NVS Greenex

The first login to the system

www.nvs-itech.com

Table of Contents

Creating a user by an administrator.

Initially, a user with sufficient authority (administrator) creates a new

user in transaction SX01, assigns roles to him/her and sets the initial password.

A detailed description of the process is beyond the scope of this instruction.

In the example, the username is USER01 and the initial password is Initial12

www.nvs-itech.com

The first login of a new user.

To log in, you need a link (URL) and information about the user name and initial

passwords, which are sent by mail.

For example:

https://192.168.10.33:8000/

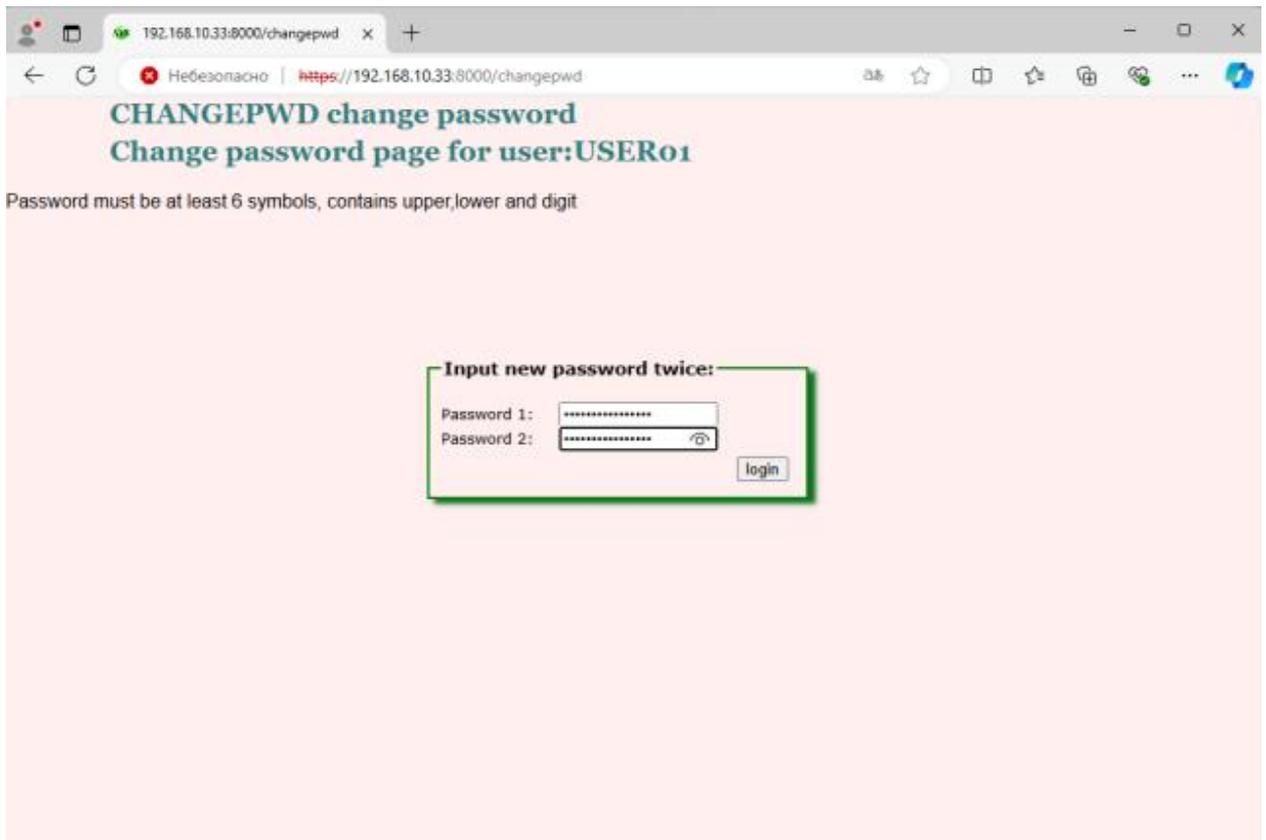the appearance of the invitation screen may look like this
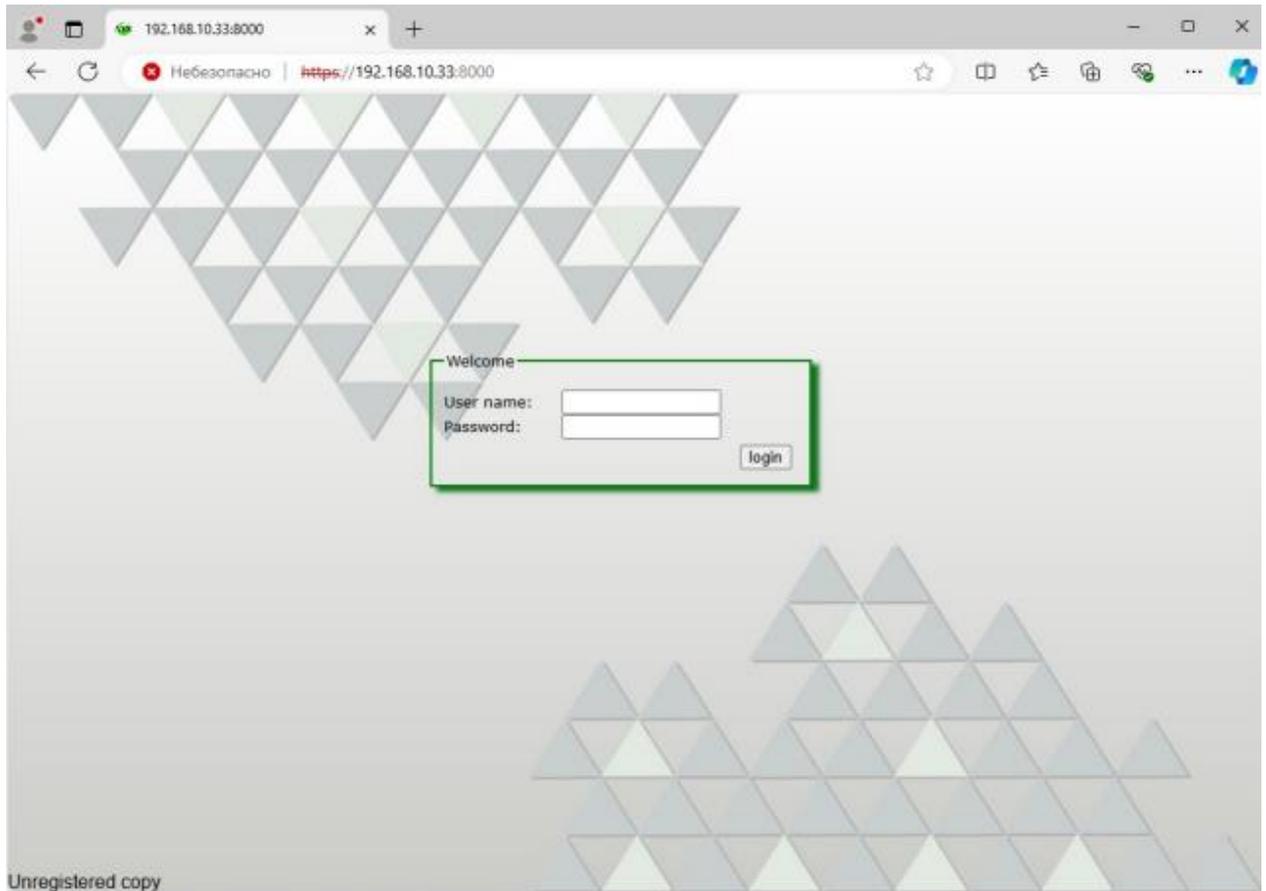
www.nvs-itech.com

The user should enter the name and initial password manually, after which he/she will

be redirected to the new password entry page.

The background color depends on the system settings.

www.nvs-itech.com

After changing the password, close the browser. In the example, this is Microsoft Edge and log in again with an already permanent password

Hint 1: Authorization via URL parameters.

In test systems, you can pass the login password through the parameters of the call string (URL).

Although SSL(TLS v1.2) encryption occurs when data is transmitted over the network.2) and

the URL string is not available for interception, it can still be visible in server logs and

screenshots when information is exchanged carelessly by mail.

An example of a call in the first way:

https://192.168.10.33:8000/bj01?login=USER01&pwd=Zaqwerty10203040
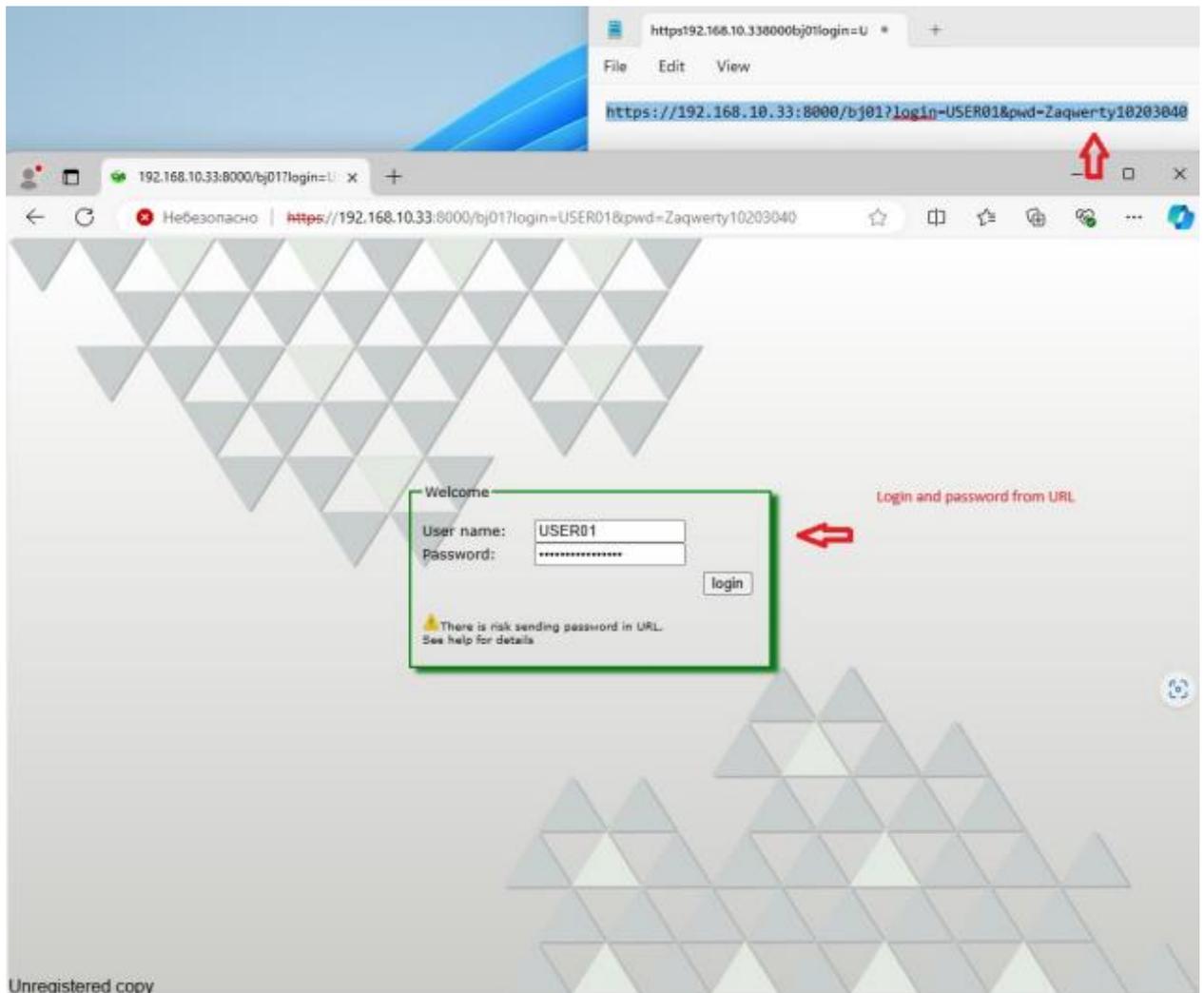
Hint 2: Authorization via a key.

A more secure transfer method is the ssokey key, which the user can

generate using a SSO9 transaction based on the username and password.

The login and password extraction takes place by the system itself and is a more advanced
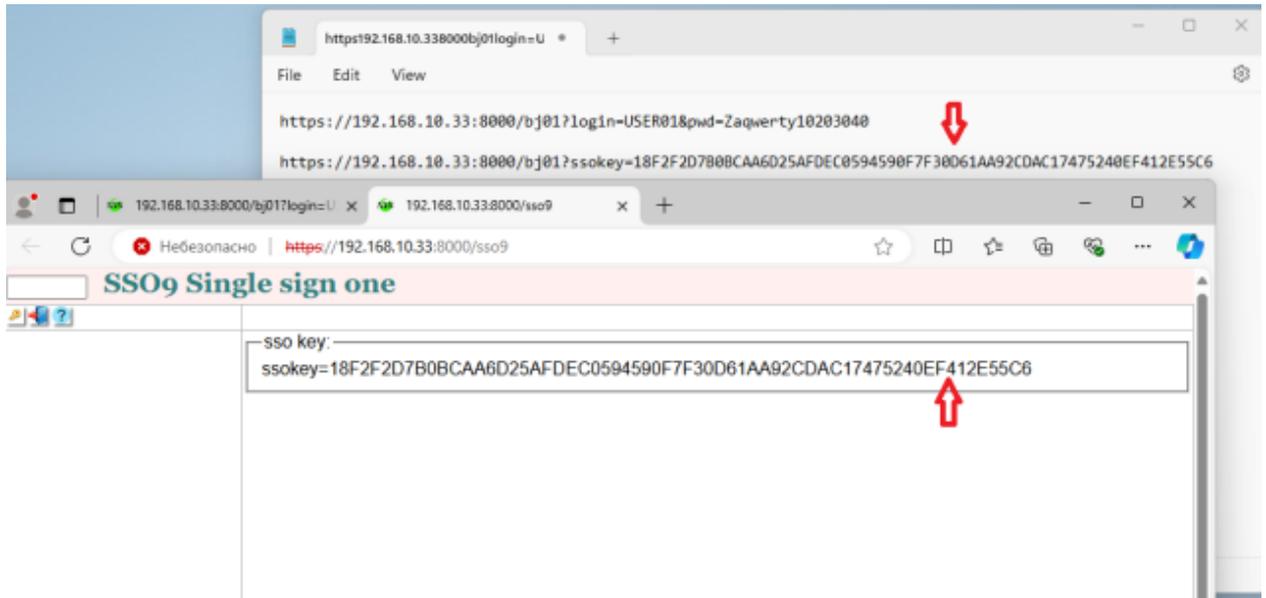
method than the first one
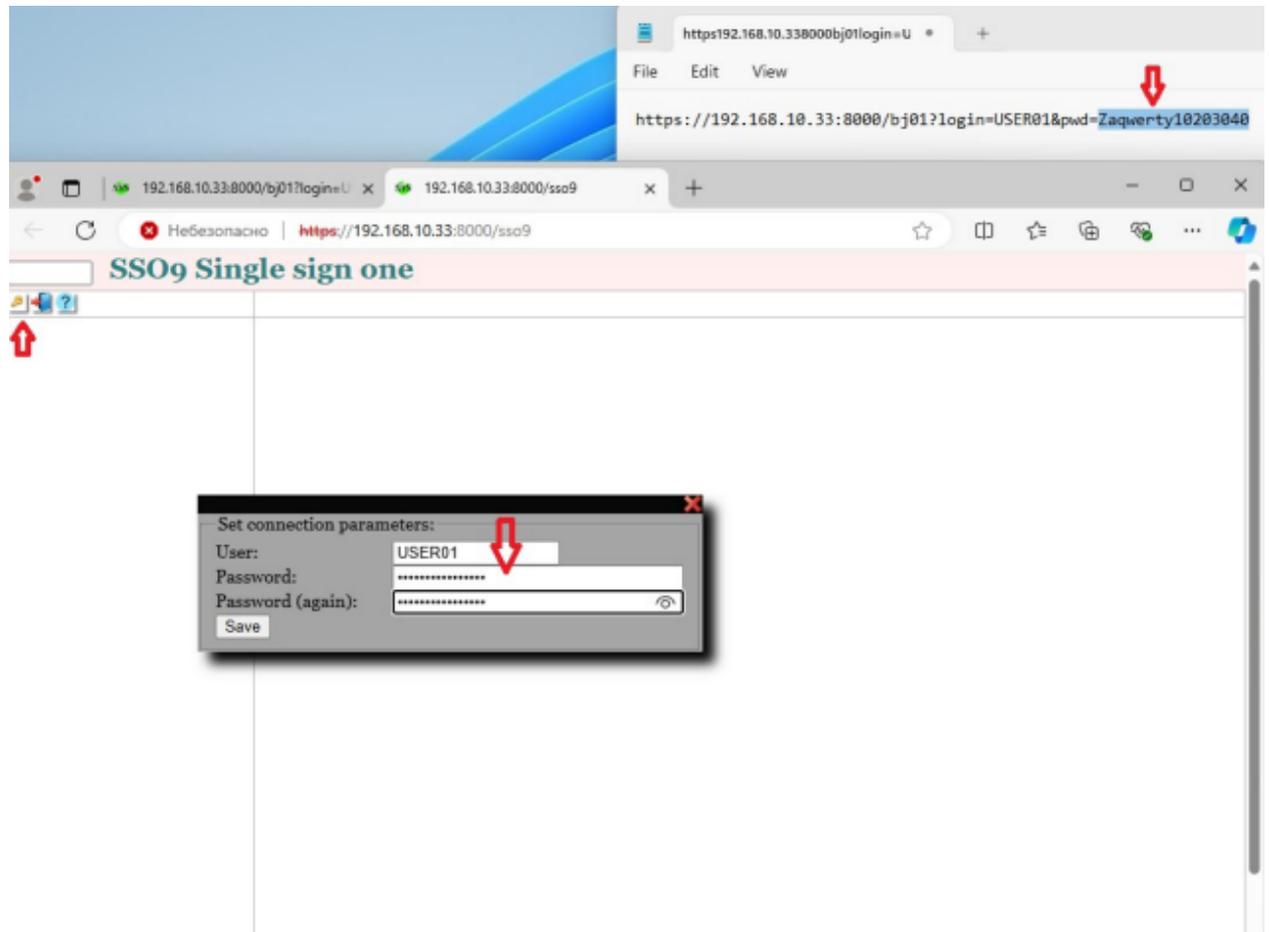
www.nvs-itech.com

As a result, the call string looks like this:

https://192.168.10.33:8000/bj01?
ssokey=18F2F2D7B0BCAA6D25AFDEC0594590F7F30D61AA92CDAC17475240EF412E55C6

But it should be recognized that the safest way is to enter the password in

the invitation window and send it to the server via a POST request.

Which way to use it is up to the user to decide based on the importance of the data in

a particular system.

Hint 3: Using the **Keepass** program.

Along with the main purpose of storing passwords, this Open-source manager

provides a convenient way to access many applications by automatically

launching the browser (in this case) with simultaneous parameter substitution.

Using KeePass allows you to organize your work in the most convenient way, reducing

the risk of errors and reducing the need for manual input
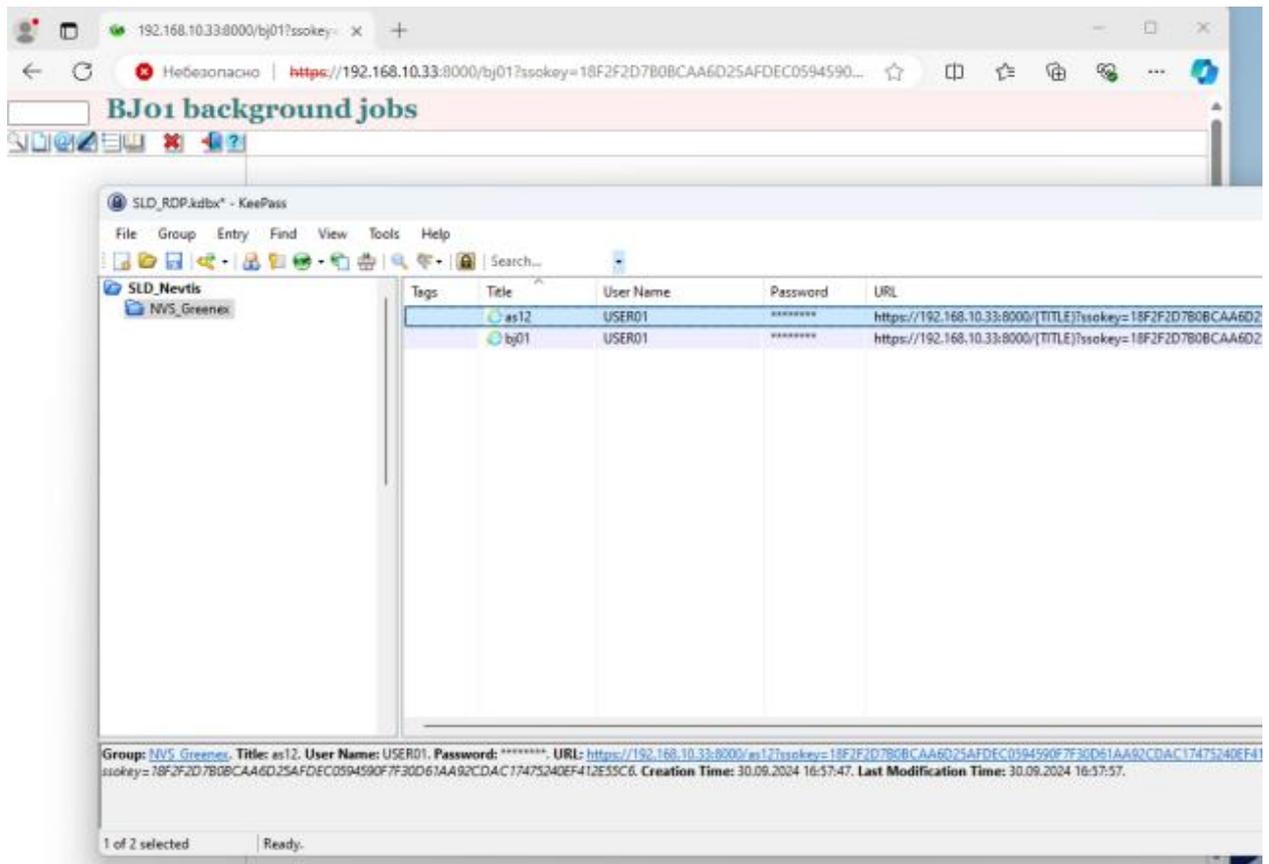
Conclusion

When working with NVS, it is important to understand the basic principles of working with the user

interface, choosing the right balance between safety and convenience of work