РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2014 115 338** (13) **A**

(51) МПК
G06F 21/00 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2014115338/08, 01.10.2012**

Приоритет(ы):
(30) Конвенционный приоритет:
24.10.2011 US 61/550,795

(43) Дата публикации заявки: **10.12.2015** Бюл. № **34**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **26.05.2014**

(86) Заявка PCT:
US 2012/058319 (01.10.2012)

(87) Публикация заявки PCT:
WO 2013/062726 (02.05.2013)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(71) Заявитель(и):
ШНЕЙДЕР ЭЛЕКТРИК ЭНДЮСТРИ САС (FR)

(72) Автор(ы):
ЛЕ САН Орельен (US)

(54) СИСТЕМА И СПОСОБ ДЛЯ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМИ ПРОЦЕССАМИ

(57) Формула изобретения

1. Устройство автоматического управления, сконфигурированное с возможностью предоставлять информацию по безопасности, причем устройство автоматического управления содержит:

- запоминающее устройство;
- по меньшей мере, один процессор, соединенный с запоминающим устройством;
- интерфейс промышленного протокола, выполняемый посредством, по меньшей мере, одного процессора и сконфигурированный с возможностью обмениваться сообщениями, отформатированными согласно промышленному протоколу; и
- пассивный компонент системы безопасности, выполняемый посредством, по меньшей мере, одного процессора и сконфигурированный с возможностью:
- обнаруживать, по меньшей мере, одну потенциальную проблему безопасности, ассоциированную с устройством автоматического управления; и
- передавать информацию, отражающую, по меньшей мере, одну потенциальную проблему безопасности.

2. Устройство автоматического управления по п. 1, в котором, по меньшей мере, одна потенциальная проблема безопасности включает в себя, по меньшей мере, одно из надежности пароля, открытого логического порта, порогового объема трафика, обнаруженного на открытом логическом порту, интернет-подключения, изменения логики управления технологическим процессом, сохраненной в устройстве

RU 2014115338 A

RU 2014115338 A

автоматического управления, изменения программного компонента, сохраненного в устройстве

автоматического управления, изменения аппаратного компонента устройства автоматического управления, изменения идентификатора компьютера, используемого идентифицированным пользователем для того, чтобы осуществлять доступ к устройству автоматического управления, нового идентификатора компьютера, используемого для того, чтобы осуществлять доступ к устройству автоматического управления, новой учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения конфигурационной информации, сохраненной в устройстве автоматического управления, попытки получения доступа к устройству автоматического управления из компьютерной системы, имеющей идентификатор, который не находится в списке идентификаторов, авторизованных на то, чтобы осуществлять доступ к устройству автоматического управления, наличия файла, сохраненного в устройстве автоматического управления, который не имеет подписи, попытки получения доступа к устройству автоматического управления из местоположения, ранее не ассоциированного с компьютерной системой, попытки осуществлять доступ к несуществующим ресурсам устройства автоматического управления, перенаправления веб-страницы, представленной посредством устройства автоматического управления, на сторонний веб-узел и возникновения порогового числа ошибок запросов на осуществление связи.

3. Устройство автоматического управления по п. 1, в котором пассивный компонент системы безопасности дополнительно сконфигурирован с возможностью принимать ответ на информацию.

4. Устройство автоматического управления по п. 3, в котором ответ включает в себя запрос на то, чтобы признавать потенциальную проблему безопасности, и пассивный компонент системы безопасности дополнительно сконфигурирован с возможностью, в ответ на прием запроса, сохранять информацию, отражающую то, что потенциальная проблема безопасности признана.

5. Устройство автоматического управления по п. 3, в котором ответ включает в себя запрос на то, чтобы разрешать потенциальную проблему безопасности, и пассивный компонент системы безопасности дополнительно сконфигурирован с возможностью, в ответ на прием запроса, выполнять корректирующий компонент.

6. Устройство автоматического управления по п. 3, в котором ответ включает в себя запрос на то, чтобы предоставлять дополнительную информацию, связанную с потенциальной проблемой безопасности, и пассивный компонент системы безопасности дополнительно сконфигурирован с возможностью, в ответ на прием запроса, предоставлять дополнительную информацию.

7. Устройство автоматического управления по п. 1, дополнительно содержащее компонент инструментальной панели, выполняемый посредством, по меньшей мере, одного процессора и сконфигурированный с возможностью запускать виджет состояния системы безопасности, при этом виджет состояния системы безопасности сконфигурирован с возможностью принимать информацию, отражающую, по меньшей мере, одну потенциальную проблему безопасности, и передавать предупреждающее уведомление, соответствующее, по меньшей мере, одной потенциальной проблеме

безопасности.

8. Способ предоставления информации по безопасности, при этом способ содержит этапы, на которых:

- обнаруживают, посредством устройства автоматического управления, по меньшей мере, одну потенциальную проблему безопасности, ассоциированную с устройством

RU 2014115338 A

RU 2014115338 A

автоматического управления; и

- передают информацию, отражающую, по меньшей мере, одну потенциальную проблему безопасности.

9. Способ по п. 8, в котором обнаружение, по меньшей мере, одной потенциальной проблемы безопасности включает в себя этап, на котором обнаруживают, по меньшей мере, одно из надежности пароля, открытого логического порта, порогового объема трафика, обнаруженного на открытом логическом порту, интернет-подключения, изменения логики управления технологическим процессом, сохраненной в устройстве автоматического управления, изменения программного компонента, сохраненного в устройстве автоматического управления, изменения аппаратного компонента устройства автоматического управления, изменения идентификатора компьютера, используемого идентифицированным пользователем для того, чтобы осуществлять доступ к устройству автоматического управления, нового идентификатора компьютера, используемого для того, чтобы осуществлять доступ к устройству автоматического управления, новой учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения конфигурационной информации, сохраненной в

устройстве автоматического управления, попытки получения доступа к устройству автоматического управления из компьютерной системы, имеющей идентификатор, который не находится в списке идентификаторов, авторизованных на то, чтобы осуществлять доступ к устройству автоматического управления, наличия файла, сохраненного в устройстве автоматического управления, который не имеет подписи, попытки получения доступа к устройству автоматического управления из местоположения, ранее не ассоциированного с компьютерной системой, попытки осуществлять доступ к несуществующим ресурсам устройства автоматического управления, перенаправления веб-страницы, представленной посредством устройства автоматического управления, на сторонний веб-узел и возникновения порогового числа ошибок запросов на осуществление связи.

10. Способ по п. 8, дополнительно содержащий этап, на котором принимают ответ на информацию.

11. Способ по п. 10, в котором ответ включает в себя запрос на то, чтобы признавать потенциальную проблему безопасности, и способ дополнительно содержит этап, на котором сохраняют, в ответ на прием запроса, информацию, отражающую то, что потенциальная проблема безопасности признана.

12. Способ по п. 10, в котором ответ включает в себя запрос на то, чтобы разрешать потенциальную проблему безопасности, и способ дополнительно содержит этап, на котором выполняют, в ответ на прием запроса, корректирующий компонент.

13. Способ по п. 10, в котором ответ включает в себя запрос на то, чтобы предоставлять дополнительную информацию, связанную

с потенциальной проблемой безопасности, и способ дополнительно содержит этап, на котором предоставляют, в ответ на прием запроса, дополнительную информацию.

14. Способ по п. 8, дополнительно содержащий этапы, на которых:

- запускают виджет состояния системы безопасности в инструментальной панели;

- принимают, посредством виджета состояния системы безопасности, информацию, отражающую, по меньшей мере, одну потенциальную проблему безопасности; и

- передают, посредством виджета состояния системы безопасности, предупреждающее уведомление, соответствующее, по меньшей мере, одной потенциальной проблеме безопасности.

15. Энергонезависимый машиночитаемый носитель, сохраняющий последовательности инструкций для предоставления информации по безопасности, включающих в себя

RU 2014115338 A

RU 2014115338 A

инструкции, кодированные с возможностью инструктировать, по меньшей мере, одному процессору:

- обнаруживать, по меньшей мере, одну потенциальную проблему безопасности, ассоциированную с устройством автоматического управления; и
- передавать информацию, отражающую, по меньшей мере, одну потенциальную проблему безопасности.

16. Машиночитаемый носитель по п. 15, в котором инструкции, кодированные с возможностью инструктировать, по меньшей мере, одному процессору обнаруживать, по меньшей мере, одну потенциальную проблему безопасности, включают в себя инструкции,

чтобы обнаруживать, по меньшей мере, одно из надежности пароля, открытого логического порта, порогового объема трафика, обнаруженного на открытом логическом порту, интернет-подключения, изменения логики управления технологическим процессом, сохраненной в устройстве автоматического управления, изменения программного компонента, сохраненного в устройстве автоматического управления, изменения аппаратного компонента устройства автоматического управления, изменения идентификатора компьютера, используемого идентифицированным пользователем для того, чтобы осуществлять доступ к устройству автоматического управления, нового идентификатора компьютера, используемого для того, чтобы осуществлять доступ к устройству автоматического управления, новой учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения учетной записи пользователя, сохраненной в устройстве автоматического управления, изменения конфигурационной информации, сохраненной в устройстве автоматического управления, попытки получения доступа к устройству автоматического управления из компьютерной системы, имеющей идентификатор, который не находится в списке идентификаторов, авторизованных на то, чтобы осуществлять доступ к устройству автоматического управления, наличия файла, сохраненного в устройстве автоматического управления, который не имеет подписи, попытки получения доступа к устройству автоматического управления из местоположения, ранее не ассоциированного с компьютерной системой, попытки осуществлять доступ к несуществующим ресурсам устройства автоматического управления, перенаправления веб-страницы, представленной

посредством устройства автоматического управления, на сторонний веб-узел и возникновения порогового числа ошибок запросов на осуществление связи.

17. Машиночитаемый носитель по п. 15, в котором инструкции кодируются с возможностью дополнительно инструктировать, по меньшей мере, одному процессору принимать ответ на информацию.

18. Машиночитаемый носитель по п. 15, в котором инструкции кодируются с возможностью дополнительно инструктировать, по меньшей мере, одному процессору сохранять информацию, отражающую то, что потенциальная проблема безопасности признана, в ответ на прием запроса на то, чтобы признавать потенциальную проблему безопасности.

19. Машиночитаемый носитель по п. 15, в котором инструкции кодируются с возможностью дополнительно инструктировать, по меньшей мере, одному процессору выполнять корректирующий компонент в ответ на прием запроса на то, чтобы разрешать потенциальную проблему безопасности.

20. Машиночитаемый носитель по п. 15, в котором инструкции кодируются с возможностью дополнительно инструктировать, по меньшей мере, одному процессору предоставлять дополнительную информацию в ответ на прием запроса на то, чтобы предоставлять дополнительную информацию, связанную с потенциальной проблемой

RU 2014115338 A
RU 2014115338 A

безопасности.

RU 2014115338 A