OpenLDAP сервер на CentOS7

Понадобилась общая адресная книга в небольшой сети без домена, основной почтовый клиент Mozilla Thunderbird. Решено было использовать OpenLDAP для этих целей.

Имеем минимально настроенный сервер с CentOS7.

Приступаем к установке и настройке OpenLDAP. Устанавливаем пакеты openldap и migrationtools:

```
yum install -y openldap* migrationtools
```

Создаем пароль администратора LDAP:

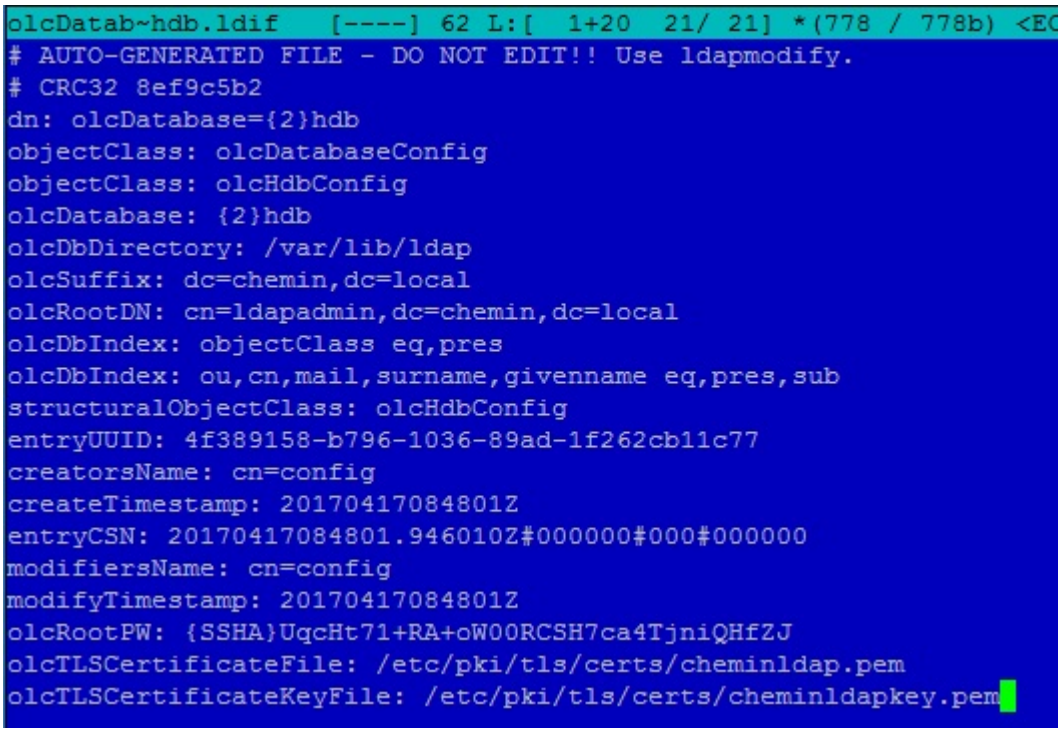
```
slappasswd
New password:
Re-enter new password:
```

Получаем пароль в зашифрованном виде – {SSHA}bHSiwuPJEypHS6z***2Uy7M69sQjmkPL, сохраняем в блокноте.
Меняем настройки конфигурационного файла:

```
cd /etc/openldap/slapd.d/cn=config
mcedit olcDatabase={2}hdb.ldif
```

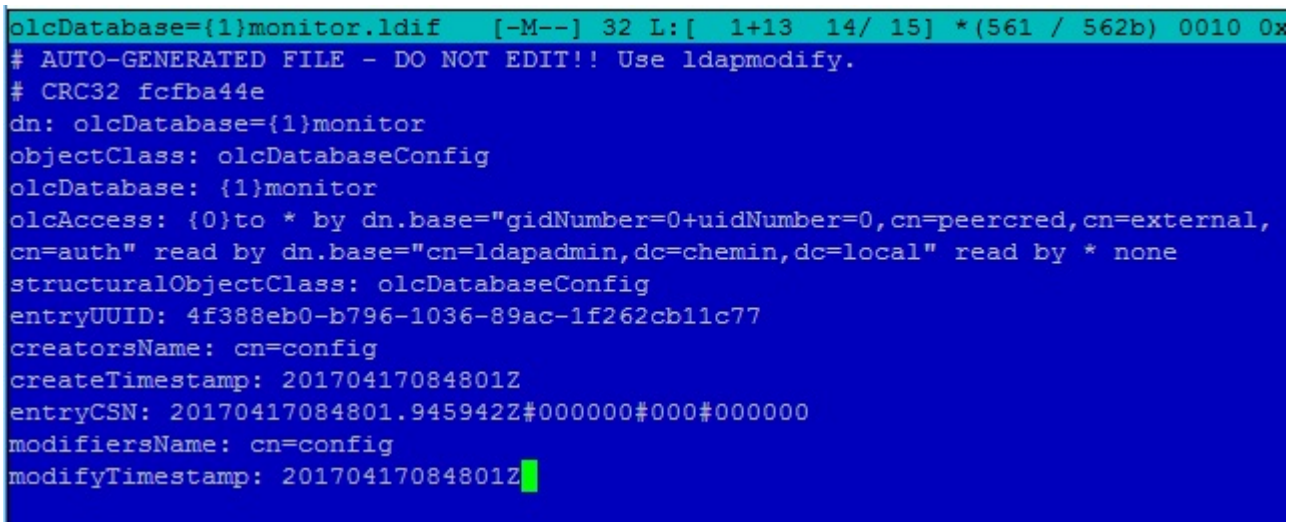
Первым делом меняем параметры “olcSuffix” и “olcRootDN” на свои. Добавляем три строчки в файл (“olcRootPW” используем сохраненный ранее зашифрованный пароль администратора):

```
olcRootPW: {SSHA}bHSiwuPJEypHS6z***2Uy7M69sQjmkPL
olcTLSCertificateFile: /etc/pki/tls/certs/cheminldap.pem
olcTLSCertificateKeyFile: /etc/pki/tls/certs/cheminldapkey.pem
```



Изменяем конфигурацию еще одного файла:

```
mcedit olcDatabase={1}monitor.ldif
olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by
dn.base="cn=ldapadmin,dc=chemin,dc=local" read by * none
```



Ранее, в конфигурацию были добавлены пути к сертификатам, сгенерируем их (сроком на 10 лет):

```
openssl req -new -x509 -nodes -out /etc/pki/tls/certs/cheminldap.pem -keyout
```

```
/etc/pki/tls/certs/cheminldapkey.pem -days 3650
```

```
Вводим свои данные при генерации сертификата:
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:KKR
Locality Name (eg, city) [Default City]:Krasnodar
Organization Name (eg, company) [Default Company Ltd]:Chemical Industry LLC
Organizational Unit Name (eg, section) []:Office
Common Name (eg, your name or your server's hostname) []:ldap.chemin.local
Email Address []:sa@chemin.ru
```

Проверяем наличие сертификатов в папке /etc/pki/tls/certs/:

```
ll /etc/pki/tls/certs/*.pem
```

```
[root@ldap cn=config]# ll /etc/pki/tls/certs/*.pem
-rw-r--r-- 1 root root 1704 Apr 17 11:55 /etc/pki/tls/certs/cheminldapkey.pem
-rw-r--r-- 1 root root 1456 Apr 17 11:55 /etc/pki/tls/certs/cheminldap.pem
[root@ldap cn=config]#
```

Проверяем конфигурацию:

```
slaptest -u
```

Ошибки “checksum” можно пропустить.

```
[root@ldap ~]# slaptest -u
58f71629 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcD
atabase={1}monitor.ldif"
58f71629 ldif_read_file: checksum error on "/etc/openldap/slapd.d/cn=config/olcD
atabase={2}hdb.ldif"
config file testing succeeded
[root@ldap ~]#
```

Включаем и запускаем сервис:

```
systemctl start slapd
systemctl enable slapd
```

Проверка:

```
netstat -lt | grep ldap
```

```
[root@ldap cn=config]# netstat -lt | grep ldap
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN
[root@ldap cn=config]#
```

Конфигурируем LDAP Database. Копируем “Sample Database” файл конфигурации и назначаем права к нему:

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown -R ldap:ldap /var/lib/ldap/
```

Добавляем “LDAP Schemas”

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

Создаем базу объектов OpenLDAP, используя установленный ранее пакет “migrationtools”. Меняем настройки файла “migrate_common.ph”

```
cd /usr/share/migrationtools/
mcedit migrate_common.ph
```

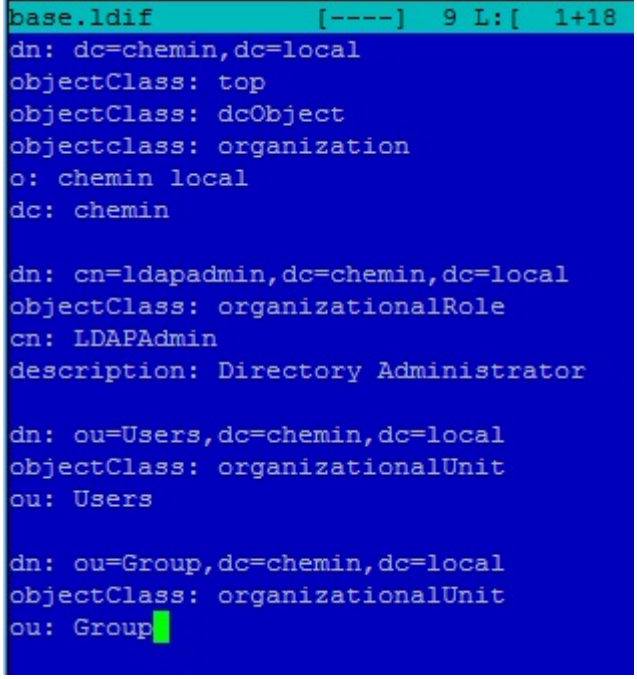
Строка 71 – свое имя домена: $DEFAULT_MAIL_DOMAIN = “chemin.local”;
Строка 74 свое имя базы $DEFAULT_BASE = “dc=chemin,dc=local”;
Строка 90 включаем $EXTENDED_SCHEMA = 1;
Сохраняем файл.

Генерируем base.ldif файл:

```
touch /root/base.ldif
```

Вставляем свои данные в этот файл:

```
mcedit /root/base.ldif
```



Создадим локального пользователя:

```
useradd sa
echo "redhat" | passwd --stdin sa
```

Filter out these user from /etc/passwd to another file:

```
grep ":10[0-9][0-9]" /etc/passwd > /root/passwd
```

Filter out user group from /etc/group to another file:

```
grep ":10[0-9][0-9]" /etc/group > /root/group
```

Конвертируем файл локальных пользователей в LDAP Data Interchange Format (LDIF). Генерируем ldif файл для пользователей

```
./migrate_passwd.pl /root/passwd /root/users.ldif
```

Генерируем ldif файл для групп

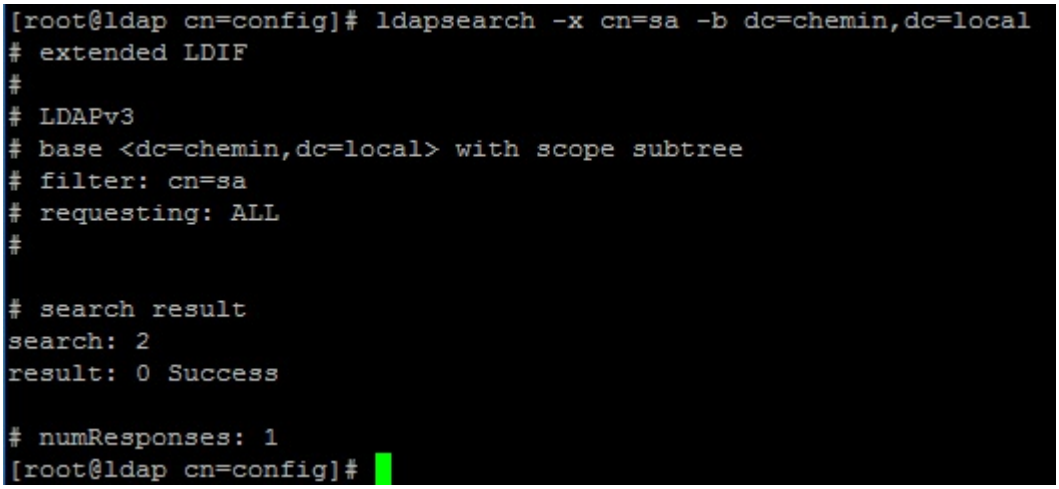
```
./migrate_group.pl /root/group /root/groups.ldif
```

Импортируем эти LDIF-файлы в LDAP Database:

```
ldapadd -x -W -D "cn=ldapadmin,dc=chemin,dc=local" -f /root/base.ldif
ldapadd -x -W -D "cn=ldapadmin,dc=chemin,dc=local" -f /root/users.ldif
ldapadd -x -W -D "cn=ldapadmin,dc=chemin,dc=local" -f /root/groups.ldif
```

Тест конфигурации:

```
ldapsearch -x cn=sa -b dc=chemin,dc=local
```



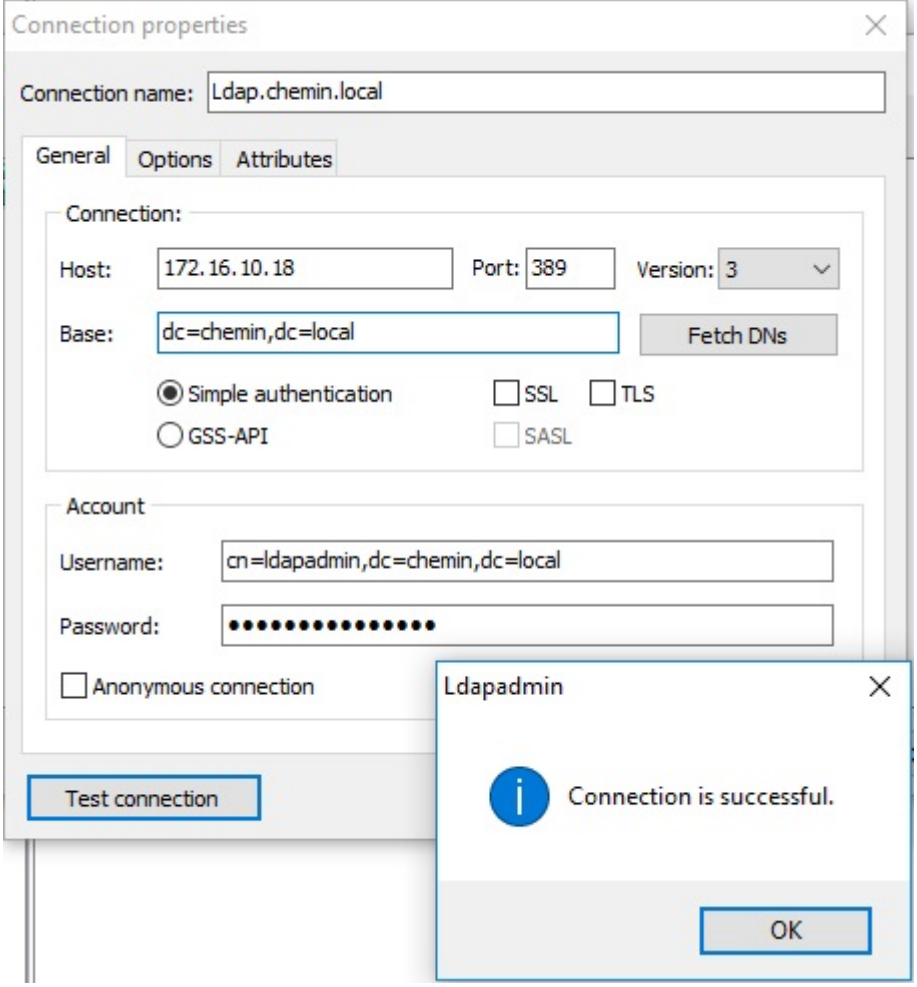
Если не отключали – сконфигурируем файервол. Добавим порты ldap:

```
firewall-cmd --permanent --add-port=389/tcp
firewall-cmd --permanent --add-port=636/tcp
firewall-cmd --permanent --add-port=9830/tcp
```

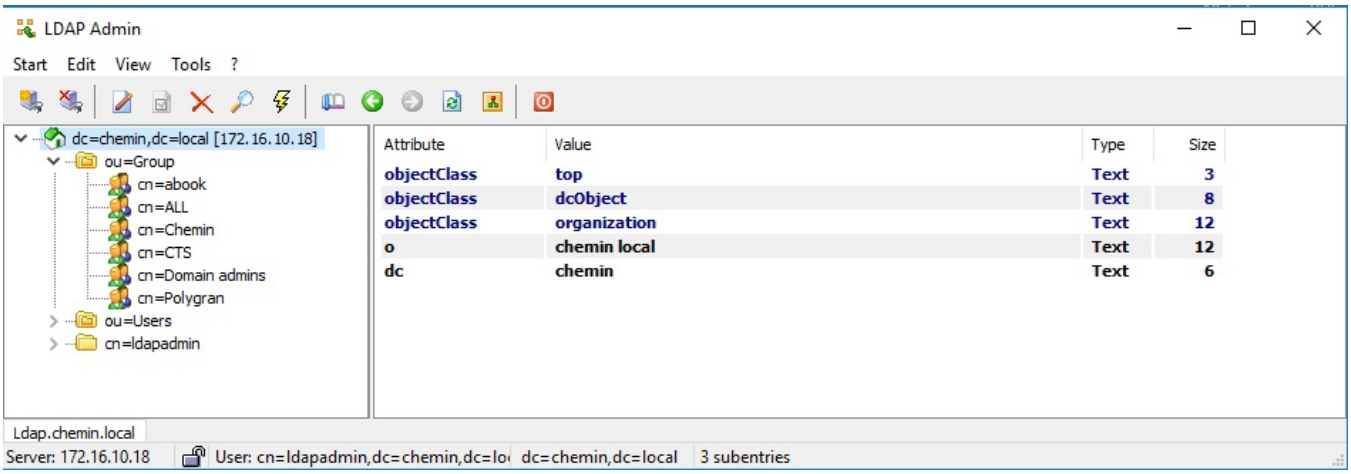
Перезапуск файервола:

```
firewall-cmd --reload
```

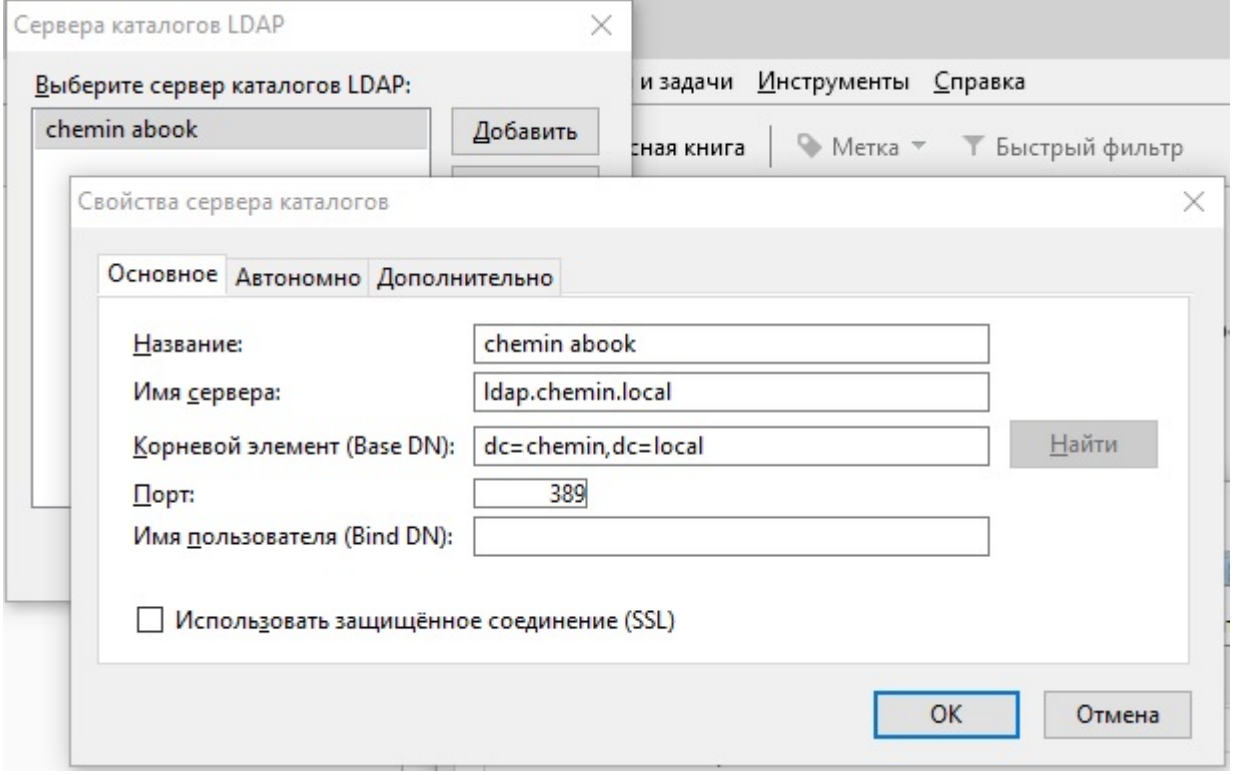
Для удобства администрирования используется утилита LDAPAdmin в Windows. Параметры подключения к LDAP:



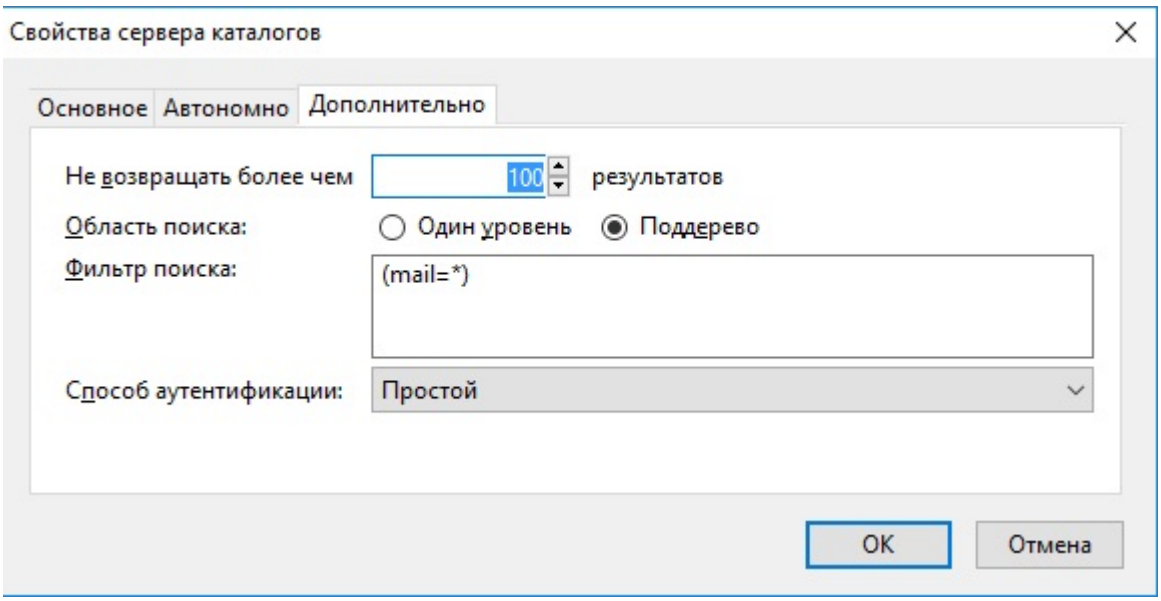
Все действия с учетными записями и группами можно производить из этой утилиты:



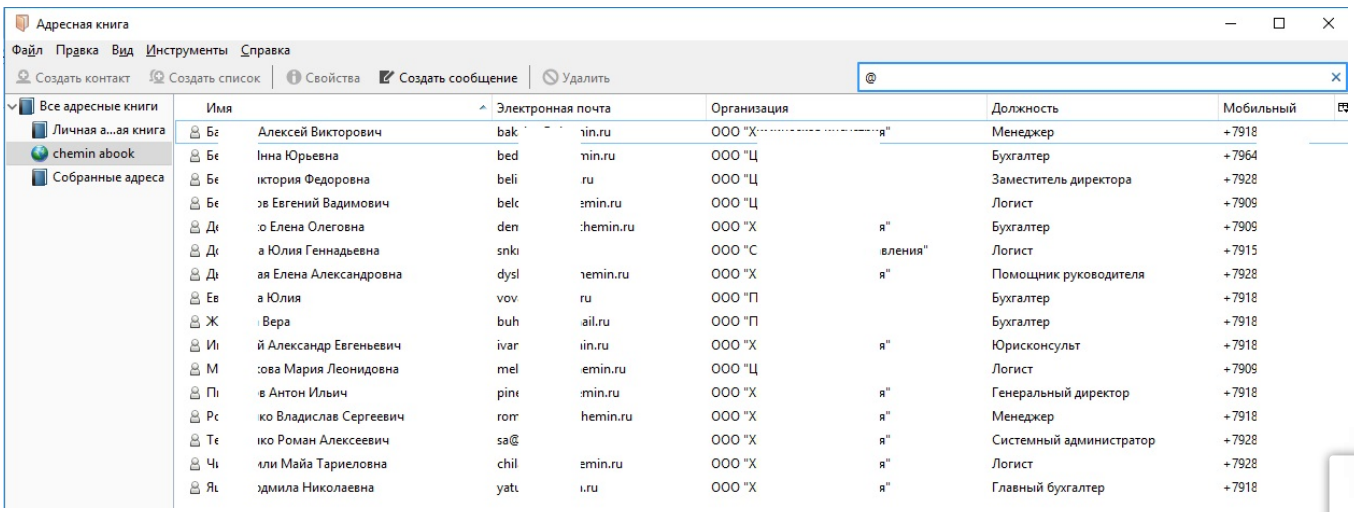
Подключим адресную книгу в почтовик



Фильтруем поиск по mail



Вводим символ @ в строке поиска и видим все записи LDAP-сервера, у которых прописан e-mail



19.04.2017 IT CentOS, LDAPAdmin, OpenLDAP, Thunderbird, Адресная книга