(19) Евразийское патентное ведомство

(11) 046630 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2024.03.29

(21) Номер заявки
202091990

(22) Дата подачи заявки
2020.09.18

(51) Int. Cl. ***G06F 16/00*** (2019.01)
G06F 21/00 (2013.01)
G06F 21/45 (2013.01)
G06F 21/50 (2013.01)
G06F 21/54 (2013.01)
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(54) СПОСОБ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И СИСТЕМА ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(31) **2019129630**
(32) **2019.09.20**
(33) **RU**
(43) **2021.05.31**

(71)(73) Заявитель и патентовладелец:
ЁРКИН АНТОН БОРИСОВИЧ (RU)

(72) Изобретатель:
Ёркин Антон Борисович,
Антипинский Андрей Сергеевич,
Богданов Валентин Викторович (RU)

(56) US-A1-20100257576
US-B1-6779120
US-A1-20150358359
Информационная безопасность АСУ ТП: Дон Кихот в эру кибероружия [онлайн]. Хабр 2016-11-26 [найдено 2021-04-23]. Найдено в <https://habr.com/ru/post/316184/>
ПИСАРЕНКО И. Автоматизация процесса управления информационной безопасностью [онлайн периодика] [найдено 2021-04-22]. Найдено в <InformationSecurity, http://information-securitv.ru/articles2/control/avtomatizatsiva-protsessa-upravleniva-informatsionnoy-bezopasnostyu>
ЯНКИН А. Создание автоматизированной системы управления информационной безопасностью [онлайн периодика] [найдено 2021-04-23]. Найдено в <OSP - Гид по технологиям цифровой трансформации, https://www.osp.ru/cio/2011/12/13012284>

(57) Изобретение относится к информационным системам, а именно к системам управления информационной безопасностью. Технический результат заключается в расширении арсенала технических средств, предназначенных для создания автоматизированных систем управления информационной безопасностью. Система создания автоматизированных систем управления информационной безопасности содержит подсистему управления данными, подсистему управления доступом, подсистему управления интеграциями, подсистему управления процессами и подсистему управления визуализацией.

046630 B1

046630 B1

Изобретение относится к автоматизированным системам, а именно к системам управления информационной безопасностью, и может быть использовано для создания автоматизированных систем управления информационной безопасностью.

С ростом организации перед ней возникают все более сложные задачи по обеспечению информационной безопасности. На начальных этапах жизненного цикла, в рамках системы управления информационной безопасностью, достаточно использование стандартных средств защиты информации. С течением времени, затраты на информационную безопасность перестают соответствовать реальному уровню защищенности информационных активов. Рост потребности в последних приводит к необходимости внедрения механизмов управления, анализа и контроля. В связи с этим возникает необходимость в способе разработки системы управления информационной безопасностью, основанной на принципах GRC: Governance (планы, люди, политики), Risk Management (риски информационной безопасности), Compliance (контроль соответствия требованиям).

Известно решение по управления информационной безопасностью, описанное в [ГОСТ Р ИСО/МЭК 27001. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования], заключающееся в непрерывности обеспечения безопасности организации на основе процессного подхода, включающего этапы создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения защиты информации. Однако данный способ ограничивается предоставлением набора организационных мер, регулирующих цикличность процесса управления и устанавливающих правила внедрения и поддержания процессного подхода в области управления информационной безопасностью. В дополнение к вышесказанному стоит отметить, что упомянутое решение не предлагает конкретных реализаций процессного подхода в контексте компьютеризации и автоматизации процессов управления информационной безопасностью, а также их моделирования.

Известны система и способ для интеграции информационной системы организации (заявка на изобретение WO № 2011/115983A1 G06Q 10/00, G06Q 99/00, опубл. 22.09.2011), где блок интеграции может включать одну или несколько корпоративных систем с системой GRC. GRC IM может получить информацию о конфигурации системы из системы предприятия. GRC IM может взаимодействовать с системой GRC с помощью совместимого интерфейса системы GRC, и может обмениваться данными с системой Enterprise с использованием совместимого с интерфейсом Enterprise System, для выполнения анализа в реальном времени, соблюдения профилактических мер безопасности доступа, а также для мониторинга транзакций GRC.

Известен способ адаптивного параметрического управления безопасностью информационных систем и система для его осуществления (заявка на изобретение РФ 2008/148040 G06F 21/00 опубл. 27.11.2008). Способ включает следующие шаги: задание условий безопасности конфигурации, определение общей функции нарушения безопасности, фиксацию воздействия на конфигурацию безопасности системы, фиксацию конфигурации безопасности системы, оценку выполнения условий безопасности конфигурации, определение управляющего воздействия на конфигурацию безопасности системы, адаптацию информационной системы к нарушениям безопасности.

Однако упомянутое выше техническое решение обладает скудным инструментарием для разработки модели процесса управления информационной безопасностью на всех стадиях жизненного цикла такого процесса. Данное техническое решение направлено, в первую очередь, на получение моделей и схем взаимодействия технических средств, эксплуатируемых в рамках системы управления информационной безопасностью. Что касается организационных мер, то данным техническим решением такие меры проигнорированы.

Существуют инструменты моделирования процессов, обеспечивающие графическое воплощение потоков операций, из которых такие процессы состоят. Данные технические решения, в частности, можно использовать для моделирования процессов управления информационной безопасностью с некоторыми ограничениями, указанными ниже.

Известно техническое решение, обеспечивающее интерактивность системы управления жизненным циклом организации (заявка на изобретение WO № 2016/054437, G06Q 40/08, опубл. 07.04.2016), в котором раскрыта интуитивно понятная автоматизированная система моделирования процессов, лежащих в основе обеспечения жизненного цикла организации. Система включает в себя модуль управления соответствием, хранилище профилей рисков для данных, модуль показателей и метрик, и набор моделей, сопряженные с графической панелью инструментов, обеспечивающей централизованное управление.

Общим недостатком для приведенных выше технических решений является их скудный инструментарий в части отслеживания хода выполнения процессов, а также отсутствие надстройки на предметную область. Заявляемое изобретение направлено, в том числе, на устранение указанных выше недостатков, но не ограничивается лишь этим.

Техническая задача заключается в создании способа создания автоматизированных систем управления информационной безопасностью и системы для его осуществления, которые предусматривают автоматизацию деятельности организации по управлению информационной безопасностью в соответствии с законодательными и бизнес-требованиями и с концепцией GRC; организацию совместной работы

различных категорий пользователей, в том числе, представителей высшего руководства организации, сотрудников подразделения ИТ, сотрудников подразделения ИБ и иных сотрудников организации, задействованных при выполнении процессов обработки информации; централизации хранения данных, относящихся к области управления информационной безопасностью, автоматизация сбора таких данных и их представление в графическом, табличном и ином удобном виде.

Технический результат заключается в расширении арсенала технических средств, предназначенных для создания автоматизированных систем управления информационной безопасностью.

В целом термины, используемые в описании, должны быть истолкованы как известные для специалиста в данной области техники. Некоторые термины определены ниже, для того, чтобы обеспечить дополнительную ясность. В случае конфликта между известным значением и представленным определением, должно быть использовано представленное определение.

Под объектом автоматизации понимается организация, деятельность по управлению информационной безопасностью которой нуждается в автоматизации для достижения стратегических целей такой организации и наиболее точного соответствия требованиям регуляторов в области информационной безопасности.

Под системой управлением информационной безопасностью понимается совокупность взаимосвязанных процессов управления информационной безопасностью.

Под прикладным модулем понимается подсистема автоматизированной системы управления информационной безопасности, предназначенная для автоматизации отдельного процесса управления информационной безопасностью. Каждый прикладной модуль содержит следующие компоненты: источники данных: сущности, описанные в виде таблиц базы данных и провайдеров данных, процессы перевода состояния сущности и связанные с состояниями шаблоны задач по обработке состояний, процессы вычисления данных, отчеты, интеграции и формы представления данных. Значение каждого из вышеперечисленных элементов дается в описании.

Под сущностью понимается объект, задействованный в каком-либо процессе управления информационной безопасностью, данные о котором необходимо сохранить. Для каждой сущности определяются атрибуты, уникально ее характеризующие, связи с другими сущностями и тип такой связи.

Под моделью доступа к данным системы управления информационной безопасностью понимается совокупность связей ролей пользователей и прав на обработку данных. Роли пользователя присваивают задачи для обработки состояния сущности. Также для роли пользователя создают рабочую область пользователя.

Под рабочей областью пользователя понимается экземпляр графического пользовательского интерфейса, определенный для роли пользователя.

Под редактором понимается функциональный блок системы создания систем управления информационной безопасностью, предоставляющий пользователю с правами администратора системы возможность создания компонентов прикладных модулей и/или внесения в них изменений в интерактивном режиме с поддержкой графического пользовательского интерфейса.

Поставленная задача решается за счет того, что в способе создания автоматизированных систем управления информационной безопасностью проводят сбор информации об объекте автоматизации и проводят структуризацию такой информации в виде прикладных модулей,

в соответствии с информацией об объекте автоматизации создают модель доступа пользователей к данным, причем в такой модели фиксируют роли пользователей, а для каждой роли фиксируют права на обработку данных, а затем каждому пользователю автоматизированной системы ставят в соответствие роль;

для каждого прикладного модуля создают список источников данных и связанные со списком источники данных, причем источники данных создают в виде таблиц базы данных и в виде провайдеров данных, причем в таблицах базы данных фиксируют сущности, характеризующие объект автоматизации, а для каждой сущности фиксируют атрибуты, связи, тип связи между сущностями и триггеры;

для каждого прикладного модуля создают список интеграций такого модуля с внешними источниками данных и, в случае если список таких интеграций не пуст, создают правила интеграции, в которых проводят сопоставление атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, а также фиксируют периодичность получения данных из внешних источников данных и фиксируют периодичность предоставления данных во внешние источники данных, обеспечивают интеграцию источника данных прикладного модуля с внешним источником данных об объекте автоматизации на основе таких правил;

для каждой сущности создают список процессов перевода состояний, и в случае, если список таких процессов не пуст, создают модели таких процессов и для каждого процесса перевода состояний фиксируют список состояний и фиксируют схему перевода из первоначального состояния в последующее, а для каждого состояния создают шаблон задачи по обработке такого состояния и связывают его с ролью пользователя, ответственной за обработку такого состояния;

для каждого прикладного модуля создают список процессов вычисления данных и, в случае если список таких процессов не пуст, создают алгоритмы процессов вычисления данных, для которых фикси-

руют аргументы процесса на входе алгоритма процесса, и аргументы процесса, значения которых необходимо вычислить на выходе в ходе работы такого алгоритма процесса;

для каждого прикладного модуля создают список форм представления данных, для которых создают элементы графического пользовательского интерфейса, причем такие элементы связывают с атрибутами сущностей и/или с процессами перевода состояний сущности для отображения их текущих значений на экране ЭВМ, а также элементы графического пользовательского интерфейса связывают с процессами вычисления данных для инициирования работы таких процессов при взаимодействия пользователя с формой представления данных;

для каждого прикладного модуля создают список отчетов, а для каждого отчета создают соответствующий ему шаблон;

в соответствии с моделью доступа пользователей к данным для каждой роли пользователя создают рабочую область, с которой связывают список прикладных модулей и формы представления данных, связанные с прикладными модулями.

Поставленная задача решается за счет того, что система создания автоматизированных систем управления информационной безопасностью, содержащая

подсистему управления данными, которая содержит редактор прикладных модулей, редактор источников данных и базу данных;

подсистему управления доступом, которая содержит редактор модели доступа и блок назначения ролей;

подсистему управления интеграциями, которая содержит редактор интеграций, блок получения данных и блок предоставления данных;

подсистему управления процессами, которая содержит редактор процессов перевода состояний сущности и редактор процессов вычисления данных;

подсистему управления визуализацией, которая содержит редактор форм представления данных, редактор отчетов и редактор рабочих областей; причем

подсистема управления данными взаимосвязана с подсистемой управления доступом, подсистемой управления процессами, подсистемой управления интеграциями и подсистемой управления визуализацией, подсистема управления доступом взаимосвязана с подсистемой управления визуализацией, подсистема управления процессами взаимосвязана с подсистемой управления визуализацией, подсистема управления интеграциями взаимосвязана с внешними системами;

редактор прикладных модулей связан с редактором источников данных, который связан с базой данных, редактор модели доступа связан с блоком назначения ролей, редактор интеграций связан с блоком получения данных и с блоком предоставления данных.

Заявленные способ и система промышленно применимы, так как основаны на средствах, широко использующихся в автоматизированных системах управления, при этом последовательность действий способа может быть реализована на основе персонального компьютера с соответствующим программным обеспечением для осуществления предусмотренных функций.

Заявленные способ и система связаны между собой с образованием единого изобретательского замысла, так как предназначены для получения моделей систем, причем выполнение операций из способа моделирования невозможно наиболее эффективным образом в отрыве от компонентов и модулей системы моделирования.

Заявляемое изобретение иллюстрируется следующими чертежами, где:

на фиг. 1 изображена блок-схема реализации способа создания автоматизированных систем управления информационной безопасностью;

на фиг. 2 изображена схема системы создания автоматизированных систем управления информационной безопасностью.

Способ создания автоматизированных систем управления информационной безопасностью реализуют приведенным ниже образом.

Проводят сбор информации об объекте автоматизации (1) и проводят структуризацию такой информации в виде прикладных модулей (2).

Сбор информации об объекте автоматизации проводят с целью выявления процессов управления информационной безопасностью и лиц, задействованных в таких процессах. Каждый прикладной модуль предназначен для автоматизации отдельного процесса управления информационной безопасностью на объекте автоматизации. Например, проводят структуризацию информации о процессе учета и классификации ИТ-активов в виде модуля учета и классификации ИТ-активов, и, аналогично, проводят структуризацию информации о процессе управлении рисками ИБ в виде модуля управления рисками ИБ.

В соответствии с информацией об объекте автоматизации создают модель доступа пользователей к данным (3), причем в такой модели фиксируют роли пользователей, а для каждой роли фиксируют права на обработку данных, а затем каждому пользователю автоматизированной системы назначают роль;

Например, могут быть созданы следующие роли: "начальник отдела", "инженер", "менеджер качества".

Затем для каждого прикладного модуля создают список источников данных (4) и связанные со спи-

ском источники данных, причем источники данных создают в виде таблиц базы данных и в виде провайдеров данных, причем в таблицах базы данных фиксируют сущности, характеризующие объект автоматизации, а для каждой сущности фиксируют атрибуты, связи, тип связи между сущностями и триггеры.

Для каждого прикладного модуля создают схему базы данных на основе принципа "сущность - связь", то есть определяют сущности, данные о которых необходимо сохранить для их последующей обработки в рамках прикладного модуля, а затем определяют характеризующие их атрибуты, связи с другими сущностями, тип такой связи и триггеры. Таким образом, для сущности создают ее описание в виде таблицы базы данных. Сущности могут входить в состав различных источников данных.

Например, сущность "проект" может быть охарактеризована следующими атрибутами: "договор", "дата начала", "дата окончания", "номер", "заказчик".

Провайдер данных представляет собой запрос к базе данных, предназначенный для формирования сложных выборок и агрегирования данных из нескольких связанных таблиц базы данных.

Для каждого прикладного модуля создают список интеграций такого модуля с внешними источниками данных (5) и, в случае если список таких интеграций не пуст, создают правила интеграции, в которых проводят сопоставление атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, а также фиксируют периодичность получения данных из внешних источников данных и фиксируют периодичность предоставления данных во внешние источники данных, обеспечивают интеграцию источника данных прикладного модуля с внешним источником данных об объекте автоматизации на основе таких правил.

Для каждой сущности создают список процессов перевода состояний сущности (6), и в случае, если список таких процессов не пуст, создают модели таких процессов, и для каждого процесса перевода состояний фиксируют список состояний и фиксируют схему перевода из первоначального состояния в последующее, а для каждого состояния создают шаблон задачи по обработке такого состояния и связывают его с ролью пользователя, ответственной за обработку такого состояния.

Например, в прикладном модуле "модуль работы с персоналом и третьими сторонами" для сущности "работник" могут быть созданы следующие процессы перевода состояний: "начало перевода работника", "начало увольнения работника", "проверка для закрытия испытательного срока".

В качестве другого примера рассмотрим процесса перевода состояний сущности "документ организации". Список его состояний может быть следующим: а - "разработка", б - "рабочее согласование", в - "рабочее утверждение", г - "корректировка", д -"использование", е - "оценка актуальности", ж - "отмена", з - "архив". Схема перевода состояний может быть следующей: из "а" в "б", затем из "б" в "в" или в "г", из "г" в "б" или "д" или в "е", из "е" в "ж", из "ж" в "з", из "в" в "д", из "д" в "ж".

При переводе сущности в определенное ее состояние пользователю автоматически присваивается задача на обработку такого состояния.

Для каждого прикладного модуля создают список процессов вычисления данных (7) и, в случае если список таких процессов не пуст, создают алгоритмы процессов вычисления данных, для которых фиксируют аргументы процесса на входе алгоритма процесса, и аргументы процесса, значения которых необходимо вычислить на выходе в ходе работы такого алгоритма процесса.

Для каждого алгоритма процесса определяют его аргументы и составные элементы, которыми могут являться, например, условия, циклы, формулы, математические и статистические функции, вызовы другого процесса. Аргументам процесса присваивают тип данных. В качестве аргумента процесса может быть использовано значение атрибута сущности, и в таком случае, типом данных может быть число, строка, дата, булево значение и иной тип данных. Также для процессов вычисления данных могут быть определены специальные типы аргументов, например, прикладной модуль, источник данных, пользователь, роль и иные составляющие автоматизированной системы управления информационной безопасностью.

Например, внешними источниками данных могут быть базы данных внешних информационных систем, базы данных Web-сервисов, данные в форматах XML или Microsoft Excel, электронная почта.

Для каждого прикладного модуля создают список форм представления данных (8), для которых создают элементы графического пользовательского интерфейса, причем такие элементы связывают с атрибутами сущностей и/или с процессом переключения состояний сущности для отображения их значений на экране ЭВМ, а также элементы графического пользовательского интерфейса связывают с процессами вычисления данных для инициирования работы таких процессов при взаимодействия пользователя с формой представления данных.

Например, для прикладного модуля "Модуль работы с персоналом и третьими сторонами" могут быть созданы следующие формы представления данных: "Создание расписания", предназначенная для создания записи в расписании для реализации плана обучения; "Третьи стороны", предназначенная для просмотра списка третьих сторон; "Управление работником", предназначенная для управления этапами жизненного цикла работника.

В качестве элементов графического пользовательского интерфейса могут быть использованы элементы "панель", "вкладка", "вложенная форма", "вертикальный разделитель", "таблица", "флажок", "изображение", "связь".

Для каждого прикладного модуля создают список отчетов (9), а для каждого отчета создают соответствующий ему шаблон.

Например, для прикладного модуля "управление рисками информационной безопасности" могут быть созданы следующие шаблоны отчетов: "приказ об оценке рисков", "план работ по оценке рисков", "акт оценки рисков". Шаблоны отчетов могут быть использованы для автоматического формирования отчетов, содержащих данные, хранение которых организовано в источниках данных прикладных модулей.

В соответствии с моделью доступа пользователей к данным для каждой роли пользователя создают рабочую область (10), с которой связывают прикладные модули и формы представления данных, связанные с прикладными модулями.

Например, могут быть созданы следующие рабочие области для ролей пользователей: "рабочая область инженера", "рабочая область эксперта по рискам", "рабочая область начальника".

Система создания автоматизированных систем управления информационной безопасностью содержит:

подсистему управления данными (11), которая содержит редактор прикладных модулей (12), редактор источников данных (13) и базу данных (14);

подсистему управления доступом (15), которая содержит редактор модели доступа (16) и блок назначения ролей пользователям (17);

подсистему управления интеграциями (18), которая содержит редактор интеграций (19), блок получения данных (20) и блок предоставления данных (21);

подсистему управления процессами (22), которая содержит редактор процессов перевода состояний сущности (23) и редактор процессов вычисления данных (24);

подсистему управления визуализацией (25), которая содержит редактор форм представления данных (26), редактор шаблонов отчетов (27) и редактор рабочих областей (28); причем

подсистема управления данными (11) взаимосвязана с подсистемой управления доступом (15), подсистемой управления интеграциями (18), подсистемой управления процессами (22) и подсистемой управления визуализацией (25), подсистема управления доступом (15) взаимосвязана с подсистемой управления визуализацией (25), подсистема управления процессами (22) взаимосвязана с подсистемой управления визуализацией (25), подсистема управления интеграциями (18) взаимосвязана с внешними системами (29).

редактор прикладных модулей (12) связан с редактором источников данных (13), который связан с базой данных (14), редактор модели доступа (16) связан с блоком назначения ролей пользователям (17), редактор интеграций (19) связан с блоком получения данных (20) и с блоком предоставления данных (21).

Редактор прикладных модулей (12) предназначен для создания прикладных модулей и создания списков компонентов таких модулей. Редактор источников данных (13) предназначен для создания источников данных в виде таблиц базы данных, фиксации в них сущностей, характеризующих объект автоматизации, фиксации атрибутов сущностей, связи, типа связи между сущностями и триггеров; и в виде провайдеров данных. База данных (14) предназначена для хранения структурированной в виде прикладных модулей информации об объекте автоматизации.

Редактор модели доступа (16) предназначен для создания модели доступа, фиксации в ней ролей пользователей и фиксации для ролей прав доступа к данным. Блок назначения ролей пользователям (17) предназначен для назначения ролей пользователям автоматизированной системы управления информационной безопасностью.

Редактор интеграций (19) предназначен для создания правил интеграции путем сопоставления атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, и путем фиксации периодичности получения данных из внешних источников данных и периодичности предоставления данных во внешние источники данных. Блок получения данных (20) предназначен для обеспечения интеграции источников данных прикладного модуля с источниками данных внешних информационных систем в части получения данных. Блок предоставления данных (21) предназначен для обеспечения интеграции источников данных прикладного модуля с источниками данных внешних информационных систем в части предоставления данных.

Редактор процессов перевода состояний сущности (23) предназначен для фиксации списка состояний сущности и, в случае если такой список состояний не пуст, фиксации схемы перевода состояний сущности из первоначального состояния в последующее, а также для создания шаблона задачи по обработки такого состояния и связывания его с ролью пользователя, ответственного за обработку такого состояния. Редактор процессов вычисления данных (24) предназначен для создания алгоритмов процессов вычисления данных и фиксации аргументов процесса на входе алгоритма процесса и аргументов процесса, значения которых необходимо вычислить на выходе в ходе работы такого алгоритма процесса.

Редактор форм представления данных (26) предназначен для создания форм представления данных и элементов графического пользовательского интерфейса для форм представления данных, а также для

связывания форм представления данных с прикладными модулями, для связывания элементов графического пользовательского интерфейса с атрибутами сущностей и/или с процессами перевода состояний сущности для отображения их текущих значений на экране ЭВМ, и для связывания элементов графического пользовательского интерфейса с процессами вычисления данных для инициирования работы таких процессов при взаимодействии пользователя с формой представления данных. Редактор шаблонов отчетов (27) предназначен для создания шаблонов отчетов для автоматического формирования отчетов, включающих значения атрибутов сущностей. Редактор рабочих областей (28) пользователя предназначен для создания рабочей области для каждой роли пользователя и связывания с ней прикладных модулей и форм представления данных, связанных с прикладным модулем.

Система создания автоматизированных систем управления информационной безопасностью используется следующим образом.

Специалист в области информационной безопасности организации, не обладающий специализированными знаниями в области программирования, предпочтительно, бизнес-аналитик (далее - бизнес-аналитик), проводит сбор информации об объекте автоматизации и проводит ее структуризацию в виде прикладных модулей в подсистеме управления данными (11). Для этого бизнес-аналитик создает списки компонентов для каждого прикладного модуля в редакторе прикладных модулей (12), а именно: список источников данных, список процессов вычисления данных, список интеграций, список отчетов, список форм представления данных.

Для каждого прикладного модуля бизнес-аналитик создает источники данных в виде таблиц базы данных и провайдеров данных в редакторе источников данных (13), причем в таблицах базы данных фиксирует сущности, характеризующие объект автоматизации, и атрибуты таких сущностей, связи, тип связи между сущностями и триггеры.

В соответствии с информацией об объекте автоматизации бизнес-аналитик создает модель доступа к данным в подсистеме управления доступом (15), для которой в редакторе модели доступа (16) фиксирует роли пользователей и права доступа к данным для таких ролей, после чего назначает пользователям автоматизированной системы управления информационной безопасности соответствующие роли в блоке назначения ролей пользователям (17).

Для каждого прикладного модуля бизнес-аналитик создает интеграции с внешними источниками данных, связанные со списком интеграций, созданного для прикладного модуля, в подсистеме управления интеграциями (18). Бизнес-аналитик создает правила интеграции, в которых проводит сопоставление атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, в редакторе интеграций (19), а также фиксирует периодичность получения данных из внешних источников данных (29) в блоке получения данных (20) и фиксирует периодичность предоставления данных во внешние источники данных (29) в блоке предоставления данных (21).

Для каждой сущности бизнес-аналитик фиксирует список процессов перевода состояний сущности в редакторе процессов перевода состояний сущности (23) и, в случае если такой список не пуст, создает модели таких процессов, для которых затем фиксирует список состояний сущности и схему перевода из первоначального состояния в последующее. Для каждого состояния создает шаблон задачи по обработке такого состояния и связывает его с ролью пользователя, ответственной за обработку такого состояния.

Для каждого прикладного модуля бизнес-аналитик создает алгоритмы процессов вычисления данных, связанные со списком таких процессов, созданного для прикладного модуля, в редакторе процессов вычисления данных (24). Для таких алгоритмов он фиксирует аргументы процесса на входе алгоритма и аргументы процесса, значение которых необходимо вычислить на выходе в ходе работы такого алгоритма.

Для каждого прикладного модуля бизнес-аналитик создает формы представления данных, связанные со списком форм представления данных, созданного для прикладного модуля, в редакторе форм представления данных (26). Затем создает элементы графического пользовательского интерфейса и связывает их с атрибутами сущностей и/или с процессом перевода состояний сущности для отображения их значений на экране ЭВМ, а также связывает элементы графического пользовательского интерфейса с процессами вычисления данных для инициирования работы таких процессов при взаимодействия пользователя с формой представления данных, в редакторе форм представления данных (26).

Для каждого прикладного модуля бизнес-аналитик создает шаблоны отчетов, связанных со списком отчетов, созданных для прикладного модуля, в редакторе шаблонов отчетов (27).

В соответствии с моделью доступа пользователей к данным бизнес-аналитик создает рабочую область для каждой роли пользователя, с которой связывают прикладные модули и формы представления данных, связанные с прикладными модулями, в редакторе рабочих областей (28).

Заявленные способ создания автоматизированных систем управления информационной безопасностью и система для его осуществления позволяют решать следующие задачи:

автоматизация деятельности организации по управлению информационной безопасностью в соответствии с законодательными и бизнес-требованиями и с концепцией GRC;

организация совместной работы различных категорий пользователей, например, представителей

высшего руководства организации, сотрудников подразделения ИТ, сотрудников подразделения ИБ и иных сотрудников организации, задействованных при выполнении процессов обработки информации;

централизация хранения данных, относящихся к области управления информационной безопасностью, автоматизация сбора таких данных и их представление в графическом, табличном и ином удобном виде.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ создания автоматизированных систем управления информационной безопасностью объекта автоматизации, при этом в способе проводят сбор информации об объекте автоматизации и проводят структуризацию такой информации в виде прикладных модулей с помощью редактора прикладных модулей, причем сбор информации об объекте автоматизации включает выявление процессов управления информационной безопасностью и лиц, задействованных в таких процессах, а объектом автоматизации является организация, деятельность по управлению информационной безопасностью которой нуждается в автоматизации;

в соответствии с информацией об объекте автоматизации создают модель доступа пользователей к данным с помощью редактора модели доступа, причем в такой модели фиксируют роли пользователей, а для каждой роли фиксируют права на обработку данных с помощью блока назначения ролей, а затем каждому пользователю автоматизированной системы ставят в соответствие роль;

для каждого прикладного модуля создают список источников данных о и связанные со списком источники данных с помощью редактора источников данных, причем источники данных создают в виде таблиц базы данных и в виде провайдеров данных, причем в таблицах базы данных фиксируют сущности, характеризующие объект автоматизации, а для каждой сущности фиксируют атрибуты, связи, тип связи между сущностями и триггеры;

для каждого прикладного модуля создают список интеграций такого модуля с внешними источниками данных с помощью редактора интеграций и, в случае, если список таких интеграций не пуст, создают правила интеграции, в которых проводят сопоставление атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, а также фиксируют периодичность получения данных из внешних источников данных и фиксируют периодичность предоставления данных во внешние источники данных, обеспечивают интеграцию источника данных прикладного модуля с внешним источником данных об объекте автоматизации на основе таких правил;

для каждой сущности создают список процессов перевода состояний с помощью редактора процессов перевода состояний сущности, и в случае, если список таких процессов не пуст, создают модели таких процессов и для каждого процесса перевода состояний фиксируют список состояний и фиксируют схему перевода из первоначального состояния в последующее, а для каждого состояния создают шаблон задачи по обработке такого состояния и связывают его с ролью пользователя, ответственной за обработку такого состояния;

для каждого прикладного модуля создают список процессов вычисления данных с помощью редактора процессов вычисления данных и, в случае, если список таких процессов не пуст, создают алгоритмы процессов вычисления данных, для которых фиксируют аргументы процесса на входе алгоритма процесса, и аргументы процесса, значения которых необходимо вычислить на выходе в ходе работы такого алгоритма процесса;

для каждого прикладного модуля создают список форм представления данных с помощью редактора форм представления данных, для которых создают элементы графического пользовательского интерфейса, причем такие элементы связывают с атрибутами сущностей и/или с процессами перевода состояний сущности для отображения их текущих значений на экране ЭВМ, а также элементы графического пользовательского интерфейса связывают с процессами вычисления данных для инициирования работы таких процессов при взаимодействии пользователя с формой представления данных;

для каждого прикладного модуля создают список отчетов, а для каждого отчета создают соответствующий ему шаблон с помощью редактора шаблонов отчетов;

в соответствии с моделью доступа пользователей к данным и с помощью редактора рабочих областей для каждой роли пользователя создают рабочую область, с которой связывают список прикладных модулей и формы представления данных, связанные с прикладными модулями, таким образом, чтобы предоставить пользователю с соответствующей ролью доступ к данным прикладных модулей через созданные для таких модулей формы представления данных.

2. Система создания автоматизированных систем управления информационной безопасностью объекта автоматизации, в которой объект автоматизации является организацией, деятельность по управлению информационной безопасностью которой нуждается в автоматизации, при этом система содержит:

подсистему управления данными, позволяющую проводить сбор информации об объекте автоматизации, включая выявление процессов управления информационной безопасностью и лиц, задействованных в таких процессах, при этом подсистема управления данными содержит редактор прикладных моду-

лей, предназначенный для создания прикладных модулей и создания списков компонентов таких модулей, редактор источников данных, предназначенный для создания источников данных в виде таблиц базы данных, фиксации в них сущностей, характеризующих объект автоматизации, фиксации атрибутов сущностей, связи, типа связи между сущностями и триггеров, и базу данных;

подсистему управления доступом, которая содержит редактор модели доступа, предназначенный для создания модели доступа, фиксации в ней ролей пользователей и фиксации для ролей прав доступа к данным, и блок назначения ролей, предназначенный для назначения ролей пользователям;

подсистему управления интеграциями, которая содержит редактор интеграций, предназначенный для создания правил интеграции путем сопоставления атрибутов сущностей источника данных прикладного модуля и атрибутов соответствующих сущностей, данные о которых хранятся во внешних источниках данных, и путем фиксации периодичности получения данных из внешних источников данных и периодичности предоставления данных во внешние источники данных, блок получения данных, предназначенный для обеспечения интеграции источников данных прикладного модуля с источниками данных внешних информационных систем в части получения данных, и блок предоставления данных, предназначенный для обеспечения интеграции источников данных прикладного модуля с источниками данных внешних информационных систем в части предоставления данных;

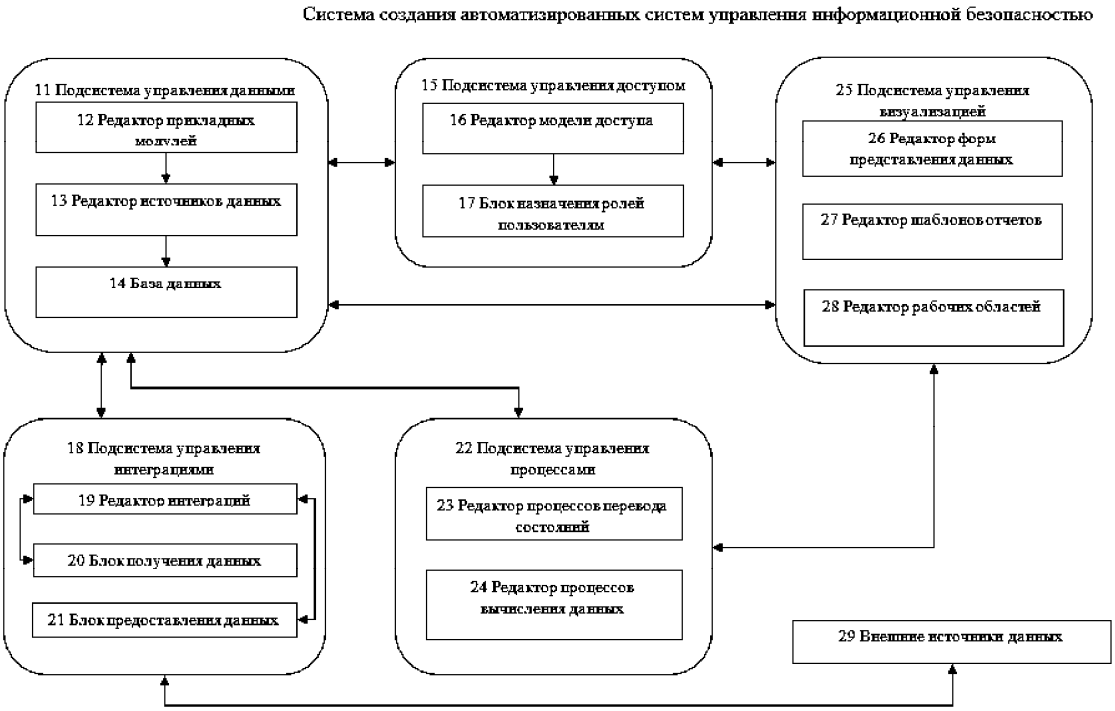
подсистему управления процессами, которая содержит редактор процессов перевода состояний сущности, предназначенный для фиксации списка состояний сущности и, в случае, если такой список состояний не пуст, фиксации схемы перевода состояний сущности из первоначального состояния в последующее, а также для создания шаблона задачи по обработке такого состояния и связывания его с ролью пользователя, ответственного за обработку такого состояния, и редактор процессов вычисления данных, предназначенный для создания алгоритмов процессов вычисления данных и фиксации аргументов процесса на входе алгоритма процесса и аргументов процесса, значения которых необходимо вычислить на выходе в ходе работы такого алгоритма процесса;

подсистему управления визуализацией, которая содержит редактор форм представления данных, предназначенный для создания форм представления данных и элементов графического пользовательского интерфейса для форм представления данных, а также для связывания форм представления данных с прикладными модулями, для связывания элементов графического пользовательского интерфейса с атрибутами сущностей и/или с процессами перевода состояний сущности для отображения их текущих значений на экране ЭВМ, и для связывания элементов графического пользовательского интерфейса с процессами вычисления данных для инициирования работы таких процессов при взаимодействии пользователя с формой представления данных редактор шаблонов отчетов, и редактор рабочих областей, предназначенный для создания рабочей области для каждой роли пользователя и связывания с ней прикладных модулей и форм представления данных, связанных с прикладным модулем, и позволяющий создавать рабочие области таким образом, чтобы предоставить пользователю с соответствующей ролью доступ к данным прикладных модулей через созданные для таких модулей формы представления данных;

при этом подсистема управления данными взаимосвязана с подсистемой управления доступом, подсистемой управления процессами, подсистемой управления интеграциями и подсистемой управления визуализацией, подсистема управления доступом взаимосвязана с подсистемой управления визуализацией, подсистема управления процессами взаимосвязана с подсистемой управления визуализацией, подсистема управления интеграциями взаимосвязана с внешними системами; редактор прикладных модулей связан с редактором источников данных, который связан с базой данных, редактор модели доступа связан с блоком назначения ролей, редактор интеграций связан с блоком получения данных и с блоком предоставления данных.


1
Сбор данных об объекте автоматизации
2
Создание прикладных модулей
3
Создание модели доступа к данным
4
Создание источников данных
5
Создание интеграций с внешними источниками данных
6
Создание процессов перевода состояний сущности
7
Создание процессов вычисления данных
8
Создание форм представления данных
9
Создание шаблонов отчетов
10
Создание рабочих областей для роли пользователя

Фиг. 1



Фиг. 2

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2