построить изначальную архитектуру анализа контроля защищенности выбранных параметров СВТ и ТКО, в которой будут включены схемы и блоки интересующих критериев параметров, их взаимосвязь.

Динамические модели применимы для описания систем непрерывной и пакетной обработки, систем с интерактивным интерфейсом, системы обработки сигналов в реальном времени.

Рассмотрим для примера типичную блок-схему модели функционирования АИС, состоящей из ряда ОЗИ, представленную на рисунке 1.

На нем в развернутом виде показана схема потока информации для двух объектов защиты информации (ОЗИ) в аспекте их взаимодействия между собой и с окружающими объектами. Ими могут быть, например, средство вычислительной техники (СВТ), телекоммуникационное оборудование (ТКО) и т.п., входящие в состав анализируемой АИС.

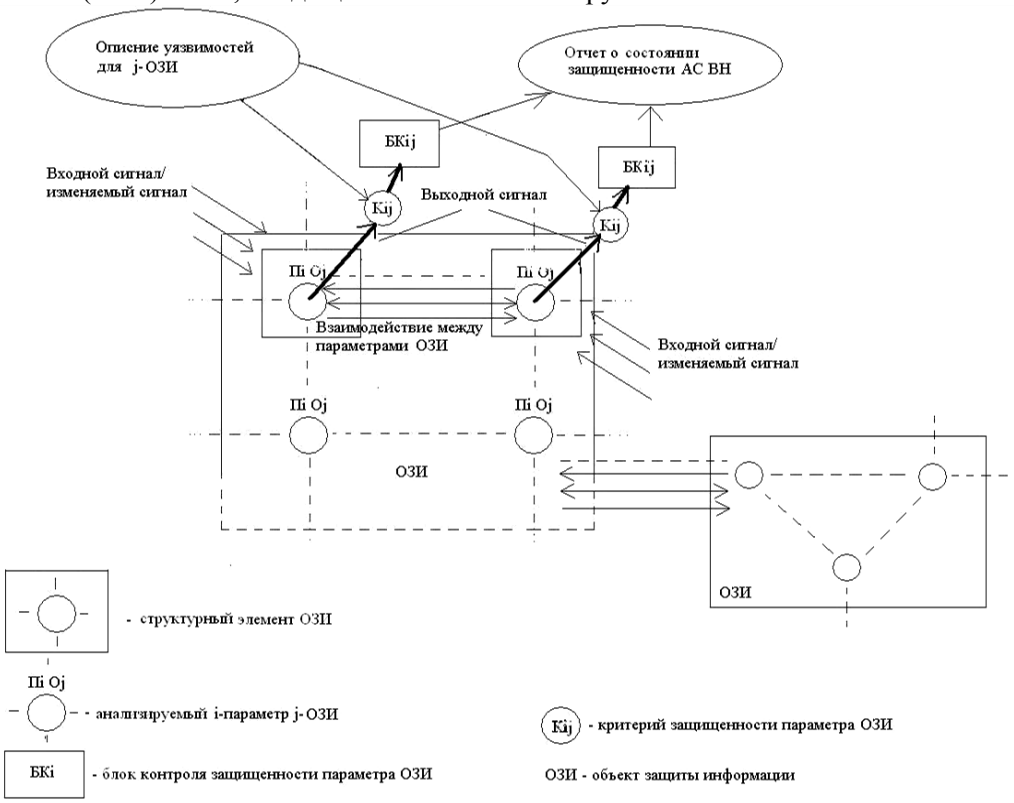

Рисунок 1. Блок-схема модели функционирования СУБД.

На рисунке 1 сплошными стрелками изображены возможные анализируемые параметры модели:

– связи и взаимодействия параметров модулей согласно перечню контролируемых параметров АИС в целом и отдельных ее элементов;

– параметры внешних факторов (уязвимостей), влияние которых полагается существенным при построении модели функционирования АИС (взаимосвязь – двойная стрелочка, подчинение – стрелка с одним указателем) или их отсутствия (пунктирная линия).

Полужирными стрелками обозначены направления потока информации (сигналов) о поведении отельных модулей и моделируемого объекта в целом при изменении входных параметров по заданной программе и в установленных диапазонах.

Данные ОЗИ могут характеризоваться различными анализируемыми параметрами $П_iО_j$ в составе структурных элементов $ОЗИ_j$, которых может быть *N-ое* количество. Каждый из параметров $П_iО_j$ имеет набор характеристических входных сигналов.
Пунктирные линии показывают связи между $ОЗИ_j$ внутри АИС.
Работа модели функционирования системы включает следующие этапы:

1) извне на $ОЗИ_j$ воздействует *i*-й входной сигнал, сгенерированный легальным пользователем АИС из массива всех исходных данных с определенным значением параметра $П_iО_j$ (или происходит изменение этого параметра);

2) реакция на *i*-й входной сигнал, сгенерированный легальным пользователем АИС в формализованном виде, анализируется модулем критериев защищенности $К_{ij}$ на соответствие одному из заданных вариантов функционирования и преобразуется в форме *i*-го выходного сигнала;

3) выходные сигналы направляются в блоки контроля защищенности $БК_i$. Блоки $К_{ij}$ взаимосвязаны с блоком описания уязвимостей для данного ОЗИ;

4) на выходе получаем стандартный отчет о состоянии защищенности $ОЗИ_j$ и АИС в целом.

Рассмотрим архитектуры моделей функционирования приведенных выше объектов защиты информации в рамках работы легальных пользователей АИС (ОЗИ).
При разработке модели функционирования информационной системы, на основе архитектуры пакетной обработки должны быть реализованы следующие этапы:

– составление системы диаграмм потоков данных по фазам выполнения процессов;
– выделение классов промежуточных объектов между последовательными фазами;
– разработка объектной модели промежуточных фаз, которые по необходимости разбиваются на подфазы.

Разработка динамической модели функционирования информационной системы реального времени предполагает этапность.
Во-первых необходимо построение диаграммы потока данных. Граничные активные объекты информационной системы выбираются и функционируют на основании структур данных, с динамическими значениями. Хранилища данных, связанные с ее внутренними фазами, отражают параметры, которые влияют на зависимость между входными и выходными данными фазы;
Во-вторых необходимо определить классы промежуточных объектов между каждой парой последовательных фаз. Каждая фаза знает об объектах, расположенных на объектной диаграмме до и после нее;
В-третьих необходимо представить каждую фазу как последовательность изменений значений элементов выходной структуры данных в зависимости от значений элементов входной.
При разработке модели функционирования системы с интерактивным интерфейсом необходимо выполнить следующие шаги:

– выделяем объекты, формирующие интерфейс;
– используем, если есть возможность, готовые объекты для организации взаимодействия (например, для организации взаимодействия системы с пользователем через экран дисплея можно использовать библиотеку системы X-Window, обеспечивающую работу с меню, формами, кнопками и т.п.);
– определяем структуру программы по ее динамической модели. Для реализации интерактивного интерфейса используем параллельное управление (многозадачный режим) или механизм событий (прерывания), а не процедурное управление;
– выделяем из множества событий физические (аппаратные, простые).

При разработке модели функционирования системы управления транзакциями необходимо выполнить следующие шаги:

– отображаем объектную модель на базу данных;
– определяем асинхронно работающие устройства и ресурсы с асинхронным доступом, в случае необходимости определяем новые классы;
– определяем набор ресурсов (в том числе структур данных), к которым необходим доступ во время транзакции (участники транзакции);

– разрабатываем параллельное управление транзакциями. Системе может понадобиться несколько раз повторить неудачную транзакцию прежде, чем выдать отказ.

5. Анализ типичной структуры сложной автоматизированной информационной системы

В качестве типичной структуры сложной системы, имеющей автоматизированное управление, следует принять систему, которая взаимодействует с объектами внешней среды (например, с другими АИС), т. е. получает входные и управляющие сигналы, и сама выдает выходные сигналы.

Элементы системы управления в зависимости от их функции в управляющем процессе для ц

Важно иметь в виду, что истинная информация не фигурирует внутри системы. Она может быть известна только постороннему наблюдателю, обладающему средствами измерения идеальной точности, способными зафиксировать значения параметров, связанных с функционированием системы.

Таким образом, средствам обработки информации передается осведомительная информация о состояниях элементов системы и воздействиях внешней среды.

Изменение характеристик моделируемых объектов в зависимости от конфигурации и выбранных параметров обнаруживаются и оцениваются посредством:

– прямого считывания показаний датчиков информации (это наиболее простой и достоверный метод);

– анализа результатов экспертных оценок (для факторов, влияние которых невозможно оценить лабораторными методами).

Эти отклонения вместе с информацией о новых воздействиях внешней среды используются для выработки новых управляющих сигналов и т.д. В таком виде может быть представлена модель практически любой из существующих и проектируемых систем управления.

Для разных объектов и систем разработан ряд динамических моделей, описывающих процессы с различной степени детальности.

На наш взгляд, можно выделить **два типа динамики системы:**

1) функционирование – процессы, которые происходят в системе, стабильно реализующей поставленную цель;

2) развитие – то, что происходит с системой при изменении ее целей.

Моделирование сложной информационной системы с управлением легальным пользователем удобно начинать с ее описания как агрегативной системы.

Построение автоматизированной информационной системы основывается на разработке моделей с математическим аппаратом пригодным для описания частного случая рассматриваемой подсистемы. Применение специальных моделей позволяет организовать более глубокое изучение свойств подсистем в аспектах, выходящих за охват общей модели, такой подход может быть реализован путем практикоориентированной детализации универсальных моделей.

6. Основные принципы динамического моделирования

Практические рекомендации по уменьшению сложности моделей:

– изменение числа переменных, достигаемое либо исключением несущественных переменных, либо их объединением (агрегированием). Например, все типы ЭВМ в модели гетерогенных сетей можно объединить в четыре типа – ПЭВМ, рабочие станции, большие ЭВМ (мейнфреймы) и кластерные ЭВМ;

– изменение природы переменных параметров. Переменные параметры рассматриваются в качестве постоянных, дискретные – в качестве непрерывных и т.д.;

– изменение функциональной зависимости между переменными. Нелинейная зависимость заменяется обычно линейной, дискретная функция – непрерывной;

– изменение ограничений (добавление, исключение или модификация). Варьируя ограничения, можно найти возможные граничные значения эффективности. Такой прием часто используется на этапе постановки задач для нахождения предварительных экспертных оценок эффективности решений;

– ограничение точности модели. Точность результатов модели не может быть выше точности исходных данных.

Баланс погрешностей различных видов. В соответствии с принципом баланса необходимо добиваться:

– баланса систематической погрешности моделирования за счет отклонения модели от оригинала и погрешности исходных данных;
– точности отдельных элементов модели;
– систематической погрешности моделирования и случайной погрешности при интерпретации и осреднении результатов.

Многовариантность реализаций элементов модели. Разнообразие реализаций одного и того же элемента, отличающихся по точности (а, следовательно, и по сложности).

Блочное строение. При соблюдении принципа блочного строения облегчается разработка сложных моделей из готовых блоков с минимальными связями между ними. Выделение блоков производится с учетом разделения модели по этапам и режимам функционирования системы. В зависимости от конкретной ситуации возможны следующие подходы к построению моделей:

– непосредственный анализ функционирования системы;
– проведение ограниченного эксперимента на самой системе;
– использование аналога;
– анализ исходных данных.

Динамическая модель функционирования АИС с управлением легальными пользователями подразумевает определение активных объектов, которые могут менять свое состояние в процессе функционирования. Изменение состояния накладывает требование на периодическое обновление значений параметров. Вторым этапом необходимо дифференцировать частные события во взаимодействии объектов. Ключевые зависимости взаимодействия объектов являются непрерывными, чаще всего такие зависимости устанавливаются между параметром и временем.

Процесс разработки и адаптации динамической модели управляется в интересах субъекта автоматами управления, которые контролируют циклы внешних событий.

7. Разработка алгоритма выявления «слабых» мест в системе защиты информации на основе анализа динамической модели функционирования автоматизированной информационной системы

Предложения по алгоритму выявления «слабых» мест в системе защиты информации на основе анализа динамической модели функционирования АИС могут быть сформулированы в аспекте обнаружения уязвимостей моделируемой АИС и выдачи сигнала тревоги. Причем, формулирование предложений по исходным требованиям ограничивается только возможностями экспертно-аналитического метода анализа функционирования предполагаемой модели АИС.

При таком подходе для полноты реализации любого создаваемого алгоритма, вообще говоря, должны быть определены следующие исходные данные:

– объекты защиты информации с изменяемой конфигурацией АИС, которые подвержены воздействию той или иной угрозы;
– характерные источники угроз и уязвимости, способствующие реализации угроз;
– возможные модели нарушителей;
– классификация предполагаемых источников угроз по степени их реализации в зависимости от выбранной конфигурации и модели нарушителя;
– выбор очередности анализа и оценка защищенности ОЗИ, исходя из классификации предполагаемых источников угроз по степени их реализации;
– идентификация угроз безопасности функционирования АИС в целом и отдельных ее элементах.

Алгоритм выявления управления легальными пользователями АИС основе анализа динамической модели функционирования АИС может быть построен на базе экспертно-

аналитического метода идентификации и классификации угроз безопасности, применяемых в работе пользователя информационных ресурсов. В качестве основных рекомендаций при формировании предложений к данному алгоритму можно выделить следующие:

– заказчиком построения АИС должен быть определен список объектов защиты информации и их изменяемые конфигурации в АИС, которые подвержены воздействию той или иной угрозы при работе легального пользователя;

– следует выделить характерные уязвимости, способствующие реализации этих угроз, которые учитываются со структурно-функциональными характеристиками АИС;

– также необходимо выбрать возможные модели нарушителей безопасности функционирования АИС (Приложение Б) для дальнейшего анализа защищенности системы;

– после этого предполагаемые источники угроз классифицируются по степени их реализации в зависимости от выбранной конфигурации и модели нарушителя, что позволяет экспертам выбрать очередность определения угроз безопасности информации ОЗИ для быстроты и эффективности анализа;

– анализ и оценка корректности и безопасности работы легальных пользователей АИС проводятся экспертами, исходя из классификации предполагаемых источников угроз по степени их реализации;

– оценка функционирования АИС в целом и отдельных ее элементов должна выводиться в виде определенного значения вероятности угрозы, рассчитанной экспертной группой и степени возможного ущерба в случае ее реализации;

– для количественной оценки степени согласованности мнений экспертов необходимо применять коэффициент конкордации, который позволяет оценить, насколько согласованы между собой ряды предпочтительности, построенные каждым экспертом;

– на основании определенного значения вероятности и степени возможного ущерба должен формироваться итоговый отчет об актуальности угрозы и, соответственно, о защищенности изучаемых частей АИС и ее защиты в целом.

Следуя такому подходу к анализу и оценке функционирования АИС и ее системы управления легальными пользователями, можно достоверно идентифицировать и классифицировать угрозы безопасности функционирования АИС по данным о способах реализации угроз и возможных нарушителях, удовлетворяющих требованиям заказчика.

При этом следует учитывать то обстоятельство, что правильно организованный экспертный метод по чувствительности превосходит многие приемы лабораторных исследований. Однако результаты экспертных измерений в определенной степени субъективны и зависят от квалификации экспертов, порядка и условий проведения экспертиз, выбора алгоритмов обработки статистической информации. Очевидно, экспертные методы позволяют избежать характерных ошибок, неизбежных при использовании формальных методов.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурно-функциональных характеристик автоматизированной системы управления легальными пользователями, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

8. Литература

[1] Саати, Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.

[2] Марков, Л.Н. Анализ и процедуры принятия решений. – Мн.: Институт управления и предпринимательства, 2001. – 168 с.

[3] Трахтенгерц, Э.А. Компьютерная поддержка принятия решений. – М.: 1998. – 246 с.

Dynamic model of control of functioning of legal users of information systems

A.V. Kalach[1], A.S. Kravchenko[1], A.A. Zenin[1]

[1]Voronezh Institute of Federal Penitentiary Service of Russia, Irkutskaya street 1a, Voronezh, Russia, 394072

Abstract. Now the trend of growth of number of the computer crimes consisting in plunder of information of limited distribution and, as a result, in significant material losses observed. Therefore, now an important role-played by ensuring information security, information security and objects of informatization. The research is devoted to development of model of audit of computer systems in terms of ensuring their information security. The dynamic model of control of work of legal users (including programmers, administrators) based on the retrospective comparative analysis of the data on their activity fixed in registers and profiles of powers for the benefit of the Federal Penitentiary Service of Russia is created.