Колледж автоматизации и информационных технологий

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Программная защита от НСД к информации ограниченного доступа в ООО «АЛЬФАКОМ»

ВЫПОЛНИЛ СТУДЕНТ ГРУППЫ

Кудряшов Борис Сергеевич

РУКОВОДИТЕЛЬ ВКР: **Филиппов А. Ю.**

КОНСУЛЬТАНТ ПО ЭКОНОМИЧЕСКОЙ ЧАСТИ: **Савина Е.А.**

Цель и задачи

Цель работы:

Защитить информацию ограниченного доступа в ООО «Альфаком» от НСД программными средствами

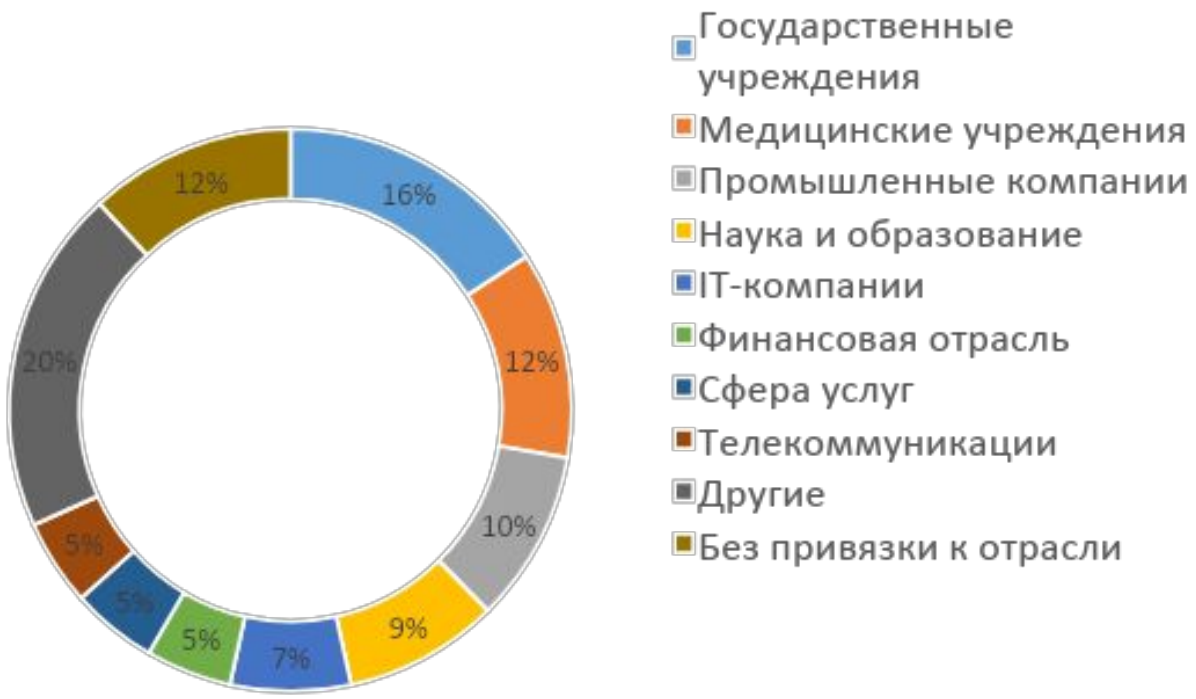
Задачи:

1. Сделать обзор программных средств, выполняющих поставленную цель
2. Провести сравнение представленных продуктов на рынке и сделать обоснованный выбор
3. Провести оценку экономической эффективности применённых средств

Актуальность

В современном десятилетии число информационных атак растёт из квартала к кварталу. Также стоит сказать, что информация в двадцать первом веке играет чуть ли не первую роль. От нее зависит не только благополучие организации, но и жизни людей. Для предотвращения потери такого важного ресурса начала развиваться сфера информационной безопасности

Информационные атаки не останавливаются на государственных и крупных компаниях, что хорошо показано на диаграмме



Колледж автоматизации и информационных технологий

Объект исследования

Объектом исследования являет конфиденциальная информация в ООО «АЛЬФАКОМ». ООО «АЛЬФАКОМ» оказывает услуги по техническому обслуживанию и ремонту средств вычислительной техники и периферийного оборудования для нужд Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека

АЛЬФАКОМ

Возможные угрозы

Актив	Угроза	Величина потерь (тыс. руб)
Проектная документация, разработанная организацией	Конфиденциальности	100
Проектная документация, разработанная организацией	Целостности	500
Проектная документация, разработанная организацией	Доступности	20
Проектная документация, полученная от заказчика	Конфиденциальности	100
Проектная документация, полученная от заказчика	Целостности	100
Проектная документация, полученная от заказчика	Доступности	20
Проектная документация, планы коммуникаций стратегического назначения.	Конфиденциальности	500
Проектная документация, планы коммуникаций стратегического назначения.	Целостности	100
Проектная документация, планы коммуникаций стратегического назначения.	Доступности	20
Личные данные клиента	Конфиденциальности	300
Личные данные клиента	Целостности	20
Личные данные клиента	Доступности	20
Личные сведения о сотрудниках	Конфиденциальности	100
Личные сведения о сотрудниках	Целостности	10
Личные сведения о сотрудниках	Доступности	10
Системное программное обеспечение	Конфиденциальности	0
Системное программное обеспечение	Целостности	100
Системное программное обеспечение	Доступности	100
Прикладное программное обеспечение	Конфиденциальности	0
Прикладное программное обеспечение	Целостности	100
Прикладное программное обеспечение	Доступности	100
Суммарная величина потерь		2320

Шаги по защите:

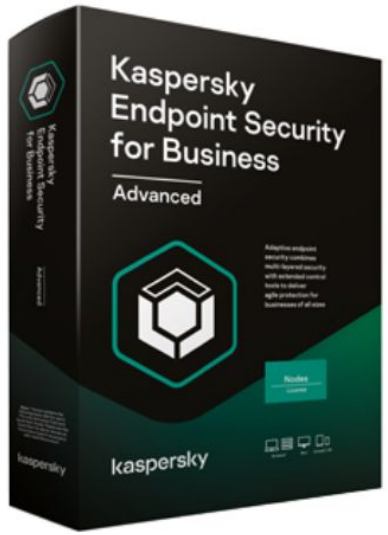
Вследствие изучения программной части и используемых решениях были определены следующие требования:

1. Необходимо усовершенствовать текущее антивирусное решение
    1. Установка Kaspersky Security
2. Установить программное решение для мониторинга всевозможных объектов корпоративной сети
    1. Установка системы виртуализации
    2. Установка системы мониторинга Zabbix

Антивирусное решение

Угрозы безопасности

1. Trend Micro
    1. Простота в эксплуатации
    2. Дешевизна
2. Dr. Web Enterprise Security
    1. Отечественный продукт
    2. Простой интерфейс
3. Kaspersky Security
    1. Высокий показатель защиты
    2. Гибкость
    3. Отечественный продукт



Системы мониторинга

Угрозы безопасности

1. Nagios
    1. Простой в эксплуатации
2. Zabbix
    1. Бесплатный
    2. Высокая гибкость
3. Elastic

Система виртуализации

Какую задачу

1. Vmware
2. Oracle
3. Hyper-V

Microsoft
Hyper-V

Выбранные решения

- Kaspersky Security

  Выбран за свою гибкость и высокие показатели защиты

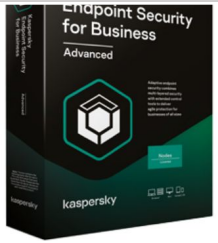
- Zabbix

  Выбран за свою простоту, гибкость

- Vmware

  Выбран за своё быстродействие и простоту

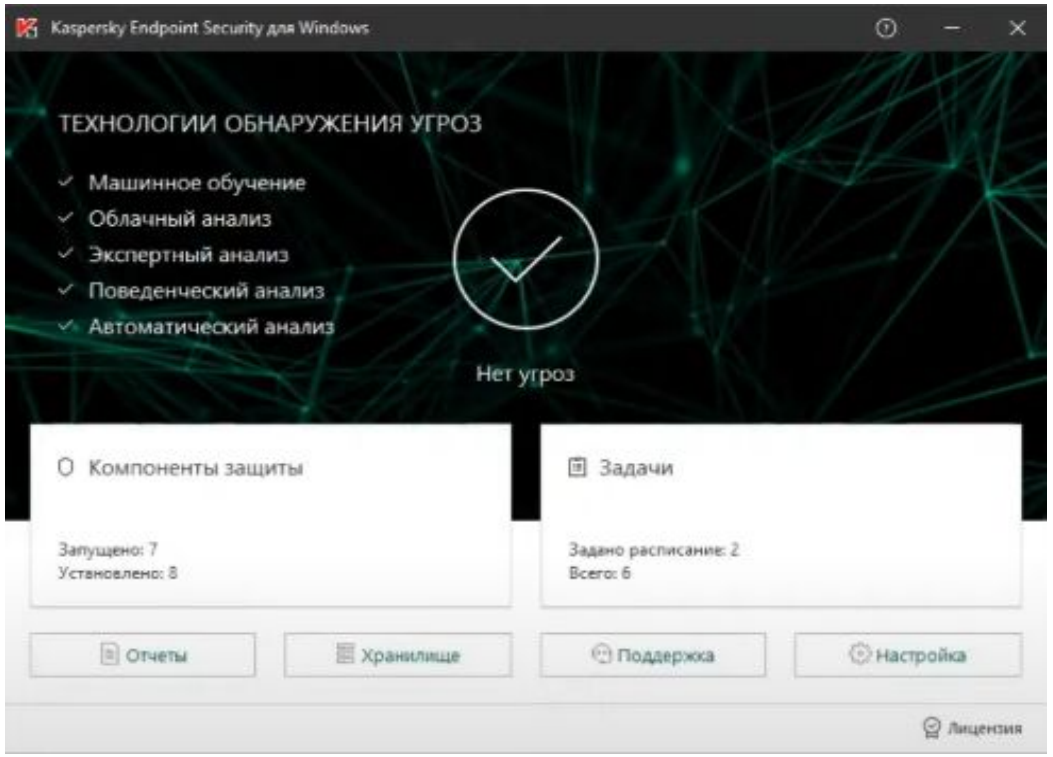
Тип	Вариант 1	Вариант 2	Вариант 3
Антивирус	Trend Micro	Dr. Web Enterprise Security	Kaspersky Security
Мониторинг	Nagios	Zabbix	Elasticsearch
Гипервизор	Vmware	Oracle	Hyper-V

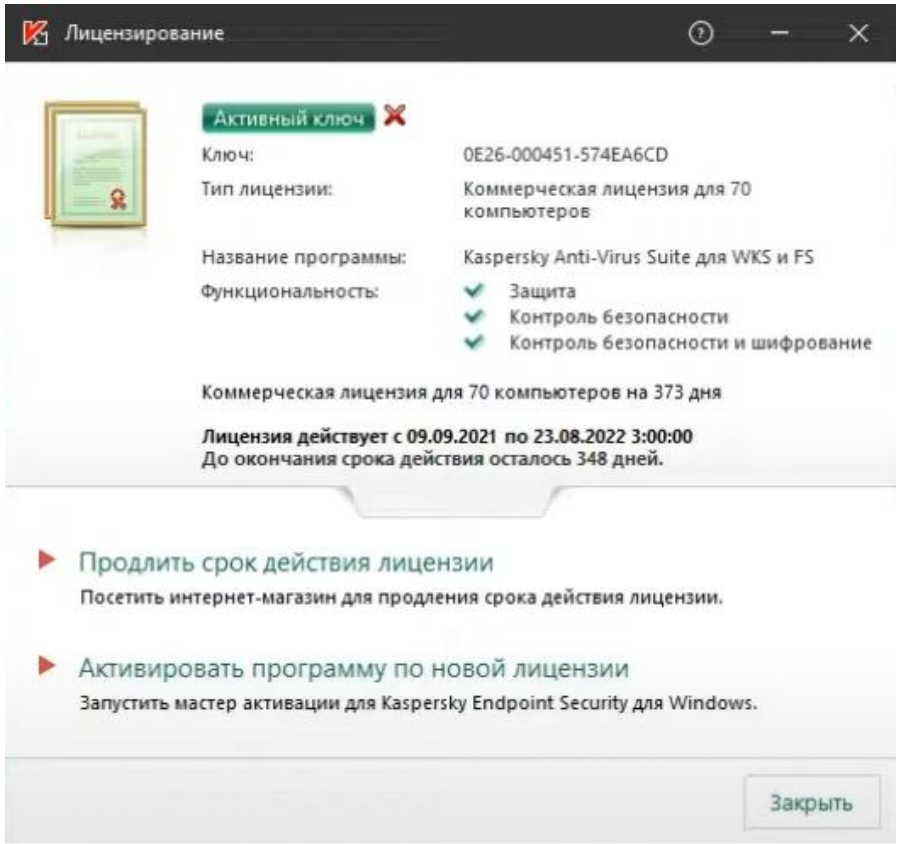


План установки

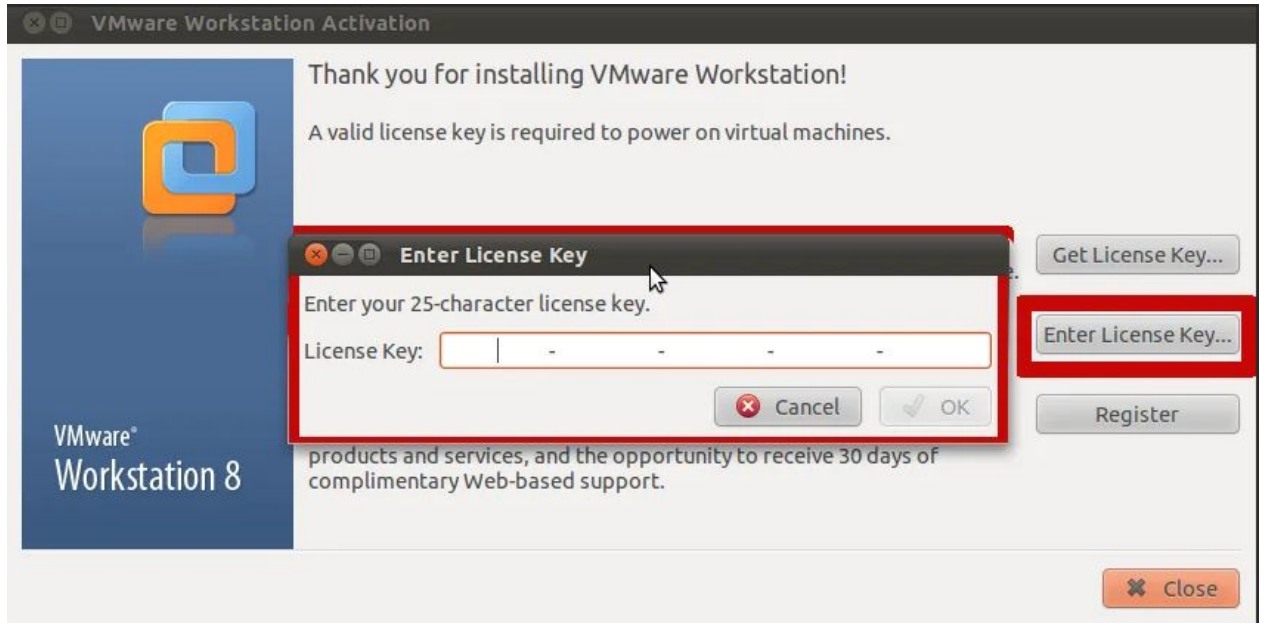
На физическом сервере развернем виртуальный сервер с системой мониторинга **Zabbix**, виртуальные среды будем создавать при помощи **VMware**. Основной дистрибутив **Debian**. Kaspersky Security, установим на все компьютеры находящиеся в корпоративной среде.

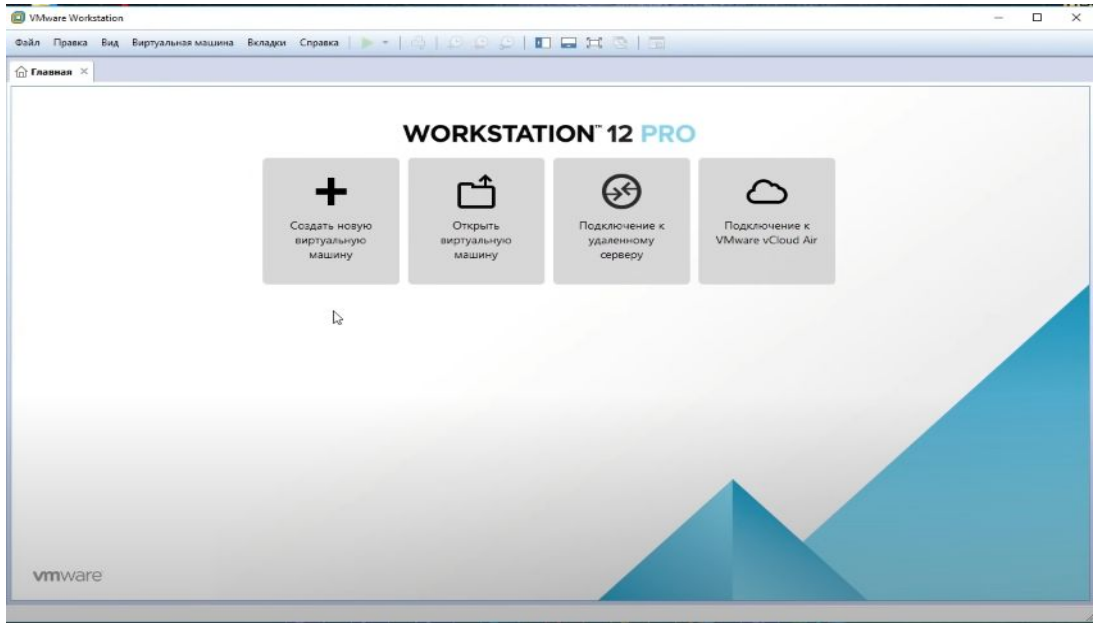
Kaspersky


Kaspersky Endpoint Security для Windows
ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ УГРОЗ
Машинное обучение
Облачный анализ
Экспертный анализ
Поведенческий анализ
Автоматический анализ
Нет угроз
Компоненты защиты
Запущено: 7
Установлено: 8
Задачи
Задано расписание: 2
Всего: 6
Отчеты
Хранилище
Поддержка
Настройка
Лицензия


Лицензирование
Активный ключ
Ключ:
0E26-000451-574EA6CD
Тип лицензии:
Коммерческая лицензия для 70 компьютеров
Название программы:
Kaspersky Anti-Virus Suite для WKS и FS
Функциональность:
Защита
Контроль безопасности
Контроль безопасности и шифрование
Коммерческая лицензия для 70 компьютеров на 373 дня
Лицензия действует с 09.09.2021 по 23.08.2022 3:00:00
До окончания срока действия осталось 348 дней.
Продлить срок действия лицензии
Посетить интернет-магазин для продления срока действия лицензии.
Активировать программу по новой лицензии
Запустить мастер активации для Kaspersky Endpoint Security для Windows.
Закрыть

Vmvare


VMware Workstation Activation
Thank you for installing VMware Workstation!
A valid license key is required to power on virtual machines.
Enter License Key
Enter your 25-character license key.
License Key:
Cancel
OK
Get License Key...
Enter License Key...
Register
products and services, and the opportunity to receive 30 days of complimentary Web-based support.
Close
VMware
Workstation 8

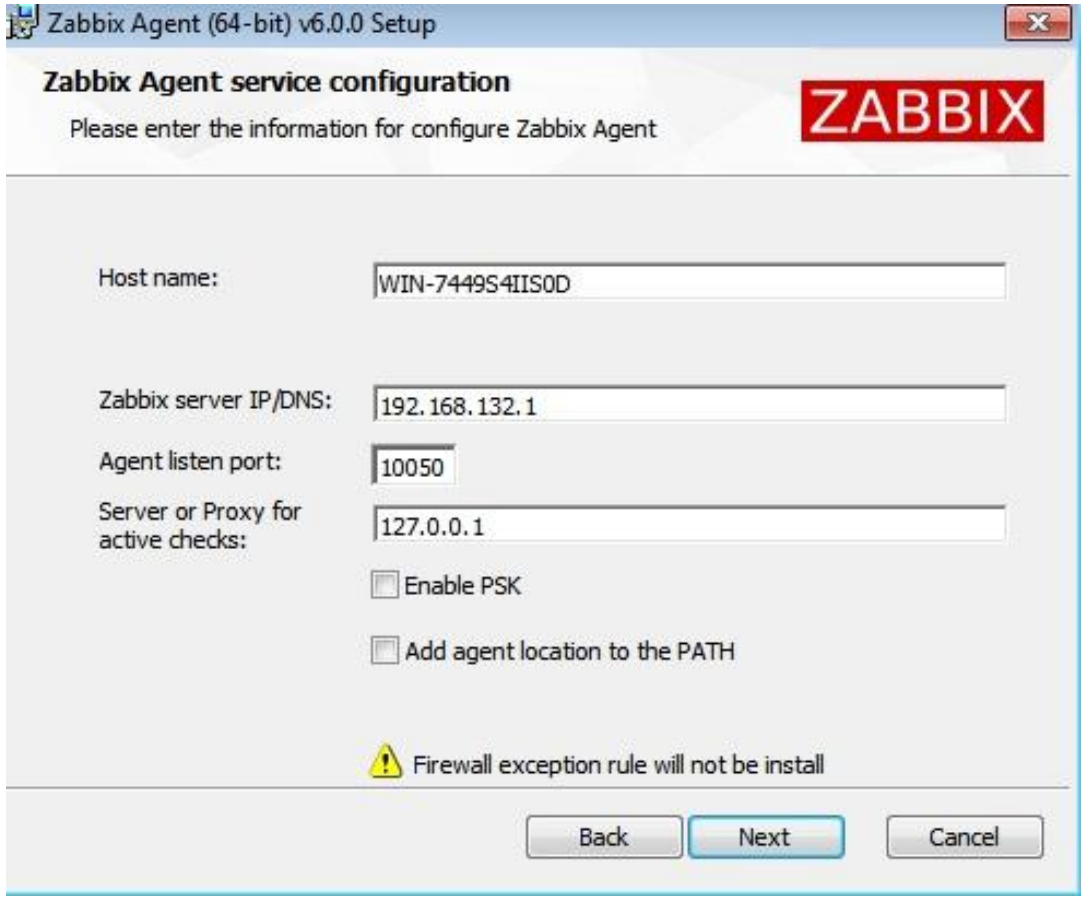

VMware Workstation
Файл
Правка
Вид
Виртуальная машина
Вкладки
Справка
Главная
WORKSTATION 12 PRO
Создать новую виртуальную машину
Открыть виртуальную машину
Подключение к удаленному серверу
Подключение к VMware vCloud Air
vmware

Zabbix

```
docker run --name zabbix-server-pgsql -t \
    -e DB_SERVER_HOST="postgres-server" \
    -e POSTGRES_USER="zabbix" \
    -e POSTGRES_PASSWORD="zabbix_pwd" \
    -e POSTGRES_DB="zabbix" \
    -e ZBX_ENABLE_SNMP_TRAPS="true" \
    --network=zabbix-net \
    -p 10051:10051 \
    --volumes-from zabbix-snmptraps \
    --restart unless-stopped \
    -d zabbix/zabbix-server-pgsql:alpine-5.4-latest
```

```
Status: Downloaded newer image for monitoringartist/zabbix-xxl:latest
e3a58d99bb088117c601bb4bd351a4e88a3a0d7ecf9c104d24fbf06e7095281e
root@zabbix-server:~# docker ps
CONTAINER ID        IMAGE                                COMMAND
  CREATED              STATUS              PORTS
                              NAMES
e3a58d99bb08        monitoringartist/zabbix-xxl:latest   "/config/bootstrap.sh"
  6 seconds ago       Up 5 seconds        0.0.0.0:80->80/tcp, 0.0.0.0:10051->100
51/tcp, 162/udp, 10052/tcp   zabbix
5d75469dafa8        monitoringartist/zabbix-db-mariadb   "/run.sh"
  3 minutes ago       Up 3 minutes        3306/tcp
                              zabbix-db
```

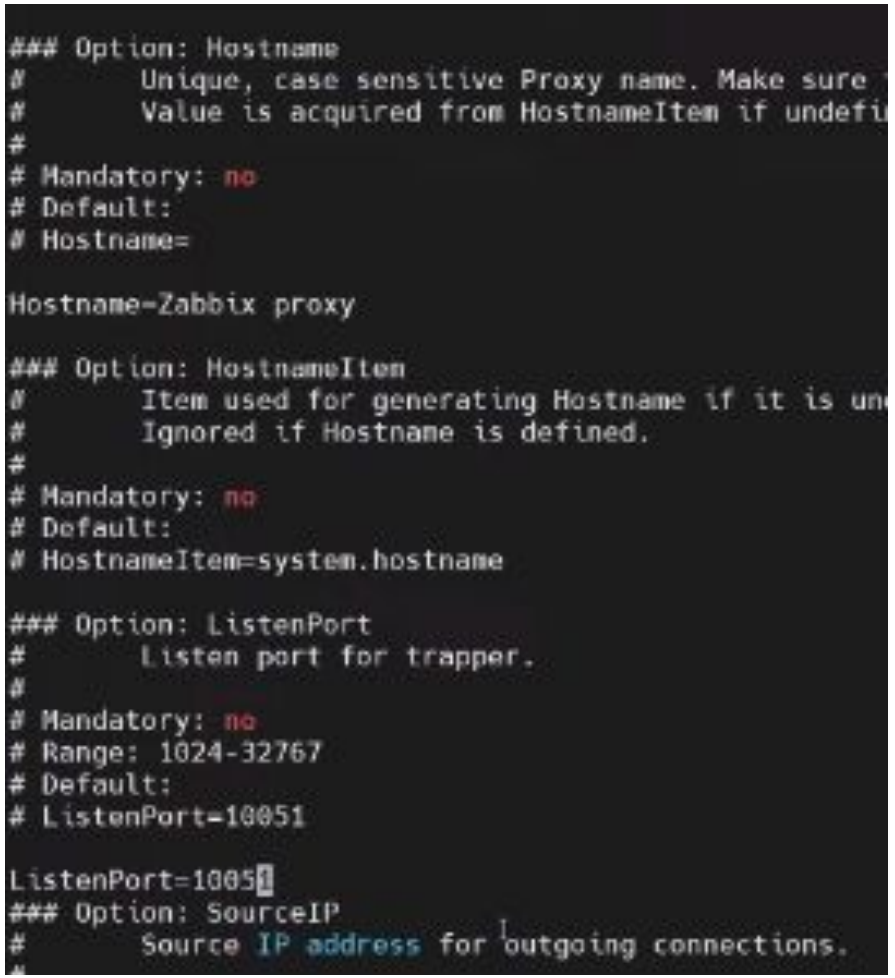
Zabbix


Zabbix Agent (64-bit) v6.0.0 Setup
Zabbix Agent service configuration
Please enter the information for configure Zabbix Agent
ZABBIX
Host name:
WIN-7449S4IIS0D
Zabbix server IP/DNS:
192.168.132.1
Agent listen port:
10050
Server or Proxy for active checks:
127.0.0.1
Enable PSK
Add agent location to the PATH
Firewall exception rule will not be install
Back
Next
Cancel


PC_ITHELP21RU: zabbix_agent_ping (5м)

Zabbix

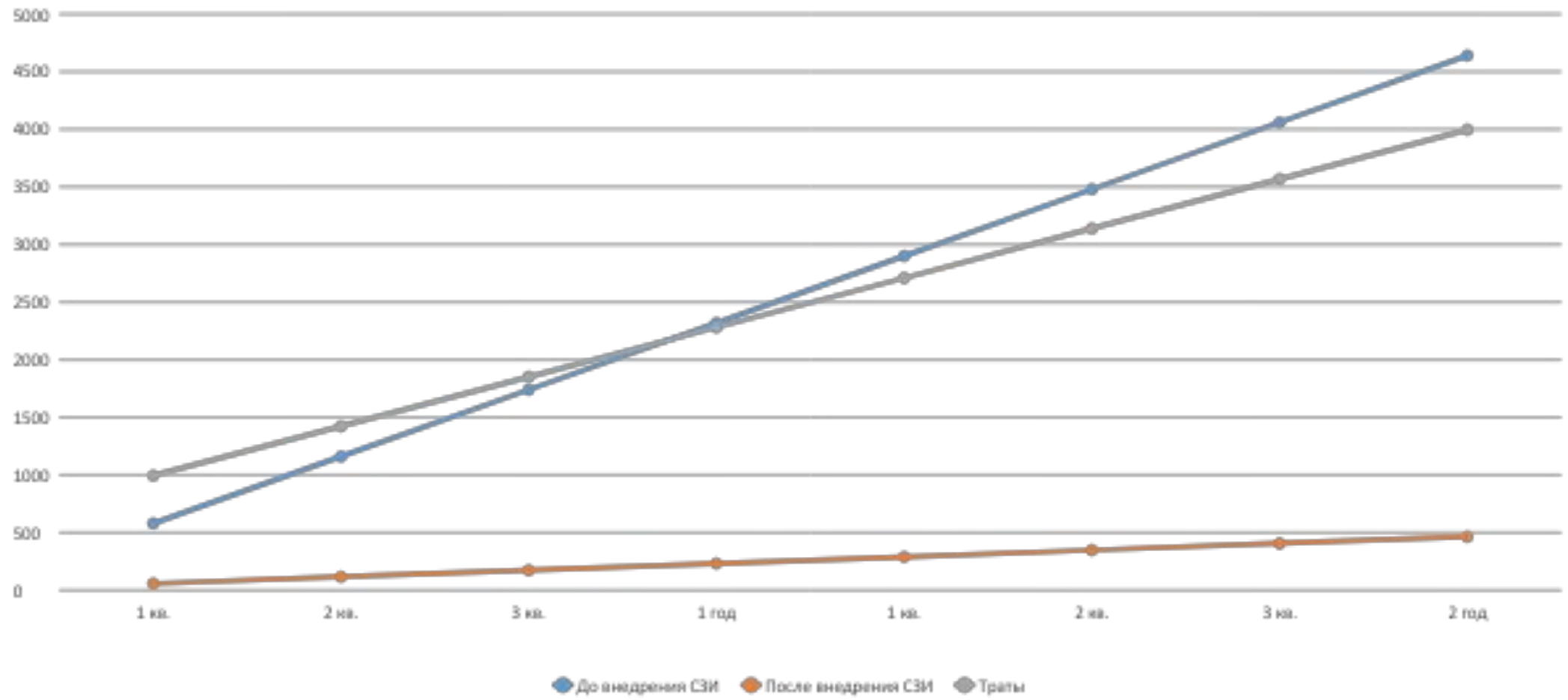
```
docker run —name zabbix-proxy-pgsql -t \
-e DB_SERVER_HOST="postgres-server" \
-e POSTGRES_USER="zabbix" \
-e POSTGRES_PASSWORD="zabbix_pwd" \
-e POSTGRES_DB="zabbix" \
—network=zabbix-net \
-p 10051:10051 \
—restart unless-stopped \
-d komivlad/zabbix-proxy-pgsql
```



Затраты

	Постоянные (руб.)	Разовые (руб. мес.)
Лицензия	19 000	50 000
Оплата труда	124 000	515 000
Всего	143 000	565 000

График снижения потерь



Заключение

В корпоративной сети может циркулировать или хранится важная информация. Была выполнена:

- Установка системы мониторинга
- Установка качественного антивирусного решения

Применение всего вышеперечисленного комплекса программных средств обеспечит хороший уровень защиты.