Информационная система по мониторингу событий информационной безопасности в межведомственной сети передачи данных электронного правительства (Система мониторинга МСПДЭП)

Инструкция по подключению серверного оборудования, используемого в МСПД к Системе мониторинга МСПДЭП

LanSec

Ver. 2.0

Содержание

1. Введение

Настоящая «Инструкция по подключению информационной системы мониторинга событий информационной безопасности к межведомственной сети передачи данных электронного правительства (LANSEC)» (далее – Инструкция) устанавливает общий порядок подключения хостов (подключенных серверов к Межведомственной сети передачи данных электронного правительство (далее - МСПД)) к системе LANSEC.

Инструкция разработана с целью создания единого порядка по подключению хостов государственных органов, использующих МСПД к системе LANSEC, с учетом установленных операционных систем в используемых серверах.

Данная Инструкция разработана согласно техническому заданию на создание «Информационной системы по мониторингу событий информационной безопасности в межведомственной сети передачи данных электронного правительство» (далее – Система мониторинга), а также учитывая функции, задачи, архитектуру и т.п. настоящей системы.

Инструкция содержит в себе информацию о Системе мониторинга, ее функциях, подключаемых объектах к данной системе, краткую информацию о программе информатор Системы мониторинга, о поддерживаемых платформах, а также о порядке регистрации и установки программы информатор, включая активацию программы информатор в разных операционных системах.

2. О системе

Система «LanSec» специализирована на выявление событий информационной безопасности возникающих в межведомственной сети передачи данных, посредством, которого ведет контроль ее работоспособности и соответствия параметрам информационной безопасности. Система автоматизирует процессы обнаружения инцидентов информационной безопасности (ИБ) в межведомственной сети на основе сбора и анализа информации о полученных событиях ИБ. Также, она отслеживает состояние сетевых устройств подключенных к МСПД на наличие активности.

Система, в целях оперативного выявления и реагирования на инциденты ИБ в межведомственной сети выполняет:

- централизованный сбор и обработку событий ИБ в режиме реального времени;
- долговременное хранение событий и инцидентов ИБ для формирования доказательной базы;
- своевременное выявление инцидентов ИБ;

- оперативное реагирование на инциденты безопасности, фокусируя внимание подразделений ИБ на реальных угрозах;

- управление процессом расследования и устранения инцидентов ИБ.

Система применяется к таким подключенным к ней объектам, таким как:

системы, которые:

— предоставляют службы безопасности (например, серверы аутентификации),

— способствуют сегментации сети (например, внутренние межсетевые экраны),

— могут влиять на безопасность среды ДДК (например, серверы разрешения имен или веб-переадресации);

компоненты виртуализации, например:

— виртуальные машины,

— виртуальные коммутаторы и (или) маршрутизаторы,

— виртуальные приложения и (или) компьютеры,

сетевые компоненты, в том числе:

— межсетевые экраны,

— коммутаторы,

— маршрутизаторы,

— беспроводные точки доступа,

— устройства сетевой безопасности,

— прочие устройства безопасности;

типы серверов, в том числе:

— веб-серверы,

— серверы приложений,

— серверы баз данных,

— серверы аутентификации,

— почтовые серверы.

Разработанная система обеспечивает реализацию следующих функциональных возможностей:

- предоставление уведомления о состоянии активности сетевых устройств, включая подключенные к ним хосты (серверы, сетевые средства и т.д.).

– сбор событий из журналов источников событий с сохранением результата обработки в централизованной базе данных.

– поддержка штатной интеграции с различными типами источников событий безопасности;

– предоставление функционала агрегации, нормализации и корреляции событий от источников. Параметры агрегации, нормализации и корреляция являются настраиваемыми;

– предоставление возможности подключения источников событий, неподдерживаемых штатно;

– предоставление функционала формирования отчетов по событиям, сохраненным в централизованной базе данных;

– обеспечение доступности информации в течение двух месяцев в прямом доступе и в течение 6 месяцев в архиве (с возможностью восстановления);

– обеспечение интеграции с репутационной базой IP и URL адресов, выявлять сетевое взаимодействие с узлами (серверы управления, коммутация и т.д.);

– реализация модели ролевого доступа.

Система интегрирована с различными современными веб-технологиями и библиотеками (Big data visualization), совокупностями подходов, инструментами и методами обработки структурированных данных больших объёмов для получения воспринимаемых специалистом (оператором) результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети.

3. Программа информатор Системы мониторинга

Основными составляющими модуля анализа является программа информатор и сервер. Программа информатор работает на каждом контролируемом хосте. Сервер, анализирует данные, полученные непосредственно от программы информатор, а также, данные полученные из других источников без программы информатор через протокол syslog таких как, брандмауэры, коммутаторы, маршрутизаторы, точки доступа, сетевые устройства и т.д.

Программа информатор передает данные о событиях в центр управления через безопасный и аутентифицированный канал, который устанавливается с использованием процесса регистрации применением уникальных предварительно разделенных ключей.

3.1. Поддерживаемые платформы

Система основана на много платформенной программе информатор, который пересылает системные данные (например, сообщения журналов, хэши файлов и обнаруженные аномалии) в модуль центр управления, где они далее анализируются и обрабатываются, что приводит к предупреждениям (оповещениям) безопасности. Программа информатор может использоваться для мониторинга физических серверов, виртуальных машин и облачных экземпляров, которые поддерживают работу в операционных системах Windows, Red Hat, CentOS, Fedora, SUSE, Ubuntu, Debian, Solaris.

3.2. Регистрация программа информатора

В процессе подключения хоста (сервера находящегося в МСПД) к Системе мониторинга, необходимо предварительно получить соответствующий ключ. Для получения соответствующего ключа проводится следующий регистрационный процесс включающий в себя два этапа:

Первый этап: В данном этапе выполняется обращение к администратору Системы мониторинга Центра информационной безопасности и содействия в обеспечении общественного порядка (далее - Центр) где администратору надо предоставить информацию IP адрес хоста подключенного к МСПД.

Второй этап: После получения обращения, согласно предоставленным информациям IP адреса, администратор Системы мониторинга регистрирует IP адрес организации (хоста) и предоставляет данному хосту соответствующий ключ, который используется при установке программы информатор, а именно для подключения хоста к Системе мониторинга. При этом в процессе подключения также используется IP адрес Системы мониторинга (предоставляется специалистами Центра).

3.3. Установка и активация программа информатора в разных семействах операционных систем

3.3.1. В операционных системах Windows

Установка и активация программы информатор Системы мониторинга в операционных системах семейства Windows осуществляется по следующему порядку:

1. Загрузка установочного приложения (программы) по ссылке ***https://infosec.uz/ru/programs/mspd-lansec/***. После загрузки следует запустить приложение и дать разрешение процессу установки, нажав кнопку «Run» (рис.1).

Примечание: В некоторых случаях после запуска установочного приложения может сразу появится окно установки на втором этапе.

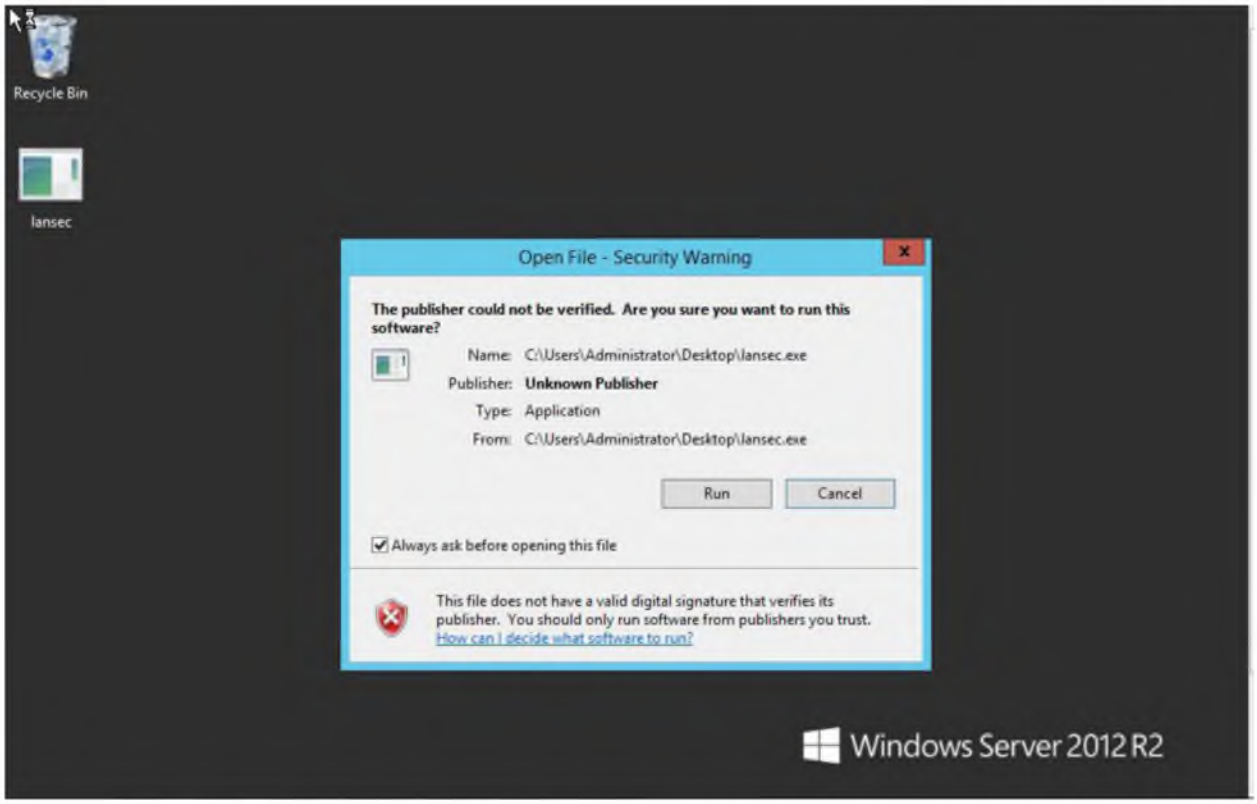

Рис. 1. Запуск установочного приложения программа информатор

2. После первого этапа на главном экране появляется окно установки программа информатор и где надо дать разрешение на установку нажав кнопку «Установить» (рис.2).

Рис. 2. Запуск процесса установки приложения программа информатор

3. После завершения процесса на главном экране выходить уведомление об успешной завершении процесса установки и для продолжения следует нажать «ОК» (рис.3).

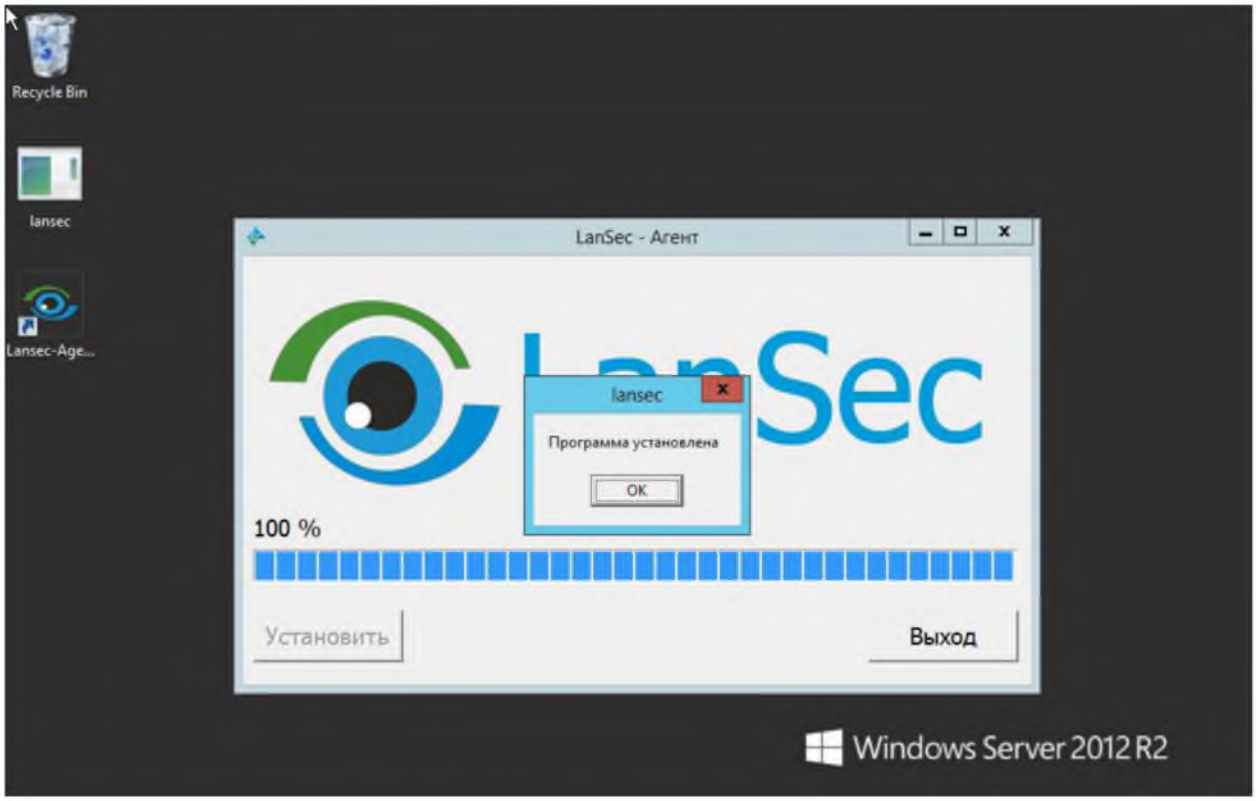

Рис. 3. Уведомление об установке приложение программа информатора

4. Установив программу информатор, следует осуществлять процесс активации программа информатора, посредством ввода полученного IP адреса Системы мониторинга и ключа регистрации согласно разделу «3.2. Регистрация программы информатор» настоящей Инструкции по соответствующим полям «Manager IP» и «Authentication key» и нажимается на сохранение. Затем, выводится уведомление об успешном подключении (добавлении) программа информатора (рис. 4 и 5).

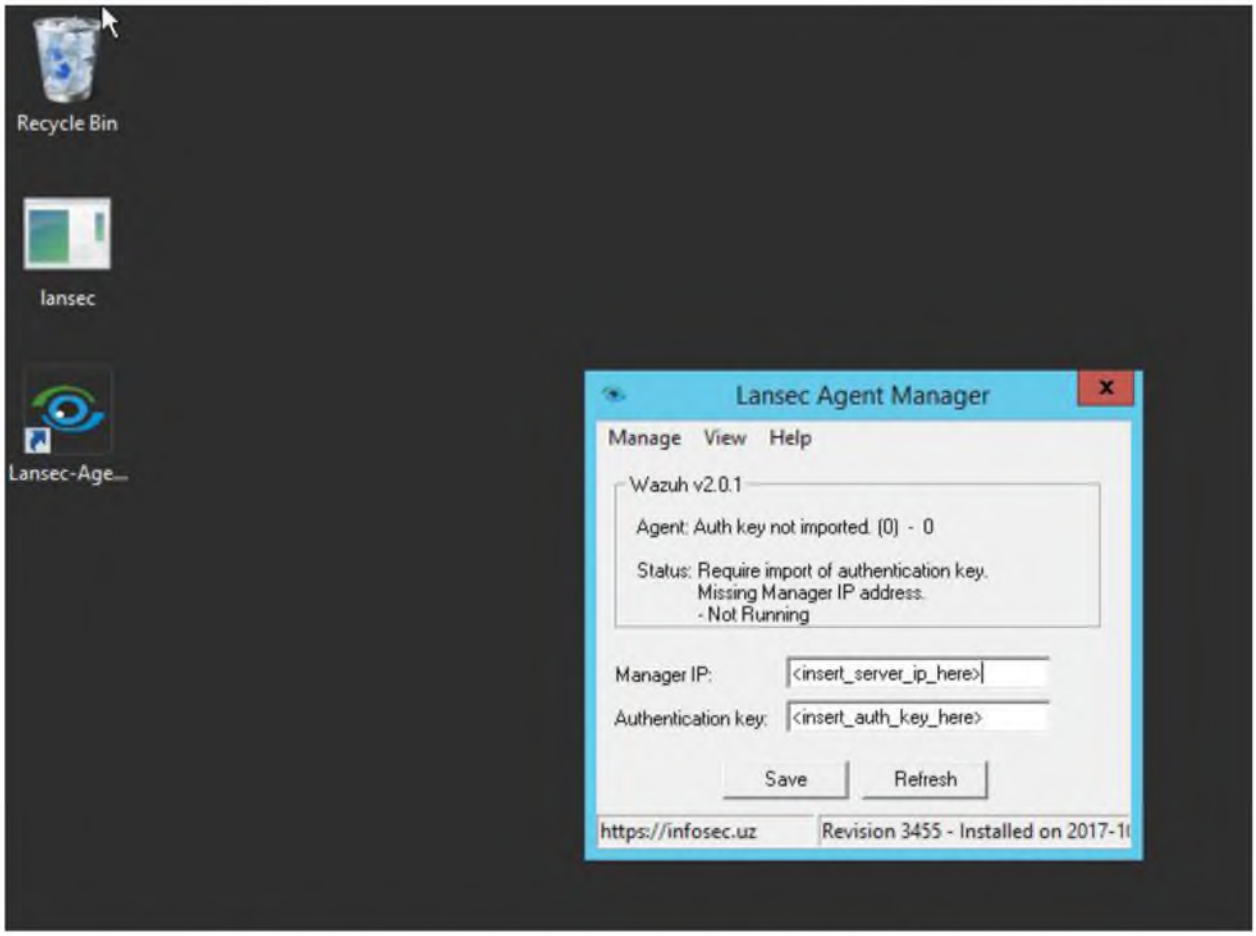

Рис. 4. Ввод и сохранение полученного ключа и IP-адреса Системы мониторинга

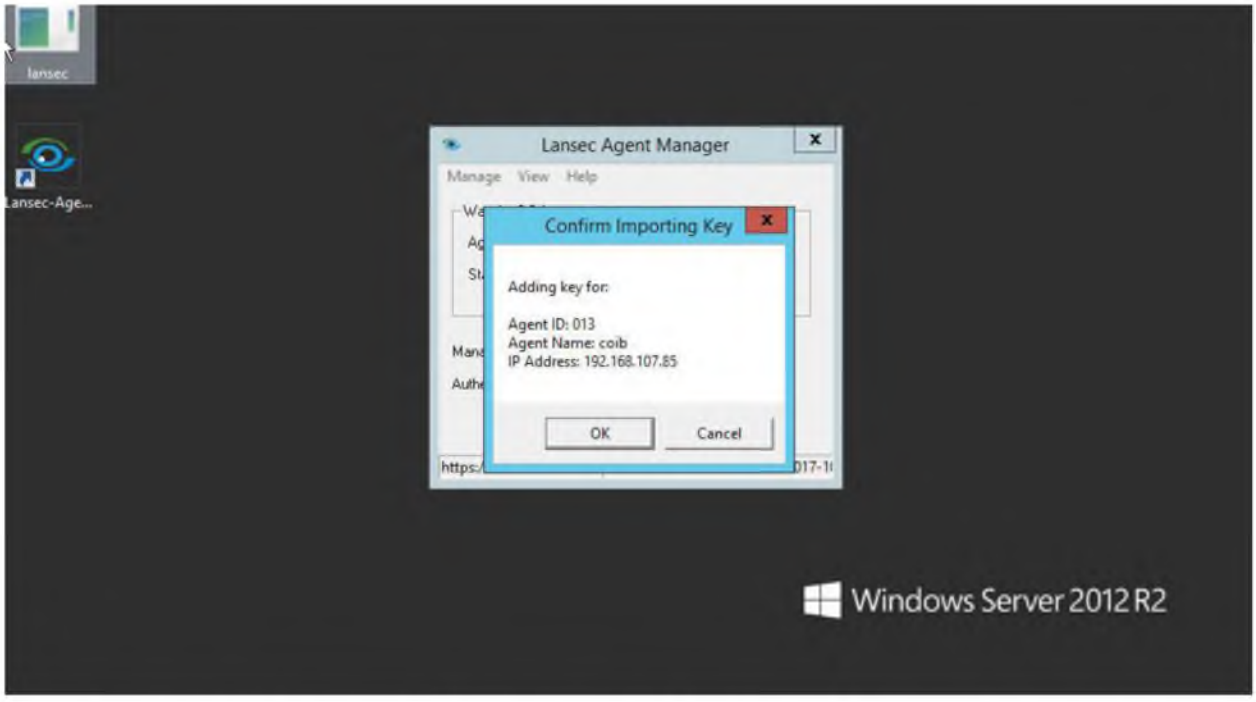

Рис. 5. Уведомление об успешном подключении программы информатор

5. Вслед за окончанием всех предыдущих этапов можно начать работу нажав кнопку «Start» из меню «Manage» в окне «Lansec Agent Manager». После нажатия «Start» на экране выходит уведомление об успешном старте/запуске программа информатора (рис. 6).

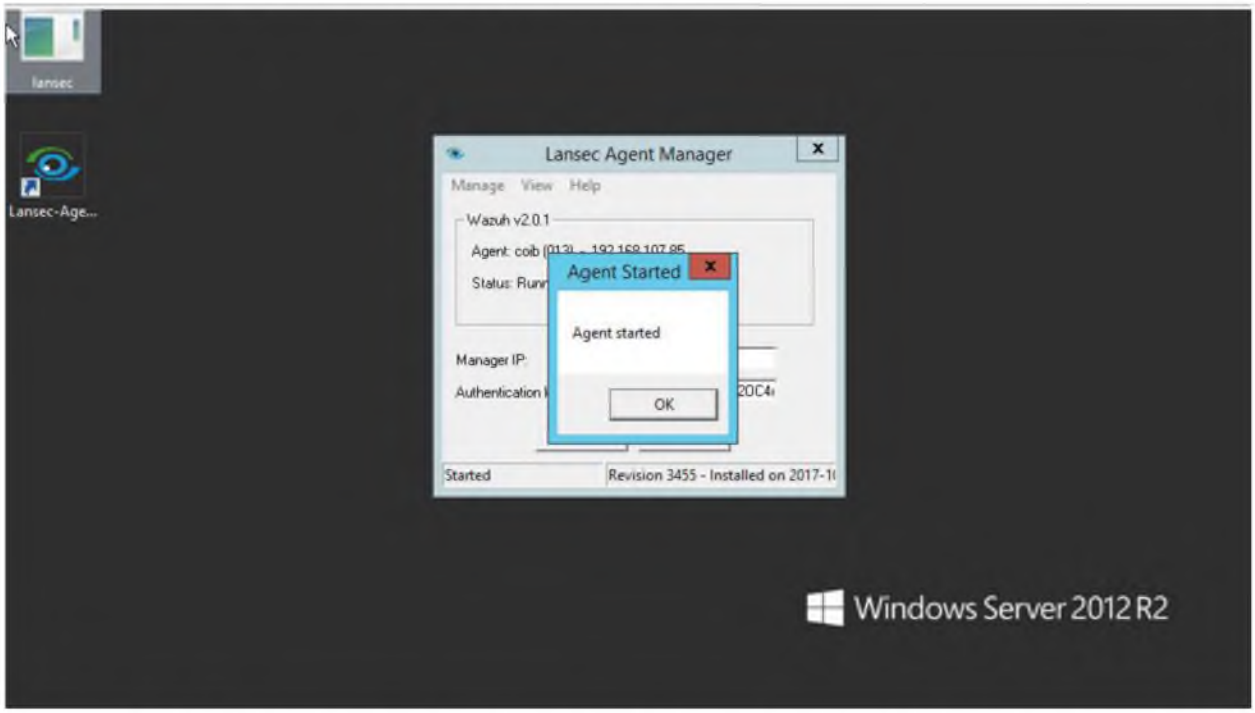

Рис. 6. Старт работы программы информатор и уведомление об успешном старте

3.3.2. В операционных системах Debian/Ubuntu

В операционных системах Debian/Ubuntu, процесс установки и активации программы информатор немного отличается. В данных семействах операционных систем данный процесс осуществляется по нижеуказанной процедуре:

1. На командном экране операционной системы вводится команда установки приложения программа информатор с помощью утилиты «dpkg», следующим образом: **dpkg –i {NAME_AGENT_FILE}.deb.** Приводится пример, где названием программы информатор является «lansec-agent-ubuntu-xemial» (рис 7).

Примечание: В данной ситуации, как и у Windows, в начале загружается установочное приложение программа информатор на сервер, по ссылке: ***https://infosec.uz/ru/programs/mspd-lansec/***.

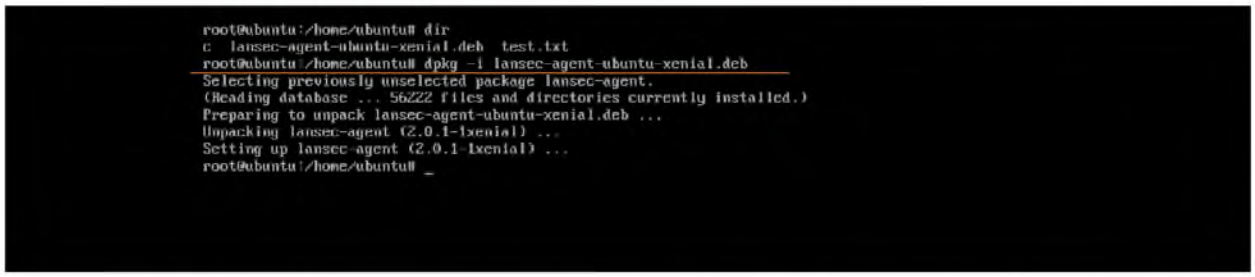

Рис. 7. Запуск установки приложения программа информатор

2. После установки программы информатор, выводится команда **nano /var/ossec/etc/ossec.conf** (рис. 8) и в теге **«SERVER_IP»** следует указать IP адрес Системы мониторинга (рис. 9) полученный согласно разделу 3.2. «Регистрация программа информатор» настоящей Инструкции.

Рис. 8. Команда для открытия файла ossec.conf

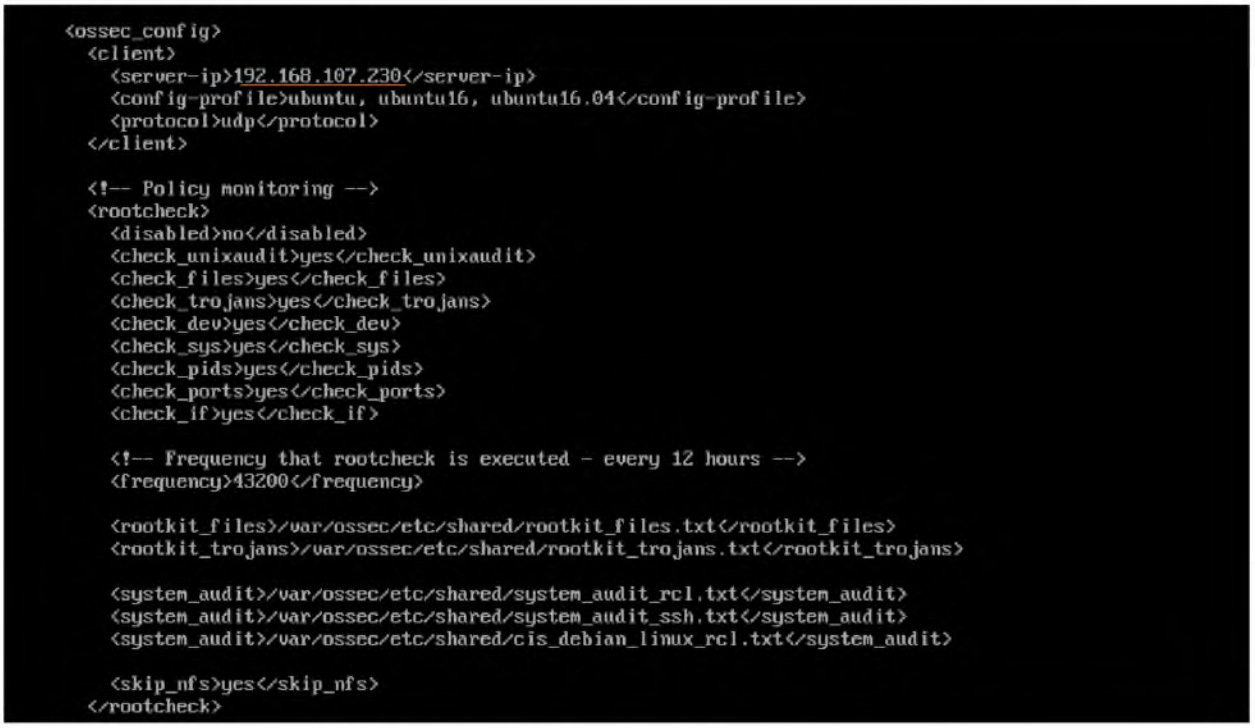

Рис. 9. IP адрес Системы мониторинга

3. Следующим шагом будет ввод команды **/var/ossec/bin/manage_agents,** где нажатием кнопки «I» импортируется и вводится генерированный ключ, полученный согласно разделу «3.2. Регистрация программы информатор» настоящей Инструкций (рис. 10).

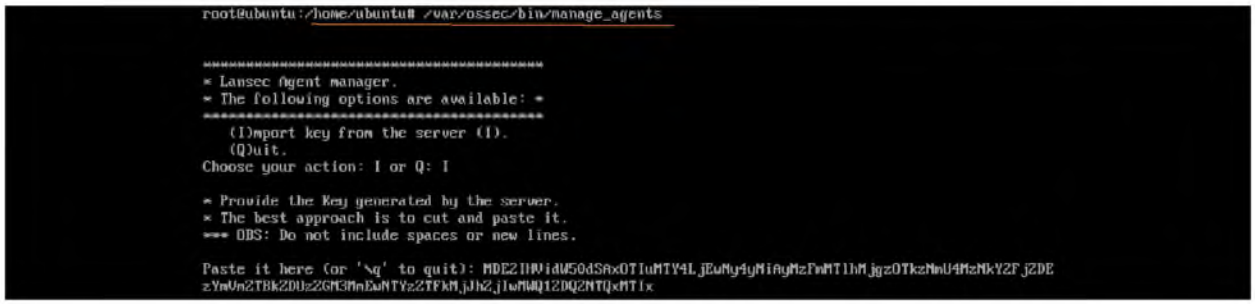

Рис. 10. Импортирование и генерация полученного ключа

4. После завершения предыдущего этапа, для подтверждения нажимается кнопка «Enter» и, затем генерированный ключ утверждается нажатием «Y» и снова нажимается «Enter», а для выхода из данного процесса нажимается «Q» (рис. 11).

Рис. 11. Подтверждение указанного ключа

5. По окончанию вышеперечисленных этапов, для осуществления эксплуатации программы информатор вводится команда перезагрузки программа информатора. В примере приводится следующим образом: **service lansec-agent restart** (рис. 12).

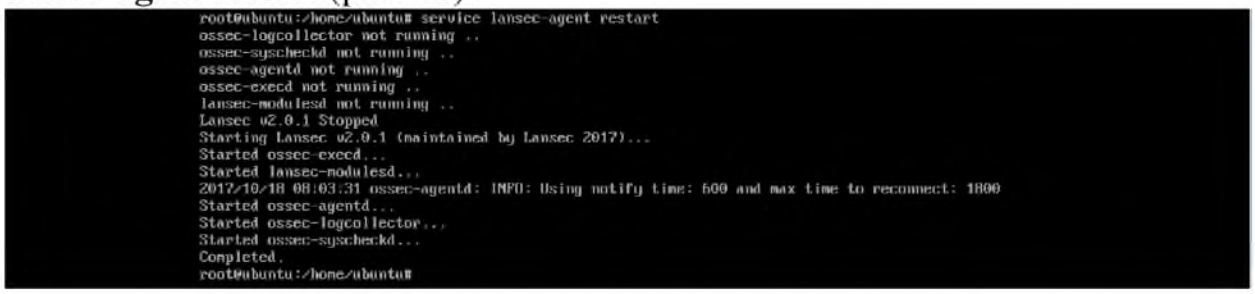

Рис. 12. Перезагрузка программы информатор для запуска в эксплуатацию

3.3.3. В операционных системах CentOS/RHEL

1. Для установки программы информатор вводим команду **rpm –I lansec-agent.rpm**

Примечание: В данной ситуации, как и у остальных операционных системах, в начале загружается установочное приложение программа информатор на сервер, по ссылке: ***https://infosec.uz/ru/programs/mspd-lansec/.***

```
[root@localhost centos]# rpm -i lansec-agent.rpm
[root@localhost centos]#
```

2. Затем следует ввести IP-адрес менеджера в программе информатор. Для этого пишем команду **nano /war/ossec/etc/ossec.conf**. В тэге **«SERVER-IP»** вводится IP-адрес сервера 192.168.107.230.

```
 GNU nano 2.3.1                File: /var/ossec/etc/ossec.conf                Modified

<!--
  Lansec - Agent - Default configuration for rhel 7
  More info at: https://infosec.uz
-->

<ossec_config>
  <client>
    <server-ip>192.168.107.230</server-ip>
    <config-profile>rhel, rhel7</config-profile>
    <protocol>udp</protocol>
  </client>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_unixaudit>yes</check_unixaudit>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>

    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>

    <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>

    <system_audit>/var/ossec/etc/shared/system_audit_rcl.txt</system_audit>
    <system_audit>/var/ossec/etc/shared/system_audit_ssh.txt</system_audit>
```

3. Теперь сгенерированный ключ надо ввести в программу информатор. Для этого набираем команду **/war/ossec/bin/manage_agents,** затем нажимаем кнопку **«I»** и вставляем сгенерированный ключ**.**

```
[root@localhost centos]# /var/ossec/bin/manage_agents

****************************************
* Lansec Agent manager.*
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDI3IGNvaWJ0ZXN0IDE5Mi4xNjguMTA3LjU4IDYyNDAzNzY2ODUxOGIxNzY3ZWFiMjIwYjYxMDRhMWJjNzZhNjQxNGE2N
zM5NDY2ZWIxMjJkNmQ0ZGUyOGY0YTg=
```

4. После этого, нажимается кнопка «ENTER», вводится «Y» и снова нажимается «ENTER». Вслед за этим, нажатием «Q» выходим из установки.