ПРОГРАММНЫЙ ПРОДУКТ
СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
NEXTSTAGE SECURITY PLATFORM:
NEXTSTAGE IRP

Руководство администратора

2020

АННОТАЦИЯ

Данный документ предназначен для специалистов, выполняющих администрирование программного продукта «Система управления информационной безопасностью **NextSTage Security Platform: NextStage IRP**» (далее - **NextStage IRP**), и включает описание действий по установке, настройке модулей данного программного продукта, а также программного обеспечения, используемого в рамках функционирования данных модулей**.**

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и условия применения

Программный продукт **NextStage IRP** предназначен для автоматизации процессов регистрации инцидентов ИБ, а также реагирования на них, управления ИТ-активами, формирования и отображения динамической отчетности, организации взаимодействия с Национальным координационным центром по компьютерным инцидентам (далее - НКЦКИ).

NextStage IRP обеспечивает автоматизацию следующих функций:

- управление инцидентами ИБ в части их ручной и автоматической регистрации, назначения ответственных, редактирования учетных карточек, фиксации результатов реагирования и расследования;
- реализация автоматических сценариев реагирования на инциденты ИБ;
- управление ИТ-активами;
- сбор информации об используемых ИТ-активах посредством сканирования сети организации;
- выгрузка проектов файлов для дальнейшей передачи в НКЦКИ в соответствии с форматами представления сведений в НКЦКИ;
- отображение сводных статистических и детальных данных об инцидентах ИБ и используемых ИТ-активах на информационных панелях (дашбордах).

1.2 Перечень функциональных модулей

Программный продукт **NextStage IRP** включает следующие функциональные модули:

- Личный кабинет пользователя **NextStage IRP** (далее – Личный кабинет пользователя);
- Модуль сканирования сети;
- Модуль визуализации;
- Модуль выполнения управляющих воздействий (оркестрации).

Личный кабинет пользователя и модуль сканирования сети представляют веб-приложения, написанные на языке программирования Python 3 версии в среде разработки Django Framework.

Модуль выполнения управляющих воздействий строится на базе ПО Apache Airflow версии 1.10.11.

Модуль визуализации строится на базе ПО Grafana версии 7.3.3.

2 УСЛОВИЯ РАБОТЫ ПРОГРАММНОГО ПРОДУКТА

2.1 Требования к аппаратному и программному обеспечению

Все компоненты **NextStage IRP** устанавливаются на один виртуальный либо физический сервер под управлением RED ОС. Данный сервер должен иметь подключение к сети Интернет с возможностью подключения к репозиториям RED ОС и скачивания необходимых программных пакетов.

2.1.1 Требования к аппаратной части

- Процессор: не менее 2 ГГц, 4 ядра.
- Оперативная память: не менее 16 Гб.
- Дисковое пространство: не менее 200 Гб свободного дискового пространства.
- Сеть: 100/1000 Мбит/с Ethernet.

2.1.2 Требования к программной части

- ОС: RED ОС (64-разрядная).
- СУБД: PostgreSQL 11 и выше.
- HTTP сервер: Nginx 1.12 и выше.
- Python: Python 3.6 и выше.
- Служба очереди сообщений: RabbitMQ версии 3.7 и выше.
- Apache Airflow версии 1.10.11 (только данная версия).

3 УСТАНОВКА ПРОГРАММНОГО ПРОДУКТА

Все действия по установке и настройке осуществляются либо непосредственно в интерфейсе ОС, либо удаленно посредством ПО Putty (выполнение команд в терминале) либо посредством ПО WinSCP (передача файлов). Для обеспечения удаленной настройки посредством ПО Putty и ПО WinSCP с АРМ, на котором выполняется настройка, до сервера должен быть открыт 22 порт по протоколу TCP.

Специалист, выполняющий установку и настройку программного продукта, должен обладать базовыми навыками администрирования ОС Linux.

3.1 Установка и первичная настройка СУБД PostgreSQL

В рамках установки и первичной настройки СУБД PostgreSQL необходимо выполнить следующую последовательность действий:

1) Установить СУБД PostgreSQL и необходимые библиотеки, выполнив следующие команды:

```
sudo yum install postgresql-server
sudo yum install postgresql-contrib
sudo yum install libpq-devel
```

2) Инициализировать сервер БД, выполнив следующую команду:

```
sudo postgresql-setup initdb
```

3) Настроить автозапуск сервера БД и запустить сервис, выполнив следующие команды:

```
sudo systemctl enable postgresql
sudo systemctl start postgresql
```

4) Настроить конфигурационный файл postgresql.conf – указать адреса для прослушивания порта, открыв данный файл для редактирований программой nano. Для этого выполнить следующую команду:

```
sudo nano /var/lib/pgsql/data/postgresql.conf
```

5) В разделе «CONNECTION AND AUTHENTICATION» раскомментировать строку listen_addresses и задать следующее значение:

```
listen_addresses = '*'
```

6) Настроить доступ пользователей к БД в файле pg_hba.conf. Для этого открыть файл в режиме редактирования программой nano, выполнив следующую команду:

```
sudo nano /var/lib/pgsql/data/pg_hba.conf
```

7) Установить следующие значения секций local:

```
# TYPE      DATABASE       USER      ADDRESS         METHOD

# "local" is for Unix domain socket connections only
local       all       postgres                      peer
local       all       all                           password
host        all       all       127.0.0.1/32        password
host        all       all       ::1/128             password
```

Если есть необходимость подключаться к СУБД удаленно, то в секции IPv4 необходимо прописать IP адреса, с которых будет осуществляться данное подключение.

8) Перезапустить службу сервера БД, выполнив следующую команду:

```
sudo systemctl restart postgresql
```

9) Задать пароль для системного пользователя БД postgres, выполнив следующую команду:

```
sudo passwd postgres
```

10) Ввести новое значение пароля с подтверждением:

```
New password: <Ввести новое значение пароля>
Retype new password: <Повторить значение пароля>
```

3.2 Установка HTTP сервера на базе ПО Nginx

В рамках установки HTTP сервера Nginx необходимо выполнить следующую последовательность действий:

1) Установить Nginx, выполнив следующую команду:

```
sudo yum install nginx
```

2) Настроить автозапуск и запустить сервис, выполнив последовательно следующие команды:

```
sudo systemctl enable nginx
sudo systemctl start nginx
```

3.3 Установка и настройка службы очереди сообщений на базе ПО RabbitMQ

Необходимо выполнить следующую последовательность действий:

1) Установить EPEL – репозиторий выполнив следующую команду:

```
sudo yum install epel-release
```

2) Обновить список пакетов, так как установлен репозиторий, следующей командой:

```
sudo yum update
```

3) Установить ПО Erlang, выполнив следующую команду:

```
sudo yum install erlang
```

4) Установить и запустить ПО RabbitMQ версии 3.8.9, выполнив последовательно следующие команды:

```
sudo wget https://dl.bintray.com/rabbitmq/rpm/rabbitmq-server/v3.8.x/el/8/noarch/rabbitmq-server-3.8.9-1.el8.noarch.rpm

sudo yum install rabbitmq-server-3.8.9-1.el8.noarch.rpm

sudo rabbitmq-plugins enable rabbitmq_management

sudo systemctl enable rabbitmq-server

sudo systemctl start rabbitmq-server
```

5) Создать пользователя airflow и задать значение пароля, выполнив следующую команду:

```
sudo rabbitmqctl add_user airflow <указать пароль>
```

6) Присвоить пользователю airflow права администратора, выполнив следующую команду:

```
sudo rabbitmqctl set_user_tags airflow administrator
```

7) Установить пользователю airflow разрешение на доступ ко всем очередям сообщений при помощи следующих команд:

```
sudo rabbitmqctl set_permissions -p / airflow ".*" ".*" ".*"
```

3.4 Установка виртуального окружения для языка программирования python

Необходимо выполнить следующую последовательность действий:

1) Установить пакеты компиляции gcc, выполнив следующую команду:

```
sudo yum install gcc
```

2) Установить пакеты разработки python3-devel, выполнив следующую команду:

```
sudo yum install python3-devel
```

3) Установить пакет виртуального окружения virtualenv, выполнив следующую команду:

```
sudo pip3 install virtualenv
```

3.5 Установка личного кабинета пользователя

3.5.1 Создание служебной учетной записи ОС

Для обеспечения установки необходимого ПО и последующей работы модуля, в ОС необходимо создать отдельного пользователя nssp, установить для него пароль и включить пользователя в группу wheel. Для этого необходимо выполнить следующую последовательность действий:

1) Создать пользователя nssp, выполнив следующую команду:

```
sudo useradd -m nssp
```

2) Включить пользователя nssp в группу wheel, выполнив следующую команду:

```
sudo usermod -aG wheel nssp
```

3) Сменить пароль пользователю nssp, выполнив следующую команду:

```
sudo passwd nssp
```

4) Ввести новое значение пароля с подтверждением:

```
New password: <Ввести новое значение пароля>
Retype new password: <Повторить значение пароля>
```

5) Переключить сессию на пользователя nssp и продолжить выполнение дальнейших действий под ним, выполнив следующую команду:

```
su nssp
```

3.5.2 Создание БД

В рамках создания БД необходимо выполнить следующую последовательность действий:

1) Запустить терминальную программу psql, выполнив следующую команду:

```
sudo -u postgres psql
```

2) Создать пользователя nssp и задать пароль, выполнив следующую команду:

```
CREATE USER nssp WITH PASSWORD '<указать пароль>';
```

3) Создать БД nssp и указать её владельцем пользователя nssp, выполнив следующую команду:

```
CREATE DATABASE nssp OWNER=nssp ENCODING=utf8;
```

4) Предоставить права на БД nssp пользователю, выполнив следующую команду:

```
GRANT ALL PRIVILEGES ON DATABASE nssp TO nssp;
```

5) Предоставить пользователю nssp роль SuperUser, выполнив следующую команду:

```
ALTER USER nssp SUPERUSER;
```

6) Выполнить выход из терминальной программы psql следующей командой:

```
\q
```

7) Осуществить попытку входа в БД nssp под пользователем nssp, выполнив следующую команду:

```
psql -U nssp nssp
```

8) Ввести пароль и убедиться, что вход успешно выполнен.

9) Добавить расширение citext следующей командой:

```
CREATE EXTENSION citext;
```

10) Выполнить выход из терминальной программы psql, выполнив следующую команду:

```
\q
```

3.5.3 Установка и первичная настройка

Для установки и первичной настройки необходимо выполнить следующую последовательность действий под пользователем nssp:

1) В директории /opt создать каталог nssp, выполнив следующую команду:

```
sudo mkdir /opt/nssp
```

2) Сменить владельца для каталога /opt/nssp, выполнив следующую команду:

```
sudo chown -R nssp:nssp /opt/nssp
```

3) Сменить права доступа на каталог /opt/nssp, выполнив следующую команду:

```
sudo chmod -R 775 /opt/nssp
```

4) Перейти в каталог /opt/nssp, выполнив следующую команду:

```
cd /opt/nssp
```

5) Из дистрибутивного комплекта под учетной записью пользователя nssp скопировать все файлы из каталога nssp в директорию /opt/nssp и перейти в /opt/nssp.

6) Установить пакет русскоязычной locale:

```
sudo yum install glibc-langpack-ru
```

7) Установить русский язык в locale:

```
localectl set-locale LANG=ru_RU.utf8
```

8) Установить виртуальное окружение:

```
python3 -m venv venv
```

9) Активировать виртуальное окружение:

```
source venv/bin/activate
```

10) Установить переменную окружения для настроек проекта в среде разработки Django Framework:

```
export DJANGO_SETTINGS_MODULE=project.settings
```

11) Добавить права на исполнения для файла initial.sh

```
sudo chmod +x initial.sh
```

12) Перейти в /opt/nssp/ и запустить скрипт initial.sh, обеспечивающий установку программных библиотек для проекта, заполнение справочников в БД и создание администратора с именем пользователя admin и паролем P@ssw0rd:

```
./initial.sh
```

13) Осуществить настройку сайта для проекта в среде разработки Django Framework, выполнив последовательно следующие команды:

```
python manage.py shell
from django.contrib.sites.models import Site
site = Site.objects.last()
site.name = '<указать ip адрес сервера личного кабинета>:8000'
site.domain = '<указать ip адрес сервера личного кабинета>'
site.save()
exit()
```

14) Открыть конфигурационный файл local_settings.py личного кабинета, расположенный в /opt/nssp/project/settings., для редактирования, выполнив следующую команду:

```
sudo nano /opt/nssp/project/settings/local_settings.py
```

15) .В файле настроить параметры подключения к БД личного кабинета, созданной в рамках п. 3.5.2, в соответствии со значениями, приведенными в таблице (Таблица 3.1).

Таблица 3.1 – Параметры настроек конфигурационного файла local_settings.py

Секция	Параметр	Значение	Описание
1	2	3	4
DATABASES	NAME	nssp	Имя БД
	USER	nssp	Имя пользователя БД
	PASSWORD	<укажите пароль>	Пароль от БД
	HOST	localhost	Хост, на котором расположена БД
	PORT	5432	Порт подключения к серверу БД

16) Нажать комбинацию клавиш Ctrl+X для выхода;

17) Ввести «y» и подтвердить наименование сохраняемого файла, нажав клавишу «Enter».

18) Открыть файл /etc/systemd/system/gunicorn.service программой nano в режиме редактирования:

```
sudo nano /etc/systemd/system/gunicorn.service
```

19) Внести в файл /etc/systemd/system/gunicorn.service следующее:

```
[Unit]
Description=nssp daemon
After=network.target


[Service]
User= nssp
Group=nginx
WorkingDirectory=/opt/nssp/
ExecStart=/opt/nssp/venv/bin/gunicorn /usr/local/bin/gunicorn --
workers 3 --bind unix:///opt/nssp/nssp.sock
project.wsgi:application


[Install]
WantedBy=multi-user.target
```

20) Нажать комбинацию клавиш Ctrl+X для выхода;

21) Ввести «y» и подтвердить наименование сохраняемого файла, нажав клавишу «Enter».

22) Добавить в автозагрузку службу gunicorn, выполнив последовательно следующие команды:

```
sudo systemctl start gunicorn
sudo systemctl enable gunicorn
```

23) Проверить статус службы gunicorn, выполнив следующую команду:

```
sudo systemctl status gunicorn
```

24) Создать папку для журналов событий Nginx, выполнив следующую команду:

```
mkdir /var/log/nginx/nssp
```

25) Добавить в файл /etc/nginx/nginx.conf в секцию http с сохранением отступов от левого края второй блок настроек server перед уже имеющимся в этом файле (стандартным) блоком server. Только необходимо указать соответствующий IP адрес сервера, на котором развернут личный кабинет пользователя.:

```
server {
        listen 8000;
        client_max_body_size 70M;
        server_name <ip адрес сервера личного кабинета>;
        charset utf-8;

        root /opt/nssp/public;

        access_log /var/log/nginx/nssp/access.log;
        error_log /var/log/nginx/nssp/error.log;

        location / {
            proxy_read_timeout 10m;
            proxy_connect_timeout 10m;
            proxy_send_timeout 10m;
            proxy_set_header Host $http_host;
            proxy_set_header X-Real-IP $remote_addr;
```

```
            proxy_set_header                        X-Forwarded-For
$proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
            proxy_pass http://unix:/opt/nssp/nssp.sock;
        }


        location /static {
            alias /opt/nssp/public/static;
            location                                                ~*
\.(js|css|png|jpg|jpeg|gif|ico|pdf|doc|docx|xls|xlsx|woff|ttf|sv
g|svgz|eot)$ {
                expires max;
                log_not_found off;
            }
            autoindex off;
        }


        location /media {
            alias /opt/nssp/public/media;
            location                                                ~*
\.(js|css|png|jpg|jpeg|gif|ico|pdf|doc|docx|xls|xlsx|woff|ttf|sv
g|svgz|eot)$ {
                expires max;
                log_not_found off;
            }
            autoindex off;
        }


        location /favicon.ico {
            alias /opt/nssp/public/static/favicon.ico;
        }


        location /favicon.png {
            alias /opt/nssp/public/static/favicon.png;
```

```
        }
    }
```

26) Перезапустить сервер nginx, выполнив следующую команду:

```
sudo service nginx restart
```

27) Проверить доступность веб-интерфейса личного кабинета пользователя, введя в адресной строке веб-обозревателя URL: http://<адрес сервера>:8000

28) Аутентифицироваться в веб-интерфейсе личного кабинета под учетной записью администратора:

- Поле «Логин» – значение «admin»;
- Поле «Пароль» – значение «P@ssw0rd».

3.6 Установка модуля оркестрации

3.6.1 Создание служебной учетной записи ОС

Для обеспечения установки необходимого ПО и последующей работы модуля, в ОС необходимо создать отдельного пользователя airflow, установить для него пароль и включить пользователя в группу wheel. Для этого необходимо выполнить следующую последовательность действий:

1) Создать пользователя airflow, выполнив следующую команду:

```
sudo useradd -m airflow
```

2) Включить пользователя airflowв группу wheel, выполнив следующую команду:

```
sudo usermod -aG wheel airflow
```

3) Сменить пароль пользователю airflow, выполнив следующую команду:

```
sudo passwd airflow
```

4) Ввести новое значение пароля с подтверждением:

```
New password: <Ввести новое значение пароля>
Retype new password: <Повторить значение пароля>
```

5) Переключить сессию на пользователя airflow и продолжить выполнение дальнейших действий под ним, выполнив следующую команду:

```
su airflow
```

3.6.2 Создание БД

В рамках создания БД необходимо выполнить следующую последовательность действий:

1) Запустить терминальную программу psql, выполнив следующую команду:

```
sudo -u postgres psql
```

2) Создать пользователя airflow и задать пароль, выполнив следующую команду:

```
CREATE USER airflow WITH PASSWORD '<указать пароль>';
```

3) Создать БД airflow и указать её владельцем пользователя airflow, выполнив следующую команду:

```
CREATE DATABASE airflow OWNER=airflow ENCODING=utf8;
```

4) Предоставить права на БД airflow пользователю

```
GRANT ALL PRIVILEGES ON DATABASE airflow TO airflow;
```

5) Выполнить выход из терминальной программы psql, выполнив следующую команду:

```
\q
```

6) Осуществить попытку входа в БД airflow под пользователем airflow, выполнив следующую команду:

```
psql -U airflow airflow
```

7) Ввести пароль и убедиться, что вход успешно выполнен.

8) Выполнить выход из терминальной программы psql следующей командой:

```
\q
```

3.6.3 Установка ПО Apache Airflow

Для установки ПО Apache Airflow необходимо выполнить следующую последовательность действий:

1) В директории /opt создать каталог airflow, выполнив следующую команду:

```
sudo mkdir /opt/airflow
```

2) Сменить владельца для каталога /opt/airflow, выполнив следующую команду:

```
sudo chown -R airflow:airflow /opt/airflow
```

3) Сменить права доступа на каталог /opt/airflow, выполнив следующую команду:

```
sudo chmod -R 775 /opt/airflow
```

4) Перейти в каталог /opt/airflow, выполнив следующую команду:

```
cd /opt/airflow
```

5) Из каталога airflow дистрибутивного комплекта под учетной записью пользователя airflow скопировать все файлы в директорию /opt/airflow и перейти в /opt/airflow.

6) Добавить системную переменную AIRFLOW_HOME и указать в значении путь до папки airflow, выполнив следующую команду:

```
echo "AIRFLOW_HOME=/opt/airflow" | sudo tee -a /etc/environment > /dev/null
```

7) Выполнить перезагрузку ОС следующей командой:

```
sudo reboot
```

8) Создать виртуальное окружение в папке airflow, выполнив следующую команду:

```
virtualenv /opt/airflow/venv
```

9) Активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

10) Установить Apache Airflow версии 1.10.11 и необходимые компоненты, выполнив последовательно следующие команды:

```
pip3 install apache-airflow==1.10.11
pip3 install apache-airflow[celery]==1.10.11
pip3 install apache-airflow[crypto]==1.10.11
pip3 install flask_bcrypt
pip3 install psycopg2
pip3 install pyamqp
```

11) В директории /opt/airflow создать папки dags, plugins и crt.

3.6.4 Создание сертификата для подключения по защищенному протоколу HTTPS

Для обеспечения подключения к веб-консоли модуля оркестрации по защищенному протоколу HTTPS необходимо выпустить сертификат и разместить его в директории /opt/airflow/crt. В случае отсутствия возможности выпустить сертификат, предлагается создать самоподписанный сертификат при помощи программы openssl. Для этого требуется выполнить следующую последовательность действий:

1) Создать файл req.conf в директории /opt/airflow/crt посредством открытия его в режиме редактирования программой nano:

```
sudo nano /opt/airflow/crt
```

Пример содержимого данного файла приведен ниже. В секциях req_distinguished_name и alt_names требуется указать значения параметров, при этом значения параметров req_distinguished_name может быть скопировано из примера ниже. Более подробная информация о параметрах приведена в документации на сайте сообщества, развивающего программный продукт OpenSSL: https://www.openssl.org/docs.

В секции alt_names обязательно необходимо указать:

— Значение параметра IP.1. Это IP адрес сервера, на котором осуществляется развертывание модулей согласно данному документу;

— Значение параметра DNS.1. Это наименование хоста, по которому будет осуществляться обращение к веб-консоли модуля оркестрации. Например, в браузере клиентского АРМ вводится URL https://airflow-srv/. Это предполагает, что в DNS записях данного АРМ прописано соответствие:

airflow-srv 192.168.177 (значение параметра IP.1)

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = VA
L = SomeCity
O = MyCompany
OU = MyDivision
CN = www.company.com
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = airflow-srv-01
```

```
IP.1 = 10.70.39.187
```

2) Выпустить сертификат и ключ, выполнив следующую команду:

```
openssl req -x509 -nodes -days 2196 -newkey rsa:2048 -keyout
/opt/airflow/crt/cert.key -out /opt/airflow/crt/cert.pem -config
/opt/airflow/crt/req.conf -extensions 'v3_req'
```

3.6.5 Настройка Apache Airflow

Для настройки ПО Apache Airflow необходимо выполнить следующую последовательность действий под пользователем airflow, созданным ранее:

1) Установить терминальный мультиплексор tmux, выполнив следующую команду:

```
sudo yum install tmux
```

2) Перейти в каталог /opt/airflow, выполнив следующую команду:

```
cd /opt/airflow
```

3) Активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

4) Инициализировать создание конфигурационного файла airflow.cfg с настройками по умолчанию, выполнив следующую команду:

```
airflow version
```

5) Отредактировать конфигурационный файл /opt/airflow/airflow.cfg, заполнив поля, представленные в таблице (Таблица 3.2):

Таблица 3.2 – Описание параметров конфигурационного файла airflow.cfg

Секция	Параметр	Значение	Описание
1	2	3	4
core	default_timezone	Europe/Moscow	Временная зона сервера
	executor	CeleryExecutor	Тип службы очереди задач
	sql_alchemy_conn	postgresql+psycopg2://airflow:<psql_password>@localhost:5432/airflow	Подключение к БД PostgreSQL <psql_password> - пароль пользователя airflow, заданный в п.3.6.2
	dags_are_paused_at_creation	False	Создание сценариев неактивным
	load_examples	False	Загрузка примеров сценариев
	load_default_connections	False	Загрузка примеров соединений
	store_serialized_dags	True	Хранение сценариев в формате json для оптимизации работы

Секция	Параметр	Значение	Описание
1	2	3	4
api	auth_backend	airflow.contrib.auth.backends.password_auth	Аутентификация по логину и паролю
webserver	base_url	https://localhost	Реальный веб-адрес Airflow
	default_ui_timezone	Europe/Moscow	Временная зона веб-консоли
	web_server_port	443	Порт работы веб-сервера
	web_server_ssl_cert	/opt/airflow/crt/cert.pem	Сертификат формата pem или crt, необходимый для работы по https. Генерация сертификата представлена в пункте 3.6.4
	web_server_ssl_key	/opt/airflow/crt/cert.key	Ключ сертификата
	authenticate	True	Включение аутентификации
	auth_backend	airflow.contrib.auth.backends.password_auth	Аутентификация по логину и паролю. Этот параметр нужно самостоятельно добавить, в сформированном стандартном файле airflow.cfg он отсутствует
	rbac	True	Включение ролевой модели
celery	broker_url	pyamqp://airflow:<rabbit_password>@localhost:5672/	Подключение к RabbitMQ <rabbit_password> - пользователя airflow, заданный в п.3.3
	result_backend	db+postgresql://airflow:<psql_password>@localhost:5432/airflow	Подключение Celery к БД PostgreSQL <psql_password> - пароль пользователя airflow, заданный в п.3.6.2

6) Инициализировать базу данных airflow, выполнив следующую команду:

```
airflow initdb
```

7) Создать пользователя с ролью администратора для доступа к веб-консоли, задав логин, имя, фамилию и пароль,:посредством следующей команды:

```
airflow create_user -r Admin -u <user> -e <email> -f <first_name>
-l <last_name> -p <password>
```

где:

— <user> - логин пользователя;

— <email> - адрес электронной почты;

— <first_name> - имя пользвоателя;

— <last_name> - фамилия пользователя;

— <password> - пароль пользвоателя.

8) В директорию /opt/airflow под учетной записью пользователя airflow скопировать файл create_api_user.py из каталога airflow дистрибутивного комплекта.

9) Создать пользователя для доступа к REST API Airflow, под которым будет осуществляться подключение со стороны личного кабинета, выполнив следующую команду:

```
python3 /opt/airflow/create_api_user.py <логин пользователя> <пароль>
```

10) В директорию /opt/airflow/plugins под учетной записью пользователя airflow скопировать каталоги common, api, resource_group из каталога airflow дистрибутивного комплекта.

11) В директорию /opt/airflow/plugins/ под учетной записью пользователя airflow скопировать каталог connectors из каталога airflow дистрибутивного комплекта.

12) В директорию /opt/airflow/dugs под учетной записью пользователя airflow скопировать все файлы из каталога airflow/dugs дистрибутивного комплекта.

13) Инициализировать добавление модулей, выполнив следующую команду:

```
airflow initdb
```

14) Деактивировать виртуальное окружение, выполнив следующую команду:

```
deactivate
```

15) В конфигурационном файле /opt/airflow/airflow.cfg установить параметр update_fab_perms в значение «False».

16) Запустить терминальный мультиплексор, выполнив следующую команду:

```
tmux
```

17) Активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

18) Запустить webserver, выполнив следующую команду:

```
airflow webserver
```

19) Открыть еще одну терминальную сессию посредством tmux. Для этого необходимо одновременно нажать клавиши Ctrl и B, а затем клавишу C.

20) В открывшейся терминальной сессии активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

21) Запустить scheduler, выполнив следующую команду:

```
airflow scheduler
```

22) Открыть еще одну терминальную сессию посредством tmux. Для этого необходимо одновременно нажать клавиши Ctrl и B, а затем клавишу C.

23) В открывшейся терминальной сессии активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

24) Запустить worker, выполнив следующую команду:

```
airflow worker
```

25) Открыть еще одну терминальную сессию посредством tmux. Для этого необходимо одновременно нажать клавиши Ctrl и B, а затем клавишу C.

26) В открывшейся терминальной сессии активировать виртуальное окружение, выполнив следующую команду:

```
source /opt/airflow/venv/bin/activate
```

27) Запустить worker, выполнив следующую команду:

```
airflow flower
```

Важно! *Все термальные сессии(вкладки) в tmux имеют номера по порядку, начиная с нуля. Соответственно, в рамках шагов 16-27 их было создано 4 с номерами от 0 до 3. Для перехода на определенную вкладку необходимо одновременно нажать клавиши Ctrl и B, а затем номер вкладки (в данном случае от 0 до 3).*

28) Проверить доступность веб-консоли Apache Airflow, открыв в веб-обозревателе URL: https://<ip адрес сервера личного кабинета>;

29) Выполнить аутентификацию под учетными данными, заданными на шаге 7 данного пункта.

Важно! *Пароль может быть изменен в веб-консоли в рамках настройках профиля, а именно посредством нажатия кнопки «Reset my password».*

3.6.6 Настройки на стороне подключаемых информационных систем

Модуль оркестрации подключается к целевым информационным системам (целевым ресурсам) посредством программных коннекторов, написанных на языке программирования

Python 3 версии. В настоящее время разработаны коннекторы к следующим информационным системам:

- Антивирусная система на базе ПО Kaspersky;
- Служба каталогов на базе MS Active Directory.

Для интеграции со службой каталогов на базе MS Active Directory необходимо создать доменную учетную запись, включенную в группу Account Operators. Под данной учетной записью со стороны модуля будет осуществляться подключение. Также необходимо разрешить подключение со стороны сервера NSSP до соответствующего контроллера домена по порту 636.

Для интеграции с антивирусной системой на базе ПО Kaspersky необходимо:

- Установить либо обновить Kaspersky Security Center до версии 11 и выше;
- Создать в Kaspersky Security Center локальную учетную запись либо предоставить доменной следующий набор ролей:
  - Администратор Сервера администрирования,
  - Главный администратор,
  - Администратор Kaspersky Endpoint Security,
  - Администратор системного администрирования.
- На Kaspersky Security Center в разделе «Задачи» создать задачу с типом «Поиск вирусов»;
- На Kaspersky Security Center в разделе «Дополнительно» → «Управление программами»→ «Категории программ» создать категорию.

3.6.7 Настройка взаимодействия с информационными системами на стороне модуля оркестрации

Информация о целевых ресурсах (целевых системах), на которые оказывает управляющие воздействия модуль оркестрации, содержится в справочнике Admin/Resources. Объединение целевых ресурсов (ЦР) в группы может осуществляться на основании совпадения типа системы ЦР и аутентификационных данных.

Ограничения:

- группа ЦР не может включать в себя ресурсы различных типов систем;
- группа ЦР имеет общие аутентификацонные данные для подключения к ресурсам, включенным в нее.

Для настройки подключения модуля оркестрации к ЦР необходимо выполнить следующие действия в веб-консоли Apache Airflow:

- Создать группу ЦР.
- Добавить ЦР в группу.

3.6.7.1 Настройка взаимодействия со службой каталогов MS Active Directory

Необходимо создать группу ЦР с наименованием «Active Directory». Для создания группы ЦР выполнить следующую последовательность действий:

1) Аутентифицироваться в веб-консоли Apache Airflow под учетной записью, созданной в рамках п. 3.6.5.

2) В веб-консоли Apache Airflow раскрыть категорию «Admin» главного меню и перейти на вкладку «Resource Groups»,

3) Нажать на кнопку добавления новой группы  .

4) Заполнить необходимые атрибуты в секциях «Group Info» согласно таблице (Таблица 3.3):

Таблица 3.3 – Описание атрибутов секции «Group Info»

Атрибут	Значение	Описание
Group Name	Active Directory	Уникальное имя группы
Description	Active Directory	Описание группы.
Group Type	Active Directory	Тип группы. Указывает на принадлежность группы определенному типу системы. Наличие различных типов систем в выпадающем списке зависит от добавленных в Airflow коннекторов.
Auth Type	Login/Password	Тип аутентификации: – логин / пароль; – сертификат – ключ-строка В зависимости от выбранного типа аутентификации, происходит отображение необходимых полей – Login и Password или Key
Login	<>	Логин доменной учетной записи для подключения, созданной в рамках настройки MS Active Directory в п.3.6.6
Password	<>	Пароль доменной учетной записи для подключения, созданной в рамках настройки MS Active Directory в п.3.6.6

5) Сохранить изменения, нажав кнопку «Save».

Необходимо добавить ЦР в группу Active Directory. Для создания ЦР в группу выполнить следующую последовательность действий:

1) Аутентифицироваться в веб-консоли Apache Airflow под учетной записью, созданной в рамках п. 3.6.5.

2) В веб-консоли Apache Airflow раскрыть категорию «Admin» главного меню и перейти на вкладку «Resource Groups».

3) Открыть группу Active Directory и перейти на вкладку «List Resources».

4) Нажать на кнопку добавления нового ресурса  .

5) Заполнить необходимые атрибуты согласно таблице (Таблица 3.4):

Таблица 3.4 – Описание атрибутов секции «List Resources»

Атрибут		Описание
Host Type	IP	Тип адреса добавляемого ресурса: – IP-адрес; – DNS-имя; – Диапазон IP-адресов В зависимости от выбранного типа адреса, происходит отображение необходимых полей – IP, DNS Name, или поля диапазона IP. **Примечание**: – при выборе диапазона IP-адресов каждый адрес из диапазона создается как отдельный ресурс; – создание ресурсов из диапазона происходит инкрементальным способом, т.е. при указании диапазона в различных подсетях, произойдет добавление IP-адресов от начала до конца указанного диапазона
IP	<ip контроллера домена>	Указывается IP адрес контроллера домена MS Active Directory
Use default port	Флаг выбран	Флаг использования порта по умолчанию. При установке флага добавление ресурса произойдет с указанием порта по умолчанию, определенного выбранным типом группы. При сбросе флага происходит отображение поля Port для указания необходимого порта
Description	test	Описание ресурса

6) Сохранить изменения, нажав кнопку «Save».

3.6.7.2 Настройка взаимодействия с антивирусной системой на базе ПО Kaspersky

Необходимо создать группу ЦР с наименованием «Kaspersky Security Center». Для создания группы ЦР выполнить следующую последовательность действий:

1) Аутентифицироваться в веб-консоли Apache Airflow под учетной записью, созданной в рамках п. 3.6.5.

2) В веб-консоли Apache Airflow раскрыть категорию «Admin» главного меню и перейти на вкладку «Resource Groups»,

3) Нажать на кнопку добавления новой группы  .

4) Заполнить необходимые атрибуты в секциях «Group Info» и «Extra Properties Info» согласно таблице (Таблица 3.5):

Таблица 3.5 – Описание атрибутов секций «Group Info»и «Extra Properties Info»

Атрибут	Значение	Описание
Параметры секции Group Info		
Group Name	Kaspersky Security Center	Уникальное имя группы
Description	Kaspersky Security Center	Описание группы.
Group Type	Kaspersky Security Center	Тип группы. Указывает на принадлежность группы определенному типу системы. Наличие различных типов систем в выпадающем списке зависит от добавленных в Airflow коннекторов.
Auth Type	Login/Password	Тип аутентификации: – логин / пароль; – сертификат – ключ-строка В зависимости от выбранного типа аутентификации, происходит отображение необходимых полей – Login и Password или Key
Login	<>	В зависимости от указанного параметра «isWindowsUser» секции Extra Properties Info указывается либо логин пользователя Windows либо логин внутреннего пользователя.
Password	<>	В зависимости от указанного параметра «isWindowsUser» секции Extra Properties Info указывается пароль либо пользователя Windows либо внутреннего пользователя
Параметры секции Extra Properties Info		
isWindowsUser	<>	Вид пользователя для подключения к Kaspersky Security Center.

		В зависимости от того, какой вид аутентификации настроен на Kaspersky Security Center, выбирается одно из двух значений: — True - пользователь Windows — False - внутренний пользователь KSC P
Domain	<>	Указывается, если параметр isWindowsUser=True Домен пользователя в случае доменного пользователя или имя компьютера в случае локального.
CategoryName	<>	Указывается наименование созданной в рамках п. 3.6.6 категории программ на Kaspersky Security Center.
TaskName	<>	Указывается наименование созданной в рамках п. 3.6.6 задачи антивирусного сканирования Kaspersky Security Center.

5) Сохранить изменения, нажав кнопку «Save».

Необходимо добавить ЦР в группу Kaspersky Security Center. Для создания ЦР в группу выполнить следующую последовательность действий:

1) Аутентифицироваться в веб-консоли Apache Airflow под учетной записью, созданной в рамках п. 3.6.5.

2) В веб-консоли Apache Airflow раскрыть категорию «Admin» главного меню и перейти на вкладку «Resource Groups».

3) Открыть группу Kaspersky Security Center и перейти на вкладку «List Resources».

4) Нажать на кнопку добавления нового ресурса  .

5) Заполнить необходимые атрибуты согласно таблице (Таблица 3.6Таблица 3.4):

Таблица 3.6 – Описание атрибутов секции «List Resources»

Атрибут		Описание
Host	<ip адрес сервера KSC>.	IP адрес сервера, на котором установлено ПО Kaspersky Security Center
Use default port	Флаг выбран	Порт подключения. Если не используется порт отличный от 13299, то необходимо снять флаг и в появившемся поле Port указать значение порта
Description	Test KSC	Описание ресурса

6) Сохранить изменения, нажав кнопку «Save».

3.7 Установка модуля визуализации

3.7.1 Создание служебной учетной записи ОС

Для обеспечения установки необходимого ПО и последующей работы модуля, в ОС необходимо создать отдельного пользователя grafana, установить для него пароль и включить пользователя в группу wheel. Для этого необходимо выполнить следующую последовательность действий:

1) Создать пользователя grafana, выполнив следующую команду:

```
sudo useradd -m grafana
```

2) Включить пользователя grafana в группу wheel, выполнив следующую команду:

```
sudo usermod -aG wheel grafana
```

3) Сменить пароль пользователю grafana, выполнив следующую команду:

```
sudo passwd grafana
```

4) Ввести новое значение пароля с подтверждением:

```
New password: <Ввести новое значение пароля>
Retype new password: <Повторить значение пароля>
```

5) Переключить сессию на пользователя grafana и продолжить выполнение дальнейших действий под ним, выполнив следующую команду:

```
su grafana
```

3.7.2 Создание БД

В рамках создания БД необходимо выполнить следующую последовательность действий:

1) Запустить терминальную программу psql, выполнив следующую команду:

```
sudo -u postgres psql
```

2) Создать пользователя grafana и задать пароль, выполнив следующую команду:

```
CREATE USER grafana WITH PASSWORD '<указать пароль>';
```

3) Создать БД grafana и указать её владельцем пользователя grafana, выполнив следующую команду:

```
CREATE DATABASE grafana OWNER=grafana ENCODING=utf8;
```

4) Предоставить права на БД grafana пользователю

```
GRANT ALL PRIVILEGES ON DATABASE grafana TO grafana;
```

5) Выполнить выход из терминальной программы psql, выполнив следующую команду:

```
\q
```

6) Осуществить попытку входа в БД grafana под пользователем grafana, выполнив следующую команду:

```
psql -U grafana grafana
```

7) Ввести пароль и убедиться, что вход успешно выполнен.

8) Выполнить выход из терминальной программы psql следующей командой:

```
\q
```

3.7.3 Установка ПО Grafana

Для установки ПО Grafana необходимо выполнить следующую последовательность действий под пользователем grafana:

1) Перейти в домашнюю директорию, выполнив следующую команду:

```
cd /home/grafana
```

2) Скачать версию ПО Grafana 7.3.3, выполнив следующую команду:

```
wget https://dl.grafana.com/oss/release/grafana-7.3.3-
1.x86_64.rpm
```

1) Установить скачанную версию, выполнив следующую команду:

```
sudo yum install grafana-7.3.3-1.x86_64.rpm
```

2) Запустить службу Grafana следующей командой:

```
sudo systemctl start grafana-server
```

3) Установить плагин для создания круговых диаграмм, выполнив следующую команду:

```
grafana-cli plugins install grafana-piechart-panel
```

4) Выполнить перезагрузку службы Grafana, выполнив последовательно следующие команды:

```
sudo systemctl stop grafana-server
sudo systemctl start grafana-server
```

5) В веб-обозревателе ввести URL: http://<ip адрес сервера личного кабинета>:3000/?kiosk и удостовериться, что веб-интерфейс приложения доступен.

3.7.4 Первичная настройка ПО Grafana

Для первичной настройки ПО Grafana необходимо выполнить следующую последовательность действий под пользоателем grafana:

1) В директории /etc/grafana/ открыть конфигурационный файл grafana.ini в режиме редактирования.

2) Отредактировать конфигурационный файл заполнив поля, представленные в таблице ниже (Таблица 3.7). В конфигурационном файле grafana.ini перед наименованием параметров при редактирвоании требуется удалить символ «;».

Таблица 3.7 – Параметры конфигурационного файла grafana.ini

Секция	Параметр	Значение	Описание
[database]	type	postgres	Тип БД
	host	<host>:<port>	Хост и порт на котором развернута БД
	name	grafana	Наименование БД
	user	grafana	Логин пользователя БД
	password	<psql_password >	Пароль пользователя БД
[auth.anonymos]	enabled	true	Гостевой доступ
	hide_version	true	Отображение версии ПО
[explore]	enabled	false	Включение компонента «Explore»

3) Скопировать файл «app.77c6cb2b767d3da10797.js» из каталога grafana дистрибутивного комплекта в каталог /usr/share/grafana/public/build на сервере.

4) Скопировать файл «undex.html» из каталога grafana дистрибутивного комплекта в каталог /usr/share/grafana/public/views на сервере.

5) Перезагрузить службу grafana

```
sudo service grafana restart
```

3.7.5 Создание подключения к источнику данных

Для создания подключения к источнику данных необходимо выполнить следующую последовательность действий:

1) Войти в веб-консоль под учетной записью администратора «admin». Пароль по умолчанию «admin». При первом входе в систему выйдет запрос и необходимости ввода нового пароля.

2) Для создания нового подключения к источнику данных, нужно перейти в раздел Configuration -> Data Sources и нажать на кнопку «Add data sources».

3) Выбрать из списка PostgreSQL.

4) В появившемся окне заполнить параметры подключения к БД личного кабинета, созданной в рамках п. 3.5.2. Параметры заполнения приведены в таблице (Таблица 3.8).

Таблица 3.8 – Параметры источника данных

Параметр	Пример заполнения	Описание
Name	nssp	Наименование создаваемого подключения
Host	127.0.0.1:5432	Хост и порт СУБД
Database	nssp	Наименование БД
User	nssp	Логин пользователя СУБД
Password	<password>	Пароль пользователя СУБД
SSL Mode	Disable	Опция, которая определяет с каким защищенное или нет соединение

5) Нажать на кнопку «Save & Test».

3.7.6 Настройка дашбордов

В первую очередь необходимо загрузить все дашборды из дистрибутивного комплекта. Это файлы с расширением JSON, расположенные в каталоге Grafana дистрибутивного комплекта. Для загрузки дашбордов необходимо выполнить следующую последовательность действий:

1) Войти в веб-консоль ПО Grafana под учетной записью администратора admin.

2) В боковом меню перейти в «Create» → «Import».

3) Нажать на кнопку «Upload JSON file», выбрать один из файлов JSON в каталоге grafana и нажать на кнопку «Import».

4) Повторить эти действия для всех файлов дашбордов (с расширением JSON), расположенных в каталоге grafana дистрибутивного комплекта.

Далее необходимо установить дашборд «Инфопанель по инцидентам ИБ и Активам» по умолчанию. Для этого необходимо сделать следующее:

1) Войти в веб-консоль под учетной записью администратора admin.

2) Открыть дашборд «Dashboards» -> «Manage» - «Инфопанель по инцидентам ИБ и Активам».

3) В верхней части страницы, рядом с наименованием дашборда, нажать на кнопку «Mark as favorite», как показано на рисунке ниже (Рисунок 3.1).

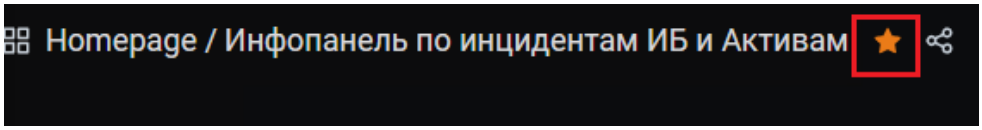

Рисунок 3.1 – Дашборд по умолчанию

3.8 Установка модуля сканирования сети

3.8.1 Создание служебной учетной записи ОС

В ОС необходимо создать пользователя nextst, задать ему пароль и включить пользователя в группу wheel для наделения необходимыми правами доступа. Для этого необходимо выполнить следующую последовательность действий:

1) Создать пользователя nextsst, выполнив следующую команду:

```
sudo useradd -m nextst
```

2) Включить пользователя nextst в группу wheel, выполнив следующую команду:

```
sudo usermod -aG wheel nextst
```

3) Сменить пароль пользователю nextst, выполнив следующую команду:

```
sudo passwd nextst
```

4) Ввести новое значение пароля с подтверждением:

```
New password: <Ввести новое значение пароля>
Retype new password: <Повторить значение пароля>
```

5) Переключить сессию на пользователя nextst и продолжить выполнение дальнейших действий под ним, выполнив следующую команду:

```
su nextst
```

3.8.2 Создание БД

В рамках создания БД необходимо выполнить следующую последовательность действий:

1) Запустить терминальную программу psql, выполнив следующую команду:

```
sudo -u postgres psql
```

2) Создать пользователя nextst и задать пароль, выполнив следующую команду:

```
CREATE USER nextst WITH PASSWORD '<указать пароль>';
```

3) Создать БД nextst и указать её владельцем пользователя neststst, выполнив следующую команду:

```
CREATE DATABASE nextst OWNER=nextst ENCODING=utf8;
```

4) Предоставить права на БД nextst пользователю

```
GRANT ALL PRIVILEGES ON DATABASE nextst TO nextst;
```

5) Выполнить выход из терминальной программы psql, выполнив следующую команду:

```
\q
```

6) Осуществить попытку входа в БД nextst под пользователем nextst, выполнив следующую команду:

```
psql -U nextst nextst
```

7) Ввести пароль и убедиться, что вход успешно выполнен.

8) Выполнить выход из терминальной программы psql следующей командой:

```
\q
```

3.8.3 Установка и первичная настройка модуля сканирования сети

Для установки и первичной настройки модуля сканирования сети необходимо выполнить следующую последовательность действий под пользователем nextst:

1) В директории /opt создать каталог nextst, выполнив следующую команду:

```
sudo mkdir /opt/nextst
```

2) Сменить владельца для каталога /opt/nextst, выполнив следующую команду:

```
sudo chown -R nextst:nextst /opt/nextst
```

3) Сменить права доступа на каталог /opt/nextst, выполнив следующую команду:

```
sudo chmod -R 775 /opt/nextst
```

4) Перейти в каталог /opt/nextst, выполнив следующую команду:

```
cd /opt/nextst
```

5) Из дистрибутивного комплекта скопировать все файлы из каталога nextst в директорию /opt/nextst и перейти в /opt/nextst

6) Настроить учетные данные БД модуля личного кабинета и модуля сканирования сети для обеспечения их синхронизации. Для этого создать файл .pgpass в режиме редактирования программой nano, выполнив следующую команду:

```
sudo nano /opt/nextst/.pgpass
```

7) Необходимо добавить строки с учетными данными для подключения к БД личного кабинета, заданными в рамках п.3.5.2, и данными для подключения к БД модуля сканирования сети, заданными в рамках п.3.8.2. Пример итогового содержания файла .pgpass:

localhost:5432:nssp:nssp:*ПАРОЛЬ*

localhost:5432:nextst:nextst:*ПАРОЛЬ*

8) Нажать комбинацию клавиш Ctrl+X для выхода;

9) Ввести «y» и подтвердить наименование сохраняемого файла, нажав клавишу «Enter».

10) Изменить права на файл .pgpass, выполнив следующую команду:

```
sudo chmod 0600 /opt/nextst/.pgpass
```

11) Предоставить право на исполнение файла wmi-1.3.14-4.el7.art.x86_64.rpm, выполнив следующую команду:

```
sudo chmod +x wmi-1.3.14-4.el7.art.x86_64.rpm
```

12) Установить пакет wmi-1.3.14-4.el7.art.x86_64.rpm, выполнив следующую команду:

```
sudo yum install wmi-1.3.14-4.el7.art.x86-64.rpm
```

13) Установить пакет krb5-devel, обеспечивающий керберос аутентифкацию:

```
sudo yum install krb5-devel
```

14) Создать виртуальное окружение в папке /opt/nextst:

```
virtualenv /opt/nextst/venv
```

1) Активировать виртуальное окружение, выполнив следующую команду:

```
source opt/nextst/bin/activate
```

2) Установить необходимые библиотеки, выполнив последовательно следующие команды:

```
pip install pip-tools setuptools
pip install -r reqirements
```

3) Настроить подключение к БД в конфигурационном файле /opt/nextst/nextst/settings.py:

```
DATABASES = {
    'default': {
        'ENGINE': 'django.db.backends.postgresql_psycopg2',
        'NAME': 'nextst',
        'USER': 'nextst',
        'PORT': '5432',
        'HOST': '127.0.0.1'
    }
```

4) Перейти в /opt/nextst и выполнить миграции, выполнив последовательно следующие команды:

```
cd /opt/nextst
python3 manage.py makemigrations
python3 manage.py migrate
```

5) Выполнить первичный запуск gunicorn:

```
gunicorn --bind 0.0.0.0:8001 nextst.wsgi
```

6) Нажать одновременно клавиши Ctrl и C для завершения сессии gunicorn

7) Деактивировать виртуальное окружение следующей командой:

```
deactivate
```

8) Создать файл, обеспечивающий запуск модуля, как службы, следующей командой:

```
sudo nano /etc/systemd/system/nextst.service
```

9) В данный файл внести следующее:

```
[Unit]
Description=nextstage daemon
After=network.target

[Service]
User=nextst
Group=nginx
```

```
WorkingDirectory=/opt/nextst

ExecStart=/opt/nextst/venv/bin/gunicorn --workers 3 --timeout 600
--bind  unix:/opt/nextst/nextst.sock  nextst.wsgi:application  -b
0.0.0.0:8001


[Install]

WantedBy=multi-user.target
```

10) Сохранить файл.

11) В файл nginx в секции http с сохранением отступов от левого края перед блоком настроек server по умолчанию добавить блок настроек server, приведенный ниже. Только необходимо указать соответствующий IP адрес сервера, на котором развернут личный кабинет пользователя.

```
    server {
        listen 80;
      server_name <ip адрес сервера>;


        location = /favicon.ico { access_log off; log_not_found
off; }
        location /static/ {
            root /opt/nextst;
        }


        location / {
            proxy_read_timeout 10m;
            proxy_connect_timeout 10m;
            proxy_send_timeout 10m;
            proxy_set_header Host $http_host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header                      X-Forwarded-For
$proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
            #proxy_pass http://unix:/opt/lk/lk.sock;
          proxy_pass http://unix:/opt/nextst/nextst.sock;
```

```
        }
    }
```

12) Настроить автозапуск и запустить сервис:

```
sudo systemctl enable nextst
sudo systemctl start nextst
```

3.9 Настройка взаимодействия модулей программного продукта

Для настройки взаимодействия модулей необходимо заполнить параметры конфигурационного файла local_settings.py личного кабинета, расположенного в /opt/nssp/project/settings/. Описание параметров данного конфигурационного файла с примерами заполнения приведен в таблице (Таблица 3.9).

Таблица 3.9 – Параметры настроек конфигурационного файла local_settings.py

Секция	Параметр	Значение	Описание
1	2	3	4
	SCANNER_URL	http://<ip адрес сервера>	URL модуля сканирования сети
	AIRFLOW_URL	https://<ip адрес сервера>	URL модуля оркестрации
	GRAFANA_URL	https://< ip адрес сервера >::3000/?orgId=1&kiosk	URL модуля визуализации
	EMAIL_HOST	<IP адрес либо сетевое имя почтового сервера>	Адрес почтового сервера, на нем должна быть разрешена анонимная отправка по протоколу SMTP
	EMAIL_PORT	25	Порт подключения к почтовому серверу
	DEFAULT_FROM_EMAIL	robot@nssp.ru	Адрес отправителя
	ADMINS	‘<логин>’, ‘<почтовый адрес администратора>’	Логин администратора и его почтовый адрес
ARCSIGHT (блок параметров считывания XML файлов по инцидентам с сервера MF ArcSight)	HOST	< >	IP адрес либо сетевое имя сервера MF ArcSight
	USER	<>	Имя, пользователя, для которого настроен доступ по сертификату
	KEY_PATH	<>	Файловый путь (с названием файла ключа) до rsa-ключа на сервере личного кабинета. Краткая инструкция по формированию пары и открытого ключа приведена на сайте:

Секция	Параметр	Значение	Описание
1	2	3	4
			https://docs.microsoft.com/ru-ru/azure/virtual-machines/linux/mac-create-ssh-keys
	ARCSIGHT_TARGET_FILE_PATH	<>	Файловый путь до каталога с xml-файлами, сформированными MF ArcSight[1]
	ARCSIGHT_PROCESSED_FILE_PATH	<>	Файловый путь до каталога, куда будут перемещаться обработанные xml-файлы
	ARCSIGHT_EVENT_PATERN	<>	Шаблон, по которому будет осуществлен поиск инцидентов в xml-файле (соответствующий названию каталога правил, из которого осуществляется выгрузка xml-файлов MF ArcSight)
	MISCELLANEOUS_PAUSE	<>	Время ожидания (в секунда) перед попыткой повторного считывания, если xml-файл еще не дописан и находится в обработке
	LOG_PATH	<>	Файловый путь до локального каталога с журналами событий

	'CATEGORY_MAPPING': {
	'category_name_1': [
	'xml_event_name_1',
	'xml_event_name_2'
	]
	}
	Пример заполнения:
	'CATEGORY_MAPPING': {
	'Заражение вредоносным программным обеспечением': [
	'Обнаружение hash вредоносных объектов',
	'Обнаружение подозрительных или вредоносных IP-адресов'
		<>	Сопоставление категории инцидента ИБ из личного кабинета с именами правил MF ArcSight (в соответствии с данным сопоставлением будет присваиваться категория инцидента ИБ в личном кабинете).
			В личном кабинете по умолчанию используются следующие категории инцидентов ИБ:
			1) Заражение вредоносным программным обеспечением;
			2) Нарушение безопасности информации;

[1] В консоли MF ArcSight необходимо создать каталог правил с именем, указанном в поле ArcSight_Event_Patern конфигурационного файла и настроить выгрузку xml-файлов для правил, находящихся в данном каталоге

Секция	Параметр	Значение	Описание
1	2	3	4
	], 'Несанкционированный доступ в систему': ['Вход в систему под учетной записью сотрудника, которого нет в офисе'] }		3) Распространение информации с неприемлемым содержимым; 4) Распространение вредоносного программного обеспечения; 5) Нарушение или замедление работы контролируемого информационного ресурса; 6) Попытки несанкционированного доступа в систему или к информации; 7) Сбор сведений с использование ИКТ; 8) Несанкционированный доступ в систему; 9) Мошенничество с использованием ИКТ.

Для обеспечения периодического считывания данных по инцидентам из XML-файлов MF ArcSight и автоматического формирования инцидентов в Личном кабинете пользователя, настроить запуск программного скрипта scan_xml.sh в планировщике ОС (cron). Для этого необходимо:

- Открыть файл планировщика cron для редактирования:

```
sudo crontab -e
```

- Добавить запись, обеспечивающую периодический запуск программного скрипта. Рекомендуется настроить запуск раз в час. Пример для данного расписания приведен ниже.

```
0 * * * * /opt/nssp/scan_xml.sh
```

1) Для обеспечения считывания данных из модуля сканирования сети в личный кабинет с целью автоматического создания технического средства настроить запуск программного скрипта scaner_sync.sh в планировщике ОС (cron). Для этого необходимо:

- Открыть файл планировщика cron для редактирования:

```
sudo crontab -e
```

- Добавить запись, обеспечивающую периодический запуск программного скрипта. Рекомендуется настроить запуск программного скрипта каждые 5 минут. Пример для данного расписания приведен ниже.

```
0/5 * * * * /opt/nextst/scaner_sync.sh
```

Важно: *для обеспечения возможности добавления сведений по портам в учетную карточку технического средства Личного кабинета необходимо, чтобы по данному техническому средству хотя бы единожды запускался тип сканирования «Сбор информации по хостам».*

4 АДМИНИСТРИРОВАНИЕ ПРОГРАММНОГО ПРОДУКТА

4.1 Администрирование личного кабинета пользователя

4.1.1 Управление пользователями

Для управления пользователями необходимо осуществить вход в веб-интерфейс личного кабинета под учетной записью администратора, введя в поле «Логин» значение «admin», а в поле «Пароль» значение «P@ssw0rd».

Для просмотра перечня учетных карточек пользователей в главном меню выбрать раздел «Пользователи». Откроется перечень учетных карточек работников, у которых имеется доступ в систему (Рисунок 4.1).

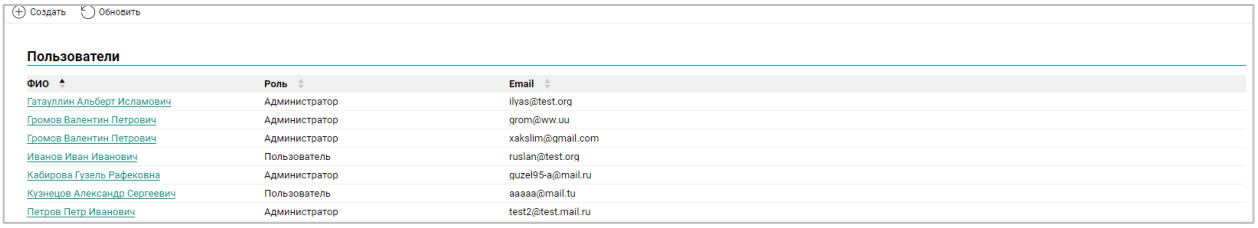

Рисунок 4.1 – Перечень пользователей

Для перехода к учетной карточке работника необходимо выбрать (щелкнув левой кнопкой мыши) соответствующую строку перечня. Откроется учетная карточка работника (Рисунок 4.2).

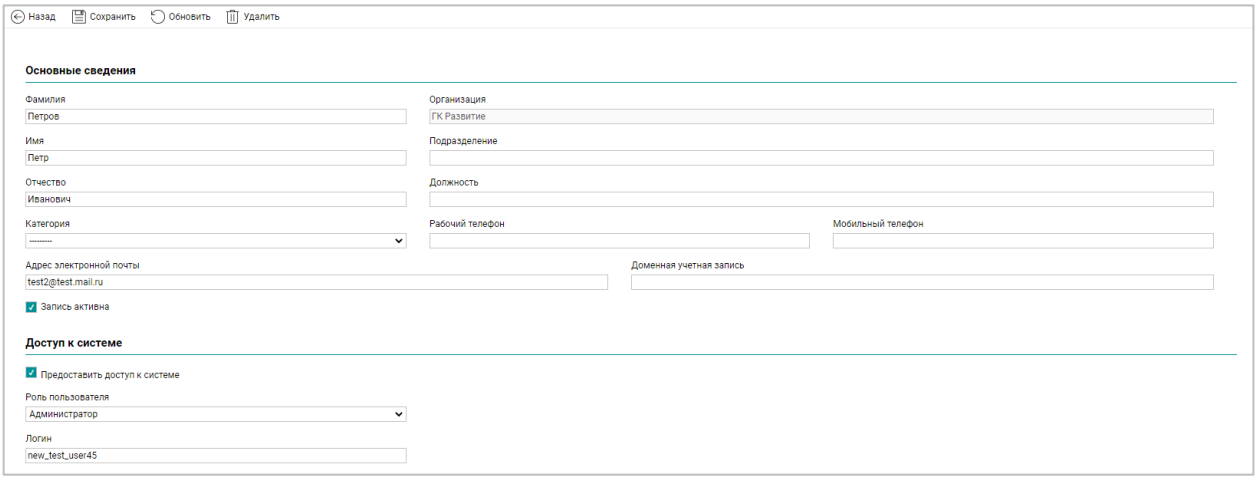

Рисунок 4.2 – Учетная карточка работника

Для обновления элементов перечня необходимо нажать на кнопку «Обновить».

Для создания пользователя для не заведенного ранее в Системе работника необходимо в перечне работников нажать на кнопку «Создать». Откроется новая учетная карточка работника (Рисунок 4.3). В поле «Предоставить доступ к системе» необходимо поставить галочку и заполнить поля.

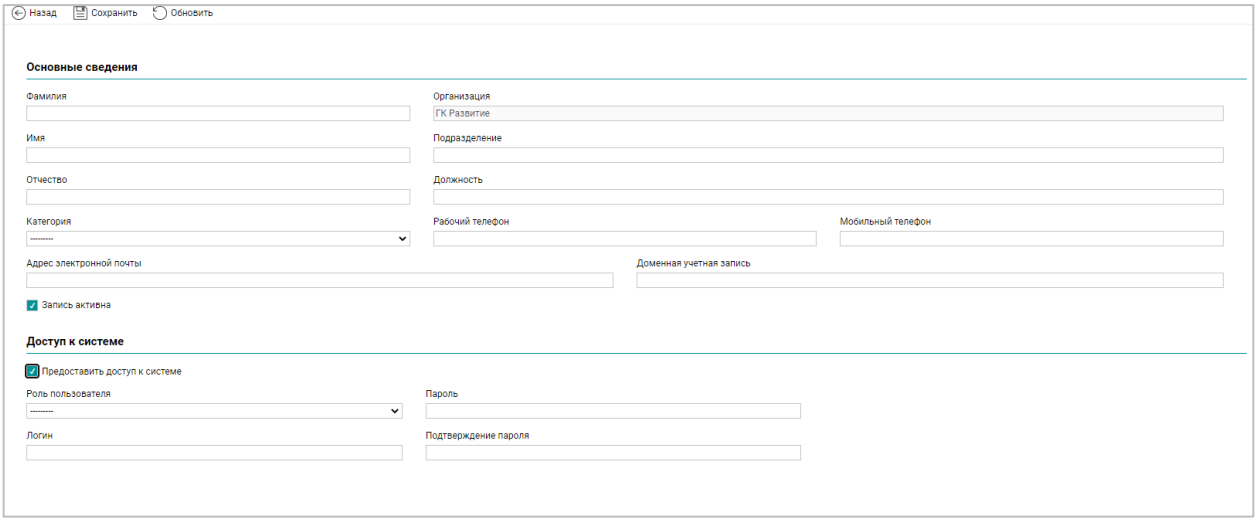

Рисунок 4.3 – Создание пользователя

Для создания пользователя для ранее заведенного в Системе работника необходимо перейти в учетную карточку работника из перечня работников. Откроется учетная карточка работника. В карточке работника необходимо поставить галочку в поле «Предоставить доступ к системе» и заполнить поля в разделе «Доступ к системе».

Для создания пользователя и (или) сохранения внесенных в учетную карточку изменений необходимо нажать на кнопку «Сохранить» в строке меню.

Для возврата к перечню работников необходимо нажать на кнопку «Назад». Для обновления учетной карточки необходимо нажать на кнопку «Обновить».

4.1.2 Удаление объектов из базы данных

Для удаления объектов из базы данных без возможности дальнейшего восстановления необходимо перейти в учетную карточку объекта и нажать на кнопку «Удалить».

4.1.3 Восстановление удаленной пользователем карточки объекта

Для восстановления ошибочно удаленной пользователем карточки объекта необходимо перейти в учетную карточку объекта и поставить галочку рядом с полем «Запись активна» (Рисунок 4.4).

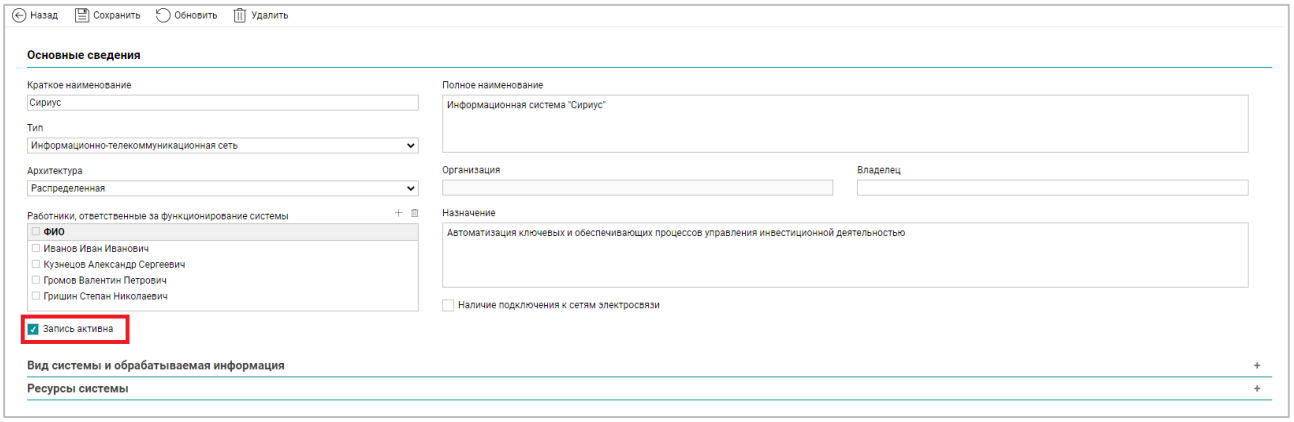

Рисунок 4.4 – Восстановление удаленной карточки объекта

4.2 Администрирование модуля сканирования сети

4.2.1 Запуск сканирования сети

Запуск сканирования сети (определенного хоста, диапазона либо всей подсети) осуществляется через веб-консоль личного кабинета пользователя. Описание запуска сканирования приведено в документе «Программный продукт NextSTage Security Platform: NextStage IRP. Руководство пользователя».

4.2.2 Настройка модуля сканирования сети

Настройка модуля сканирования сети осуществляется посредством выполнения GET запросов. Настройка модуля заключается в добавлении либо удалении учетных данных для обеспечения сбора информации по хосту, а именно информации о логических дисках, процессорах, объему оперативной памяти, мониторах и т.д.

В настоящее время сканирование в режиме сбора вышеперечисленной информации по хосту осуществляется для хостов под управлением следующих версий ОС:

- ОС семейства Microsoft Windows (клиентские – Windows Vista и выше, серверные – Windows Server 2008 и выше);

- ОС семейства Linux: в том числе, RED ОС.

Важно! *Учетная запись, под которой осуществляется сбор информации должна обладать определенными правами на уровне ОС. Для разных типов ОС права различаются:*

- для ОС семейства Windows учетная запись должна входить в группу локальных администраторов;
- для ОС семейства Linux учетная запись должна быть включена в группу sudo и обладать правами на выполнение следующих команд:
  - hostname,
  - arch,
  - dmidecode,
  - cat /etc/os-release,
  - lsb_release -a,
  - ifconfig -a,
  - cat /etc/resolv.conf,
  - ip route,
  - lscpu,
  - cat /proc/meminfo,
  - df -TPk,
  - rpm -qa,
  - dpkg-query,
  - last,
  - cat /etc/passwd,
  - cat /etc/group,
  - service --status-all,
  - systemctl.

4.2.2.1 Добавление учетных записей для сбора информации по хостам

Добавление учетных записей для модуля сканирования сети осуществляется GET запросом следующего формата в общем виде:

http://<ip адрес сервера>/profile/?login=<username>&password=<password>&linux=True&windows=False&ip=<ip адрес>, где:

- <ip адрес сервера> - сетевой адрес размещения модуля;

– <username> - имя пользователя, обладающего необходимыми правами доступа (указаны в п. 4.2.2). В случае если используется доменная учетная запись, то используется следующий формат записи «домен\имя пользователя». Например, http://192.168.1.123/profile/?login=TEST\admin&password=123&windows=True&linux=False&ip=192.168.1.124;

– <password> - пароль;

– Значения параметров windows и linux определяют тип целевой ОС. Они не могут одновременно иметь значение True. Также в значениях True и False регистр написания важен.

– <ip адрес> - сетевой адрес целевого хоста, с которого должна быть собрана информация.

4.2.2.2 Смена пароля для сохраненных учетных записей

Смена пароля учетной записи для модуля сканирования сети осуществляется GET запросом следующего формата в общем виде:

http://<ip адрес сервера>/profile/?login=<username>&ip=<ip адрес>&new_password=<password>, где:

– <ip адрес сервера> - сетевой адрес размещения модуля;

– <username> - имя пользователя, для которого необходимо сменить пароль в БД модуля сканирования сети;

– <password> - новое значение пароля;

– <ip адрес> - сетевой адрес целевого хоста. Для доменных учетных записей ОС семейства Microsoft Windows этот параметр GET запросе не указывается.

4.2.2.3 Удаление учетных записей из БД модуля сканирования сети

Удаление учетной записи для модуля сканирования сети осуществляется GET запросом следующего формата в общем виде:

http://<ip адрес сервера>/profile/? ip=<ip адрес>&profile_delete=True, где:

– <ip адрес сервера> - сетевой адрес размещения модуля;

– <ip адрес> - сетевой адрес целевого хоста, для которого будет удалена учетная запись.

5 СОВЕРШЕНСТВОВАНИЕ ПРОГРАММНОГО ПРОДУКТА

В рамках каждого выпуска обновлений программного продукта производителем предоставляется сопроводительная инструкция по обновлению.

6 ДИАГНОСТИКА ПРОБЛЕМ И НЕИСПРАВНОСТЕЙ

В данном разделе рассматриваются случаи недоступности компонентов программного продукта и необходимые действия по поиску причин.

6.1 Недоступность веб-интерфейса личного кабинета пользователя

При недоступности веб-интерфейса личного кабинета пользователя необходимо выполнить следующую последовательность действий:

1) Перезапустить сервер nginx и проверить статус:

```
sudo systemctl restart nginx
sudo systemctl start nginx
```

2) Если сервер не запущен, открыть журнал событий nginx и проверить на наличие ошибок:

```
sudo journalctl -u nginx.service
```

3) Попытаться самостоятельно устранить неисправности согласно журналу событий. Если этого сделать не получается, сформировать запрос производителю программного продукта.

6.2 Недоступность веб-интерфейса модуля оркестрации

При недоступности веб-консоли Apache Airflow необходимо выполнить следующие действия:

1) Осуществить остановку веб-сервера

```
sudo systemctl stop airflow
```

2) Провести анализ логов, выводимых в консоль терминальной сессии, а также логов, расположенных в директории /opt/airflow/logs, на наличие ошибок.

3) При обнаружении ошибок, влияющих на работоспособность веб-сервера и необходимых компонент, произвести устранение неисправностей.

4) В случае, если неисправности не получается устранить самостоятельно, необходимо сформировать запрос производителю программного продукта. К запросу приложить логи, скриншоты и описание выполняемых действий.

5) Запустить веб-сервер Airflow и необходимые компоненты. Описание запуска компонентов Airflow посредством tmux описано в п. 3.6.5.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Полное наименование
БД	База данных
ИТ	Информационные технологии
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
ЦР	Целевой ресурс
JSON	Java Script Object Notation
IP	Internet Protocol
URL	Uniform Resource Locator
XML	Extensible Markup Language