Приложение
к решению Федеральной службы
по интеллектуальной собственности

ЗАКЛЮЧЕНИЕ
по результатам рассмотрения ☒ возражения ☐ заявления

Коллегия в порядке, установленном пунктом 3 статьи 1248 Гражданского кодекса Российской Федерации (далее – Кодекс) и Правилами подачи возражений и заявлений и их рассмотрения, утвержденными приказом Роспатента от 22.04.2003 № 56, зарегистрированным в Министерстве юстиции Российской Федерации 08.05.2003 № 4520 (далее – Правила ППС), рассмотрела возражение Закрытого акционерного общества «Лаборатория Касперского» (далее – заявитель), поступившее 18.12.2015, на решение Федеральной службы по интеллектуальной собственности (далее – Роспатент) об отказе в выдаче патента на изобретение по заявке № 2013129555/08, при этом установлено следующее.

Заявка на изобретение «Способ и система обнаружения вредоносного программного обеспечения путём контроля исполнения программного обеспечения, запущенного по сценарию» была подана 28.06.2013.

Совокупность признаков заявленного предложения изложена в уточненной формуле изобретения, представленной заявителем в корреспонденции, поступившей 15.04.2015, в следующей редакции:

«1. Способ обнаружения вредоносного программного обеспечения, в котором:

а) подконтрольно исполняют исследуемое приложение в соответствии со сценарием на модифицированной программно-аппаратной части устройства;

б) протоколируют модифицированной программно-аппаратной частью устройства информацию о событиях на устройстве, вызванных исполнением исследуемого приложения, исполняемого по сценарию;

в) обнаруживают вредоносное программное обеспечение, анализируя информацию, протоколируемую в п.б) на наличие событий, характерных для вредоносного программного обеспечения;

2. Способ по п.1, в котором сценарий это список из набора событий, создание которых в системе активирует вредоносный функционал приложения.

3. Способ по п.1, в котором анализ протоколируемой информации осуществляется путем сравнения протоколируемой информации о событиях, вызванных работой исследуемого приложения, с шаблонами поведения, содержащими события, характерные для вредоносного программного обеспечения;

4. Система обнаружения вредоносного программного обеспечения содержит:

а) модифицированную программно-аппаратную часть устройства, предназначенную для:

- подконтрольного исполнения исследуемого приложения, запущенного модулем управления;

- протоколирования информации о событиях на устройстве, вызванных исполнением исследуемого приложения, исполняемого по сценарию;

б) модуль управления, предназначенный для подконтрольного запуска приложения в соответствии со сценарием;

в) модуль анализа, связанный с модулем управления и модифицированной программно-аппаратной частью устройства, предназначенный для обнаружения вредоносного программного обеспечения, анализируя информацию, протоколируемую

модифицированной программно-аппаратной частью устройства на наличие событий, характерных для вредоносного программного обеспечения;

5. Система по п.4, в которой система дополнительно включает базу сценариев, которая связана с модулем управления и предназначена для хранения сценариев;

6. Система по п.4, в которой система дополнительно включает базу шаблонов, связанную с модулем анализа и предназначенную для хранения шаблонов поведения.»

При вынесении решения Роспатента от 10.06.2015 об отказе в выдаче патента на изобретение, к рассмотрению была принята вышеприведенная уточненная формула.

Решение Роспатента мотивированно несоответствием заявленной группы изобретений условию патентоспособности «новизна».

Данный вывод аргументирован известностью из уровня техники на дату подачи заявки технического решения, описанного в патентном документе:

- US 2012/0222123 A1 30.08.2012 (далее – [1]).

На решение об отказе в выдаче патента на изобретение в соответствии с пунктом 3 статьи 1387 Кодекса поступило возражение 18.12.2015, в котором заявитель выражает несогласие с выводом упомянутого решения.

По мнению заявителя, в решении Роспатента не были проанализированы все признаки приведенной выше уточненной формулы заявленного изобретения.

Изучив материалы дела и заслушав участников, коллегия установила следующее.

С учетом даты подачи заявки (28.06.2013) правовая база для оценки

патентоспособности заявленного изобретения включает Кодекс, Административный регламент исполнения Федеральной службой по интеллектуальной собственности, патентам и товарным знакам государственной функции по организации приема заявок на изобретение и их рассмотрения, экспертизы и выдачи в установленном порядке патентов Российской Федерации на изобретение, утвержденный приказом Министерства образования и науки Российской Федерации от 29.10.2008 №327, зарегистрированный в Министерстве юстиции Российской Федерации 20.02.2009 №13413 (далее – Регламент ИЗ).

В соответствии с пунктом 1 статьи 1350 Кодекса изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

В соответствии с пунктом 2 статьи 1350 Кодекса изобретение является новым, если оно не известно из уровня техники. Уровень техники включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

Согласно подпункту 4 пункта 24.5.2 Регламента ИЗ изобретение признается известным из уровня техники и не соответствующим условию новизны, если в уровне техники раскрыто средство, которому присущи все признаки изобретения, выраженного формулой, предложенной заявителем.

Существо заявленной группы изобретений выражено в приведенной выше уточненной формуле изобретения, представленной заявителем 15.04.2015, которую коллегия приняла к рассмотрению.

Анализ доводов, содержащихся в решении Роспатента и в возражении, показал следующее.

Можно согласиться с заявителем в том, что в патентном документе [1] не раскрыты все признаки заявленной группы изобретений, охарактеризованной в указанной выше уточнённой формуле.

Так при анализе решения, раскрытого в патентном документе [1] не

было выявлено указанных в независимом пункте 1 уточнённой формулы признаков, характеризующих, что при реализации известного способа обнаружения вредоносного программного обеспечения

обнаруживают вредоносное программное обеспечение, анализируя протоколируемую модифицированной программно-аппаратной частью устройства информацию о событиях на устройстве, вызванных исполнением исследуемого приложения, запущенного по сценарию, на наличие событий, характерных для вредоносного программного обеспечения.

Также в патентном документе [1] не было выявлено указанных в независимом пункте 4 уточнённой формулы признаков, характеризующих, что известная система обнаружения вредоносного программного обеспечения содержит

«модуль анализа, связанный с модулем управления и модифицированной программно-аппаратной частью устройства, предназначенный для обнаружения вредоносного программного обеспечения, анализируя информацию, протоколируемую модифицированной программно-аппаратной частью устройства на наличие событий, характерных для вредоносного программного обеспечения».

Таким образом, представленные сведения, выявленные из уровня техники при проведении экспертизы заявки по существу, являются недостаточными для вывода о несоответствии заявленной группы изобретений, охарактеризованной в рассматриваемой уточнённой формуле, условию патентоспособности «новизна».

Дополнительно было установлено, что в решении об отказе в выдаче патента от 10.06.2015 не были проанализированы признаки зависимых пунктов 2, 3, 5, 6.

Поскольку поиск, послуживший основанием для вынесения упомянутого решения, был проведен не в полном объеме, в соответствии с пунктом 5.1 Правил ППС дело заявки было направлено для проведения дополнительного поиска.

По результатам проведения дополнительного поиска 15.08.2016 были представлены заключение экспертизы и отчет о дополнительном информационном поиске.

В заключении сделан вывод о несоответствии заявленной группы изобретений условию патентоспособности «изобретательский уровень» ввиду известности решений, описанных в следующих источниках информации:

US 2013/0122861 A1 16.05.2013 (далее [2]);

US 2010/0107252 A1 29.04.2010 (далее [3]);

В.М. Рувинская и др. «Эвристические методы детектирования вредоносных программ на основе сценариев», 31.12.2008 (далее [4]).

Заявитель был ознакомлен с заключением и отчетом о дополнительном информационном поиске.

На коллегии от 24.10.2016 заявитель подал ходатайство о переносе рассмотрения возражения на более поздний срок с целью подготовки скорректированной формулы.

Указанное ходатайство было удовлетворено.

В корреспонденции, поступившей 18.11.2016, была представлена скорректированная формула изобретения в следующей редакции:

«1. Способ обнаружения вредоносного программного обеспечения на устройстве пользователя, в котором:

а) модифицируют программно-аппаратную часть устройства путем модификации элементов уровней архитектуры устройства для подконтрольного исполнения приложения, которое заключается в контроле над исполнением на всех уровнях архитектуры,

причем контроль предполагает протоколирование информации о событиях на всех уровнях архитектуры, а также остановку исполнения или внесения корректировки в исполнения приложения на любом уровне архитектуры;

б) выбирают по крайней мере один сценарий для активации вредоносного функционала приложения из базы сценариев, при этом под сценарием понимается список из набора событий активации;

в) подконтрольно исполняют исследуемое приложение в соответствии со сценарием на модифицированной программно-аппаратной части устройства, где исполнение сценария заключается в создании уровнями архитектуры событий активации;

г) протоколируют модифицированной программно-аппаратной частью устройства информацию о событиях на уровнях архитектуры устройства, вызванных подконтрольным исполнением на каждом уровне архитектуры устройства исследуемого приложения, исполняемого по сценарию;

д) обнаруживают вредоносное программное обеспечение, анализируя во время подконтрольного исполнения исследуемого приложения информацию, протоколируемую на шаге г), на наличие событий на уровнях архитектуры, характерных для вредоносного программного обеспечения,

при этом подконтрольное исполнение исследуемого приложения на модифицированной программно-аппаратной части устройства не даст обнаруженному вредоносному функционалу выполниться.

2. Способ по п.1, в котором сценарий — это список из набора событий, создание которых модифицированной программно-аппаратной частью устройства активирует вредоносный функционал приложения.

3. Способ по п.1, в котором анализ протоколируемой информации осуществляется путем сравнения протоколируемой информации о событиях, вызванных работой исследуемого приложения с шаблонами поведения, содержащими события, характерные для вредоносного программного обеспечения.

4. Система обнаружения вредоносного программного обеспечения на устройстве пользователя, при этом система содержит:

а) модифицированную программно-аппаратную часть устройства, где модификация заключается в модификации элементов уровней архитектуры устройства для подконтрольного исполнения приложения, которое заключается в контроле над исполнением на всех уровнях архитектуры,

причем контроль предполагает протоколирование информации о событиях на всех уровнях архитектуры, а также остановку исполнения или внесения корректировки в исполнения приложения на любом уровне архитектуры,

при этом упомянутая часть предназначена для:

- подконтрольного исполнения исследуемого приложения, запущенного модулем управления, где исполнение сценария заключается в создании уровнями архитектуры событий активации;

- протоколирования информации о событиях на уровнях архитектуры устройства, вызванных исполнением на каждом уровне архитектуры устройства исследуемого приложения, исполняемого по сценарию;

б) модуль управления, предназначенный для:

- подконтрольного запуска приложения в соответствии со сценарием, выбранным для активации вредоносного функционала приложения из базы сценариев, при этом под сценарием понимается список из набора событий активации,

- остановки исполнения приложения или внесения корректировки в исполнения приложения на любом уровне архитектуры, при обнаружении модулем анализа вредоносного программного обеспечения, не дав обнаруженному вредоносному функционалу выполниться;

в) базу сценариев, связанную с модулем управления и предназначенную для хранения сценариев;

г) модуль анализа, связанный с модулем управления и модифицированной программно-аппаратной частью устройства, предназначенный для обнаружения вредоносного программного обеспечения, анализируя информацию, протоколируемую

модифицированной программно-аппаратной частью устройства на наличие событий на уровнях архитектуры, характерных для вредоносного программного обеспечения.

5. Система по п. 4, в которой система дополнительно включает базу шаблонов, связанную с модулем анализа и предназначенную для хранения шаблонов поведения.»

Данная скорректированная формула была принята к рассмотрению (п. 4.9 Правил ППС).

В соответствии с пунктом 5.1 Правил ППС дело заявки было направлено для проведения дополнительного информационного поиска в виду представления скорректированной формулы изобретения.

В заключении, которое было представлено 07.04.2017, экспертизой был сделан вывод о соответствии заявленной группы изобретений, охарактеризованной в указанной выше скорректированной формуле изобретения, всем условиям патентоспособности, предусмотренным статьей 1350 Кодекса.

Учитывая вышеизложенное, на заседании от 29.05.2017 коллегия пришла к выводу о наличии оснований для принятия Роспатентом следующего решения:

удовлетворить возражение, поступившее 18.12.2015, отменить решение Роспатента об отказе в выдаче патента от 10.06.2015, выдать патент Российской Федерации по заявке №2013129555/08 с формулой, представленной заявителем 18.11.2016.

Форма № 81а ИЗ

(21) 2013129555/08

(51) МПК

G06F 21/56 (2006.01)
G06F 21/53 (2006.01)

(57) 1. Способ обнаружения вредоносного программного обеспечения на устройстве пользователя, в котором:

а) модифицируют программно-аппаратную часть устройства путем модификации элементов уровней архитектуры устройства для подконтрольного исполнения приложения, которое заключается в контроле над исполнением на всех уровнях архитектуры,

причем контроль предполагает протоколирование информации о событиях на всех уровнях архитектуры, а также остановку исполнения или внесения корректировки в исполнения приложения на любом уровне архитектуры;

б) выбирают по крайней мере один сценарий для активации вредоносного функционала приложения из базы сценариев, при этом под сценарием понимается список из набора событий активации;

в) подконтрольно исполняют исследуемое приложение в соответствии со сценарием на модифицированной программно-аппаратной части устройства, где исполнение сценария заключается в создании уровнями архитектуры событий активации;

г) протоколируют модифицированной программно-аппаратной частью устройства информацию о событиях на уровнях архитектуры устройства, вызванных подконтрольным исполнением на каждом уровне архитектуры устройства исследуемого приложения, исполняемого по сценарию;

д) обнаруживают вредоносное программное обеспечение, анализируя во время подконтрольного исполнения исследуемого приложения информацию, протоколируемую на шаге г), на наличие событий на уровнях архитектуры, характерных для вредоносного программного обеспечения,

при этом подконтрольное исполнение исследуемого приложения на модифицированной программно-аппаратной части устройства не даст обнаруженному вредоносному функционалу выполниться.

2. Способ по п.1, в котором сценарий — это список из набора событий, создание которых модифицированной программно-аппаратной частью устройства активирует вредоносный функционал приложения.

3. Способ по п.1, в котором анализ протоколируемой информации осуществляется путем сравнения протоколируемой информации о событиях, вызванных работой исследуемого приложения с шаблонами поведения, содержащими события, характерные для вредоносного программного обеспечения.

4. Система обнаружения вредоносного программного обеспечения на устройстве пользователя, при этом система содержит:

а) модифицированную программно-аппаратную часть устройства, где модификация заключается в модификации элементов уровней архитектуры устройства для подконтрольного исполнения приложения, которое заключается в контроле над исполнением на всех уровнях архитектуры,

причем контроль предполагает протоколирование информации о событиях на всех уровнях архитектуры, а также остановку исполнения или внесения корректировки в исполнения приложения на любом уровне архитектуры,

при этом упомянутая часть предназначена для:

- подконтрольного исполнения исследуемого приложения, запущенного модулем управления, где исполнение сценария заключается в создании уровнями архитектуры событий активации;

- протоколирования информации о событиях на уровнях архитектуры устройства, вызванных исполнением на каждом уровне архитектуры устройства исследуемого приложения, исполняемого по сценарию;

б) модуль управления, предназначенный для:

- подконтрольного запуска приложения в соответствии со сценарием, выбранным для активации вредоносного функционала приложения из базы сценариев, при этом под сценарием понимается список из набора событий активации,

- остановки исполнения приложения или внесения корректировки в исполнения приложения на любом уровне архитектуры, при обнаружении модулем анализа вредоносного программного обеспечения, не дав обнаруженному вредоносному функционалу выполниться;

в) базу сценариев, связанную с модулем управления и предназначенную для хранения сценариев;

г) модуль анализа, связанный с модулем управления и модифицированной программно-аппаратной частью устройства, предназначенный для обнаружения вредоносного программного обеспечения, анализируя информацию, протоколируемую модифицированной программно-аппаратной частью устройства на наличие событий на уровнях архитектуры, характерных для вредоносного программного обеспечения.

5. Система по п. 4, в которой система дополнительно включает базу шаблонов, связанную с модулем анализа и предназначенную для хранения шаблонов поведения.

Приоритет:

28.06.2013

(56) US 2013/0122861 A1, 16.05.2013;

US 2010/0107252 A1, 29.04.2010;

В.М. Рувинская и др. «Эвристические методы детектирования вредоносных программ на основе сценариев», 31.12.2008;

US 2012/0222123 A1, 30.08.2012;

US 2003/0159063 A1, 21.08.2003.

Примечание: при публикации сведений о выдаче патента будут использованы первоначальное описание и чертежи.