OSTIS-2016
(Open Semantic Technologies for Intelligent Systems)

УДК 004.822:514

КОНЦЕПЦИЯ ИНСТРУМЕНТАЛЬНОГО КОМПЛЕКСА ДЛЯ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Грибова В.В., Иванова А.В.

Институт автоматики и процессов управления
Дальневосточного отделения Российской Академии наук,
г. Владивосток, Россия

gribova@iacp.dvo.ru, 2395146@gmail.com

В статье рассмотрены существующие подходы к построению комплексных систем защиты информации (СЗИ) и их недостатки. Сформированы принципы создания и концепция инструментария, обеспечивающего администратора платформы единой средой для управления разнородными СЗИ, а также рекомендациями по их выбору и настройке в соответствии с конфигурацией и особенностями конкретной информационной системы.
Ключевые слова: онтологии, информационные ресурсы, защита информации, безопасность информационных систем.

Введение

Обеспечение безопасности информационных систем (ИС) является одной из ключевых проблем в области информационных технологий. Здесь и далее под информационной системой будет пониматься любая информационная система, вне зависимости от типа платформы (локально-вычислительная сеть, автоматизированное рабочее место, распределенная платформа и т.д.). В настоящее время можно выделить два основных подхода к защите информации в ИС.

Первый подход заключается в использовании единого комплексного средства защиты, которое сочетает в себе функции каждого из отдельных узконаправленных компонентов. Такое решение обладает централизованным интерфейсом, что упрощает управление для администратора безопасности [Код Безопасности, 2015]. Второй, и наиболее популярный, подход заключается в использовании комплекса средств защиты информации (СЗИ) [ФСТЭК, 2014]. Отдельные компоненты специфичны, узконаправленны и предназначены для нейтрализации сходных угроз и могут быть разделены по типам: антивирусные средства, средства защиты от несанкционированного доступа, межсетевые экраны, криптографические средства защиты информации, системы обнаружения вторжений и др.

Однако оба подхода обладают рядом недостатков [PCMagazine, 2007]. В первом случае это:

- отсутствие совместимости с другими СЗИ;
- высокая стоимость конечного решения;
- невозможность отключения и последующей замены отдельных элементов на решения от другого разработчика (к примеру, отключение антивируса из комплекса и установка другого более репутационного антивируса или имеющего сертификат на класс выше);
- в случае невозможности эксплуатации (окончание срока действия сертификата, компрометация лицензионного ключа, сбой процедуры обновления и т.д.) нарушается работоспособность всех подсистем системы защиты информации.

Во втором случае это:

- отсутствие единого интерфейса управления;
- отсутствие механизмов оперативного контроля (необходимо напрямую вмешиваться в настройки СЗИ);
- проблемы совместимости СЗИ между собой (после установки одного СЗИ, другое может перестать функционировать, либо обнаруживаются конфликты совместного использования).

Кроме рассмотренных выше аспектов перед администратором безопасности возникает ряд новых проблем. Задача обеспечить информационную безопасность системы требует от него ряда специальных знаний и навыков для определения требований к системе, в том числе законодательных, выбора способов и средств защиты, их последующей настройки, поддержанию

непрерывного функционирования системы, разрешению конфликтных ситуаций, изучения возможностей улучшения системы и повышения ее эффективности [M. Rhodes-Ousley, 2014].

Подход к обеспечению защиты информационных систем с использованием комплекса СЗИ является наиболее популярным методом и используется в большинстве информационных систем. Исходя из вышесказанного, актуальным является создание инструментария, обеспечивающего администратора платформы единой средой для выбора и управления разнородными СЗИ, а также рекомендациями по их выбору и настройке в соответствии с конфигурацией и особенностями конкретной информационной системы. Такое решение обеспечит высокую эффективность технологий выявления, предупреждения и предотвращения атак и выполнение законодательных требований. Целью данной работы является описание общих принципов и концепции, обеспечивающих такую среду управления безопасностью.

1. Принципы построения инструментария

На основе анализа литературы, опыта работы в профилированной компании, приобретенных практических навыков, с учетом условий современной стадии развития технологий защиты информации, преимуществ и недостатков подхода, основанного на использовании набора разнопрофильных узконаправленных СЗИ, можно выделить основные принципы построения инструментального комплекса для организации безопасности информационных систем:

1. Наличие единого интерфейса для управления разнородными СЗИ. Такой подход обеспечит администратора ИС средствами оперативного управления набором разнородных СЗИ без необходимости настройки последовательно каждого СЗИ. Единый интерфейс является необходимым условием централизованного сбора и систематизации сведений о текущем состоянии и конфигурации, полученных от различных средств защиты.

2. Инструментальный комплекс для управления безопасностью ИС должен поддерживать функцию выбора СЗИ. Выбор средств защиты информации в соответствии с конкретной конфигурацией ИС и требованиями к уровню ее защиты, настройка каждого средства, являются достаточно сложной задачей для любого администратора и часто требуют приглашения сторонних специалистов, как правило, из профилированных компаний, которые осуществляют функции консультирования, настройки системы безопасности, а также сопровождение ее в процессе эксплуатации. Однако такое решение является дорогостоящим, не всегда обеспечивает необходимый уровень эффективности и не позволяет оперативно решать конфликтные ситуации в случае их возникновения.

3. Наличие единого централизованного инструмента, обеспечивающего поддержку в актуальном состоянии информации, необходимой для принятия управленческих решений в конкретной ИС. Очевидно, что выбор набора СЗИ, их настройка в соответствии с требованиями безопасности для ИС требуют специальных знаний и навыков в области защиты компьютерных систем. Более того, это знания стремительно развиваются и изменяются. Соответственно, при их реализации в компьютерных системах необходимо учитывать эти аспекты. Во-первых, информация должна быть доступна и понятна экспертам в области информационной безопасности для анализа, исправления ошибок и неточностей, а также дальнейшего развития в связи с изменениями в предметной области. Во-вторых, необходимо создать централизованную "среду", аккумулирующую информацию о безопасности систем в едином информационном пространстве для того, чтобы обеспечить ее накопление, совместное развитие и использование для исключения "повторной разработки готовых решений". В-третьих, наличие централизованного хранилища, поддерживающего актуальность и постоянное обновление информации, позволит минимизировать человеческие ресурсы в существующих условиях кризиса высококвалифицированных специалистов в области информационной безопасности и позволит заметно сократить расходы на сопровождение комплекса средств защиты.

Для осуществления принципов предлагается:

Реализовать единую среду для хранения информационных ресурсов в области компьютерной безопасности и управления ими всем заинтересованным сообществом. Для обеспечения широкой доступности этих ресурсов, разместить их в "облаке", а также предоставить набор облачных сервисов (редакторов) для создания и управления информационными ресурсами в процессе жизненного цикла.

2. Концептуальная архитектура программного комплекса

Концептуальная архитектура инструментального комплекса для управления безопасностью ИС представлена на рисунке 1. Инструментальный комплекс состоит из: среды управления информационными ресурсами (на рисунке в верхнем блоке) и множества клиентских сред управления безопасностью информационной системы.

Среда управления информационными ресурсами состоит из интерфейса, структурного редактора онтологий, редактора информационных ресурсов, а также непосредственно информационных ресурсов и «Модуля выбора средств защиты».

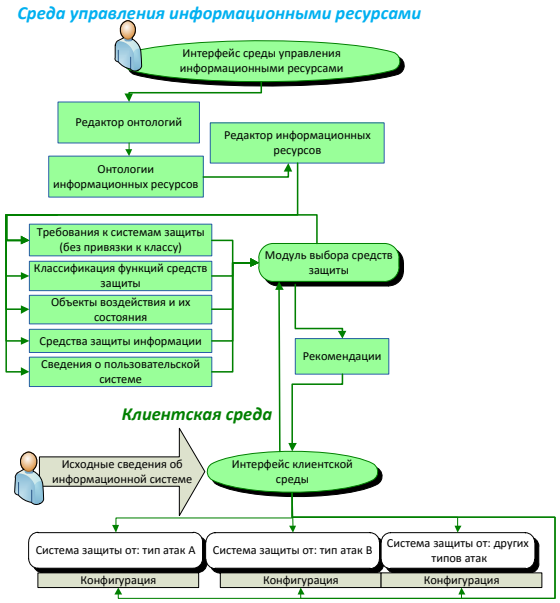

Рисунок 1 – Концептуальная архитектура инструментального комплекса для управления безопасностью информационных систем

Структурные редакторы предназначены для централизованного формирования и сопровождения (поддержки в актуальном состоянии) экспертами предметной области информации, которая используется в клиентских системах для помощи администратору в выборе и настройке СЗИ. Информационными ресурсами являются: «Требования к системам защиты (без привязки к классу)», «Классификация функций средств защиты», «Объекты воздействия и их состояния», «Средства защиты информации», «Сведения о пользовательской системе». Подробное описание информационных ресурсов дано в разделе **«Информационные ресурсы»**.

В качестве средства реализации среды управления информационными ресурсами предлагается платформа IACPaaS [Грибова В.В., и др. 2011]. Она представляет собой программно-информационный интернет-комплекс для обеспечения поддержки разработки, управления и удаленного использования прикладных и инструментальных (системных) мультиагентных облачных сервисов (прежде всего интеллектуальных) и их компонентов. Комплекс основан на технологии облачных вычислений и обеспечивает удаленный доступ конечным пользователям к интеллектуальным системам, а разработчикам и управляющим – к средствам создания интеллектуальных систем и управления ими. В состав платформы входит универсальный двухуровневый редактор для формирования данных и знаний. Он предназначен для описания метаинформации - онтологии информационного ресурса (первый уровень), по которой затем автоматически генерируется специализированный интерфейс для эксперта (второй уровень). Наличие универсального редактора, во-первых, не требует разработки специализированных редакторов для необходимых информационных ресурсов, во-вторых, позволяет экспертам предметной области без инженеров знаний формировать и модифицировать информационные ресурсы в терминах онтологии. Таким образом, использование платформы IACPaaS обеспечивает всю необходимую инфраструктуру для хранения и наполнения фонда информационных ресурсов.

Клиентская среда управления безопасностью информационной системы включает в себя Интерфейс управления клиентской среды, который выступает основным инструментом для взаимодействия Администратора ИС с различными СЗИ, а также Модулем выбора средств защиты. Через интерфейс клиентской среды Администратор получает сведения о состоянии подконтрольных СЗИ, определяет требования к клиентской ИС, ознакомление с информацией о минимальном наборе требуемых функций и СЗИ, реализующих их выполнение.

Рекомендации по настройке, выявление требований к набору средств защиты предусматривают централизованное управление и уведомления через Интерфейс управления клиентской среды. Функционирование этого блока основано на принципах кроссплатформенности, взаимозаменяемости компонентов выстроенной системы защиты, адаптации к таким изменениям,

«Модуль выбора средств защиты» предназначен для определения набора требований на основании входных параметрах клиентской ИС. Данный модуль также предусматривает определение набора средств защиты в случае, если в клиентской ИС уже функционируют средства защиты, которые удовлетворяют предъявленным требованиям и могли бы быть использованы.

Разрабатываемый инструментальный комплекс предусматривает определение требований к системе, определение набора допустимых средств защиты и выдачу рекомендаций по настройке конкретных программных модулей СЗИ.

3. Информационные ресурсы

Основными информационными ресурсами (ИР) являются :

1) «Сведения о пользовательской системе» содержит информацию об определяющих характеристиках клиентской информационной системы. Позволяет пользователю, описать конфигурацию о конкретной ИС в формализованном виде для дальнейшего использования. При наличии в клиентской системе предустановленных (закупленных) СЗИ, может ссылаться на ИР «Средства защиты информации» для учета этой информации и исключения избыточности рекомендаций. Фрагмент ИР изображен на рисунке 2. Взаимодействие ИР между собой будет рассмотрено ниже.

В примере указано три возможных варианта обрабатываемой информации и их цифровое обозначение: «1.1. Персональные данные», «1.2. Конфиденциальная информация», «1.3. Для служебного пользования». Также имеются поля, которые могут быть заполнены пользователем без предложенных вариантов: «Количество рабочих мест» - любая целочисленная количественная характеристика.

2) «Требования к системе защиты (без привязки к классу)» включает в себя перечень законодательных и пользовательских требований к защите информационной системы. Используется при определении требуемого к реализации набора функций защиты клиентской системы на основе конфигурации информационной системы.

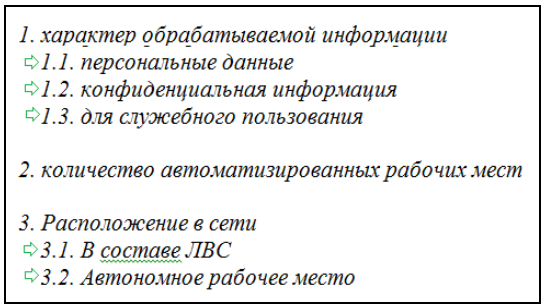

Рисунок 2 – Фрагмент ИР «Сведения о пользовательской системе»

3) «Классификация функций средств защиты», изображена на Рис. 3, представляет собой многоуровневую структуру и включает в себя классификацию функций СЗИ, определяемых нормативными документами [ФСТЭК, 2015], а также ряд дополнительных функций, которые разработчики встраивают в программное обеспечение и декларируют в «Руководствах по эксплуатации» своих программных продуктов. На рисунке 4 различными маркерами (треугольники справа) обозначены функции средств защиты. Каждое средство защиты закодировано своим маркером. Если указанная функция имеется в средстве защиты, то напротив нее проставляется соответствующий ему маркер.

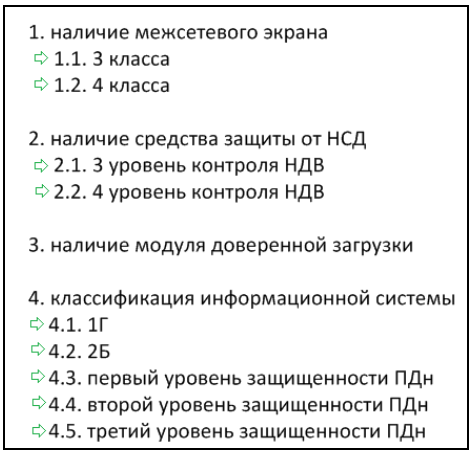

Рисунок 3 – Фрагмент ИР «Требования к системам защиты (без привязки к классу)»

Такое обозначение позволяет определить полный набор функций средства защиты, их иерархию, а также определить, являются они основными в средстве защиты или дополнительными, основываясь на глубине классификационного «дерева» конкретной функции.

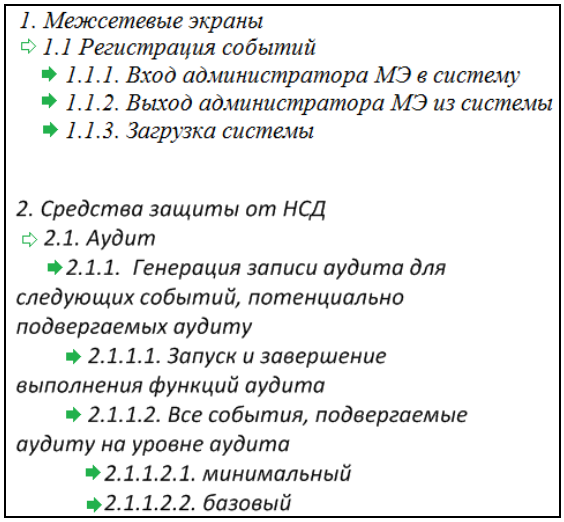

Рисунок 5 – Фрагмент ИР «Классификация функций средств защиты»

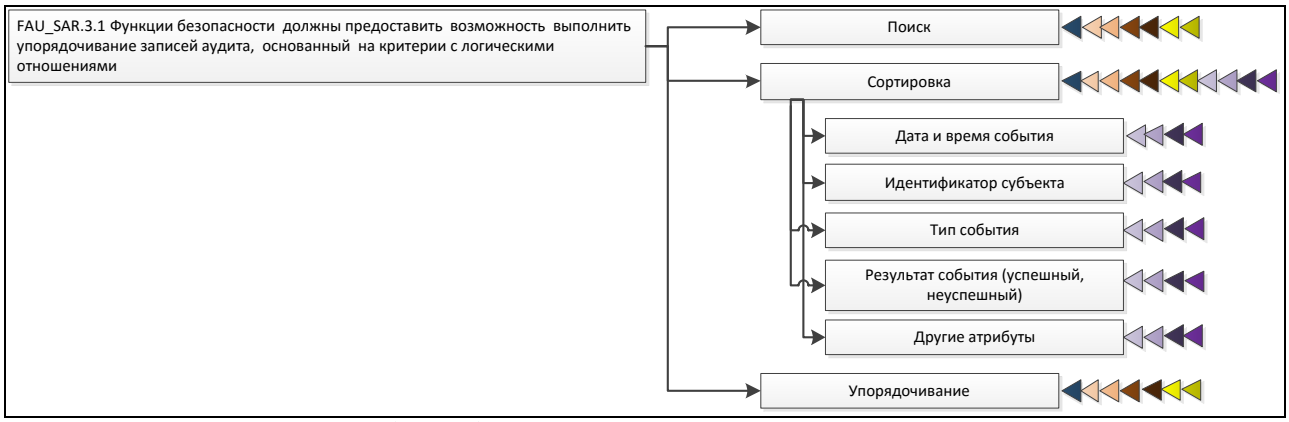

Рисунок 4 – Иерархическая классификация функций средств защиты в соответствии с нормативно-законодательными актами

ИР «Классификация функций средств защиты» содержит сводную информацию о всех функциях средств защиты без привязки к конкретному профилю (типу СЗИ). Фрагмент базы данных изображен на рисунке 5.

В качестве примера рассмотрена одна из функций межсетевых экранов: «1.1. Регистрация событий», а также возможные события регистрации: «1.1.1. Вход администратора МЭ вы систему», «1.1.2. Выход администратора…», 1.1.3. «Загрузка системы». У указанных событий также могут быть параметры регистрации, такие как время, предъявленный идентификатор, а также другие атрибуты регистрации, которые в рамках примера не рассматриваются для межсетевых экранов. Вторым типом рассмотренных наборов функционала является функционал «2. Средства защиты от НСД». В примере изображена функция, которая имеет множество параметров и детализирована более глубоко, чем «1.1. Регистрация событий» для «1. Межсетевые экраны».

4) «Средства защиты информации» содержит информацию о наборе функций конкретных СЗИ, представленных на рынке сертифицированных продуктов для обеспечения информационной безопасности (Kaspersky Endpoint Security, Dr.Web, SecretNet, TrustAccess и др.). Используется для определения перечня СЗИ, необходимых к установке в клиентской системе, для определения набора функций, которые фактически будут активны в системе с привязкой к конкретным СЗИ.

Структура БД имеет порядковую нумерацию, в качестве вложений используются цифровые обозначения из других БД, в частности из БД «Классификация функций средств защиты» вместо текстового наименования функции используется ее цифровой код. Так, в п. 1.1. тип СЗИ указывается в соответствии с БД «Классификация функций средств защиты» (Пример: средство защиты от НСД; антивирусное средство или межсетевой экран), в п. 1.2. перечисляются только цифровые обозначения имеющихся функций (см. Рисунок 5).

2. SecretNet
- 1.1. Средство защиты от НСД
- 1.2. Функции: *2.1, 2.1.1, 2.1.1.1., 2.1.1.2., 2.1.1.2.1., 2.1.1.2.2**
- 1.3. Уровень контроля НДВ: 3

**Функции из БД «Классификация функций средств защиты*

Рисунок 6 - Фрагмент ИР «Средства защиты информации»

Стоит отметить, что часть функций, встроенных в качестве обязательных в одно СЗИ, может присутствовать в качестве дополнительных функций (на усмотрение разработчика) в СЗИ другого профиля защиты.

5) «Объекты воздействия и их состояния» включает в себя перечень возможных объектов воздействия, их атрибуты и допустимые значения функций СЗИ над этими объектами. Фрагмент ИР изображен на рисунке 7.

1. Сетевой порт (номер)
- 1.1. Функции: (*2.1, 2.1.1, 2.1.1.1., 2.1.1.2., 2.1.1.2.1.*)
- 1.2. Состояния
  - 1.2.1. Открыт
  - 1.2.2. Закрыт

Рисунок 7 - Фрагмент базы данных «Объекты воздействия и их состояния»

ИР содержит объекты воздействия, а в качестве вложений указываются их допустимые состояния. Например, на рисунке 7, указано, что для объекта воздействия «1. Сетевой порт (<номер>)», доступны следующие управляющие им функции (см. рисунок 5): «2.1. Аудит», и далее по дереву вложенных функций можно увидеть, что доступен только «2.1.1.2.1. минимальный» уровень аудита. Это значит, что в расширенном уровне аудита указанный порт не контролируется. Исходя из того, что аудит, это лишь операция чтения, «1.2. Состояние» с детализацией «1.2.1. Открыт» можно интерпретировать как включенный аудит для данного порта. В п. 1.1. перечисляются только цифровые обозначения имеющихся функций (см. Рисунок 5).

В результате поэтапного взаимодействия всех ИР (Рис. 8) инструментального комплекса управления безопасностью будет сформировано следующее:

- Требования к системе;
- Требования к включенным функциям;
- Перечень средств защиты, которые требуется установить, с указанием возможных вариантов, а также с учетом эффективности тех средств защиты, которые уже предустановлены;
- Параметры средств защиты, которые необходимо активировать.

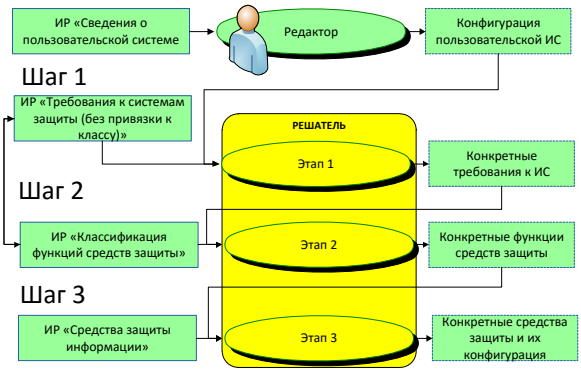

Рисунок 8 - Алгоритм работы с ИР

Заключение

В настоящей статье рассмотрены предпосылки формирования необходимости обеспечения информационной безопасности в информационных системах, существующие подходы к созданию

систем защиты (комплекс средств защиты и монолитные решения), достоинства и недостатки указанных подходов. Обосновывается необходимость создания архитектуры, объединяющей качественные средства защиты информации в единую систему. Формируются основные принципы создания такой архитектуры. Предложена концептуальная архитектура среды управления информационными ресурсами, позволяющая осуществить системное описание информационной системы, выбор средств защиты и их последующую настройку в соответствии с заданными требованиями. Описаны основные компоненты указанных сред и их функции.

На сегодняшний день в рамках решения данной задачи разработан набор описанных выше информационных ресурсов, начата реализация программных компонентов инструментального комплекса на платформе IACPaaS.

Благодарности

Работа выполнена при частичной финансовой поддержке РФФИ, грант 16 -07-00340, программы "Дальний Восток", грант 262-2015-0069.

Библиографический список

[Код Безопасности, 2015] Код Безопасности. Security Studio Endpoint Protection. Сертифицированная защита компьютера от сетевых вторжений, вредоносных программ и спама // Код безопасности - 2015. [Электронный ресурс: http://www.securitycode.ru/products/security_studio_endpoint_protection/]

[ФСТЭК, 2014] Федеральная служба по техническому и экспортному контролю (ФСТЭК России), «Меры защиты информации в государственных информационных системах» , Москва, 2014. pp. 5-15.

[PCMagazine, 2007] PCMagazine. Курс лекций «Вирусы и борьба с ними» // «Лаборатория Касперского» - 2007. [Электронный ресурс: http://www.pcmag.ru/elearning/course/lesson.php?COURSE_ID=10&ID=62]

[M. Rhodes-Ousley, 2014] M. Rhodes-Ousley, Information Security. The Complete Reference, Second Edition. Silicon Valley: California, 2014, pp.578–595.

[Грибова В.В., и др. 2011] Грибова В.В., Клещев А.С., Крылов Д.А., Москаленко Ф.М., Смагин С.В., Тимченко В.А., Тютюнник М.Б., Шалфеева Е.А. Проект IACPaaS. Комплекс для интеллектуальных систем на основе облачных вычислений // Искусственный интеллект и принятие решений. − 2011. − №1. − С.27- 35

[ФСТЭК, 2015] Федеральная служба по техническому и экспортному контролю. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации // ФСТЭК России – 2015. [Электронный ресурс] - Режим доступа. - URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty.

CONCEPT OF A TOOL FOR CREATING OF INFORMATION SECURITY SYSTEMS

Gribova V.V., Ivanova A.V.

Institute of Automation and Control Processes FEBRAS, Vladivostok, Russia

gribova@iacp.dvo.ru,

2395146@gmail.com

The article describes the existing approaches to creation of integrated information security systems (ISS) and their shortcomings. Principles of a tool development are presented. It provides the administrator of an information system an unified interface for managing different ISS, as well as recommendations for their selection according to the configuration and characteristics of the information system.

Introduction

The security of information systems (IS) is one of the key issues in the field of information technology. There are two main approaches to information security of IS. The first approach is based on using a single tool, which combines functions of some different tools, the second and the most popular one is based on using a combination of information security tools. Two types of approaches have both advantages and disadvantages. The aim of the paper is to describe the basic principles of the tool and their components. The tool is based on the second approach to ISS.

Main Part

The tool consists of the information resources control system and a set of client systems for IS security control.

The information resources control system includes structural editors for ontologies and information resources creation, as well as the information resources and a tool for choosing ISS.

A client systems for IS security control has an interface for receiving information about state of different ISS and interaction with the choosing ISS tool.

The information resources are: Requirements to ISS, Classification of ISS functions, Impacted objects and their conditions, Information security systems, and Client system Information.

Conclusion

In our research we proposed the tool for determination the requirements to ISS, as well as the guidance for choosing a set of ISS and their settings based on configuration of the IS.

We completed the development of the information resources on the IACPaaS platform, and currently implementing the program components.