R. E. Asratian, Leading Researcher, rea@ipu.ru, **V. N. Lebedev,** Head of Laboratory, lebvini@ipu.ru,
V. L. Orlov, Leading Researcher, ovl@ipu.ru, Institute of Control science RAS

Efficiency of a Secure Communication Channels Based on the Use of the HTTPS in Proxy Servers

The article is devoted to experimental study of characteristics of the new method of secure interactions organization in multi-network environment. The method is based on the use of HTTPS protocol and proxy server technology. The essence of approach consists in the organization of the protected HTTPS connections between proxy servers for safe transfer of information queries from one private local network in another through a global network while client and server components of distributed system are released from of information protection functions. In this approach client and server programs use HTTP protocol and proxy servers have additional functions of "HTTP -> HTTPS" and "HTTPS -> HTTP" gateways. The main advantage of approach over known (for example, VPN) consists in providing "high-level" means of HTTP queries routing and filtration the based on headers of HTTP queries, but not on separate IP packages. The application of approach is limited to situations in which private local networks can be considered as "a trust zone", and the only source of threats is the global network. The experimental study of efficiency of the offered approach in terms of influence of protection gateways on the speed of electronic services calls processing is conducted. This research showed that the area of effective application of the approach is made by electronic services with performance time over 1—2 s.

Keywords: *distributed systems, Internet technologies, network protocols, proxy servers, remote interactions, data security, web-services*

References

1. **Krishnamurti B., Reksford D.** *Web protokoly*. Moscow: Binom, 2010. 592 p.
2. **Shaposhnikov I. V.** *Web-servisy Microsoft.NET*. SPb: BHV-Peterburg, 2002. 336 p.
3. **Mak-Donal'd M., Shpushta M.** *Microsoft ASP.NET 3.5 s primerami na C# 2008 i Silverlight 2 dlja professionalov*. Moscow: Vil'jams, 2009. 1408 p.
4. **Zgoba A. I., Markelov D. V., Smirnov P. I.** Kiberbezopasnost': ugrozy, vyzovy, reshenija, *Voprosy kiberbezopasnosti*, 2014, no. 5, pp. 30—38.
5. **Shheglov A. V.** *Zashhita komp'juternoj informacii ot nesankcionirovannogo dostupa*. SPb.: Nauka i tehnika, 2004, 384 p.
6. **Asratjan R.Je., Lebedev V. N., Orlov V. L.** Organizacija zashhishhennyh kanalov vzaimodejstvija na osnove primenenija protokola HTTPS v proksi-serverah, *Informacionnye tehnologii*, 2015, vol. 21, no. 9, pp. 670—674.
7. **Hant K.** TCP/IP. *Setevoe administrirovanie*. SPb.: Piter, 2007. 816 p.
8. **Andreev A. G., Bezzubov E. Ju., Emel'janov** i dr. *Windows 2000: Server i Professional*. SPb.: BHV-Sankt-Peterburg, 2001. 1055 p.

УДК 004.45

В. В. Грибова, д-р техн. наук, зам. директора по научной работе, e-mail: gribova@iacp.dvo.ru,
А. В. Иванова, аспирант, e-mail: 2395146@gmail.com,
Институт автоматики и процессов управления Дальневосточного отделения Российской Академии наук

Концепция программного комплекса для управления безопасностью информационных систем

Рассмотрены существующие подходы к созданию систем защиты, их достоинства и недостатки. Описаны основные требования, принципы и концептуальная архитектура программного комплекса для управления безопасностью информационных систем, состоящая из двух подсистем: среды управления информационными ресурсами и клиентской среды управления безопасностью информационной системы. Описаны основные компоненты программного комплекса и их функции.

Ключевые слова: *информационная безопасность, управление, интеллектуальные системы, базы данных, онтологии, базы знаний, защита информации, информационные системы*

Введение

Обеспечение защиты информации в информационных системах является очень актуальной задачей. Исследование компании Dell, проведенное в 2014 г., показало [1], что из 1440 опрошенных компаний подавляющее большинство (90 % специалистов) отметили, что информационная безопасность становится одним из главных приоритетов в планируемом бюджете, и примерно 20 % всех затрат на информационные технологии (ИТ) будет

потрачено на всевозможные сервисы и продукты по защите информации. Три четверти опрошенных планируют увеличить расходы на информационную безопасность в этом году, причем 58 % из них планируют приобрести недешевые системы информационной защиты. 40 % ИТ-профессионалов все еще сомневаются в эффективности существующих решений. Общие взгляды на управление информационной безопасностью в целом и без учета специфичных технических особенностей защищаемых платформ сформированы достаточно давно и закреплены в стандарте [2], а такие новые понятия, как "виртуализация", "облака", "кластеры", "распределенные вычисления" и т.д., только начинают вхождение в законодательный фундамент.

Можно выделить два основных подхода к защите информации в информационных системах всех типов [3].

Первый подход заключается в использовании единого средства защиты. Такое решение комплексно решает проблему обеспечения безопасности информационной системы (ИС)[1], обладает централизованным интерфейсом, что упрощает управление для администратора ИС [4], однако имеет и ряд существенных недостатков [5]: отсутствие совместимости с другими системами защиты, 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), нарушение работоспособности всех подсистем системы защиты информации по окончании срока действия сертификата, компрометация лицензионного ключа, сбой процедур обновления и т.д.

Второй, и наиболее популярный, подход заключается в использовании комплекса средств защиты информации (СЗИ). Отдельные компоненты СЗИ специфичны, узконаправлены, предназначены для нейтрализации сходных угроз и могут быть разделены по типам: антивирусные средства, СЗИ от несанкционированного доступа, межсетевые экраны, системы обнаружения вторжений и др. Для обеспечения защиты ИС может быть выбран различный набор таких средств. При всей гибкости такого подхода он также обладает набором существенных недостатков [5]: отсутствие единого интерфейса управления и механизмов оперативного контроля (необходимо напрямую вмешиваться в настройки СЗИ), возможная несовместимость СЗИ между собой (после установки одного СЗИ другое может перестать функционировать, либо обнаруживаются конфликты совместного использования). Кроме того, перед администратором возникает ряд дополнительных задач по обеспечению информационной безопасности ИС: ему необходимо знать и определять требования к ИС, в том числе законодательные, для правильного выбора набора СЗИ, их последующей настройки, поддержания непрерывного функционирования системы, разрешения конфликтных ситуаций, изучения возможностей улучшения системы и повышения ее эффективности [6].

В связи с тем, что подход, основанный на использовании комплекса разнородных СЗИ, применяется в подавляющем большинстве ИС, актуальной задачей является разработка программных средств, обеспечивающих администратора ИС единой средой для управления и мониторинга разнородными СЗИ, рекомендациями по их выбору и настройке в соответствии с конфигурацией ИС и ее конкретными особенностями. Такое решение обеспечит высокую эффективность технологий выявления, предупреждения и предотвращения атак и выполнение законодательных требований. Целью данной работы является разработка общих принципов, концепции и архитектуры комплекса программных средств, обеспечивающих такую функциональность.

Принципы построения программного комплекса

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, а также законодательных требований к защите ИС, можно выделить ключевые требования к функциональности и использованию комплекса программных средств.

- *Программный комплекс должен обеспечивать администратора конкретной ИС помощью в определении класса ИС, требований к ней, а также рекомендациями по выбору наборов СЗИ с учетом конфигурации ИС.*
- *Набор СЗИ для конкретной ИС должен включать рекомендации по настройке, обеспечивающие бесконфликтность их функционирования в ИС.*

Выбор СЗИ в соответствии с конкретной конфигурацией ИС и требованиями к уровню ее защиты, а также настройка каждого СЗИ таким образом, чтобы не возникало конфликтов совместимости между различными СЗИ, являются достаточно сложной задачей для любого администратора и часто требуют приглашения сторонних специалистов, как правило, из профилированных компаний, которые осуществляют функции консультирования по определению набора СЗИ в соответствии с конфигурацией ИС и требованиями к ее защите, настройку комплекса СЗИ, а также сопровождение в процессе эксплуатации.

- *Программный комплекс должен поддерживать функцию анализа и обнаружения возникших конф-*

[1] Под информационной системой будем понимать любую информационную систему вне зависимости от типа платформы (локально-вычислительная сеть, автоматизированное рабочее место, распределенная облачная платформа и т.д.).

ликтных ситуаций при функционировании разнородных СЗИ в единой ИС.

При функционировании разнородных СЗИ возможно возникновение конфликтных ситуаций. Их анализ, обнаружение, информирование администратора о таких конфликтах и возможных способах их устранения поможет администратору оперативно решать возникающие в процессе эксплуатации ИС проблемы.

- *Наличие единого интерфейса для управления разнородными СЗИ.* Такой подход обеспечит администратора ИС средствами оперативного управления набором разнородных СЗИ для централизованного сбора и отображения сведений о текущем состоянии ИС, полученных от различных СЗИ.

Учитывая, что архитектура ИС, требования к обеспечению их защиты, сами СЗИ и их функции постоянно изменяются, предлагаются следующие ***основные принципы*** создания программного комплекса:

1. Представление информации о стандартах, требованиях к ИС и их классификации, СЗИ и их функциях, методах устранения конфликтов СЗИ в форме, одинаково понятной как экспертам для модификации, исправления ошибок и неточностей, а также дальнейшего развития в связи с изменениями в данной предметной области, так и компьютерным системам для их обработки.

2. Создание централизованной "среды", аккумулирующей знания в едином информационном пространстве с целью обеспечить их накопление, совместное развитие и использование для исключения повторной разработки готовых решений и минимизации человеческих ресурсов в существующих условиях кризиса высококвалифицированных специалистов в области информационной безопасности и сокращения расходов на сопровождение комплекса СЗИ.

3. Размещение всех информационных ресурсов и сервисов в облаке для обеспечения их широкой доступности как для использования, так и модифицирования в процессе жизненного цикла.

4. Использование методов искусственного интеллекта для формирования и сопровождения данных и знаний. В качестве таких методов предлагается онтологический подход, обеспечивающий пользователя системой понятий (онтологией) для формирования целевых баз данных и баз знаний и исключающий необходимость использования посредников в лице инженеров знаний для преобразования опыта и навыков экспертов в форматы хранения, "понимаемые" программными системами.

Концептуальная архитектура программного комплекса

Концептуальная архитектура программного комплекса для управления безопасностью ИС представлена на рис. 1.

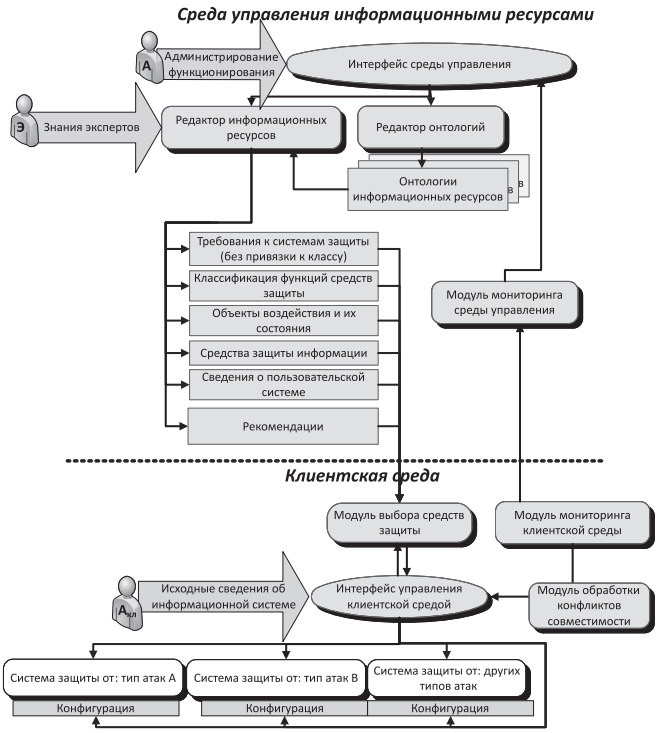

Рис. 1. Концептуальная архитектура программного комплекса для управления безопасностью информационных систем

Программный комплекс состоит из среды управления информационными ресурсами и множества клиентских сред управления безопасностью ИС.

Среда управления информационными ресурсами состоит из программных и информационных ресурсов. Информационными ресурсами являются онтологии, базы данных и базы знаний, программными — структурные редакторы онтологий, база данных и база знаний, а также *"Модуль мониторинга среды управления"*, который предназначен для сбора, систематизации и анализа служебной информации обо всех подключенных к глобальной среде клиентских средах управления безопасностью ИС и выполняемых ими функциях. Данная информация необходима для получения новых знаний о совместном функционировании разнородных СЗИ для выработки рекомендаций по их настройке, устранению конфликтных ситуаций при совместном функционировании.

Редактор онтологий предназначен для создания онтологий баз данных и баз знаний, по которым эксперты предметной области с помощью редактора будут формировать и сопровождать соответствующие информационные ресурсы — базы данных и базы знаний. Информационные ресурсы используются в клиентских системах для помощи администратору в классификации ИС, определении требований к ней, выборе и настройке СЗИ, обеспечении их бесконфликтной работы. Информационные ресурсы состоят из множества баз данных и баз знаний. Базами данных 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". Базы знаний содержат знания об информационных системах, их классификации, а также знания о разрешении конфликтов совместного функционирования СЗИ. Подробное описание информационных ресурсов дано в разделе "Информационные ресурсы".

В качестве средства реализации среды управления информационными ресурсами выбрана облачная платформа IACPaaS [7]. 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 администраторам — 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 базы данных или базы знаний (первый уровень), по которой затем автоматически генерируется специализированный интерфейс для эксперта (второй уровень). Наличие универсального редактора, во-первых, не требует разработки специализированных редакторов информационных ресурсов, во-вторых, позволяет экспертам предметной области без инженеров знаний формировать и модифицировать базы знаний и базы данных в терминах онтологии.

Все информационные ресурсы (метаинформация и объектная информация) представляются в форме семантической сети понятий (иерархического однородного бинарного ориентированного графа с возможными петлями и циклами). Таким образом, использование платформы IACPaaS обеспечивает всю необходимую инфраструктуру для хранения и наполнения фонда информационных ресурсов.

Клиентская среда управления безопасностью информационной системы *(клиентская среда)* предназначена для мониторинга состояния подконтрольных СЗИ, оперативного централизованного управления ими (без необходимости внесений изменений администратором в каждое СЗИ), а также для определения требований к клиентской ИС, формированию минимального набора требуемых функций и СЗИ, реализующих их выполнение. Доступ к данным функциям реализуется через *Интерфейс управления клиентской средой.*

Программными элементами комплекса помимо редакторов являются: *Модуль выбора средств защиты, Модуль мониторинга клиентской среды, Модуль обработки конфликтов совместимости.*

Модуль выбора средств защиты предназначен для определения набора требований на основании входных параметров клиентской ИС. Данный модуль также предусматривает помощь в выборе СЗИ, которые удовлетворяют предъявленным требованиям и могли бы быть использованы в конкретной ИС.

Модуль мониторинга клиентской среды предназначен для сбора актуальных сведений о состоянии системы защиты ИС. Указанный модуль взаимодействует со встроенными средствами аудита средств защиты информации и *Интерфейсом управления клиентской средой,* который позволяет собирать уточненные данные, основанные на типе СЗИ. Например, функции аудита, доступные в межсетевом экране, позволяют собрать более расширенную статистику о трафике, чем аналогичные функции аудита в антивирусном средстве. Помимо расширенной статистики осуществляется сбор информации об ошибках в системе, а также о произведенных администратором клиентской ИС описаниях параметров конкретной системы.

Модуль обработки конфликтов совместимости предназначен для выявления конфликтных ситуаций совместного функционирования СЗИ по собранной *Модулем мониторинга клиентской среды* информации об ошибках в системе. Ввиду того, что не каждая ошибка является результатом конфликта настройки или конфликта совместимости СЗИ, система осуществляет анализ полученной информации и в случае выявления конфликта уведомляет о событии администратора клиентской среды через *Интерфейс управления клиентской средой.* Также указанный модуль предусматривает определение специфики конфликта и возможные варианты его решения: в автоматическом либо интерактивном режиме, о чем также уведомляет администратора клиентской среды. В случае "автоматического" решения конфликта требуемые изменения параметров вносятся через доступные элементы управления для конкретного СЗИ (командная строка, изменения значений реестра и т.д.) на основе "Базы знаний о конфликтах". При выборе интерактивного режима решения конфликта администратору клиентской среды выдаются рекомендации по внесению изменения в настройки через штатный интерфейс СЗИ на основе "Интерфейса управления клиентской средой".

Разрабатываемый инструментальный комплекс предусматривает устранение конфликтных ситуаций в клиентской информационной системе в автоматическом режиме при наличии такой возможности, а в случае ее отсутствия — выдачу рекомендаций в "*Интерфейс управления клиентской средой"* для внесения изменений в настройки в ручном режиме.

Информационные ресурсы

Информационными ресурсами являются базы данных, базы знаний и их онтологии.

Блок базы данных (БД) включает в себя следующие информационные ресурсы:

1. ***"Сведения о пользовательской системе"*** описывает структуру данных, по которой администратор может описать характеристики клиентской информационной системы (рис. 2), необходимые для определения требований к ней.

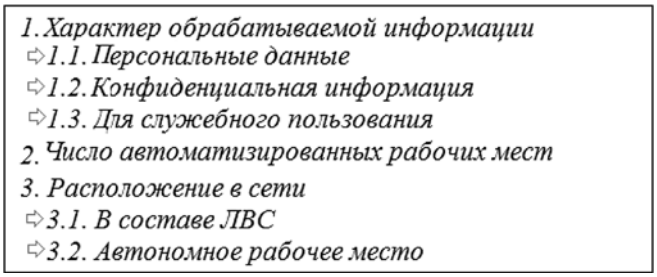

Рис. 2. Фрагмент базы данных "Сведения о пользовательской системе"

2. ***"Требования к системе защиты (без привязки к классу)"*** включает в себя формализованное описание перечня законодательных и пользовательских требований к защите ИС. Используется при определении требуемого набора функций защиты клиентской ИС на основе ее конфигурации (рис. 3).

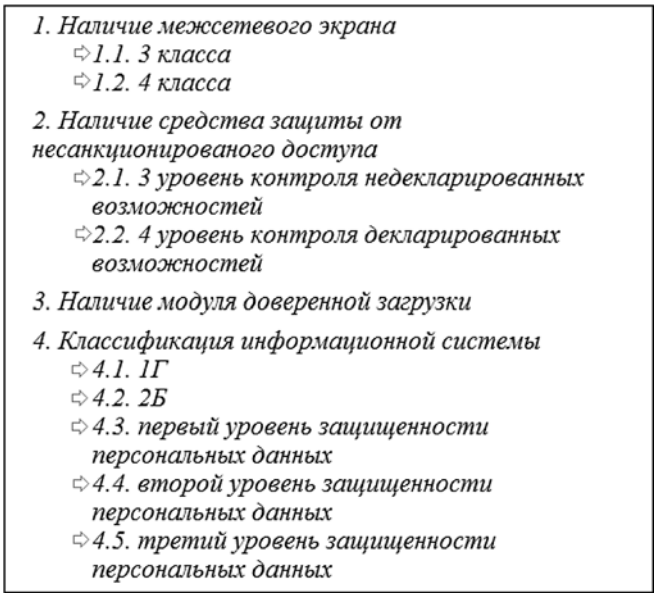

Рис. 3. Фрагмент базы данных "Требования к системам защиты (без привязки к классу)"

3. ***"Классификация функций средств защиты"*** является многоуровневой структурой и включает в себя классификацию функций СЗИ (рис. 4), определяемую нормативными документами [8], а также дополнительные функции, встраиваемые разработчиками в программное обеспечение. Используется при выявлении конфликтов, связана с БД "Средства защиты информации", которая содержит сводную информацию о всех функциях СЗИ.

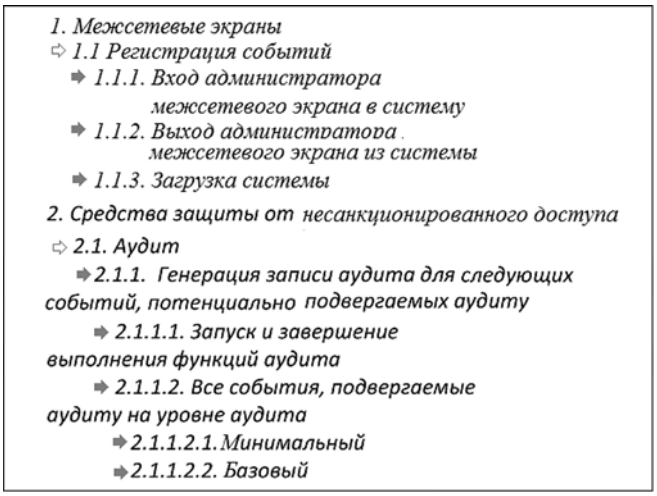

Рис. 4. Фрагмент базы данных "Классификация функций средств защиты"

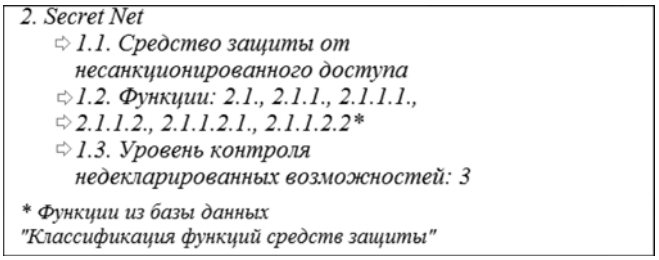

Рис. 5. Фрагмент базы данных "Средства защиты информации"

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 для установки в клиентской ИС, для определения набора функций, которые фактически будут активны с привязкой к конкретным СЗИ (рис. 5).

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: СЗИ от НСД; антивирусное средство или межсетевой экран), в п. 1.2 перечисляются только цифровые обозначения имеющихся функций (рис. 5).

Часть функций, встроенных в качестве обязательных в одно СЗИ, может использоваться в качестве дополнительных функций 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 (рис. 6).

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

Рис. 6. Фрагмент базы данных "Объекты воздействия и их состояния"

Блок "Базы знаний" (БЗ) включает в себя базу знаний о классификации и базу знаний о конфликтах.

1. ***База знаний о классификации*** содержит знания о классификации пользовательской информационной системы на основе ее конфигурации (рис. 7). Класс ИС необходим для определения требований к информационной системе, определения набора СЗИ и их функций. Классификация определяется на основе регламентирующих документов [9, 10].

(<режим доступа> =многопользовательский AND
<конфиденциальность носителей информации> = различная AND
<уровень полномочий> = различный AND
<наивысший уровень конфиденциальности информации> =персональные данные AND
<характер персональных данных> = (сотрудники оператора OR внешние контрагенты) AND
<категория персональных данных> = специальная AND
<число субъектов персональных данных> > [100 000] AND
<тип актуальные угрозы> = (третий OR второй)) ⇒
<класс системы> = 1В

(<наивысший уровень конфиденциальности информации>= персональные данные AND
<характер персональных данных> = сторонние контрагенты AND
<категория персональных данных> = общедоступные AND
<количество субъектов персональных данных> < [100 000] AND
<тип актуальные угрозы> = третий) ⇒
<класс системы> = УЗ4

Рис. 7. Фрагмент базы знаний о классификации

2. ***База знаний о конфликтах*** содержит знания о конфликтных ситуациях в конкретных СЗИ с учетом специфики произошедшего события и конфигурации ИС: разрядность и версия операционной системы (ОС), наличие выхода в Интернет, предустановленное программное обеспечение и др. Очевидно, что не каждая ошибка является результатом конфликта настройки или конфликта совместимости СЗИ. Для возникновения конфликта необходимо, чтобы два различных процесса (СЗИ, штатный процесс ОС и др.) в один момент времени запросили доступ к одному объекту доступа, в результате которого система повела себя таким образом, который не предусмотрен установленной политикой безопасности: отказ при предусмотренном предоставлении прав либо, наоборот, предоставление доступа при предусмотренном запрете. Ввиду того, что при возникновении конфликтной ситуации система может повести себя нештатным образом (рис. 8), фактический результат выполнения операции может не соответствовать зафиксированному журналами ОС и журналами СЗИ. Из рисунка видно, что в один момент времени (22:28:54) в систему осуществлено несколько мгновенных попыток доступа ("Открытие каталога"), результатом каждой из которых являются две операции "Закрытие объекта", т.е. фактически доступ к объекту не предоставлен несмотря на фиксацию ус-

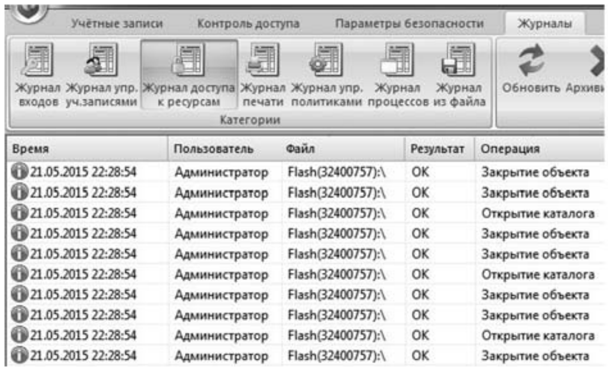

Рис. 8. Нештатное поведение системы защиты

(<число процессов> = 2 AND
<процесс 1 > = avp.exe AND
<процесс 2> = dl.exe AND
<время. процесс1> =<время. процесс 2> AND
<объект воздействия процесс 1> = локальный OR устройство OR внешнее устройство OR USB устройство OR съемный носитель AND
<объект воздействия процесс 1> =<объект воздействия процесс 2>
<название операции. процесс 1> = чтение AND
<название операции. процесс 2> = запись) ⇒<состояние конфликта> = потенциальный конфликт

Рис. 9. Фрагмент базы знаний о конфликтах

пешного результата операции. Для точного выявления конфликтов необходимо предусматривать такие ситуации. Для этого вводится понятие потенциального конфликта: ситуация, когда два различных процесса в один момент времени запрашивают доступ к одному объекту доступа.

Параллельно анализируя другие системные журналы, можно сделать вывод о том, является ли потенциальный конфликт фактическим конфликтом. Если результат операции доступа двух процессов к одному объекту в один момент времени соответствует заданной политике доступа, то потенциальный конфликт *не является конфликтом.*

Потенциальный конфликт может возникнуть при настройке схожих функций защиты различных СЗИ, установленных в одной информационной системе. К примеру, функция контроля доступа есть во многих СЗИ и выполняет не только операцию чтения прав доступа к объекту, но и операцию записи в случае их изменения. Конфликт может возникнуть в ситуации, когда к одному объекту воздействия будет осуществляться доступ нескольких функций в целях установки противоположных (противоречащих друг другу) состояний объекта. Результат этой операции может зависеть от множества факторов: приоритетов назначенных прав, режимов доступа (дискретный, мандатный), типов СЗИ, конкретных объектов доступа и т. д. Знания об устранении таких конфликтов описаны в базе знаний о конфликтах (рис. 9).

Программные компоненты

Основными программными компонентами являются редакторы информационных ресурсов, модули мониторинга, а также модули выбора СЗИ и обработки конфликтов совместимости. Редакторы

информационных ресурсов являются компонентами платформы IACPaaS, их функциональность и особенности подробно изложены в работе [11]. Функциональность модулей мониторинга достаточно понятна, поэтому в данном разделе более детально описаны два программных компонента — модуль выбора средства защиты информации и модуль обработки конфликтов совместимости.

Модуль выбора средств защиты информации последовательно решает следующие основные задачи:

- определение множества требований к ИС на основе ее конфигурации;
- определение множества функций СЗИ и их параметров, которые должны функционировать в конкретной ИС;
- перечень СЗИ, которые требуется установить, с указанием возможных вариантов, а также с учетом эффективности тех СЗИ, которые уже предустановлены в ИС;
- параметры СЗИ, которые необходимо активировать.

Стоит отметить, что на основе сформированной администратором клиентской среды конфигурации информационной системы нельзя сразу определить исчерпывающий перечень требований. Некоторые требования являются причинно-следственными. К примеру: в конфигурации ИС заявлено, что она подключена к сети. В качестве требования следствием будет "1. Межсетевой экран". Однако определить требуемый класс межсетевого экрана можно только на основе классификации информационной системы. Если указано, что характер обрабатываемой информации — персональные данные, можно присвоить один из уровней защищенности, к примеру, "4.5. Третий уровень защищенности" (конкретизация определяется также и другими параметрами конфигурации ИС). Используя установленный класс, а также дополнительные сведения о конфигурации, можно определить требуемый класс межсетевого экрана для конкретной ИС — "1.2 4 класс", а также дополнительные требования к устанавливаемому ПО — "2.2. 4 уровень контроля НДВ". Соответствия между конфигурацией ИС и требованиями к этой ИС описываются в БЗ "О классификации". Таким образом, можно сказать, что эта база последовательно и циклично использует определяемые характеристики для получения исчерпывающего перечня требований к ИС. Общая схема алгоритма работы модуля выбора СЗИ представлена на рис. 10.

Модуль обработки конфликтов совместимости предназначен для выявления конфликтных ситуаций. Общий алгоритм модуля представлен на рис. 11. На первом шаге работы алгоритма определяется наличие потенциального или истинного конфликта. Задачей второго шага работы алгоритма является выдача рекомендаций администратору по устранению возникшего конфликта либо предупреждение о потенциальной возможности конфликта с

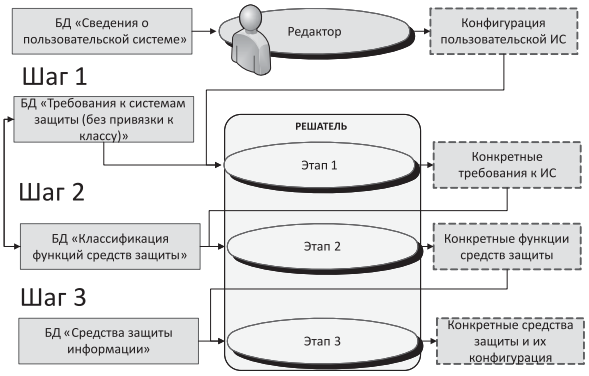

Рис. 10. Алгоритм работы модуля выбора СЗИ

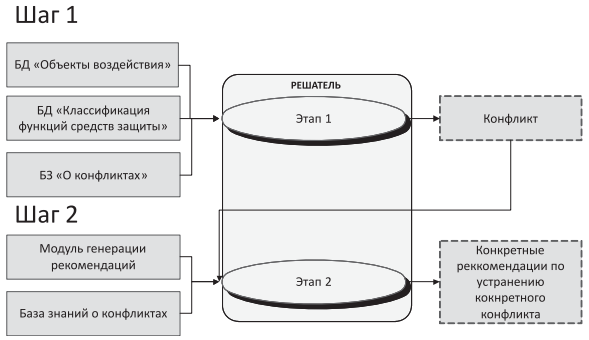

Рис. 11. Алгоритм работы модуля обработки конфликтов совместимости

Формальное описание

В рамках назначенной политики [*значение политики*] для [*название процесса*] по операции [*название операции*] для объекта [*название объекта*] необходимо выполнить следующие действия: [*описание действий, схемы, картинки, инструкции*]

Фактическое представление

В рамках назначенной политики [Разрешительная] для [dl.exe] по операции [Запись] для объекта [Prod&220HW] необходимо выполнить следующие действия: [Открыть консоль администратора Dallas…]

Рис. 12. Структура описания рекомендаций

объяснением, какие СЗИ, процессы, операции и др. могут быть источниками конфликтов.

Генерация рекомендаций осуществляется соответствующим модулем, структура выдачи рекомендаций представлена на рис. 12.

С учетом того, что пользователь может несвоевременно осуществлять настройку системы защиты в соответствии с рекомендациями, предлагается использовать механизм выявления дубликатов конфликтов. Для этого при взаимодействии модуля мониторинга клиентской среды и модуля обработки конфликтов совместимости выявляются такие конфликты, которые полностью дублируют друг друга лишь с разницей во времени.

Заключение

В настоящей статье рассмотрены существующие подходы к созданию систем защиты (комплекс СЗИ и монолитные решения), достоинства и недостатки указанных подходов. Обосновывается необходимость создания программного обеспечения, объединяющего разнородные СЗИ в единую сис-

тему. Описаны основные требования, принципы и концептуальная архитектура программного комплекса, состоящая из двух подсистем: среды управления информационными ресурсами и клиентской среды управления безопасностью информационной системы. Описаны основные компоненты указанных сред и их функции.

На сегодняшний день в рамках решения данной задачи разработаны базы данных, ведется наполнение баз знаний и реализация программных компонентов программного комплекса на платформе IACPaaS.

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

Список литературы

1. **Securing** the cloud in a BYOD world: "No one really has this figured out" [Электронный ресурс]. Business Cloud News. Лондон. 2014. URL: http://www.businesscloudnews.com/2014/02/21/securing-the-cloud-in-a-byod-world-no-ones-really-has-this-figured-out/

2. **Управление** технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии, ГОСТ Р ИСО/МЭК 27001—2006. Государственный стандарт. 2006. 31 с.

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

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

5. **Rhodes-Ousley M.** Information Security. The Complete Reference, Second Edition. California: Silicon Valley, 2014. P. 578—595.

6. **Меры** защиты информации в государственных информационных системах. М.: Федеральная служба по техническому и экспортному контролю (ФСТЭК России), 2014. Р. 5—15.

7. **Gribova V. V., Kleshchev A. S., Krylov D. A.** Project IACPaaS. Complex for intelligent software based on cloud computing // Artificial Intelligence and Decision Making. 2011. N. 1. P. 27—35.

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

9. **Автоматизированные** системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г.

10. **Об утверждении** требований к защите персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства РФ от 01.11.2012 № 1119.

11. **Грибова В. В., Клещев А. С.** Технология разработки интеллектуальных сервисов, ориентированных на декларативные предметные базы знаний. Часть I. Информационные ресурсы // Информационные технологии. 2013. № 9. С. 7—11..

V. V. Gribova, Research Deputy Director, e-mail: gribova@iacp.dvo.ru,
A. V. Ivanova, e-mail: 2395146@gmail.com, PhD Student,
Institute of Automation and Control Processes for Eastern Branch of the Russian Academy of Sciences

Software for Security Control of Information Systems

This article reviewed modern approaches to the creation of information security systems, the advantages and disadvantages of these approaches. The motivation to create a software that incorporates heterogeneous information security systems into an integrated system is explained. The basic requirements, principles and architecture of software including two subsystems are described. These subsystems are: a subsystem for control of information resources and a client subsystem for security control of an information system. The subsystem for control of information resources is implemented on the cloud platform IACPaaS. The cloud platform is an Internet software for development, control and usage of intelligent services. The client subsystem is intended for monitoring the state of installed systems, as well as for determine the security requirements for the client information system and a security configuration tool in accordance with requirements. By now data and knowledge bases are realized, development of software components is in progress.

Keywords: *security system, intelligent system, databases, ontologies, knowledge bases, data protection, information systems, data security solution*

References

1. **Securing** *the cloud in a BYOD world: "No one really has this figured out"* [Electronic resource]. Business Cloud News — London, 2014. URL: http://www.businesscloudnews.com/2014/02/21/securing-the-cloud-in-a-byod-world-no-ones-really-has-this-figured-out/.

2. **Upravlenie** *tekhnicheskogo regulirovaniya i standartizacii Federalnogo agentstva po tekhnicheskomu regulirovaniyu i metrologii GOST R ISO MEHK 27001—2006.* Gosudarstvennyj standart. 2006. 31 p.

3. **PCMagazine**. Course of lectures "Virusy i bor'ba s nimi". *Course of lectures "Viruses and opposing them".* Moscow, 2007. URL: http://www.pcmag.ru/elearning/course/lesson.php?COURSE_ID=10&ID= 62.

4. **Kod** Bezopasnosti. Security Studio Endpoint Protection. Sertificirovannaya zashchita komp'yutera ot setevyh vtorzhenij, vredonosnyh programm i spama, *Kod bezopasnosti*, 2015. [Elektronnyj resurs]. URL: http://www.securitycode.ru/products/security_studio_endpoint_protection/.

5. **Rhodes-Ousley M.** *Information Security. The Complete Reference*, Second Edition. Silicon Valley: California, 2014, pp. 578—595.

6. **Mery** *zashchity informacii v gosudarstvennyh informacionnyh sistemah*, Moscow: Federal'naya sluzhba po tekhnicheskomu i ehksportnomu kontrolyu (FSTEHK Rossii), 2014. pp. 5—15.

7. **Gribova V. V., Kleshchev A. S., Krylov D. A.** Project IACPaaS. Complex intelligent software based on cloud computing, *Artificial Intelligence and Decision Making*, 2011, no. 1, pp. 27—35.

8. **Dokumenty** *po sertifikacii sredstv zashchity informacii i attestacii ob"ektov informatizacii po trebovaniyam bezopasnosti informacii*, Federal'naya sluzhba po tekhnicheskomu i ehksportnomu kontrolyu, FSTEHK Rossii — 2015. [Elektronnyj resurs]. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty.

9. **Avtomatizirovannye** *sistemy. Zashchita ot nesankcionirovannogo dostupa k informacii. Klassifikaciya avtomatizirovannyh sistem i trebovaniya po zashchite informacii.* Rukovodyashchij dokument. Reshenie predsedatelya Gostekhkomissii Rossii ot 30 marta 1992 g.

10. **Ob utverzhdenii** *trebovanij k zashchite personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh*. Postanovlenie Pravitel'stva RF ot 01.11.2012 N 1119.

11. **Gribova V. V., Kleshchev A. S.** Technology of Intelligent Services Development Oriented on Declarative Domain Knowledge Bases. Part 1. Information Resources, *Information Technologies*, 2013, no. 9, pp. 7—11.