РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 657 170**(13) **C2**

(51) МПК
*H04L 29/06* (2006.01)
*G06F 21/57* (2013.01)

# (12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
*H04L 29/06 (2015.12); G06F 17/30864 (2015.12); G06F 21/577 (2015.12)*

(21)(22) Заявка: **2012156341, 01.07.2011**

(24) Дата начала отсчета срока действия патента:
**01.07.2011**

Дата регистрации:
**08.06.2018**

Приоритет(ы):
(30) Конвенционный приоритет:
**01.07.2010 US 61/360,610**

(43) Дата публикации заявки: **27.06.2014** Бюл. № **18**

(45) Опубликовано: **08.06.2018** Бюл. № **16**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **25.12.2012**

(86) Заявка PCT:
**IB 2011/052918 (01.07.2011)**

(87) Публикация заявки PCT:
**WO 2012/001667 (05.01.2012)**

Адрес для переписки:
**410000, г. Саратов, главпочтамт, а/я 62, Н.В. Романовой**

(72) Автор(ы):
**НУНЕЗ ДИ СРОСЕ Мариано (AR)**

(73) Патентообладатель(и):
**Онапсис, Инк. (US)**

(56) Список документов, цитированных в отчете о поиске: **US 2003/0212779 A1, 13.11.2003. US 2003/0217039 A1, 20.11.2003. US 2008/256638, 16.10.2008. WO 03/060717 A1, 24.07.2003. US 2009/0259748 A1, 15.10.2009.**

## (54) Автоматизированная оценка безопасности критически важных для бизнеса компьютерных систем и ресурсов

(57) Реферат:

Изобретение относится к безопасности компьютерных систем. Технический результат – обеспечение эффективной безопасности компьютерных систем. Способ оценки конфигурации системы безопасности целевой компьютерной среды включает: a) сканирование идентифицированных IP-адресов и портов; b) снятие отпечатков пользования выявленных открытых портов для распознавания исполняемых через них сервисов; c) «дактилоскопирование» - определение активности названной целевой среды; d) обращение к базе модулей и выполнение, по меньшей мере, одного из таких модулей, предназначенных для нахождения факторов уязвимости в системе безопасности, доступных через указанные IP-адреса и порты; при этом - обозначенный, по меньшей мере, один модуль выполняется исходя из его конфигурации; - обозначенная целевая компьютерная среда используется для выполнения критически важных бизнес-приложений, причем, по меньшей мере, один из вышеуказанных модулей выполняет способ, включающий:



RU 2657170 C2

RU 2657170 C2

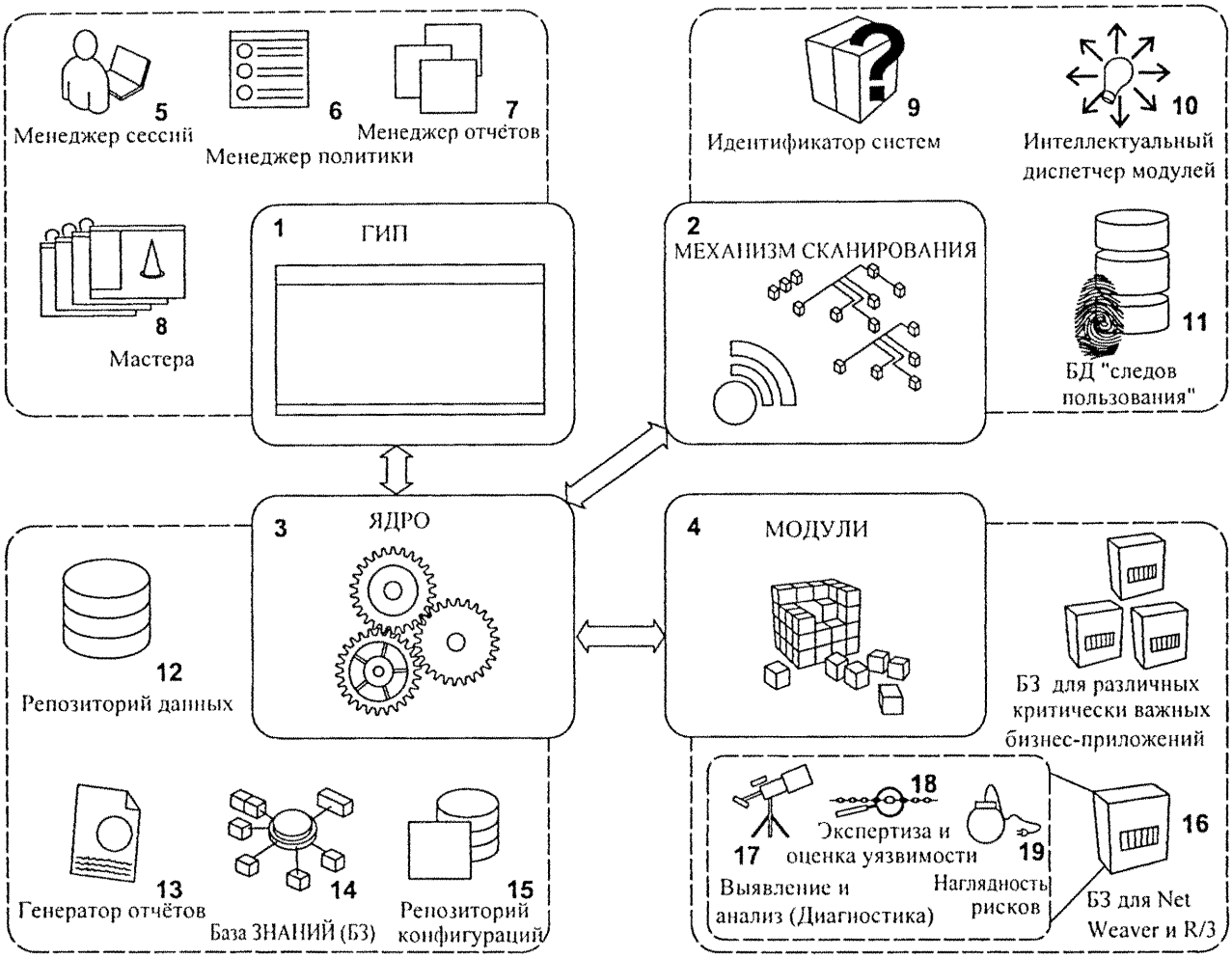
сс-1) поиск таблиц адресатов для удаленных вызовов функций и других интерфейсов для прикладных серверов, ассоциированных с указанной целевой средой;

сс-2) поиск журнальных файлов с приложениями для указанной целевой среды;

сс-3) выявление на основе найденных таблиц адресатов и журнальных файлов связей между различными системами, имеющими отношение к указанной целевой среде;

сс-4) графическое отображение выявленных связей;

сс-5) предоставление пользователю сформированного графического отображения выявленных связей. 9 з.п. ф-лы, 4 ил.




ФИГ. 2

RU 2657170 C2

RU 2657170 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 657 170**(13) **C2**

(51) Int. Cl.
*H04L 29/06* (2006.01)
*G06F 21/57* (2013.01)

## (12) ABSTRACT OF INVENTION

(52) CPC
*H04L 29/06 (2015.12); G06F 17/30864 (2015.12); G06F 21/577 (2015.12)*

(21)(22) Application: **2012156341, 01.07.2011**

(24) Effective date for property rights:
**01.07.2011**

Registration date:
**08.06.2018**

Priority:
(30) Convention priority:
**01.07.2010 US 61/360,610**

(43) Application published: **27.06.2014** Bull. № **18**

(45) Date of publication: **08.06.2018** Bull. № **16**

(85) Commencement of national phase: **25.12.2012**

(86) PCT application:
**IB 2011/052918 (01.07.2011)**

(87) PCT publication:
**WO 2012/001667 (05.01.2012)**

Mail address:
**410000, g. Saratov, glavpochtamt, a/ya 62, N.V. Romanovoj**

(72) Inventor(s):
**NUNEZ DI SROSE Mariano (AR)**

(73) Proprietor(s):
**Onapsis, Ink. (US)**

RU 2657170 C2

RU 2657170 C2

## (54) AUTOMATED SAFETY ASSESSMENT OF BUSINESS-CRITICAL COMPUTER SYSTEMS AND RESOURCES

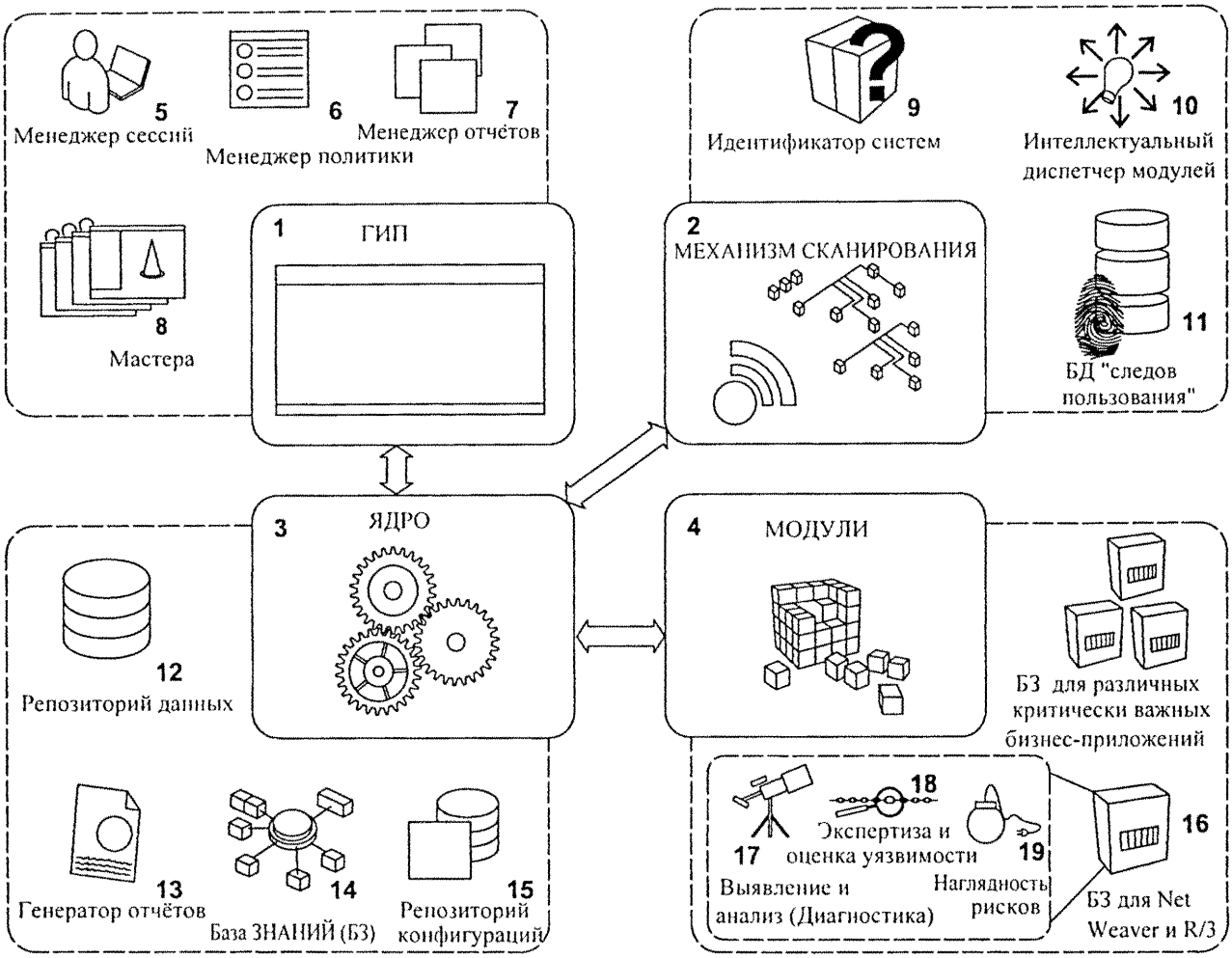
(57) Abstract:

FIELD: physics, computer engineering.

SUBSTANCE: invention relates to security of computer systems. Method of assessment of target computing environment security configuration include: a) scanning of identified IP-addresses and ports; b) dactyloscopic recording from detected open ports to detect services that were through; c) "fingerprinting" - determination of activity of said target environment; d) appealing to modules base and performing at least one of these modules which are designed to find vulnerabilities in the security system, available through IP-address and ports; in this case, at least one said module is executed based on its configuration; said target computer environment is used for business-critical applications execution, wherein at least one of said modules performs a method comprising: cc-1) recipients table search for remote function calls and other interfaces for application services associated with said targeted environment; cc-2) search of journal files with applications for said targeted environment; cc-3) determining of connections between different systems related to said targeted environment based on found recipients tables and journal files; cc-4) graphic display of determined connections; cc-5) provision of formed grafic display of determined connections to a user.

EFFECT: invention provides effective computer

systems security. 9 cl, 4 dwg




ФИГ. 2

RU 2657170 C2

RU 2657170 C2

ОБЛАСТЬ ТЕХНИКИ

Настоящее изобретение в целом относится к безопасности компьютерных систем и, в частности, к автоматизированной оценке безопасности систем и ресурсов, определяющих для ведения бизнеса.

УРОВЕНЬ ТЕХНИКИ

В настоящее время большинство средних и крупных предприятий мира в управлении ключевыми бизнес-процессами полагаются на информационные системы.

Примерами такого типа систем являются комплексные решения, известные как EnterpriseResourcePlanning (ERP) ("Планирование ресурсов предприятия (ПРП)"), CustomerRelationshipManagement (CRM) ("Управление взаимоотношениями с клиентом"), SupplierRelationshipManagement (SRM) ("Управление связями с поставщиками"), SiipplyChainManagement (SCM) ("Управление системой поставок (логистика)"), ProductLife-cycleManagement (PLM) ("Управление жизненным циклом продукта"), HumanCapitalManagement (HCM) ("Управление персоналом"), Businesslntelligence (BI) ["Интеллектуальные ресурсы (корпоративный интеллект)", бывшая BusinessWarehouse (BW) - создание корпоративных хранилищ данных и их анализ)], интеграционные платформы и т.п.

Признанными в промышленности программными продуктами в этой области являются разработки на базе SAP NetWeaver и платформа SAP R/3, программный комплекс OracleE-BusinessSuite, JDEdwardsEnterpriseOne, PeopleSoft, Siebel и MicrosoftDynamics.

Этим программным обеспечением в мире пользуется большинство членов списка "Fortune 100" и крупные правительственные организации.

Только SAP [немецкая компания SAP AC (нем. Systemanalyse und Progrummentwickliing, англ. System Analysis and Program Development, рус. Системный анализ и разработка программ) - разработчик и производитель ПО для бизнеса] имеет более 90000 пользователей более чем в 120 странах.

Такие системы ответственны за обработку закрытой деловой информации и управление ключевыми процессами организации, такими как снабжение, выписывание счетов-фактур и накладных, финансовое планирование, производство, ведение платежных ведомостей, и т.п. Следовательно, вопросы конфиденциальности, достоверности и доступа к этой информации являются определяющими для безопасной и бесперебойно работы бизнеса.

Концепция архитектуры подобной критической для ведения бизнеса системы, представленная в данном документе, отражена на фигуре I.

До настоящего времени оценка безопасности таких систем осуществлялась, в основном, на двух уровнях: функциональном [21] и базовом. На функциональном (оперативном) уровне [21] в большинстве случаев решения направлены на предотвращение нарушения разделения обязанностей. При таком подходе разрабатывают комплексную матрицу несовместимых бизнес-функций и вводят ее в систему для обеспечения автоматизированного санкционирования. С другой стороны, разработки на базовом уровне, главным образом, направлены на определение уязвимых мест в системе безопасности базовой операционной системы [24] и базы данных [23].

В то время как этот вид оценки безопасности безусловно важен, было замечено, что сфера защиты и контроля до сих пор упускала из виду основной источник риска: безопасность технологических компонентов этих систем [22].

Каждый из этих прикладных комплексов разрабатывается на базе оригинальных (а также общедоступных) рабочих платформ, целевых протоколов и архитектур

безопасности.

В силу сложности проведения надлежащего анализа и оценки этого уровня защиты в сочетании с нехваткой систематизированной общедоступной информации на эту тему должная защищенность здесь, как правило, остается без внимания, как на стадии осуществления, так и в ходе дальнейшего контроля безопасности систем.

Важно отметить, что, несмотря на отсутствие должного внимания, многие риски этого уровня более опасны, чем на функциональном уровне [21], в силу следующих причин:

кибервзломщик не обязательно должен иметь учетную запись пользователя в атакуемой системе, что увеличивает вероятность взлома;

так как большое количество кибератак совершается дистанционно и анонимно. отследить злоумышленника и место его локализации гораздо сложнее, чем обнаружить местных взломщиков;

для вторжения на функциональном уровне [21] необходимо хорошее знание бизнес-процессов и средств управления изнутри организации.

Взлом на технологическом уровне [22] выполняется автоматически, с использованием даже общедоступных средств в Интернете.

Как следует из практики экспертизы специальной безопасности пользователей по всему миру, более 95% проанализированных систем оказались уязвимыми для вредительства, шпионажа и злонамеренных атак из-за наличия рисков для информационной безопасности именно в технологических компонентах. Удивительно, что многие из этих систем прошли нормативную аттестацию на соответствие.

Следует также отметить, что за последние годы актуальность этой проблемы резко возросла. Об этом можно судить из соответствующих презентаций на международных конференциях по безопасности и роста числа выявляемых технически уязвимых элементов схем безопасности. Характерно, что количество ежегодно выпускаемых уведомлений о уязвимости компонентов SAP за последние годы увеличилось радикально - более, чем на 3800%, если сравнивать 2010 год с 2007.

Проведение такого объема всесторонней экспертизы в ручном режиме не реально с точки зрения оценки перспективных затрат в силу того, что аппаратная реализация этих систем может включать в себя от десятков до сотен прикладных серверов, каждый из которых отслеживает несколько аспектов безопасности, которые подлежать экспертизе.

В то же время в ряде подходов, например, в программном приложении "Самообслуживание в оптимизации безопасности SAP" сделана попытка автоматизировать некоторые операции тестирования, однако практическое значение этих подходов как профессиональных систем экспертизы и оценки безопасности утрачивается из-за предусмотренных в них предварительных технических условий, к числу которых относятся перечисленные ниже.

Выполнение изнутри самой системы SAP, что означает, что анализирующая система одновременно может являться анализируемой. Это противоречит основным принципам проведения экспертизы, согласно которым проверяющая и проверяемая системы должны быть разными для обеспечения добросовестности экспертизы и достоверности ее результатов.

Предыдущее условие выполнения тестирования изнутри системы SAP требует от пользователя подробного знания функционирования SAP для эффективного применения системы.

Ограничение возможностей отладки в соответствии с требованиями пользователя.

Пользователь не имеет возможности настроить тестирование мелкомодульных конфигураций и, следовательно, не может проверить систему па защищенность или соответствие тем или иным внешним или внутренним стратегиям.

Ограниченность набора тестируемых аспектов. Большинство тестов связано с контролем разделения обязанностей и анализом наиболее важных позиций машинной авторизации для назначенных пользователей. В силу этого многие установки системы безопасности игнорируются этим приложением при автоматической оценке, оставляя брешь для потенциальных злоумышленных воздействий.

Отсутствие поддержки платформ SAP Java. Данное приложение может быть применено только для проверки платформ SAPABAP.

Отсутствие функции обнаружения вслепую. Данное приложение способно тестировать только системы, сконфигурированные пользователем вручную. Это - крайне непрактично в объемных средах с сотнями или тысячами систем.

Отсутствие функции тестирования на уязвимость черных ящиков. Приложение предусматривает только тестирование на безопасность белых (прозрачных) ящиков.

Отсутствие функции визуализации степени риска. Приложение не предусматривает поддержку проводимого тестирования средствами наглядности распознаваемых рисков для безопасности.

Другие существующие в настоящее время автоматизированные программные комплексы безопасности не обладают надежными и перспективными существенными признаками, обеспечивающими идентификацию угроз защите решающих для ведения бизнеса прикладных программных средств, с комплексным подходом (соединяющим в себе анализ белого ящика, экспертизу черного ящика и наглядное представление рисков), следствием чего является недостаточное выявления существующих угроз и создание ложного ощущения безопасности в организациях, доверяющих таким системам.

Принимая во внимание рассмотренные выше недостатки, приходится констатировать наличие потребности в системах и способах автоматизированной оценки безопасности критических для бизнеса систем с позиций совершенно нового подхода, направленного на преодоление слабых сторон традиционных наборов средств.

## КРАТКОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Настоящее изобретение представляет системы и способы апробации системы защиты программных приложений в рамках новой инфраструктуры, обеспечивающей возможность автоматизированной экспертизы систем на безопасность и соответствие, выявления технически уязвимых мест системы безопасности и наглядного представления (визуализации) уровня соответствующих угроз защите основополагающего для предпринимательства ПО. Примерами подобных критических для ведения бизнеса программных продуктов являются: EnterpriseResourcePlanning (ERP) ("Планирование ресурсов предприятия (ПРП)"), CustomerRelationshipManagement (CRM) ("Управление взаимоотношениями с клиентом"), SupplierRelationshipManagement (SRM) ("Управление связями с поставщиками"), SupplyChainManagement (SCM) ("Управление системой поставок (логистика)"), ProductLife-cycleManagement (PLM) ("Управление жизненным ifUK.w.M продукта"), HumanCapitalManagement (HCM) ("Управление человеческим капиталом"), платформы интеграции, BusinessWarehouse (BW) ("Хранилище бизнес-информации")/ Businesslntelligence (B1) ("Интеллектуальные ресурсы (корпоративный интеллект) ")\\ интегрированные прикладные системы, разработанные SAP, Oracle, Microsoft, Siebel, JDEdwards и PeopleSoft.

Задачей заявляемого изобретения является сокращение рисков в предпринимательской сфере, связанных со злоумышленным использованием изъянов в защите информации,

приведение систем безопасности в соответствие с требованиями и снижение издержек по их экспертизе для организаций-пользователей основными программными средствами ведения бизнеса.

В представленном изобретении преодолены недостатки разработок известного уровня техники и предложена программа, выполняемая из обособленной вычислительной среды (с сервера) и предназначенная для удаленного тестирования безопасности технологических компонентов важнейших бизнес-приложений, основанных на различных подходах, и, следовательно, обеспечивающая комплексную оценку текущего уровня безопасности целевых систем.

Эти и другие результаты достигаются за счет введения компонента, который обеспечивает автоматизированное обнаружение, распознавание и структурирование критических для бизнеса систем в специализированной компьютерной сети.

Кроме того, в изобретении предложен модульный способ оценки безопасности, при котором модули выполняются строго в соответствии с заданным регламентом, обеспечивая благодаря этому состоятельность и безызбыточность результатов.

Эти и другие цели достигаются также за счет введения ряда специализированных модулей оценки рисков для безопасности специальной информации, исходящих от технологических компонентов ПО SAP.

Первым аспектом данного изобретения является комплекс автоматического тестирования, по меньшей мере, одной целевой (объектной) компьютерной среды на уязвимость ее системы безопасности, в состав которого интегрированы:

- подсистема ядра, ответственная за хранение данных о факторах уязвимости и конфигурациях системы безопасности, но меньшей мере. одной целевой компьютерной системы или сети компьютерных систем;

- по меньшей мере, одна подсистема сканирования, взаимодействующая с указанной подсистемой ядра ОС, включающая в себя в качестве субкомпонентов:

- идентификатор системы, оценивающий ресурсы названной, по меньшей мере, одной целевой компьютерной системы;

- множество модулей тестирования и диагностики для автоматического обследования ресурсов названной, по меньшей мере, одной целевой компьютерной системы и для нахождения слабых мест таких ресурсов;

- интеллектуальный диспетчер запуска, но меньшей мере, одного из названных модулей тестирования и диагностики в зависимости от конфигурации указанного модуля; при этом названная, по меньшей мере, одна целевая компьютерная система выполняет основополагающие бизнес-приложения.

Вторым аспектом данного изобретения является способ нахождения уязвимых мест в системе безопасности вычислительных сетей или компьютерных систем, включающий в себя:

a) определение адресов, по меньшей мере, одного объекта тестирования на уязвимость системы безопасности, который имеет в своем составе, по меньшей мере, одну из вычислительных сетей, компьютерные системы и компьютерные сис1емы в составе названных вычислительных сетей;

b) определение адресов ресурсов, по меньшей мере, одного объекта;

c) определение характеристик названных ресурсов;

d) выбор, по меньшей мере, одного модуля тестирования или диагностики для каждого ресурса исходя из характеристик, определенных на шаге c);

e) выполнение, по меньшей мере, одного названного выбранного на шаге d) модуля тестирования или диагностики для каждого ресурса, при этом выбранный, по меньшей

мере, один модуль тестирования или диагностики имеет конфигурацию, соответствующую характеристикам названного ресурса, для которого выбран данный модуль тестирования или диагностики;

f) получение данных от названного, по меньшей мере, одного модуля тестирования или диагностики, выполненного на шаге c);

g) оценка уязвимых мест системы безопасности названного, по меньшей мере, одного объекта, исходя из данных, полученных на шаге f).

Другим аспектом изобретения является система автоматического нахождения уязвимых мест защиты вычислительных сетей или компьютерных систем, включающая в свой состав:

- подсистему ядра ОС, ответственную за хранение данных о факторах уязвимости и конфигурациях системы безопасности, по меньшей мере, одной целевой компьютерной системы или сети компьютерных систем;

- подсистему сканирования, взаимодействующую с указанной подсистемой ядра ОС, интегрирующую:

- модуль идентификатора системы для обнаружения и распознавания названной, по меньшей мере, одной целевой компьютерной системы или сети и ее соответствующих ресурсов;

- модуль интеллектуального диспетчера, запускающий, по меньшей мере, один модуль тестирования или диагностики, исходя из характеристик, по меньшей мере, одного соответствующего ресурса, обнаруженного и распознанного названным модулем идентификатора системы;

- по меньшей мере, один модуль тестирования и диагностики для автоматического обследования и оценки уязвимости названного, по меньшей мере, одного соответствующего ресурса, при этом названным, по меньшей мере, одним модулем тестирования и диагностики управляет указанный модуль интеллектуального диспетчера, и при этом конфигурации системы безопасности обозначенного объекта вводятся в базу данных, при чем, названные модули выполняются на основе указанных данных обозначенной базы данных.

Еще одним аспектом изобретения является способ оценки конфигурации системы безопасности целевой компьютерной среды, включающий в себя:

a) сканирование идентифицированных IP-адресов и портов;

b) "дактилоскопирование" (снятие отпечатков пользования) выявленных открытых портов для распознавания исполняемых через них сервисов;

c) определение активности названной целевой системы;

d) обращение к базе модулей и выполнение, по меньшей мере, одного из таких модулей, предназначенных для нахождения уязвимых мест в системе безопасности, доступных через указанные IP-адреса и порты; при этом

- обозначенный, по меньшей мере, один модуль выполняется исходя из его конфигурации;

- обозначенная целевая компьютерная среда используется для выполнения основополагающих бизнес-приложений.

## КРАТКОЕ ОПИСАНИЕ ФИГУР

Существенные признаки и преимущества изобретения более наглядно представлены в подробном описании со ссылкой на прилагаемые фигуры, где: фигура 1 представляет собой блок-схему возможной архитектуры реализации критических для бизнеса комплексов в соответствии с заявляемым изобретением; фигура 2 представляет собой структурную схему возможной компоновки комплекса в соответствии с одним из

аспектов изобретения; фигура отображает фрагмент рабочего экрана пользовательского интерфейса согласно одному из аспектов изобретения; фигура 4 отображает фрагмент рабочего экрана при сеансе поэлементного тестирования системы безопасности в соответствии с одним из аспектов изобретения.

## ПОДРОБНОЕ ОПИСАНИЕ ИЗОБРЕТЕНИЯ

Заявляемые система и способ представляют собой инфраструктуру автоматизированной экспертизы важнейших бизнес-приложений на безопасность и соответствие, выявление технически уязвимых мест системы защиты и наглядного представления уровня соответствующих угроз такой защите. Примерами критических, те основополагающих, для бизнеса прикладных программ являются ERP, CRM, HCM, SRM, SCM, интерфейсные системы и платформы интегрированной среды, разработанные компаниями SAP, Oracle, Microsoft, Siebel, JDEdwards и PeopleSoft.

Данное изобретение состоит из 4 основных логических компонентов: пользовательского интерфейса, ядра ОС, механизма сканирования и модулей. В целом и как подробнее описано ниже, пользователь через пользовательский интерфейс задает конфигурацию целевой системы, подлежащей экспертной оценке, выбирает модули, которые он хочет выполнить, запускает или составляет маршрутную карту экспертизы и получает подробный отчет о выявленных угрозах безопасности. При этом пользовательский интерфейс не является необходимым компонентом для практической реализации изобретения. Остальные компоненты предусматривают автоматическое и автономное от пользователя функционирование.

Предпочтительный вариант осуществления изобретения представляет собой программное приложение, выполняемое в операционных системах (ОС) MicrosoftWindows, UNIX/Linux или MacOSX. Пользователи обращаются к этой программе посредством различных типов интерфейса через Интернет или с рабочего стола. Программа через удаленное соединение с целевыми системами выполняет запрашиваемые операции тестирования. Результаты оценки сохраняются в централизованной базе данных сервера программы.

Возможен вариант технического решения, при котором соответствующая информация о безопасности целевой системы извлекается и вводится в базу данных. Запрашиваемые действия по экспертизе осуществляются согласно информации репозитория базы данных.

В другом варианте решения изобретения на центральном сервере реализуют только пользовательский интерфейс и ядро программы, в то время как механизм сканирования и модули выполняются в операционной системе объектного компьютера. Ядро выдает сканирующему механизму инструкции, какие действия необходимо выполнять в целевой системе. Механизм сканирования выполняет заданные модули локально и возвращает результаты в ядро, где они сохраняются и позже обрабатываются его субкомпонентами.

Еще одна версия исполнения настоящего изобретения предусматривает работу пользовательского интерфейса и ядра программы на центральном сервере, а функционирование сканирующего механизма и выполнение модулей - на промежуточном сервере. Ядро выдает сканирующему механизму инструкции, какие действия необходимо выполнять в целевой системе. Механизм сканирования выполняет заданные модули дистанционно и возвращает результаты в ядро, где они вводятся в память и в дальнейшем обрабатываются его субкомпонентами.

Притом что представленное описание рассматривает архитектуру, базирующуюся на указанных четырех основных компонентах, важно понимать, что другие технические решения по этому изобретению могут включать в себя группирование или дальнейшее разделение функций каждого компонента между различными элементами в ином наборе

и иной компоновке.

АРХИТЕКТУРА

Как сказано выше, настоящее изобретение преимущественно воплощено в четырех основных компонентах: пользовательском интерфейсе, ядре, механизме сканирования и модулях. В свою очередь, эти компоненты состоят из ряда субкомпонентов, ответственных за выполнение в приложении специфических функций. Они представлены на фигуре 2 и детализированы в соответствующих разделах далее.

Для лучшего понимания следующих разделов необходимо пояснить, какие элементы среды задействованы в процессе:

Ландшафт/группа активов (ресурсов): произвольная группа систем/активов и/или компонентов, идентифицируемых по имени, заданному пользователем.

Система/актив: группа компонентов. Компоненты представляют систему критически важной для бизнеса среды и идентифицируются по имени.

Компонент: группа соединительных элементов. Соединительные элементы (коннекторы) представляют такие обособленные компоненты системы/активов, как сервер приложений или сервер базы данных и т.п.Они идентифицируются по имени и специфическим свойствам.

Соединительный элемент: интерфейс с определенным сервисом компонента. Соединительные элементы создаются автоматически в ходе процедуры обнаружения или вручную пользователем. Соединительные элементы идентифицируются по их специфическим свойствам.

ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

Интерфейс пользователя (User-Interface) [01] - это средство взаимодействия пользователей с программным приложением. Такое взаимодействие в основном состоит в выборе и конфигурировании заданий, выборе модулей для выполнения, запуске или планировании сеанса и рассмотрении и сохранении генерируемых отчетов. Кроме того, пользователь может выбрать регламент проведения специальных сессий с помощью специализированного программного "мастера" (Wizard) [08] {DiscoveryandExploration ("Выявление и анализ"). Audit&Compliance ("Экспертиза и соответствие"), VulnerabilityAssessment ("Оценка уязвимости"), BizRiskIllustration ("Наглядное представление бизнес-рисков")}, который автоматизирует и упрощает многие процедуры приложения в конфигурации, относящейся к изобретению, для неопытных пользователей.

Целевую конфигурацию строят с помощью "Менеджера ландшафта" (LandscapeManager) [20] (см. фигуру 3).С помощью этого подкомпонента пользователь может выбирать между заданием каждой целевой конфигурации вручную или автоматическим поиском существующих систем в предоставленном диапазоне адреса сетевого протокола IP. Такой автоматический поиск выполняет подкомпонент "Идентификатор системы" (Systemldentifier) [09] механизма сканирования (ScanEngine) [02]. Этот подкомпонент описан в специальном разделе дальше. Конфигурации ландшафта сохраняются в субкомпоненте "репозиторий конфигураций" (ConfigurationRepository) [15].

Если пользователю необходим специальный набор и конфигурация модулей для дальнейших (и, возможно, многократных) сессий, он может это сделать, взаимодействуя с субкомпонентом "менеджер политики (денариев)" (PolicyManager) [Об]. Посредством этого субкомпонента осуществляется доступ пользователя ко всем возможным модулям/категориям модулей. Пользователь может выбирать и задавать варианты конфигураций модулей, сохраняя их затем как сценарии, идентифицируемые по уникальным именам.

Пользовательский интерфейс может быть реализован в различных аппаратных

версиях в зависимости от назначения. Например, настольный графический интерфейс пользователя лучше всего подходит для обеспечения доступа к установкам одиночного пользователя. Возможно также техническое решение интерфейса на веб-основе для обеспечения доступа к централизованным вычислительным средам на крупных предприятиях с множеством пользователей, обращающихся к приложению из множества локализаций. В другом варианте компоновки предусмотрен неинтерактивный интерфейс с веб-поддержкой для обеспечения взаимодействия с приложениями и системами третьей стороны.

При использовании интерактивного интерфейса пользователя (UI) приложение будет выдавать результаты сессии (сеанса) через субкомпонент "менеджер сессии" (SessionManager) [05]. Этот подкомпонент выводит информацию о сеансе, когда субкомпонент задействован. Выходные данные сессии могут включать в себя информацию о обнаруженных угрозах безопасности в каждом компоненте проанализированных ландшафтов, о состоянии выполняемого модуля, о времени прохождения сеанса, сообщения модуля, сообщения ядра, предупреждения и сообщения отладки. На фигуре 4 дан пример отображения на экране дисплея типовой информации по такой сессии.

По завершении сеанса пользователь может обратиться к субкомпоненту "менеджер отчетов" (ReportManager) [07]. Этот подкомпонент пользовательского интерфейса взаимодействует с генератором отчетов (ReportGenerator) [13] для извлечения содержания сгенерированных отчетов. Пользователь может получить различные виды отчетов. Пользователь может выбрать различные отчеты для анализа или сохранить их во внешний файл локальной файловой системы. Поддерживаются файловые форматы PDF, XML, HTML, DOC, XLS, CSV и другие.

ЯДРО

Этот компонент [03] отвечает за несколько функций в приложении.

Субкомпонент "репозиторий данных" (DataRepository) [12] хранит информацию, относящуюся к описаниям факторов уязвимости, к данным модулей и наборов запросов SQL для каждой поддерживаемой базы данных. Вся информация, хранящаяся в репозиториях, локализована. Благодаря этому приложение совместимо со множеством языков. В предпочтительном варианте репозиторий выполнен как локальная реляционная база данных.

Субкомпонент "репозиторий конфигураций" (ConfigurationRepository) [15] хранит в памяти информацию о конфигурациях ландшафта, сценарии, параметры конфигураций ядра и статистические данные.Эта информация выборочно извлекается и сохраняется другими компонентами приложения. В предпочтительном варианте репозиторий выполнен как локальная реляционная база данных.

Субкомпонент "генератор отчетов" (ReportGenerator) [13] формирует на выходе отчет о завершенном сеансе. Этот подкомпонент извлекает необходимую информацию из базы знаний (K-nowledgeBase) [14]. Данный субкомпонент генерирует строку, содержащую всю информацию сеанса, в формате XML или в других открытых или патентованных форматах. Строка может быть интерпретирована другими компонентами данного приложения или приложениями третьей стороны.

МЕХАНИЗМ СКАНИРОВАНИЯ

Субкомпонент "идентификатор систем" (Systemldentifier) [09] автоматически обнаруживает, распознает и упорядочивает основные бизнес-системы, присутствующие в вычислительной сети. Соответствующая процедура запускается, когда в субкомпонент вводят базовое имя ландшафта (Landscapename), комплект адреса IP и/или имен хостов

(адресатов), набор портов для сканирования (ports_to_scan) и опции поиска. IP-адреса могут быть указаны индивидуально или в пределах диапазонов. Опции поиска могут включать в себя: проверку активности адресатов, "дактилоскопирование" (снятие идентифицирующих следов пользования) обнаруженных открытых портов для распознавания скрытых сервисов с низкой частотностью ложных допусков, попытку автоматического распознавания и упорядочения систем, а также другие опции.

Для каждого адресата субкомпонент может выполнять описанные ниже действия.

1. Определять активность целевой системы, если задействована соответствующая опция. Эта функция реализуется путем направления запросов 1CMP (межсетевого протокола управления сообщениями) и/или пакетов TCP (протокола управления передачей) в определенные порты целевой системы, обычно выделяемые для поддерживаемых критически важных для бизнеса прикладных программ.

2. Сканировать каждый из портов протоколов TCP и UDP (протокола пользовательских дейтаграмм) целевой системы, заданных в ports_to_scan как открытые, закрытые и имеющие фильтр.

3. Если задействована соответствующая опция, пересылать все образцы идентификационных признаков, находящихся в "базе дактилоскопических данных" (базе идентификационных признаков пользования) (FingerprintDatabase) [11], в каждый обнаруженный порт с открытым доступом и анализировать генерируемые отклики. Если принятые отклики соответствуют ожидаемой реакции, сервис успешно идентифицирован. В противоположном случае сервис маркируется как "неопознанный". Каждый сервис, маркированный как "опознанный", проверяется на соответствие ему какого-либо из соединительных элементов приложения. Если опознанному сервису соответствует соединительный элемент приложения, для этого сервиса этой целевой системы создается новый соединительный элемент.

4. Если задействована опция автоматического распознавания и упорядочения систем, выполняется специальная процедура, описанная ниже.

Исходя из перечня соединительных элементов процесс идентификации включает в себя следующие шаги:

Каждый соединительный элемент присваивается определенному компоненту. Если у данного соединительного элемента еще нет компонента, такой компонент создается. В ином случае соединительный элемент присваивается существующему компоненту.

Каждый соединительный элемент содержит полные сведения о сервисе, с которым он соединяет, и пытается идентифицировать "имя системы" (SystemName) компонента, которому он присвоен. Это осуществляется путем послания целевой системе отличительных для данного сервиса тестовых сообщений. Если соединительный элемент успешно распознает имя системы, то в результате процесса идентификации данный компонент присоединяется к соответствующей системе.

Если соединительный элемент не может распознать имя системы, соблюдаются определенные правила:

Если компонент соединительного элемента уже существует, а другой соединительный элемент, относящийся к тому же самому компоненту, смог распознать имя системы, то данное имя соотносится с данной системой.

При наличии компонента-брата (относящегося к этой же системе) системе задается имя но этому компоненту.

Если соединительный элемент не определяет имя системы, может быть применен метод проверки специального имени системы. После идентификации всех возможных системных имен процесс переходит к проверке каждого неопознанного соединительного

элемента на способность определения достоверности выявленного имени системы.

Этот компонент возвращается к древовидному отображению, как на фигуре 3, иерархической структуры каждого сформированного ландшафта. Когда выявлены доступные порты и IP-адреса, могут быть запущены различные модули оценки конфигурации, параметров и настроек целевой системы.

Субкомпонент "база дактилоскопических данных" (FingerprintDatabase) [11] содержит в памяти набор тестовых сообщений (запросов сети) для каждого поддерживаемого коннектора, а также ожидаемые отклики (представленные в виде регулярных выражений или посредством эквивалентного механизма) на каждое тестовое сообщение. Этот репозиторий используется, главным образом, субкомпонентом "идентификатор систем" (Systemldentifier) [09] для анализа выявленных открытых портов известных сервисов.

Одной из задач, встающих при оценке безопасности системы SAP в режиме "черного ящика", является область проверки: некоторые проверки затрагивают систему в целом, часть проверок применяется лишь на элементном уровне, а другие - на уровне соединительного элемента. Без учета этого аспекта выполнение каждого модуля для каждого совместимого соединительного элемента привело бы к генерации избыточной информации и увеличению времени оценки.

Для решения этой задачи в настоящем изобретении реализован интеллектуальный диспетчер модулей (ModuleIntelligentDispatcher) [10], который учитывает область применения модулей (определяемую для каждого из модулей) и выполняет их согласно следующей процедуре:

Если областью применения модуля является СИСТЕМА, то диспетчер запускает этот модуль для всех совместимых соединительных элементов целевой системы до тех пор, пока он не будет успешно выполнен. Это означает, что модуль может быть успешно выполнен только один раз для каждой системы данного ландшафта.

Если областью применения модуля является КОМПОНЕНТ, то диспетчер запускает этот модуль для всех совместимых соединительных элементов целевого компонента до тех пор, пока он не будет успешно выполнен. Это означает, что модуль может быть успешно выполнен только один раз для каждого компонента данной системы.

Если областью применения модуля является СОЕДИНИТЕЛЬНЫЙ ЭЛЕМЕНТ, то диспетчер запускает этот модуль для всех совместимых соединительных элементов. Это означает, что модуль может быть выполнен только один раз для каждого коннектора.

Эта относящаяся к изобретению процедура обеспечивает надлежащую оценку каждого ландшафта/системы/компонента/коннектора при отсутствии избыточности генерируемой информации.

Субкомпонент "база знаний" [14] выполняет функции репозитория для хранения всей информации, выработанной в ходе сеанса сканирования. Эта информация содержит данные оцененных адресатов, использованных сценариев модулей, состояния выполнения модулей и выведенные результаты. Эта информация включает в себя базовые данные для генерации отчета, а также выполняет еще одну важную функцию: обеспечивает разделение данных между модулями во время сессии. Каждый генерируемый модулем результат сохраняется в базе знаний [14] под определенным ключом. Таким образом, любой исполняемый модуль может запросить информацию из базы знаний [14] с помощью соответствующего ключа. Это способствует формированию связанных модулей и имитирует некоторые ручные настройки, при которых информация, полученная через определенные точки доступа, может быть использован для других точек.

Модули

Модули [04] представляют собой элементы, выполняющие обусловленные действия или функции в отношении целевых систем. Как показано на фигуре 2, модули могут относиться к одной из 3 категорий: выявление и анализ, экспертиза и оценка уязвимости или наглядное представление рисков. Каждый модуль также входит в обособленный пакет знаний (в котором сгруппированы модули, совместимые с одни и тем же видом критически важного бизнес-приложения). Примерами пакетов знаний являются: пакет знаний для SAP NetWeaver и R/3, пакет знаний для Oracle и пакет знаний для Microsoft.

В силу того, что критически важные программные бизнес-приложения состоят из нескольких компонентов, каждый со своим интерфейсом, протоколами и параметрами защиты, для каждого компонента разработан набор модулей, выполняющих определенные функции, что описано в разделе: Процедуры обнаружения, анализа, распознавания уязвимости и наглядного представления рисков для безопасности интерфейса RFC прикладных серверов SAP (RFCInterfaceo/SAPApplicationServers)

Автоматизированная проверка внешнего сервера запроса инструкций RFC на поддержку программы SAPXPG:

Эта проверка осуществляется путем соединения с внешним сервером RFC и вызова функции RFC_DOCU. Если отклик содержит функции, начинающиеся с имени "SAPXPG", сервер распознается как поддерживающий SA.PXPG(SAPX/OpenPortabilityGuide=сборник стандартов по открытым системам SAP, сертифицированных компанией X/Open).

Другие процедуры включают в себя попытки выполнения функций SAPXPG_START_XPG или SAPXPG_START_XPG_LONG и проверку успешности их выполнения.

Автоматизированная проверка возможности запуска внешних серверов RFC через межсетевой шлюз SAP

На основе параметра tpnames, заданного пользователем в опциях модуля, модуль соединяется с адресным шлюзом SAP и пытается запустить сервер RFC в заданном tphost. Модуль сообщает в ответ, какое из имен tpnames (при наличии) может быть запущено в указанном хосте tphost через целевой межсетевой шлюз SAP.

При этом данный модуль осуществляет следующий способ:

a) модуль принимает от пользователя, по меньшей мере, один идентификатор программы;

b) для каждого идентификатора программы модуль выполняет:

b1) соединение со шлюзом для целевой системы,

b2) попытку инициации определенного сервера, ассоциированного с программным идентификатором хоста для программы, идентифицированной идентификатором программы;

c) модуль определяет, какие программы, ассоциированные с идентификаторами программ, могут быть инициированы на основании результата шага b1) для каждого программного идентификатора.

Обработка в интерактивном режиме и направление вызовов функции RFC серверам приложений SAP

Данный модуль предоставляет графический интерфейс пользователя для формирования и пересылки запросов RFC партнеру по RFC без необходимости задействования системы SAP. После указания системы назначения параметров доступа и выполняемого функционального модуля модуль устанавливает связь с удаленной стороной и получает требуемые параметры и таблицы, заявленные функциональным модулем в его интерфейсе. Затем, пользователь может задать конфигурацию каждого

параметра и выполнить вызов функции. Результаты обрабатываются модулем и графически представляются пользователю.

Автоматизированный анализ безопасности адресатов RFC

Модуль получает RFCDES (запрошенные инструкции RFC no стандарту кодирования данных DES) или таблицу пересчета от сервера приложений SAP и анализирует их содержимое, выдавая отчет об угрозах безопасности, исходящих от существующих связей с хранящимися в памяти учетными записями, доверительными отношениями и незакодированными интерфейсами.

Графическое отображение интерфейсов входящих/исходящих соединений в системах SAP

Модуль получает RFCDES или таблицу пересчета и журнальные файлы уровня приложений от каждого сервера приложений SAP и анализирует их содержимое, графически представляя связи между различными системами SAP и с внешними системами таким образом, чтобы пользователь мог быстро определить, какие связи могут представлять риск для защиты используемого приложения. Информация по каждой связи представлена в виде диаграммы.

Таким образом, этот модуль осуществляет способ, в котором модуль:

a) находит таблицы адресатов для удаленных обращений к функциям и других интерфейсов серверов приложений, ассоциированных с целевой системой;

b) находит журнальные файлы приложений для целевой системы;

c) устанавливает связи между различными системами, связанными с целевой системой на базе таблиц адресатов и журнальных файлов;

d) графически отображает такие связи;

e) предоставляет пользователю графическое отображение разнообразных связей.

Автоматизированная оценка защиты файла reginfo

Модуль получает содержимое файла reginfo или с помощью специальных функциональных модулей RFC, или путем извлечения файла из файловой системы сервера приложений, открывая доступ к файлу, сконфигурированному в параметрах профиля gw/reg_info.

Модуль построчно анализирует этот файл и сообщает о риске для безопасности при наличии любого из следующих условий:

если файл не существует;

если строка не содержит параметр TP, или параметр TP содержит *;

если строка не содержит параметр HOST, или параметр HOST содержит *;

если строка не содержит параметр N0, или параметр N0 содержит *;

если строка не содержит параметр ACCESS, или параметр ACCESS содержит *.

если строка не содержит параметр CANCEL, или параметр CANCEL содержит *.

При наличии любого другого сочетания заданных/возможных параметров, которое могло бы привести к риску для безопасности сервера или системы приложений.

Автоматизированная оценка безопасности файла secinfo Модуль получает содержимое файла secinfo или с помощью специальных функциональных модулей RFC, или путем извлечения файла из файловой системы сервера приложений, открывая доступ к файлу, сконфигурированному в параметрах профиля gw/secJnfo.

Затем, модуль построчно анализирует этот файл и сообщает о риске для безопасности при наличии любого из следующих условий:

если файл не существует;

если строка не содержит параметр USER, или параметр USER содержит *.

если строка не содержит параметр PWD, или параметр PWD содержит *.

если строка не содержит параметр USER-HOST, или параметр USER-HOST содержит *.

если строка не содержит параметр HOST, или параметр HOST содержит *;

если строка не содержит параметр TP, или параметр TP содержит *;

При наличии любого другого сочетания заданных/возможных параметров, которое могло бы привести к риску для безопасности сервера или системы приложений.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядного представления рисков для безопасности компонента SAProuter

Автоматизированный анализ таблицы маршрутизации доступа SAProuter в режиме "черного ящика"

Пользователь конкретизирует перечень диапазонов IP и портов для тестирования. Модуль проверяет соединение с каждым заданным сочетанием IP и порта через целевой маршрутизатор SAProuter. Модуль оценивает сообщения, генерируемые маршрутизатором SAProuter. Если в ответном сообщении SAProuter содержится отказ на протрассированное соединение, соединение по этому маршруту обозначается как невыполнимое. В противоположном случае соединение обозначается как успешное. В отчете модуля содержится указание на состояние всех выполненных соединений и оценка рисков по ним.

Точнее говоря, этот модуль осуществляет способ, где модуль:

a) принимает от пользователя диапазоны адресов IP и порты;

b) выполняет пробное соединение с каждой из комбинаций IP-адреса и порта, взятых из диапазонов адресов IP и портов из п. a), через программный маршрутизатор, ассоциированный с целевой системой:

c) определяет соединение (в котором задействована определенная комбинация IP-адреса и порта) как успешное, если программный маршрутизатор не отвечает отказом на попытку соединения с использованием данного сочетания IP-адреса и порта;

d) формирует пользовательский перечень прошедших и отклоненных соединений.

Автоматизированный анализ таблицы маршрутизации доступа SAProuter в режиме "белого (прозрачного) ящика"

Данный модуль выполняет анализ файла Таблицы маршрутизации доступа SAProuter, Это - файл открытого текста, где одна строка составляет одну запись. Модуль анализирует каждую запись и сообщает о рисках для безопасности при наличии следующих условий:

если оцененная запись - P * * * или P * * * *,

если оцененная запись - S * * * или S * * * *,

если оцененная запись - KP * * * или KP * * * *,

если оцененная запись - KS * * * или KS * * * *,

если оцененная запись начинается с KT и содержит * в параметре<src-host>,

если оцененная запись содержит * в параметре<source-host>,

если оцененная запись содержит * в параметре<dest-host>,

если оцененная запись содержит * в параметре<dest-serv>,

если оцененная запись содержит * в параметре<password>,

если оцененная запись содержит 22 в параметре<dest-serv>,

если оцененная запись содержит 23 в параметре<dest-serv>,

если оцененная запись содержит 80 в параметре<dest-serv>,

если оцененная запись содержит 1503 в параметре<dest-serv>,

если оцененная запись содержит 5601 в параметре<dest-serv>,

если оцененная запись содержит 1527 в параметре<dest-serv>,

если оцененная запись содержит 1433 в параметре<dest-serv>,

если оцененная запись содержит другой, отличный от SAP, сервис в параметре<dest-serv>,

если оцененная запись начинается с "P", a<dest-srv>является сервисом приложения SAP,

последняя запись не равна D * * * *.

При наличии любого другого сочетания заданных/возможных параметров, которое могло бы привести к риску для безопасности программного приложения.

Автоматизированный поиск информации от удаленного маршрутизатора SAProuter Модуль создает сетевой пакет запроса информации и отправляет его целевому SAProuter. Если связь прошла, модуль представляет информацию, полученную от адресата.

Автоматизированный анализ в режиме "черного ящика" возможности маршрутизации локальных протоколов посредством SAProuter

Пользователь задает этому модулю диапазоны IP и порты для тестирования. Модуль проверяет соединение с каждой заданной комбинацией IP и порта через целевой маршрутизатор SAProuter, активируя специальный флажок в пакете N1, обозначающий, что в запросе использованы локальные протоколы (регламентирующие взаимодействие данной конкретной среды). Модуль оценивает сообщения, генерируемые маршрутизатором SAProuter. Если в ответном сообщении SAProuter содержится отказ на протрассированное соединение, соединение по этому маршруту обозначается как невыполнимое. В противоположном случае соединение обозначается как успешное. В отчете модуля содержится указание на состояние всех выполненных соединений и оценка рисков по ним.

Модуль выполняет следующие шаги:

a) принимает от пользователя диапазоны адресов IP и порты;

b) выполняет пробное соединение с каждой из комбинаций IP-адреса и порта (из диапазонов адресов IP и портов, принятых от пользователя), через программный маршрутизатор, ассоциированный с целевой системой. Эти соединения с программным маршрутизатором выполняются с установлением специальных маркеров использования локальных протоколов;

c) затем модуль определяет, было ли успешным соединение (представляющее специальную комбинацию IP-адреса и порта), если программный маршрутизатор не отвечает отказом на попытку подключения с использованием этой конкретной комбинации IP-адреса и порта;

d) после попыток связи по всем возможным комбинациям адресов IP и портов по перечню шага a) модуль выдает пользователю листинг успешных и неуспешных соединений.

Способ маршрутизации программ локальной сети посредством SAProuters Модуль создает локальную конечную точку, состоящую из прокси или виртуального интерфейса протокола SOCKS, и второй компонент, состоящий из транслятора протокола SAProuter. Пользователь соединяется с локальной конечной точкой, используя сетевое ПО. Сетевой трафик проходит от локальной конечной точки к транслятору протокола SAProuter, который пакетирует его в совместимые с SAProuter пакеты N1 (сетевой информации) и отправляет их целевому SAProuter. Принимается ответ и выполняется обратный процесс. Транслятор протокола SAProuter распаковывает ответ N1 и передает его в локальную конечную точку, которая, в свою очередь, возвращает его к исходному сетевому ПО. Функция модуля может быть выражена как способ, где модуль:

a) создает конечную точку, имеющую прокси-сервер и транслятор протоколов;

(Транслятор протоколов преобразует протоколы, ассоциированные с целевой системой и ее программными маршрутизаторами.)

b) принимает исходящий сетевой трафик от сетевого ПО, соединенного с указанной конечной точкой;

c) направляет исходящий сетевой трафик на транслятор протокола;

d) упаковывает с помощью транслятора протокола исходящий сетевой трафик в исходящие пакеты, совместимые с программными маршрутизаторами целевой системы;

e) направляет исходящие пакеты на программные маршрутизаторы целевой системы;

f) получает входящие пакеты от программных маршрутизаторов;

g) отправляет входящие пакеты на транслятор протоколов;

h) распаковывает входящие пакеты во входящий сетевой трафик; и

i) вперед входящий сетевой трафик сетевому программному обеспечению.

Автоматизированный анализ параметров инициализации SAProuter Модуль получает на входе строку команды, используемую для запуска программы SAProuter. Модуль сообщает о риске для безопасности при обнаружении следующих условий:

строка команды не содержит аргумент "-G".

строка команды не содержит аргумент "-Y 0".

строка команды не содержит аргумент "-Z".

любое другое сочетание заданных возможных параметров, способное создать угрозу безопасности программного приложения.

Автоматизированное использование уязвимостей в качестве контрсредств в SAPRouter Данный модуль использует выявленные уязвимости в качестве контрсредств в компонентах маршрутизатора SAProuter. В зависимости от выявленного фактора уязвимости модуль посылает специальный сетевой запрос целевой системе. Это позволяет пользователю предпринять действия по защите целевой системы.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядное представление рисков для безопасности в компоненте SAPJntcrnetCommunicationManager ("менеджер коммуникации с Интернетом" SAP).

Автоматизированный анализ состояния сервисов ICM/ICF(сервисов "менеджера коммуникации с Интернетом" / функции преобразования информации) в режиме черного ящика

Данный модуль снабжен файлом базы данных, содержащей сводный список существующих сервисов ICM/ICF (сервисов, внесенных в перечень посредством трансакции SICF). Выделив сервис в базе данных, модуль соединяется с адресным сервисом ICM и отправляет запрос HTTP(S) GET/HEAD идентификатора ресурса (URL) данного сервиса. Модуль анализирует синтаксис ответа HTTP(S), сгенерированный сервером, и в соответствии с HTTP-кодом состояния выдает отчет о состоянии этого сервиса по следующим критериям:

Если код состояния находится в диапазоне 200-299, сервис расценивается как "доступный".

Если код состояния - 401, сервис расценивается как "пользователь не уполномочен".

Если код состояния находится в диапазоне 500-599, сервис расценивается как "отчет об ошибке".

Если код состояния - другой, сервис расценивается как "не доступен".

Данный модуль осуществляет способ, описываемый следующими шагами:

a) получение реестра существующих сервисов целевой системы;

b) для каждого входящего в реестр сервиса:

b1) соединение с сервисом,

b2) отправка запроса по соответствующему адресу сервиса,

b3) получение ответа от сервиса;

c) определение на основании полученных ответов состояния каждого сервиса в реестре;

d) пересылка пользователю статуса каждого сервиса.

Автоматизированный анализ состояния сервисов 1CM/1CF в режиме белого (прозрачного) ящика

Модуль обращается к базе данных сервера назначения и анализирует содержание таблиц ICFAPPLICAT10N, ICFDOCU, ICFHANDLER, ICFINSTACT, ICFSECPASSWD, ICFSERVICE, ICFSERVLOC, ICFVIRTHOST и других. Модуль выдает отчет о состоянии сервисов и конфигурации их защиты.

Автоматизированный анализ использования протокола HTTP в режиме черного ящика Модуль делает попытку соединения с целевым сервисом ICM и отправляет HTTP запрос любого URL. Если ответ сервера не содержит ошибки на уровне протокола, модуль выдает отчет о риске для безопасности как "сервис недостаточно защищен шифром".

Автоматизированный анализ использования протокола HTTP в режиме прозрачного ящика

Этот модуль соединяется с сервером назначения и отыскивает параметры профилей icm/server_port_0-9 и icm/HTTPS/verify_client или подобного. Если модуль определяет, что сервер не использует [протокол безопасных соединений] SSL, он сообщает о риске для безопасности.

Автоматическое обнаружение раскрытия информации в сообщениях об ошибке Модуль посылает запрос HTTP(S) сервису ICM, который, как известно, вызывает исключение в сервере, и делает синтаксический анализ ответа сервера. Если модуль обнаруживает, что сгенерированный ответ содержит идентификационные данные (ID) системы SAP и/или другую информацию о конфигурации, выдается отчет о риске для безопасности.

Автоматизированный анализ безопасности конфигурации ssl.b сервисе ICM

Модуль проверяет свойства SSL целевого сервиса ICM. Модуль сообщает о риске для безопасности при наличии любого из следующих условий:

сертификат SSL просрочен,

сертификат SSL выдан на имя, отличное от имени хоста сервера,

сертификат SSL не подписан уполномоченным органом сертификации,

сертификат SSL подписан с использованием слабого алгоритма хэширования,

протокол SSL поддерживает слабые шифры,

протокол SSL поддерживает слабые протоколы (SSLv2).

Автоматическое обнаружение наличия интерфейса администрирования ICM (управления менеджером коммуникации с Интернетом) SAP

Данный модуль информирует о риске для безопасности, если сконфигурирован интерфейс администрирования ICM SAP. Для проверки сервису ICM посылается запрос HTTP(S) для уточнения URL, предположительно содержащего сконфигурированный интерфейс администрирования ICM (значение по умолчанию /sap/icm/admin). Если в ответе сервера HTTP(S) содержит код состояния, отличный от 404, сигнализируется риск для безопасности. Данный модуль также может выполнять эту проверку, анализируя icm/HTTP/admin_<xx>или аналогичный параметр профиля. Если конфигурация этого параметра содержит значение, отличное от "" (пустые кавычки),

сигнализируется риск для безопасности.

Автоматическое обнаружение сервисов ICM с выявленными проблемами безопасности

Модуль связывается с целевым сервисом ICM и посылает запрос HTTP(S) по каждому сервису, хранящемуся в специальном файле базы данных. Этот файл базы данных содержит URL каждого сервиса, имеющего выявленную уязвимость системы безопасности, известную из "Уведомлений о безопасности SAP" или подобных источников. Если в ответе сервера содержится код, отличный от 404, выдается сообщение о риске для безопасности.

Автоматизированное использование уязвимостей в качестве контрсредств в сервисах ICM

Данный модуль использует выявленные уязвимости в качестве контрсредств в сервисах ICF, приложениях BSP и приложениях ABAPWebDynpro. В зависимости от выявленного фактора уязвимости модуль посылает специальный запрос HTTP(S), который позволяет пользователю выполнить мероприятия по адресной защите соответствующего сервиса ICM.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядное представление рисков для безопасности компонентов SAP Enterprise Portal ("SAP-портал предприятия") и J2EEEngine ("движок" платформы "Java 2 EnterpriseEdition")

Автоматизированный анализ состояния приложений Java в режиме черного ящика

Модуль снабжен файлом базы данных, содержащей сводный список существующих приложений Java (прикладных программных средств, внесенных в перечень через консоль WebDynpro или администрированием контента механизма J2EE Engine). В отношении каждого приложения, выделенного в базе данных, модуль связывается с целевым сервисом и посылает запрос HTTP(S) GET/HEAD о URL данного приложения. Модуль анализирует синтаксис ответа HTTP(S), сгенерированный сервером, и в соответствии с кодом состояния и телом HTTP выдает отчет о состоянии по следующим критериям:

если код состояния - 200, а тело не содержит строку "InternalServerError" ("внутренняя ошибка сервера") или директиву переназначения, приложение расценивается как "доступное";

если код состояния - 200, а тело содержит строку "InternalServerError" или директиву переназначения, приложение расценивается как "недоступное";

если код состояния - 200, а тело содержит строку "не развернуто", приложение расценивается как "неразвернутое".

Автоматизированный анализ инициации саморегистрации пользователя Модуль соединяется с целевым механизмом J2EE Engine SAP адресата и посылает запрос URL-страниц /webdynpro/dispatcher/sap.com/tc~sec~ume~wd~enduser/SelfregApp и/или /useradmin/selfReg или идентичных. Если ошибка в ответе сервера не обнаружена, сигнализируется риск для безопасности.

Автоматизированный анализ возможности анонимного доступа к управлению базами знаний SAP "SAPKnowledgeManagement"

Данный модуль связывается с целевым сервисом портала SAPEnterprisePortal и посылает запрос HTTP компоненту "управление знаниями SAP", не детализируя мандат (учетную запись с параметрами доступа пользователя). Если сервер не генерирует ошибку, модуль выдает отчет о риске для безопасности.

Автоматизированный удаленный поиск версии SAP-портала предприятия "SAPEnterprisePortal"

Модуль связывается с целевым механизмом J2EE Engine SAP и запрашивает страницы

URL /irj/portal или аналогичные. Ответ сервера проходит синтаксический анализ, при котором отыскивается строка после строки PortalVersion в контенте HTML и выдается в качестве отчета.

Автоматизированный анализ использования протокола HTTP в режиме черного ящика Модуль делает попытку связаться с целевым сервисом механизма J2EE Engine и запрашивает в HTTP любой URL. Если сервер отвечает без ошибок, модуль докладывает о риске для безопасности из-за ослабленного шифрования в сервисе.

Автоматизированный анализ защиты конфигурации SSL в сервисе механизма J2EE Engine

Модуль проверяет свойства протокола безопасных соединений SSL целевого сервиса механизма J2EE Engine. Модуль сообщает о риске для безопасности при наличии любого из следующих условий:

сертификат SSL просрочен,

сертификат SSL выдан на имя, отличное от имени хоста сервера,

сертификат SSL не подписан уполномоченным органом сертификации,

сертификат SSL подписан с использованием слабого алгоритма хэширования,

протокол SSL поддерживает слабые шифры,

протокол SSL поддерживает слабые протоколы (SSLv2).

Автоматизированное выявление и анализ в режиме черного ящика глобальных сервисов посредством администратора базы знаний SAP "SAPKnowledgeManager"

Модуль связывается с целевым SAP-порталом предприятия и посылает запрос HTTP на /irj/go/km/navigation/runtime/ или т.п.Если ответ сервера содержит перечень глобальных сервисов (GlobalServices), модуль выдает информационное сообщение о них.

Автоматизированное удаленное создание пользователя в SAP-портале предприятия "SAPEnterprisePortal"

Если в целевом сервисе инициируется процедура саморегистрации пользователя, модуль посылает специально сгенерированное сообщение-запрос HTTP на создание пользователя в удаленной системе.

Автоматизированный удаленный поиск пути инсталляции SAP-портала предприятия "SAPEnterprisePortal"

Модуль связывается с адресным SAP-порталом предприятия и посылает запрос URL /irj/servlet/prt/soap или эквивалентного с именем файла прямого доступа (т.е. /irj/servlet/prt/soap/<random_value>.wsdl). Ответ сервера проходит синтаксический разбор, в результате которого выводится путь инсталляции, о котором составляется отчет.

Автоматизированное внутреннее сканирование портов с использованием навигатора веб-сервисов J2EE "J2EEEngine\VebServicesNavigator"

Сначала данный модуль определяет, активировано ли у адресата приложение навигатора веб-сервисов WebServicesNavigator. Если да, то модуль посылает этому сервису специально сгенерированные HTTP-запросы GET и POST, базирующиеся на наборе диапазонов IP и портов, задаваемых пользователем, чтобы побудить навигатор веб-сервисов связаться с этими системами и сервисами. Ответ сервера проходит синтаксический разбор с анализом результатов контактов и изложением итогов пользователю в отчете.

Автоматизированная рассылка электронной почты через SAP-портал предприятия "SAPEnternrisePortal"

Данный модуль испытывает компонент "сотрудничество SAP" (SAPCollaboration) SAP-портала предприятия. Модуль рассылает специально сгенерированные HTTP-запросы GET и POST для отправки специфических e-mail пользователям

SAPEnterprisePortal, которые имеют четко сконфигурированные адреса электронной почты.

Автоматизированный удаленный поиск технической информации в SAP-портале предприятия и автоматизированная экспертиза защиты

Данный модуль связывается с целевым SAP-порталом предприятия и загружает файл, содержащий параметры конфигурации механизма J2EE Engine SAP. Модуль открывает этот файл и анализирует каждый параметр конфигурации на угрозу безопасности. При обнаружении риска для безопасности модуль информирует об этом пользователя.

Автоматизированное использование уязвимостей в качестве контрсредств в компонентах "SAP-портал предприятия" (SAPEnterprisePortal) и "механизм J2EE" (J2EEEngine)

Данный модуль использует выявленные уязвимости в качестве контрсредств в компонентах "SAP-портал предприятия" и "J2EEEngine". В зависимости от выявленного фактора уязвимости модуль посылает специальный сетевой запрос, который позволяет пользователю осуществить мероприятия по адресной защите соответствующей системы.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядное представление рисков для безопасности компонента "консоль управления SAP" (SA PManagementConsole)

Автоматизированный удаленный поиск способов администрирования консоли управления SAPManagementConsole

Этот модуль связывается с целевым сервисом консоли управления SAP ManagementConsole и посылает HTTP-запрос URL, заканчивающегося на "?wsdl" или т.п. После обработки этого запроса сервер назначения отвечает файлом WSDL, который обрабатывается данным модулем. Модуль анализирует, какие средства протокола SOAP реализованы на сервере назначения, и информирует пользователя о вытекающих рисках для безопасности.

Автоматизированное осуществление методов администрирования, не относящихся к приложению SAP

Данный модуль обеспечивает интерфейс для реализации существующих средств "Протокола простого доступа к объектам" SOAP как с мандатом аутентификации, так и без него. Благодаря реализации алгоритмов SOAP можно выполнять следующие операции с целевым сервисом: проверять, защищена ли SAPMC консоль управления SAP) паролем, получать информацию о среде сервера, извлекать информацию о конкретном объекте хоста, находить параметры профиля экземпляра SAP, получать содержимое профиля запуска SAP, получать файл трассировки SAP, получать с сервера SAP информацию о версиях, вести список следов разработчика, вести список журнальных файлов, находить определенный журнальный файл, находить определенный след разработчика, выключать экземпляр SAP анонимно, выключать сервис SAPMC анонимно, читать системный журнал ABAP, выполнять команды операционной системы и другие. Модуль анализирует сгенерированный ответ после выполнения каждого алгоритма SOAP и выдает пользователю отчет о результатах анализа. Модуль сигнализирует наличие рисков для безопасности в случае их обнаружения.

Автоматизированное использование уязвимостей в качестве контрсредств в компонентах консоли управления SAP ManagementConsole

Данный модуль использует выявленные уязвимости в качестве контрсредств в компонентах консоли управления SAP ManagementConsole. В зависимости от выявленного фактора уязвимости модуль посылает специальный сетевой запрос,

который позволяет пользователю осуществить мероприятия по адресной защите соответствующей системы.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядное представление рисков для безопасности в компоненте SAPMessageServer ("сервер сообщений SAP")

Автоматизированный поиск параметров профиля SAP

Данный модуль связывается с HTTP-портом администрирования целевого сервера сообщений SAP и посылает HTTP-запрос на /msgserver/text/parameter URL или подобный, задавая имя параметра профиля, предоставленное пользователем как параметр запроса. Этот модуль, кроме того, может быть снабжен файлом базы данных, содержащей имена всех возможных параметров профиля. Далее, модуль посылает HTTP-запрос каждому возможному параметру и посредством этого получает все параметры профиля целевого сервера приложений SAP. Затем, модуль анализирует конфигурацию для каждого полученного параметра на угрозу безопасности и при обнаружении рисков сигнализирует об этом пользователю.

Процедуры нахождения модификаций обновлений SAP ABAP в системе SAP

Автоматический моментальный снимок (snapshot) текущего состояния защиты обновлений SAP ABAP

Этот модуль связывается с сервером базы данных диагностируемой системы SAP и обращается к типу/логической структуре базы данных, применяемым для хранения информации системы SAP.

Модуль вычисляет сигнатуру (выполненную посредством циклического контроля избыточности CRC, алгоритма хэширования или подобным образом) всей или некоторой из указанной ниже информации:

поле "DATA" таблицы REPOSRC.

поле "LDATA" таблицы REPOLOAD.

поле "QDATA" таблицы REPOLOAD.

поле "LOGICINFO" таблицы DYNPSOURCE.

поле "CLUSTD" таблицы 02PAGCON.

любые поля любой другой таблицы или таблиц, содержащих информацию, целостность которой необходимо проверить.

Выделенные сигнатуры сохраняются в локальных репозиториях. Такой репозиторий может быть реализован в форме локальной реляционной базы данных.

Данный модуль осуществляет указанный способ посредством следующих шагов:

a) связь с выбранной базой данных целевой системы;

b) доступ к выбранной базе данных и поиск в ней определенных записей в определенных полях;

c) расчет значения сигнатуры на основе выбранных записей;

d) сохранение значения сигнатуры в репозиторий, удаленном от целевой системы (возможен подходе использованием локального репозитория),

f) если для целевой системы существует множество значений сигнатур, каждое значение сигнатуры сохраняется отдельно.

Автоматическое сравнение моментальных снимков текущего состояния безопасности обновлений SAP ABAP

После снятия описанным выше модулем двух "стоп-кадров" (A и B) обновлений SAP ABAP они могут быть автоматически сопоставлены.

Данный модуль сравнивает сохраненные сигнатуры обоих стон-кадров и выдает отчет по следующей форме:

сигнатура элемента X отличается на сравниваемых снимках;

элемент X отсутствует на снимке B, но присутствует на снимке A;

элемент X отсутствует на снимке A, но присутствует на снимке B.

Таким образом, этот модуль расширяет функциональные возможности предыдущего модуля, выполняя следующие шаги (основываясь на вышеописанном способе):

g) шаги a)-f), выполняются, по меньшей мере, дважды в разное время;

h) значения сигнатур, выведенные при каждом прогоне, сравниваются друг с другом;

i) разница между значениями сигнатур сообщается пользователю.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядного представления рисков для безопасности операционной системы и баз данных на основе протоколов прикладного уровня SAP

Автоматизированный анализ прав доступа и целостности исполняемых и конфигурационных файлов SAP посредством протоколов прикладного уровня SAP

Данный модуль связывается с системой SAP с помощью интерфейса SAPRFC или HTTP или другого протокола прикладного уровня SAP независимо от базовой операционной системы. После вхождения в систему назначения этоn модуль выполняет специальную функцию верификации надлежащего оформления прав доступа файлов, относящихся к серверу приложений SAP ApplicationServer, и информирует пользователя о сопряженных рисках для безопасности. Наряду с этим модуль отслеживает возможную модификацию анализируемых файлов, вычисляя для них сигнатуру безопасности, сравнивая ее с известной сигнатурой и информируя пользователя о различиях.

Модуль осуществляет указанный способ, выполняя следующие шаги:

a) установление связи с системой назначения;

b) выполнение специальной функции верификации надлежащего оформления прав доступа файлов, ассоциированных с определенным прикладным сервером;

c) информирование пользователя о результатах верификации, выполненной на шаге b). Шаг a) вышеуказанного способа выполняется независимо от базовой операционной системы целевой системы.

Автоматизированный анализ безопасности пользователей и групп пользователей SAP Данный модуль связывается с системой SAP с помощью интерфейса SAPRFC или HTTP или другого протокола прикладного уровня SAP независимо от базовой операционной системы. После вхождения в систему назначения этот модуль выполняет специальную функцию верификации существующих групп пользователей SAP на включение в них только надлежащих пользователей. Модуль информирует пользователя о сопряженных рисках для безопасности.

Процедуры обнаружения, анализа, распознавания уязвимости и наглядного представления рисков для безопасности оборудования графического интерфейса пользователя SAP GUI

Автоматизированный анализ версии SAP GUI

Данный модуль связывается с операционной системой адресата, используя собственные интерфейсы или сетевые службы администрирования. Модуль получает версию SAP GUI из MicrosoftWindowsRegistry. Модуль сравнивает эту версию с самой последней доступной версией. Если действующая инсталлированная версия старше самой последней доступной версии, пользователь информируется о риске для безопасности.

Автоматизированный анализ настроек безопасности SAP GUI

Данный модуль связывается с операционной системой адресата, используя собственные интерфейсы или сетевые службы администрирования. Данный модуль

заимствует конфигурации модуля безопасности SAP GUI SccurityModule и других соответствующих настроек средств защиты из MicrosoftWindowsRegistry, например, такие продукты как конфигурация KillBit для уязвимого или опасного SAP GUI ActiveX, опции SAP GUI Scripting и конфигурация SAP GUI InputHistory. Этот модуль сравнивает обнаруженные настройки с лучшей применяемой на практике конфигурацией. Если выявляется несоответствие, пользователь получает уведомление о риске для безопасности.

Соответственно, модуль осуществляет необходимый способ, выполняя следующие шаги:

a) установление связи с операционной системой целевой среды;

b) поиск конфигурации и защитных настроек для определенных модулей и компонентов операционной системы;

c) сравнение данных конфигурации и защитных настроек со специальными конфигурацией и настройками, которое считаются надежными (такие настройки и конфигурации со временем могут измениться, как и все освоенные на практике лучшие технологии);

d) если лучшие и наиболее надежные, проверенные практикой конфигурации и настройки не соответствуют конфигурации и настройкам, выявленным на шаге b), пользователь получает уведомление о риске для безопасности.

Процедуры по расширению компрометации уязвимых средств SAP

Способ автоматизации испытания на проникновение через агенты SAP ABAP/Java

После компрометации системы SAP посредством модуля контрсредств ("эксплойтов"} большой интерес представляет анализ возможностей взломщика расширить свое влияние на другие системы в сети назначения.

Для такого анализа необходимо иметь возможность провеет ряд оценочных действий с использованием скомпрометированной системы. Для этого в заявляемом изобретении предусмотрено приложение ABAP/Java, которое развертывается в скомпрометированной системе SAP. Это приложение получает инструкции от пользователя. Это приложение обеспечивает следующие функциональные возможности:

- читать и писать файлы в локальной операционной системе;

выполнять произвольные команды операционной системы в локальной операционной системе;

- открывать и закрывать сетевые связи с удаленными системами;

- быть средством доступа ("proxy") через сетевой трафик к оговариваемым системам.

В силу этого, назначение данного модуля может состоять в осуществлении способа, состоящего из следующих шагов:

a) получение от пользователя инструкций относительно конфигурации;

b) попытка выполнять множественные команды операционной системы в операционной системе целевой среды;

c) попытка открывать и закрывать сетевые связи между целевой средой и другими удаленными системами;

d) попытка оказывать прокси-услуги по сетевому трафику между целевой средой и обусловленными сетевыми системами.

Безусловно, данный модуль запускают изнутри целевой среды и указанные шаги выполняют внутри операционной системы целевой среды.

Необходимо указать на то, что в то время как в детализованных выше примерах использованы программные приложения, серверы, сервисы и системы SAP, способы и принципы, раскрытые в этих примерах, также могут быть применены в других системах.

Другие критически важные для бизнеса системы могут быть аналогичным образом проанализированы, протестированы и оценены в соответствии с описанными выше способами с использованием рассмотренных выше систем.

Шаги способов, входящих в изобретение, могут быть реализованы в комбинациях исполняемого машинного кода, хранящегося в множестве различных форматов, таких как объектный код или исходный текст. Здесь для упрощения такой код в целом описан как программный код или как компьютерная программа. Понятно, что исполнимый машинный код может быть интегрирован с кодом других программ, реализованных как подпрограммы, внешними вызовами программы или другими наборами средств, известными на существующем уровне техники.

Варианты осуществления изобретения могут быть выполнены компьютерным процессором или подобным устройством, запрограммированным в соответствии с шагами способа, или могут быть выполнены электронной системой, оснащенной средствами для выполнения этих шагов. Аналогично этому на выполнение шагов способа могут быть запрограммированы такие средства электронной памяти, как компьютерные дискеты, CD-ROM (компакт-диски), оперативная память (ОЗУ/ЗУПВ, RAM), постоянное запоминающее устройство (ПЗУ, ROM) или подобные им среды хранения компьютерного программного обеспечения, известные на существующем уровне техники. Также электронные сигналы, представляющие шаги способа, могут передаваться через систему связи.

Варианты реализации изобретения могут быть выполнены на любом стандартном языке программирования. В частности, предпочтительными для осуществления изобретения могут быть процедурно-ориентированный язык программирования (например "C") или объектно-ориентированный язык (например "C++"). Альтернативно изобретение может быть решено в форме предварительно запрограммированных аппаратных средств, иных соответствующих компонентов, или как совокупность аппаратного и программного обеспечения.

Возможны варианты реализации в виде компьютерного программного продукта для использования с вычислительной системой. Подобные осуществления могут включать в себя последовательность машинных команд или зафиксированных на материальном носителе, таком как компьютерный читаемый носитель (например, дискета, CD-ROM, ROM, или жесткий диск), или передаваемых на компьютерную систему через модем или другой интерфейс, такой как адаптер связи, сопряженный с сетью через среду передачи. Среда передачи может быть или физической (например, оптические или электрически линии связи), или построенной на беспроводных технологиях трансляции сигнала (например, микроволновой, инфракрасной или иной). Такая последовательность машинных команд охватывает все или часть функциональных возможностей, описанных здесь ранее. Для специалистов в данной области очевидно, что машинные команды могут быть написаны на ряде языков программирования для использования с разнообразными архитектурами вычислительных сред или операционными системами. Кроме того, такие команды могут быть сохранены на любом запоминающем устройстве, таком как полупроводниковое, магнитное, оптическое или иное ЗУ, и могут быть переданы с использованием любой коммуникационной технологии, такой как оптическая, инфракрасная, микроволновая, или иной техники передачи сигнала. Логично предположить, что такой компьютерный программный продукт может распространяться на сменном носителе с сопроводительной документацией в печатном или электронном виде (например, в виде упакованных программных средств), предварительно загруженной компьютерной

системой (например, на системное ПЗУ или жесткий диск), или в форме дистрибутива с сервера через сеть (например, Интернет или Всемирную паутину). Разумеется, предусматривается вариант конструктивных решений изобретения как комбинации программного обеспечения (например, компьютерного программного продукта) и аппаратных средств. Предполагаются и варианты целиком схемотехнического исполнения или полного программного обеспечения (например, компьютерного программного продукта).

Лицо, разобравшееся в технической сути данного изобретения, имеет представление о возможных компоновках и конструктивных решениях или версиях, альтернативных описанным выше, все из которых должны вписываться в рамки изобретения, обозначенные в пунктах патентной формулы, которая следуют ниже.

## (57) Формула изобретения

1. Способ оценки конфигурации системы безопасности целевой компьютерной среды, включающий:

a) сканирование идентифицированных IP-адресов и портов;

b) снятие отпечатков пользования выявленных открытых портов для распознавания исполняемых через них сервисов;

c) «дактилоскопирование» - определение активности названной целевой среды;

d) обращение к базе модулей и выполнение, по меньшей мере, одного из таких модулей, предназначенных для нахождения факторов уязвимости в системе безопасности, доступных через указанные IP-адреса и порты; при этом

- обозначенный, по меньшей мере, один модуль выполняется исходя из его конфигурации;

- обозначенная целевая компьютерная среда используется для выполнения критически важных бизнес-приложений, причем, по меньшей мере, один из вышеуказанных модулей выполняет способ, включающий:

cc-1) поиск таблиц адресатов для удаленных вызовов функций и других интерфейсов для прикладных серверов, ассоциированных с указанной целевой средой;

cc-2) поиск журнальных файлов с приложениями для указанной целевой среды;

cc-3) выявление на основе найденных таблиц адресатов и журнальных файлов связей между различными системами, имеющими отношение к указанной целевой среде;

cc-4) графическое отображение выявленных связей;

cc-5) предоставление пользователю сформированного графического отображения выявленных связей.

2. Способ по п. 1, в котором шаг b), в свою очередь, включает в себя шаги:

b1) доступ к базе "дактилоскопических" идентификационных данных (Fingerprint Database), содержащей множество предварительно сформулированных сетевых запросов, каждому из которых присвоен, по меньшей мере, один ожидаемый отклик;

b2) посылка, по меньшей мере, одного предварительно сформулированного сетевого запроса из названного множества на указанные открытые порты;

b3) получение, по меньшей мере, одного ответа на указанные запросы;

b4) анализ указанного, по меньшей мере, одного ответа для определения, является ли он ожидаемым откликом; при этом получение ожидаемого отклика является показателем доступности конкретного сервиса в указанной целевой среде.

3. Способ по п. 1, в котором, по меньшей мере, один из названных модулей выполняет свои функции на основе способа, включающего:

aa-1) установление для такого, по меньшей мере, одного модуля объема выполняемых

им функций, которые для каждого модуля задают предварительно и в кодированном виде вводят в каждый модуль;

aa-2) выполнение одной функции каждым модулем один раз для одной целевой среды, если указанный объем выполняемых функций рассчитан на систему;

aa-3) выполнение одной функции каждым модулем для одного выбранного соединительного элемента, соответствующего одному целевому компоненту, если указанный объем выполняемых функций рассчитан на компонент;

aa-4) выполнение одной функции каждым модулем для одного выбранного соединительного элемента, если указанный объем выполняемых функций рассчитан на соединительный элемент.

4. Способ по п. 1, в котором, по меньшей мере, один из указанных модулей выполняет способ, включающий:

bb-1) получение от пользователя, по меньшей мере, одного идентификатора программы;

bb-2) для каждого такого, по меньшей мере, одного идентификатора программы:

bb-2-1) соединение с межсетевым шлюзом для указанной целевой среды;

bb-2-2) попытку инициировать заданный сервер, ассоциированный с указанным идентификатором программы на хосте программы, идентифицируемой указанным идентификатором программы;

bb-3) определение, какая программа, ассоциированная с названным, по меньшей мере, одним идентификатором программы, может быть инициирована на основании результата шага bb-2-1).

5. Способ по п. 1, в котором, по меньшей мере, один из указанных модулей выполняет способ, включающий:

dd-1) получение от пользователя диапазонов адресов IP и портов;

dd-2) выполнение пробных соединений с каждой комбинацией IP-адреса и порта посредством программного маршрутизатора, относящегося к указанной целевой среде, при этом каждая комбинация выведена из полученных от пользователя на ступени dd-1) диапазонов IP-адресов и портов и каждая комбинация представляет собой соединение;

dd-3) заключение, что соединение с определенной комбинацией IP-адреса и порта успешно, если названный программный маршрутизатор не отвечает отказом на попытку соединения с использованием выбранной комбинации IP-адреса и порта;

dd-4) предоставление указанному пользователю списка успешных и неуспешных соединений.

6. Способ по п. 1, в котором, по меньшей мере, один модуль выполняет способ маршрутизации сетевого трафика посредством программного маршрутизатора, относящегося к обозначенной целевой среде, включающий:

ee-1) создание конечной точки, комплектуемой прокси-сервером и транслятором протоколов, транслирующим протокол обслуживаемой целевой среды, и программными маршрутизаторами, относящимися к указанной целевой среде;

ee-2) прием исходящего сетевого трафика от сетевых программных средств, сопряженных с указанной конечной точкой;

ee-3) направление принятого исходящего сетевого трафика на указанный транслятор протоколов;

ee-4) пакетирование указанным транслятором протоколов принятого исходящего сетевого трафика в исходящие пакеты, совместимые с программными маршрутизаторами обслуживаемой целевой среды;

ee-5) направление упакованных исходящих пакетов на программные маршрутизаторы

обслуживаемой целевой среды;

ee-6) получение входящих пакетов от указанных программных маршрутизаторов;

ee-7) пересылка полученных входящих пакетов на указанный транслятор протоколов;

ee-8) распаковка указанных входящих пакетов во входящий сетевой трафик;

ee-9) направление указанного входящего сетевого трафика в адрес указанных сетевых программных средств.

7. Способ по п. 1, в котором, по меньшей мере, один модуль выполняет способ, включающий в себя:

ff-1) соединение с базой данных обслуживаемой целевой среды;

ff-2) обращение к этой базе данных для поиска заданных гнезд в ее заданных полях;

ff-3) расчет на основании найденных заданных гнезд значения сигнатуры;

ff-4) сохранение рассчитанного значения сигнатуры в репозитории, удаленном от обслуживаемой целевой среды;

ff-5) сохранение каждого значения сигнатуры отдельно в случае вычисления множества значений сигнатур для указанной целевой среды.

8. Способ по п. 8, в котором описанный способ включает в себя последующие шаги:

ff-6) выполнение шагов с ff-1) по ff-5), по меньшей мере, дважды в разное время;

ff-7) сравнение значений сигнатур, рассчитанных при каждом прогоне;

ff-8) предоставление информации о различиях между рассчитанными значениями сигнатур после сравнения на шаге ff-7).

9. Способ по п 1, в котором, по меньшей мере, один модуль выполняет способ, включающий:

gg-1) соединение с целевой средой;

gg-2) выполнение функции верификации надлежащего оформления прав доступа файлов, относящихся к целевому серверу приложений;

gg-3) предоставление информации о результатах верификации, выполненной на шаге gg-2); при этом шаг gg-1) выполняется независимо от базовой операционной системы обслуживаемой целевой среды.

10. Способ по п 1, в котором, по меньшей мере, один модуль выполняет способ, включающий:

hh-1) получение от пользователя инструкций относительно конфигурации;

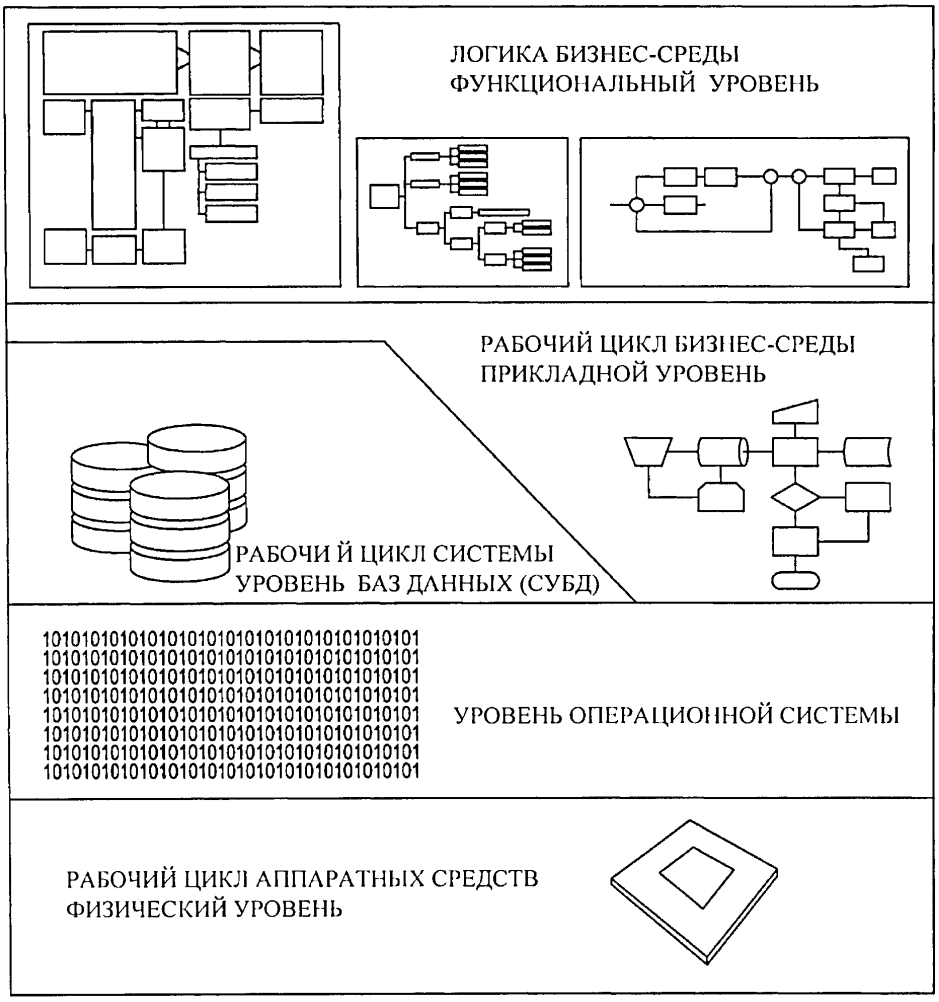
hh-2) попытка выполнять множество команд операционной системы в операционной системе обслуживаемой целевой среды;

hh-3) попытка открывать и закрывать сетевые соединения между обслуживаемой целевой средой и удаленными системами;

hh-4) попытки оказывать прокси-услуги через сетевой трафик между указанной целевой средой и оговоренными сетевыми системами; при этом данный модуль логически реализован в операционной системе обслуживаемой целевой среды.

1

АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ

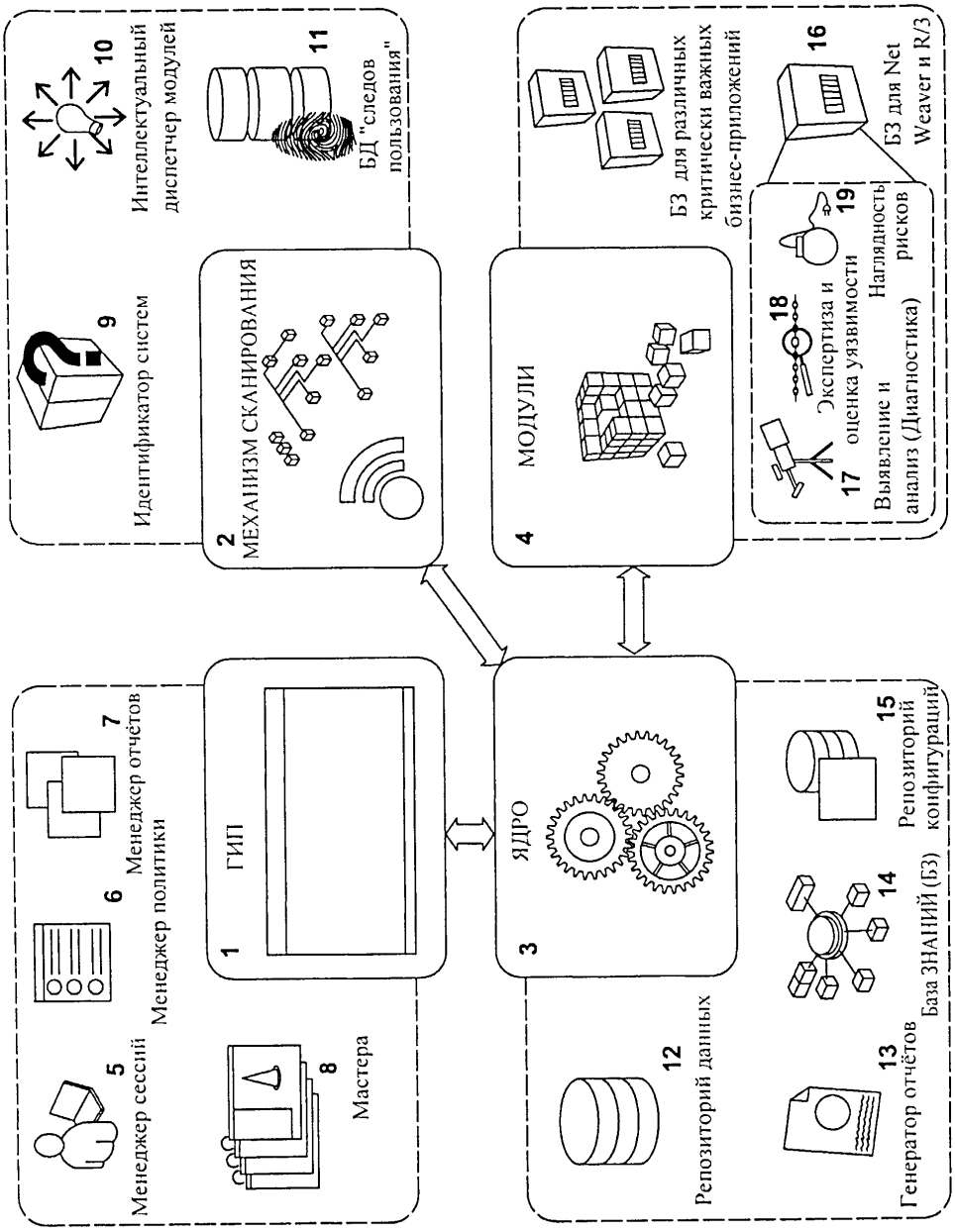



ФИГ. 1

1

2

АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ



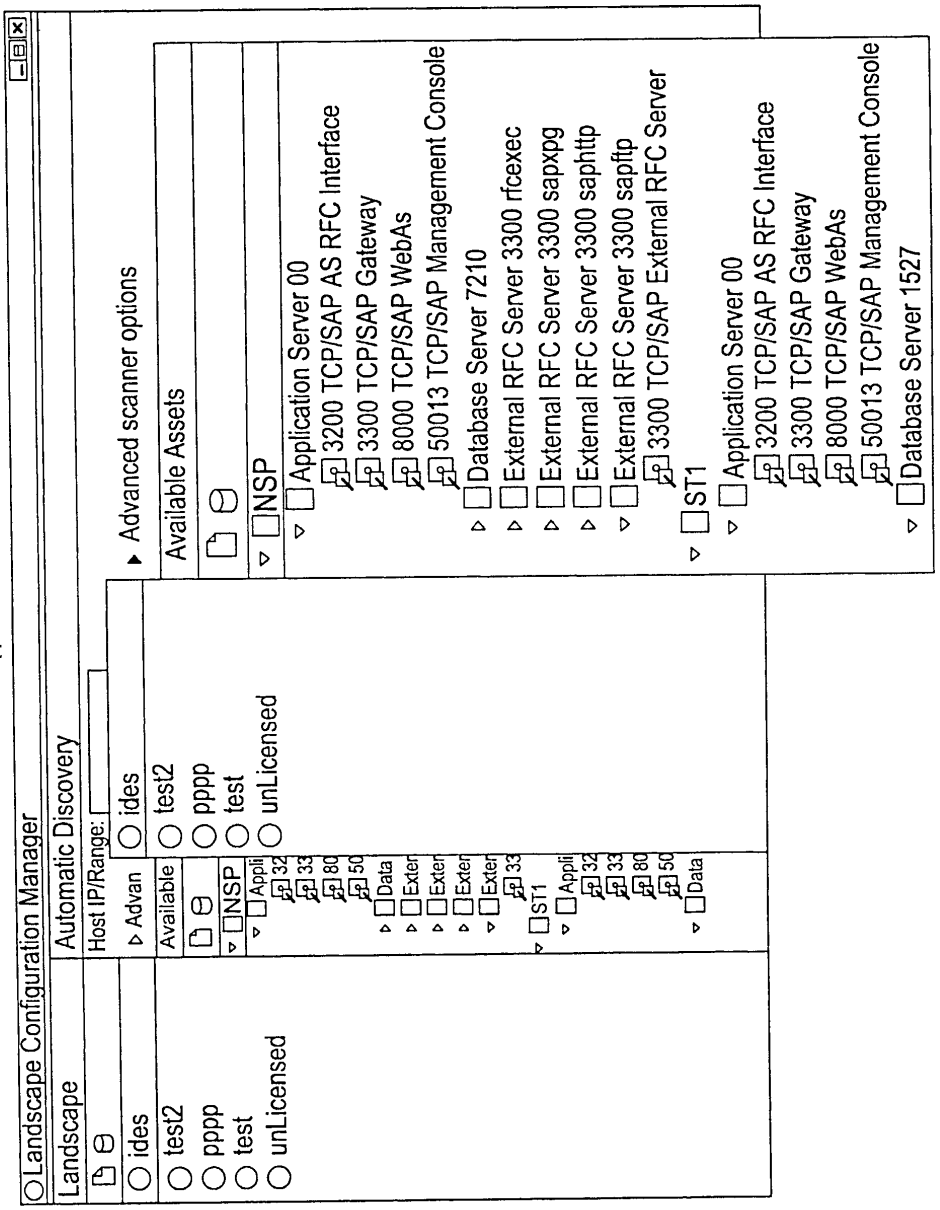

ФИГ. 2

2

3

АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ

Рабочий фрагмент пользовательского интерфейса

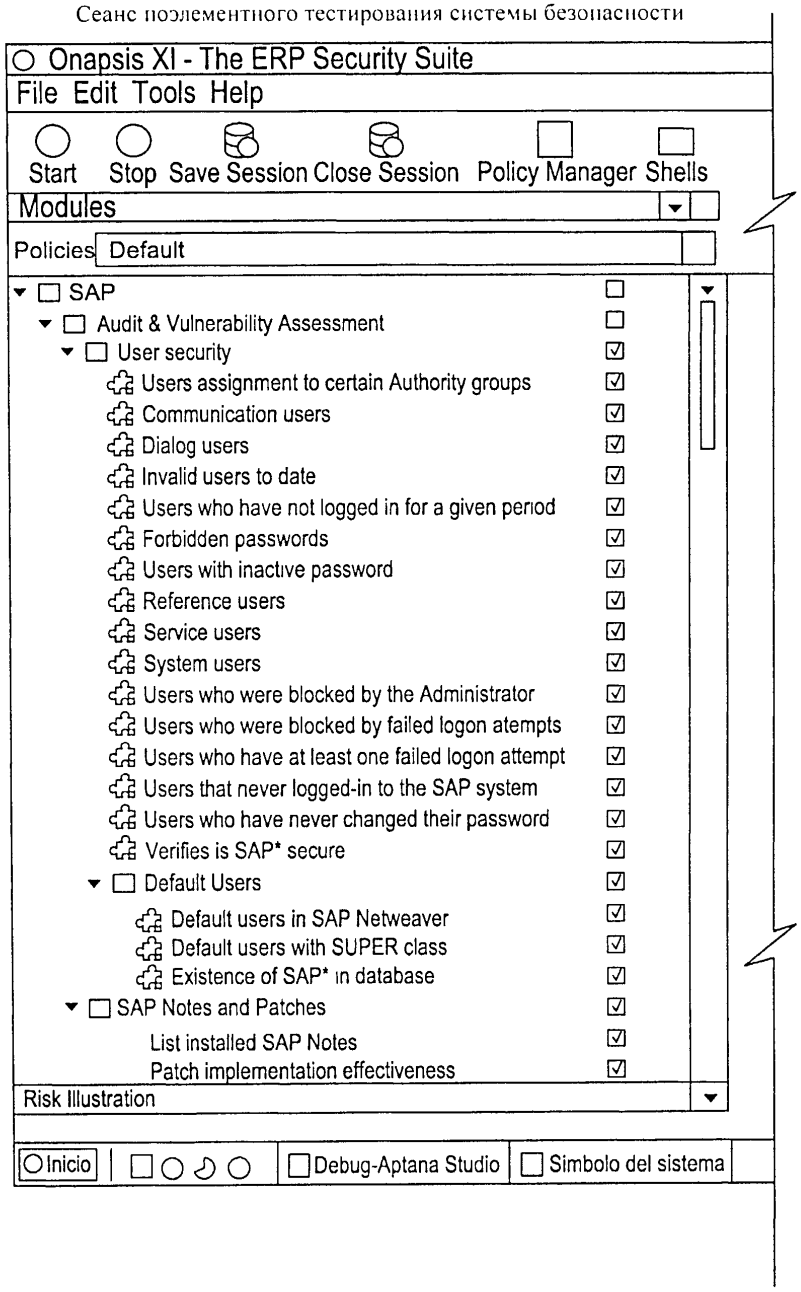



ФИГ. 3

3

4

# АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ

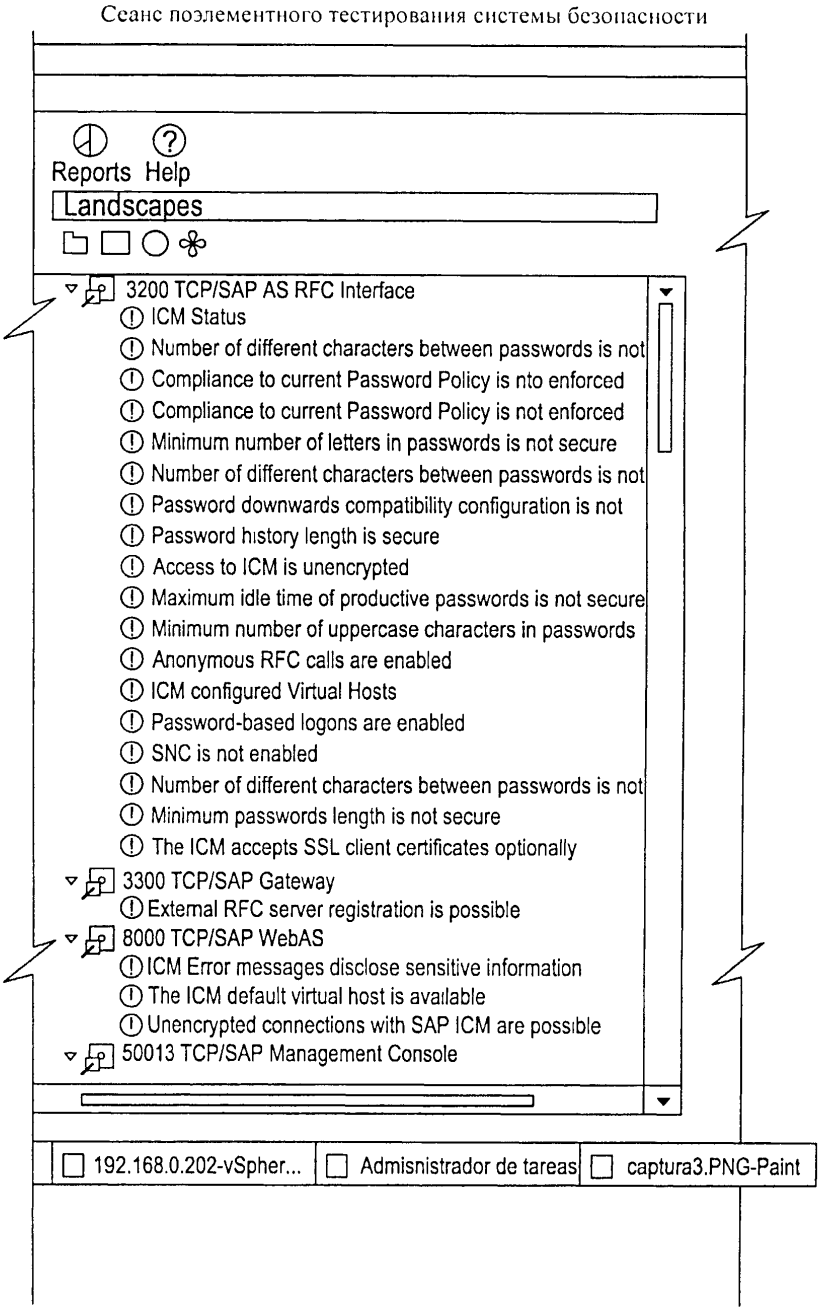



ФИГ. 4



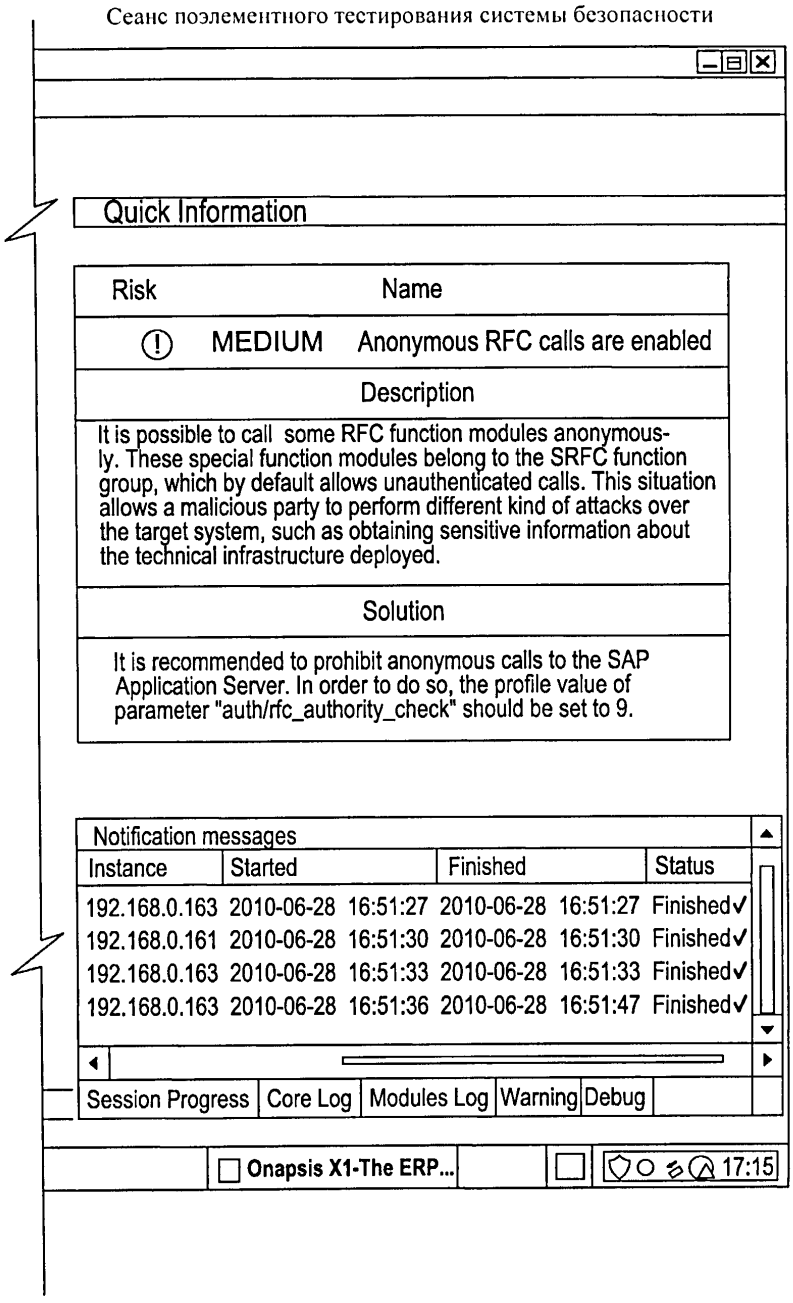
5

АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ




ФИГ. 4 (Продолжние)

АВТОМАТИЗИРОВАННАЯ ОЦЕНКА БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ДЛЯ БИЗНЕСА КОМПЬЮТЕРНЫХ СИСТЕМ И РЕСУРСОВ




ФИГ. 4 (Продолжние)