Инструкция по установке и настройке
Программного комплекса электронных оперативных журналов «Элжур»

Москва, 2020

Оглавление

Системные требования:

CPU: 2x3.0 GHz CPU (4x3.5 GHz рекомендовано)
ОЗУ: 8 GB RAM (16 GB рекомендовано)
HDD: 100 GB
ОС: Windows Server 2016 Standard или новее (с графическим интерфейсом) / Windows 10 Professional 1903 или новее

Необходимые дистрибутивы:

1) Microsoft SQL Server 2017 (версии Standard на сервере и Express на рабочих станциях) – https://www.microsoft.com/en-US/download/details.aspx?id=55994
2) SQL Server Management Studio 18.5.1 (English) – https://go.microsoft.com/fwlink/?linkid=2132606&clcid=0x409
3) Microsoft .NET Core 2.2.7 Windows Hosting Bundle – https://dotnet.microsoft.com/download/dotnet-core/thank-you/runtime-aspnetcore-2.2.7-windows-hosting-bundle-installer
4) Microsoft .NET Framework 3.5 – https://dotnet.microsoft.com/download/dotnet-framework/net35-sp1
5) RabbitMQ Server 3.8.4 – https://github.com/rabbitmq/rabbitmq-server/releases/download/v3.8.4/rabbitmq-server-3.8.4.exe
6) Erlang/OTP 22.3 – http://erlang.org/download/otp_win64_22.3.exe

Установка ПК:

1) Установка Web Server (IIS 10)

a. Windows Server
   i. Открыть диспетчер серверов (Server Manager)
   ii. Выбрать раздел Добавить роли и компоненты (Add Roles and Features), в появившемся окне нажать Далее (Next)
   iii. Выбрать (Role-based or feature-based installation) и нажать Далее (Next)

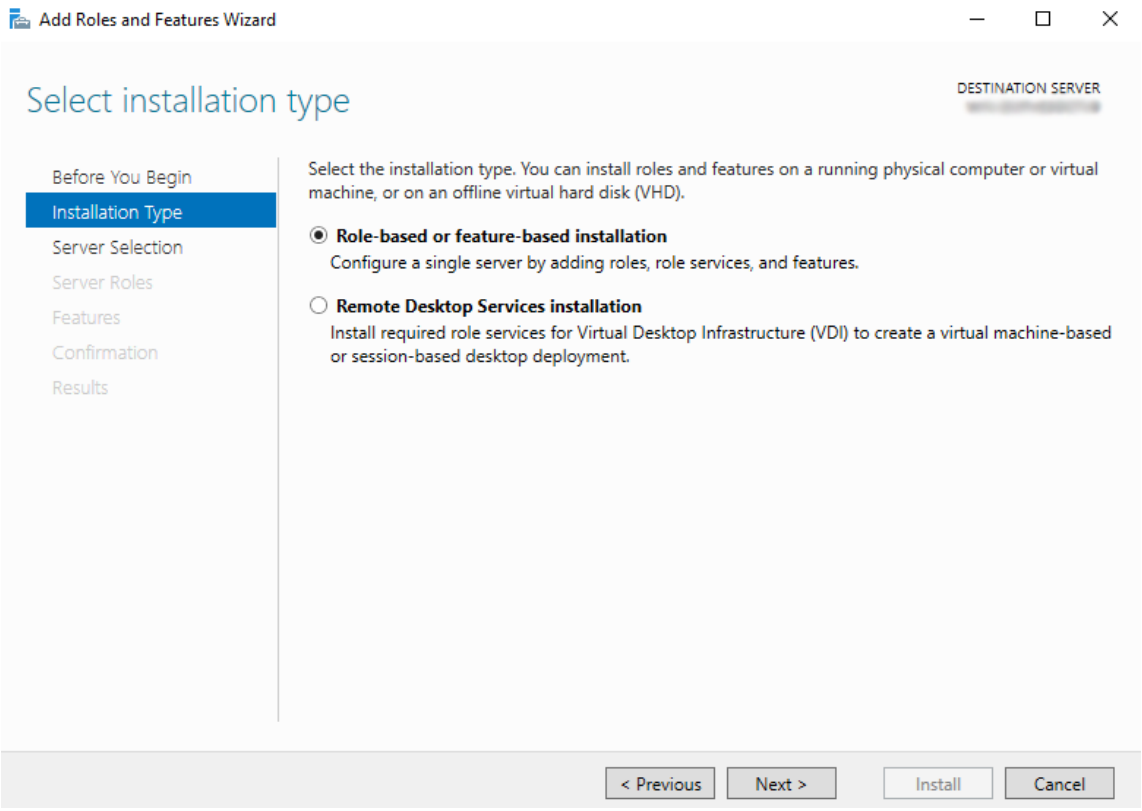


Рисунок 1

iv. Выбрать настраиваемый сервер (Select a server from the server pool) и нажать Далее (Next);

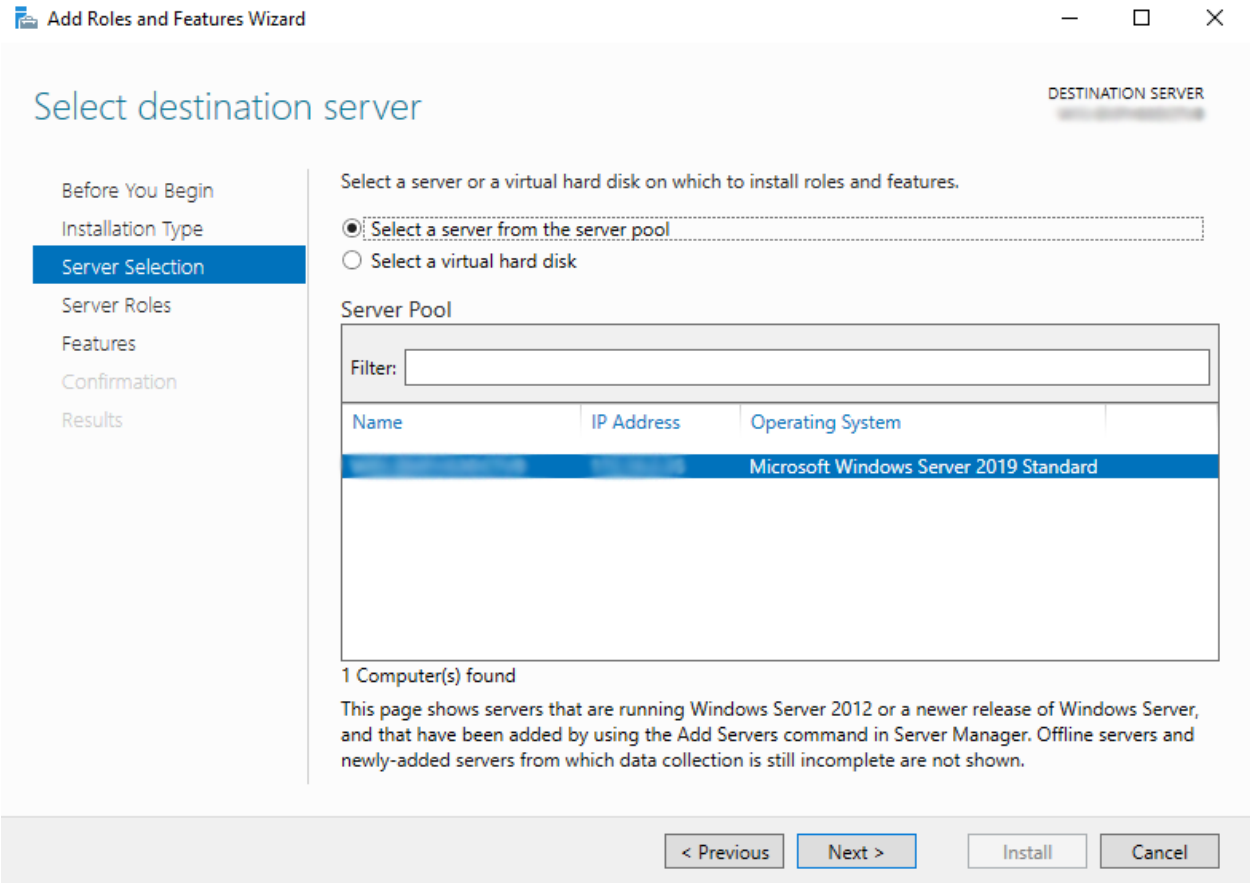


Рисунок 2

v. В окне выбора ролей добавить роль (Web Server (IIS)), согласиться с предложением в появившемся окне и нажать Далее (Next);

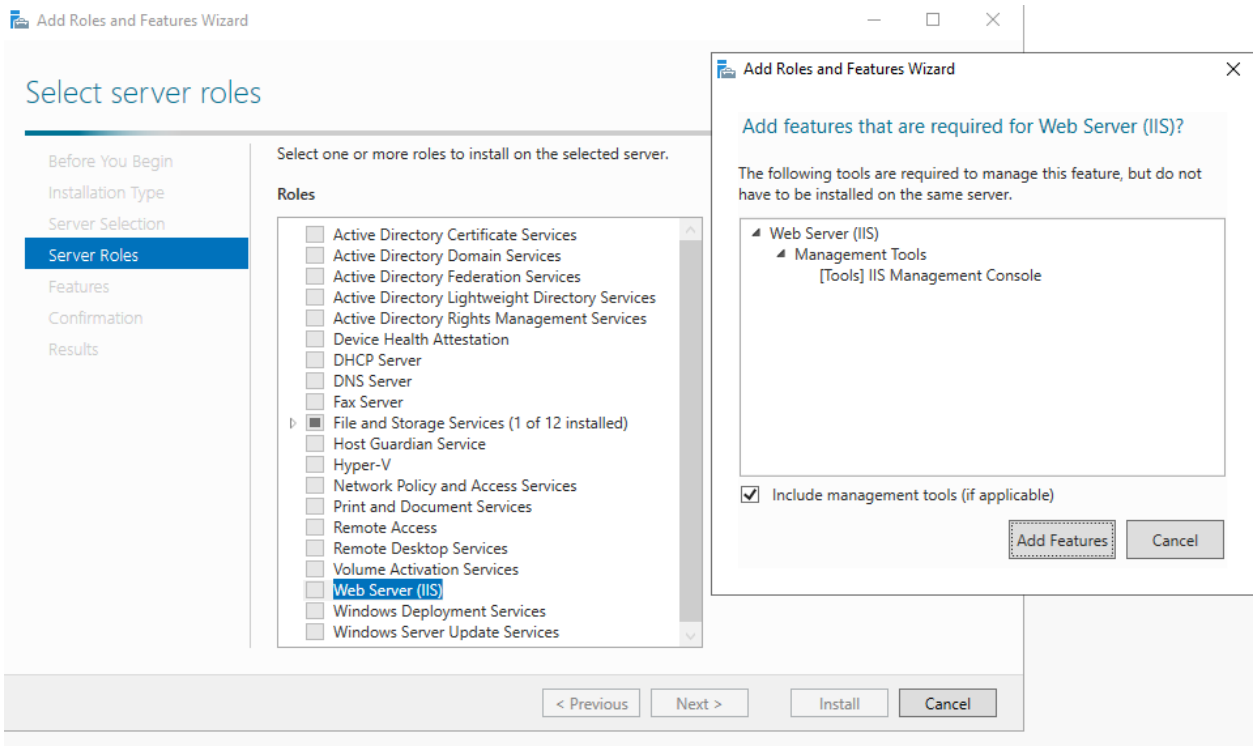


Рисунок 3

vi. В окне выбора компонентов раскрыть список компонентов .NET Framework 3.5 Features и выбрать компоненты .NET Framework 3.5 (includes .NET 2.0 and 3.0) и HTTP Activation, после чего согласиться с предложением в появившемся окне и нажать Далее (Next);

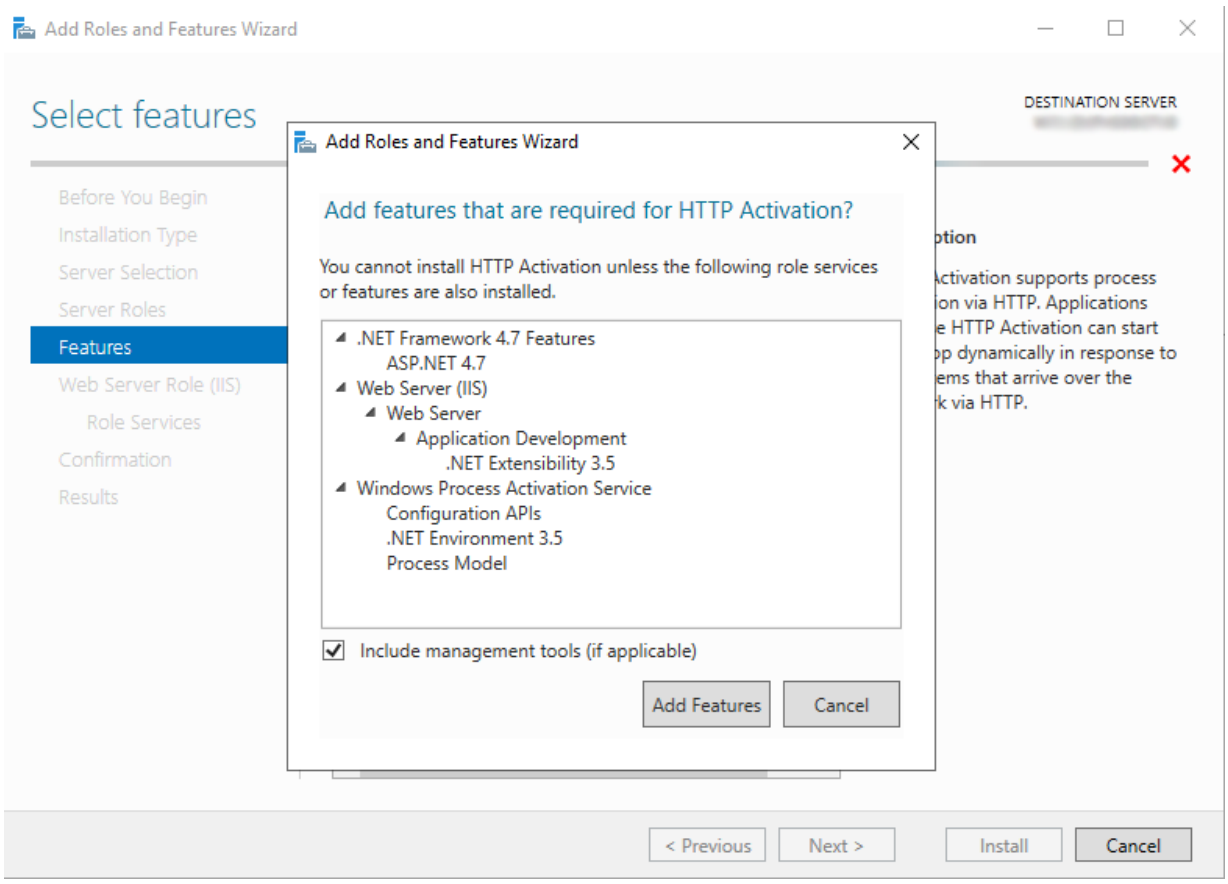


Рисунок 4

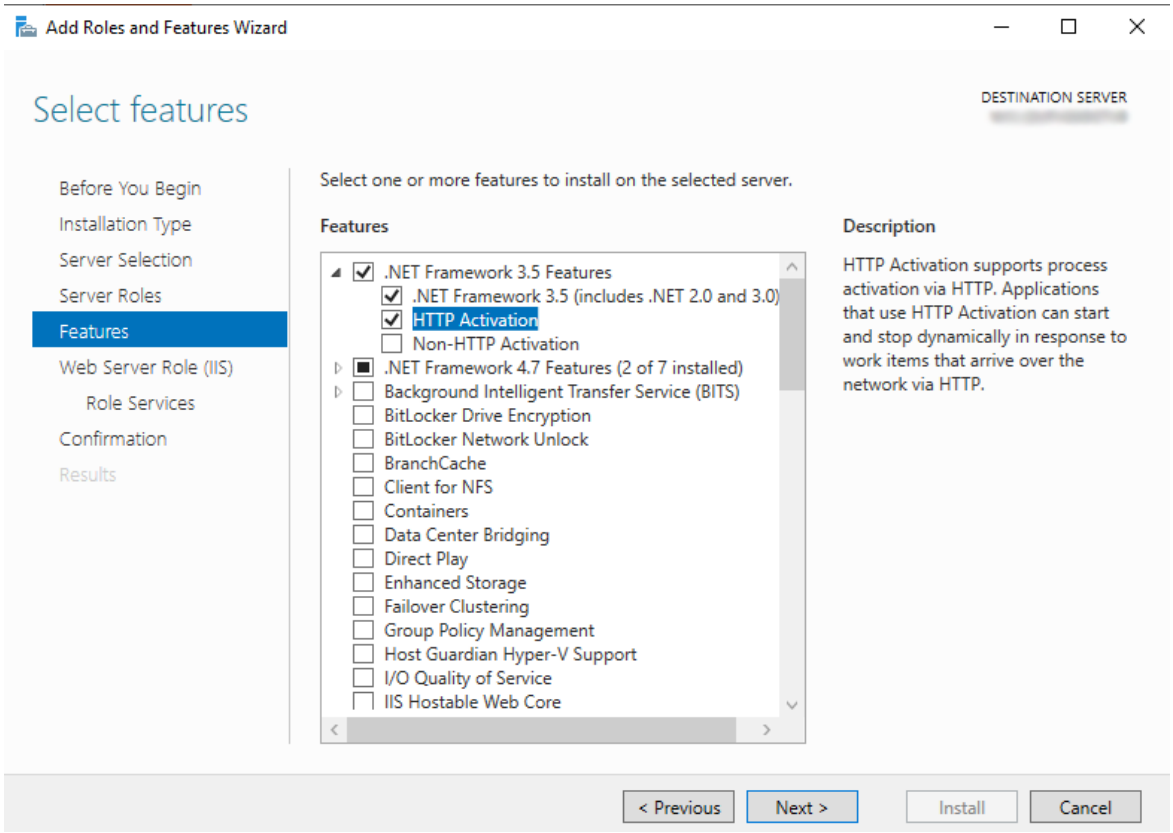


Рисунок 5

vii. Ознакомиться с описанием роли Web Server (IIS) и нажать Далее (Next)

viii. В окне настройки сервисов роли (Role Services) помимо выбранных по умолчанию сервисов необходимо добавить: Common HTTP Features - HTTP Redirection, все сервисы в разделе Security (Request Filtering, Basic Authentication, Centralized SSL Certificate Support, Client Certificate Mapping Authentication, Digest Authentication, IIS Client Certificate Mapping Authentication, IP and Domain Restrictions, URL Authorization и Windows Authentication), Application Development - .NET Extensibility 4.7, ASP.NET 3.5 (включая предложенные зависимости), ASP.NET 4.7, Server Side Includes и WebSocket Protocol, а также Management Tools – IIS Management Scripts and Tools и Management Service, после чего нажать Далее (Next)

ix. В окне подтверждения необходимо сверить приведённый список установленных компонентов с выбранным ранее и нажать Установить (Install)

x. Дождаться окончания работы мастера установки и закрыть его

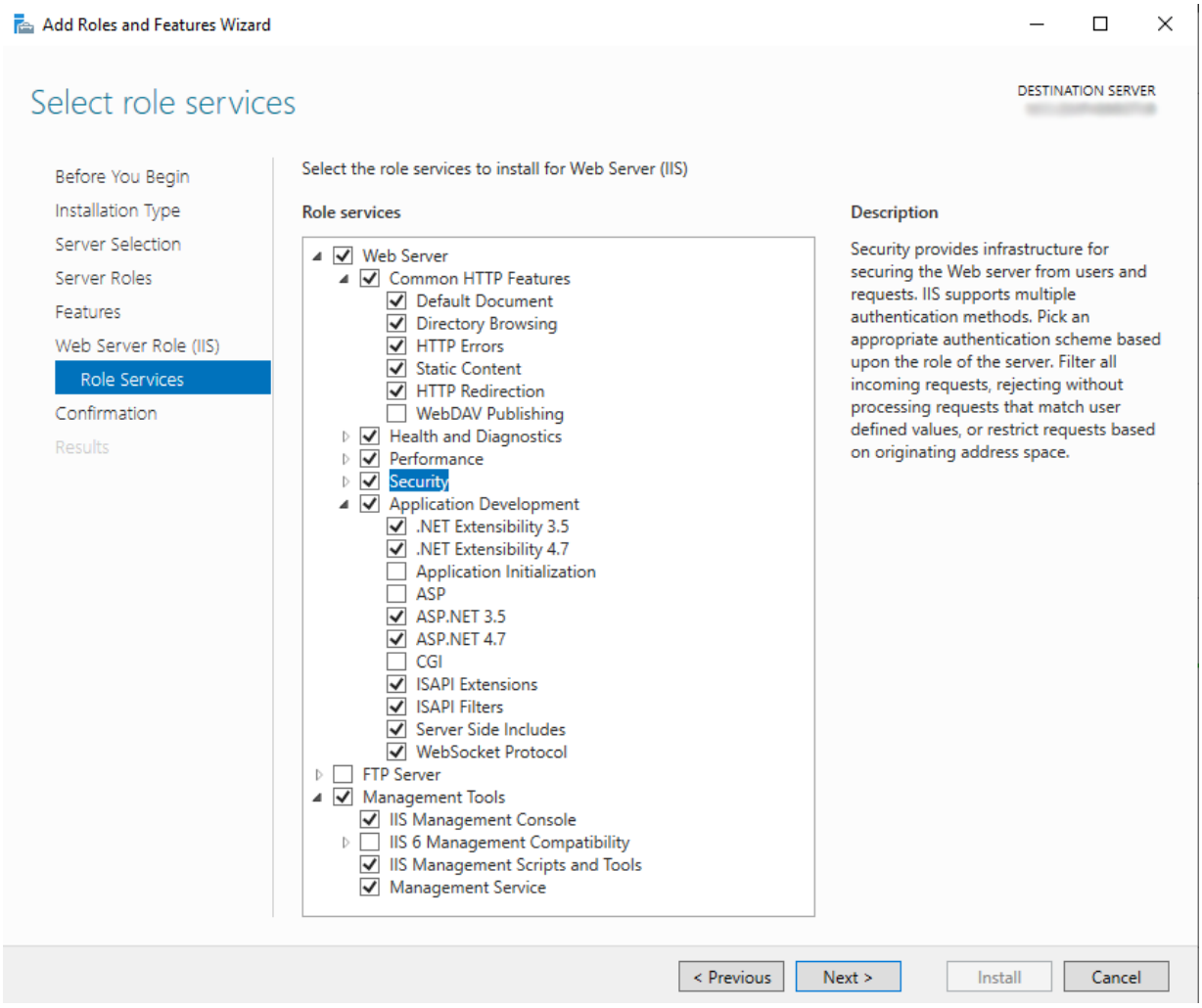


Рисунок 6

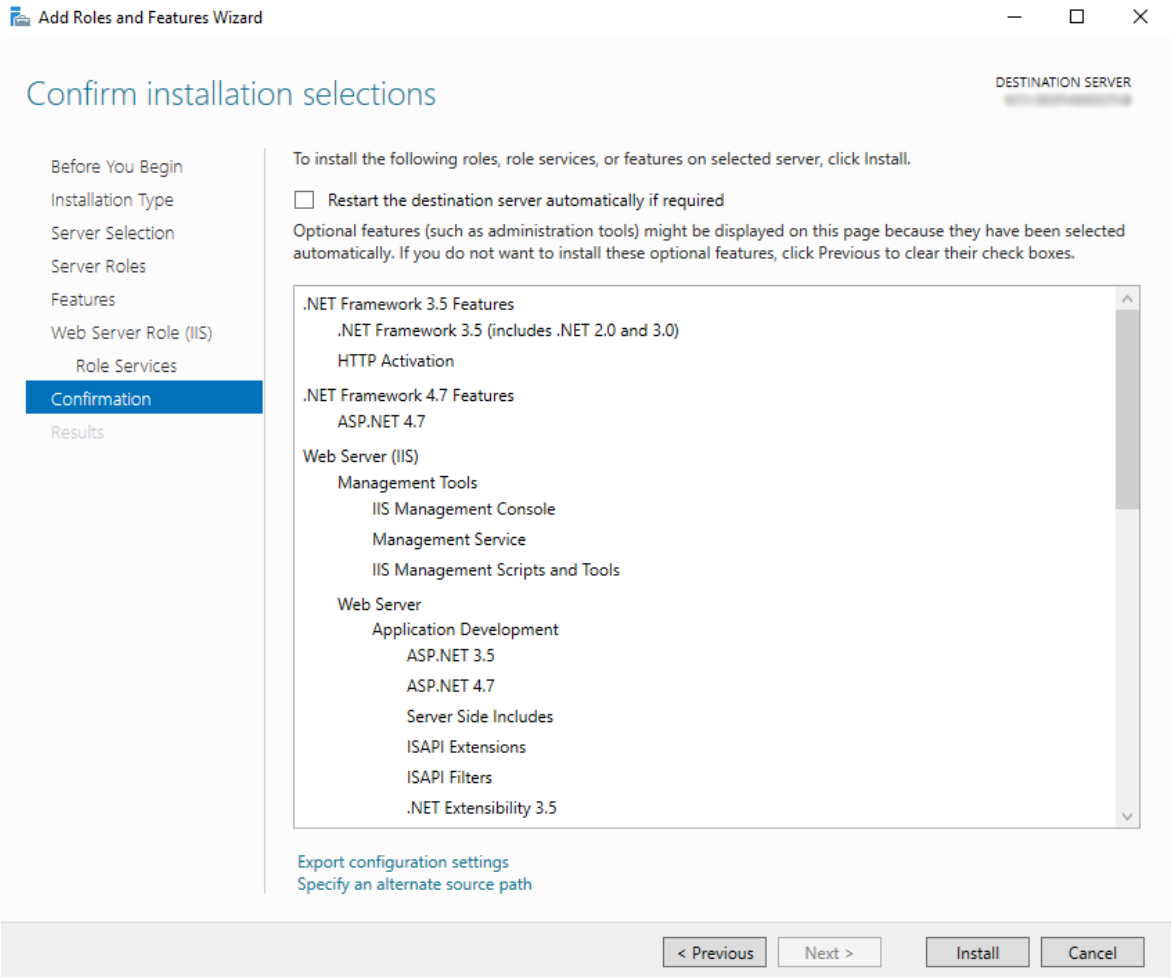


Рисунок 7

b. Windows 10
    i. Открыть Панель управления (Control Panel)
    ii. В разделе Программы и компоненты (Programs and Features) выбрать пункт Включение или отключение компонентов Windows ()
    iii. В появившемся окне выбрать раздел Службы IIS и выбрать компоненты в соответствии с пунктом 1.a.viii и нажать ОК
    iv. Дождаться окончания работы мастера установки и закрыть его

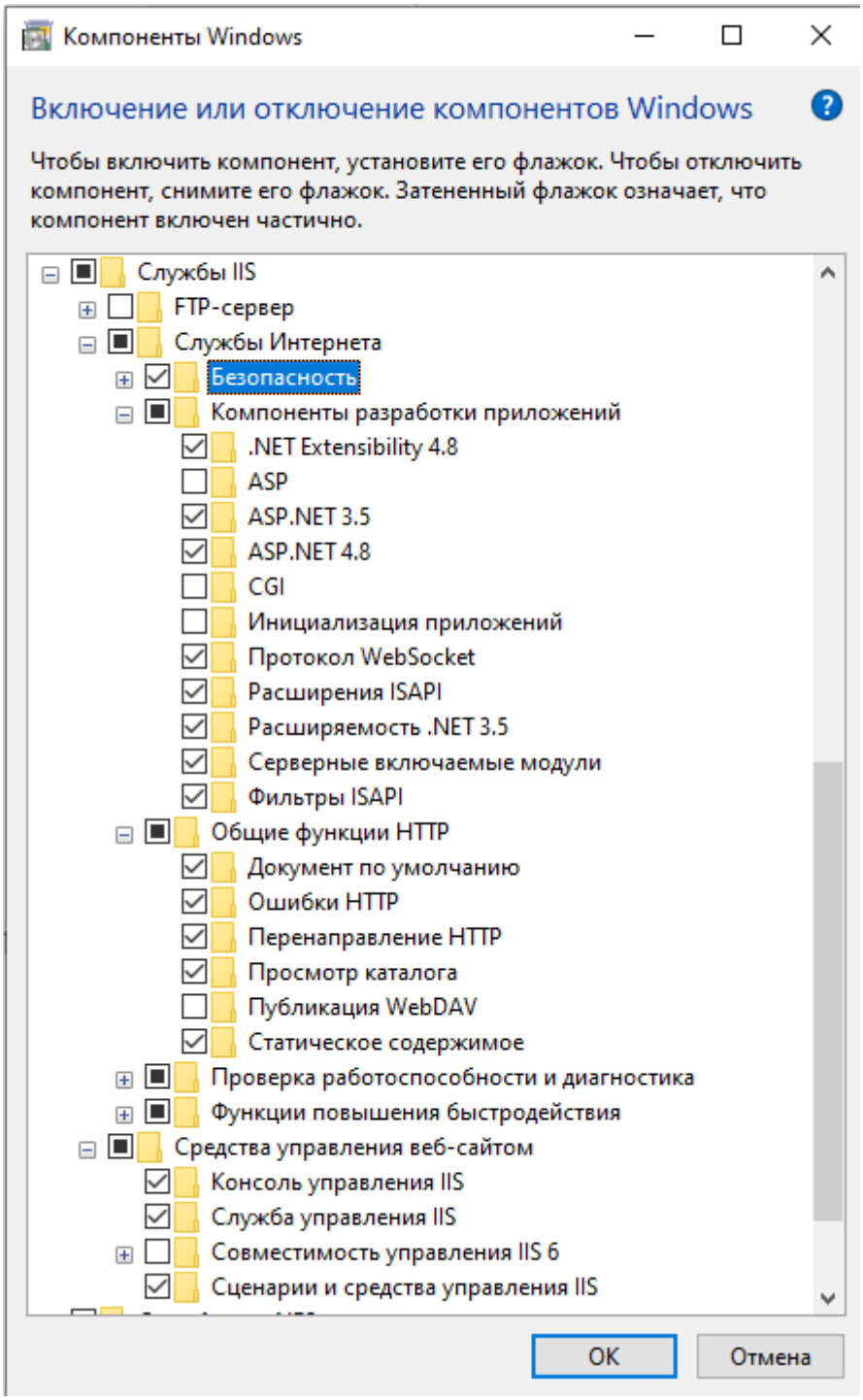


Рисунок 8

2) Установка .NET Core 2.2.7 Windows Hosting Bundle

a. Запустить установочный файл;
b. Ознакомиться с лицензионным соглашением, подтвердить согласие с его условиями, установив галочку I agree to the terms and conditions и нажать Install;
c. Дождаться окончания работы мастера установки и закрыть его.

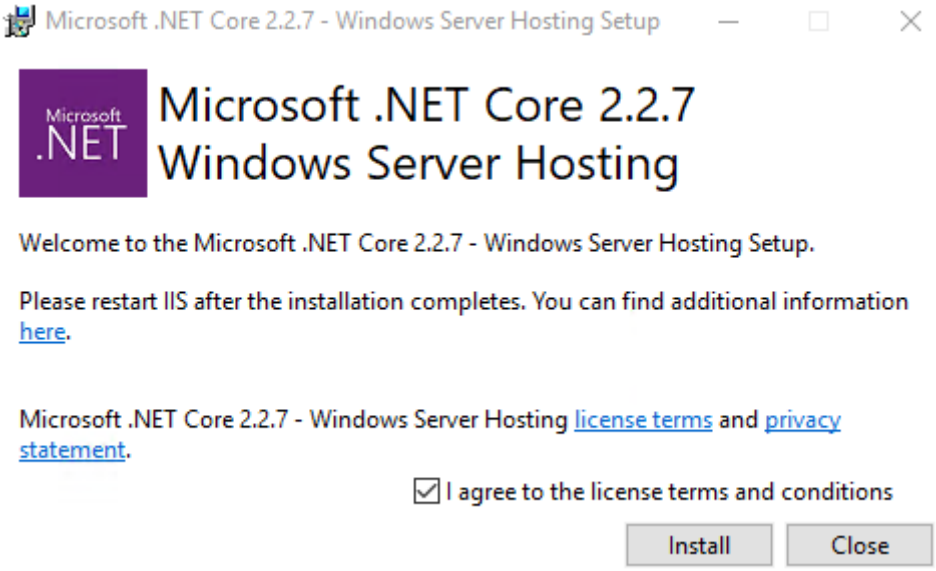


Рисунок 9

3) Установка СУБД Microsoft SQL Server 2017

a. Запустить мастер установки SQL Server 2017;
b. Выбрать в разделе Установка (Installation) первый пункт (New SQL Server stand-alone installation or add features to an existing installation);
c. В окне выбора устанавливаемой редакции SQL Server выбрать необходимый вариант (Specify a free edition – Express на рабочих станциях или ввести ключ продукта от редакции Standard в соответствующее поле), после чего нажать Далее (Next);

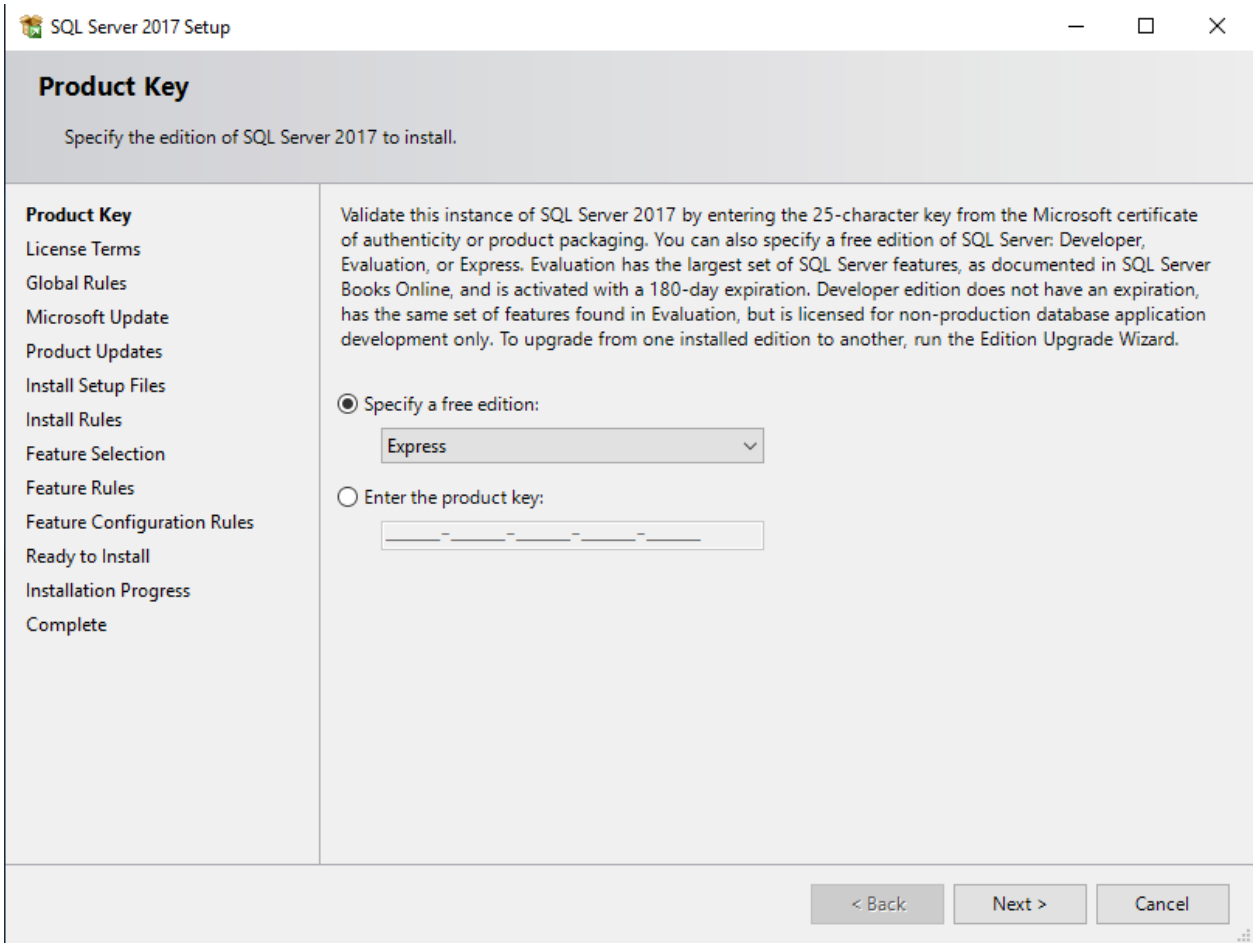


Рисунок 10

d. Ознакомиться с условиями лицензионного соглашения, подтвердить согласие с ними, установив галочку I accept the license terms и нажать Далее (Next);
e. В окне настройки схемы обновления выбрать установку обновлений с использованием Microsoft Update и нажать Далее (Next);
f. В окне проверки наличия проблем, мешающих дальнейшей установке, дождаться окончания проверки и в случае отсутствия ошибок нажать Далее (Next). Если мастером установки были выявлены какие-то проблемы, необходимо нажать на соответствующий статус и выполнить отображаемые рекомендации, после чего запустить установку повторно;

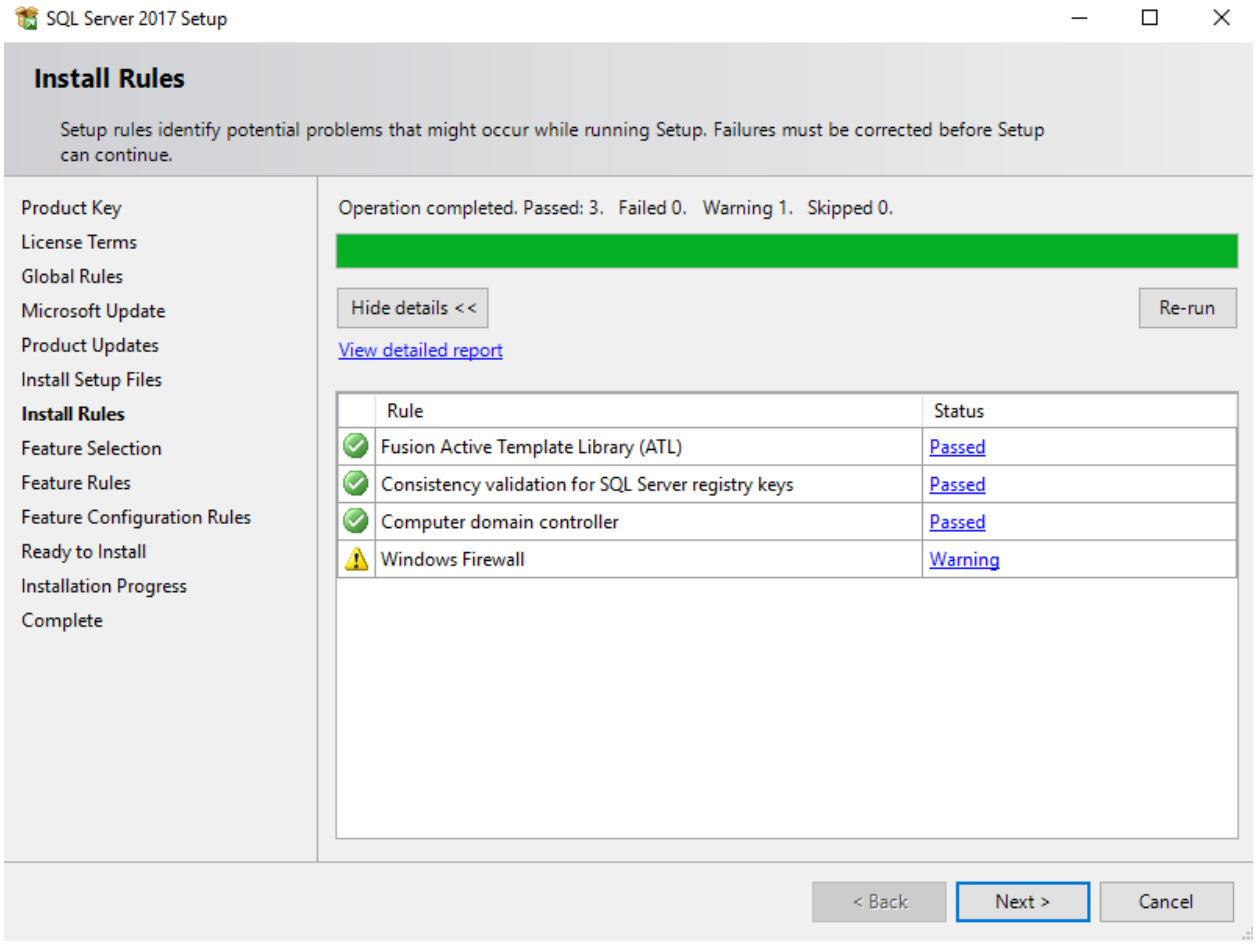


Рисунок 11

g. В окне выбора компонентов нажать Выбрать все (Select All), после чего снять галочки с компонентов Machine Learning Services (In-Database), PolyBase Query Service for External Data для всех редакций, а также с компонента Machine Learning Server (Standalone) в случае установки версии Standard. Остальные параметры оставить по умолчанию и нажать Далее (Next);

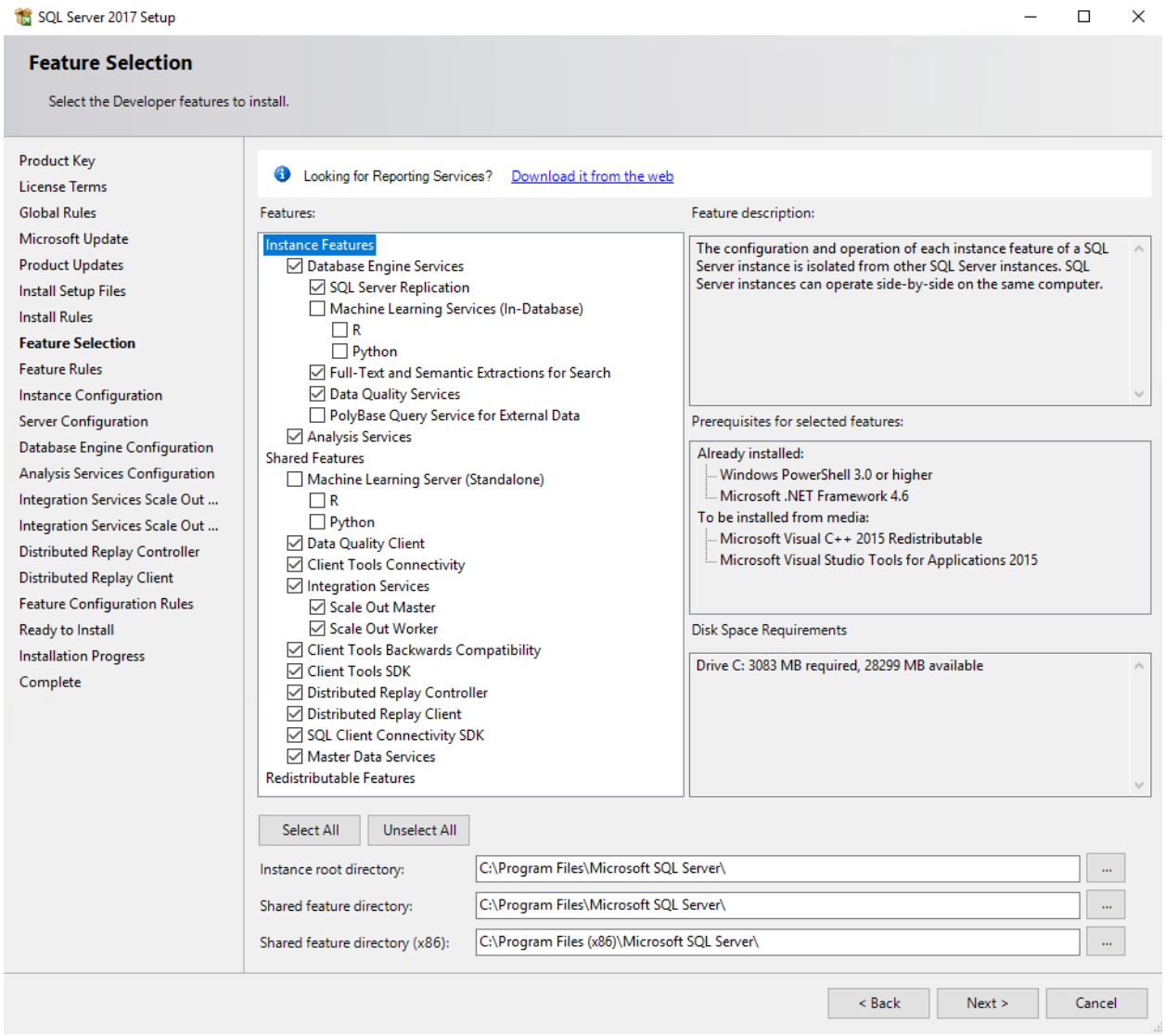


Рисунок 12

h. В следующем окне (Instance Configuration) оставить значения по умолчанию и нажать Далее (Next);
i. В окне настройки сервера (Server Configuration) на вкладке Service Accounts необходимо изменить параметр Startup Type у сервисов SQL Server Agent и SQL Server Browser на Automatic, после чего нажать Далее (Next);
j. В окне Database Engine Configuration во вкладке Server Configuration необходимо выбрать смешанный тип аутентификации и задать пароль для встроенного пользователя sa, после чего обязательно добавить пользователя, под которым идёт установка ПО в список администраторов SQL Server. Для этого необходимо нажать кнопку Add Current User в нижней части окна, дождаться появления пользователя в соответствующем списке и нажать Далее (Next). При установке редакции Express перейти к пункту o данной инструкции;

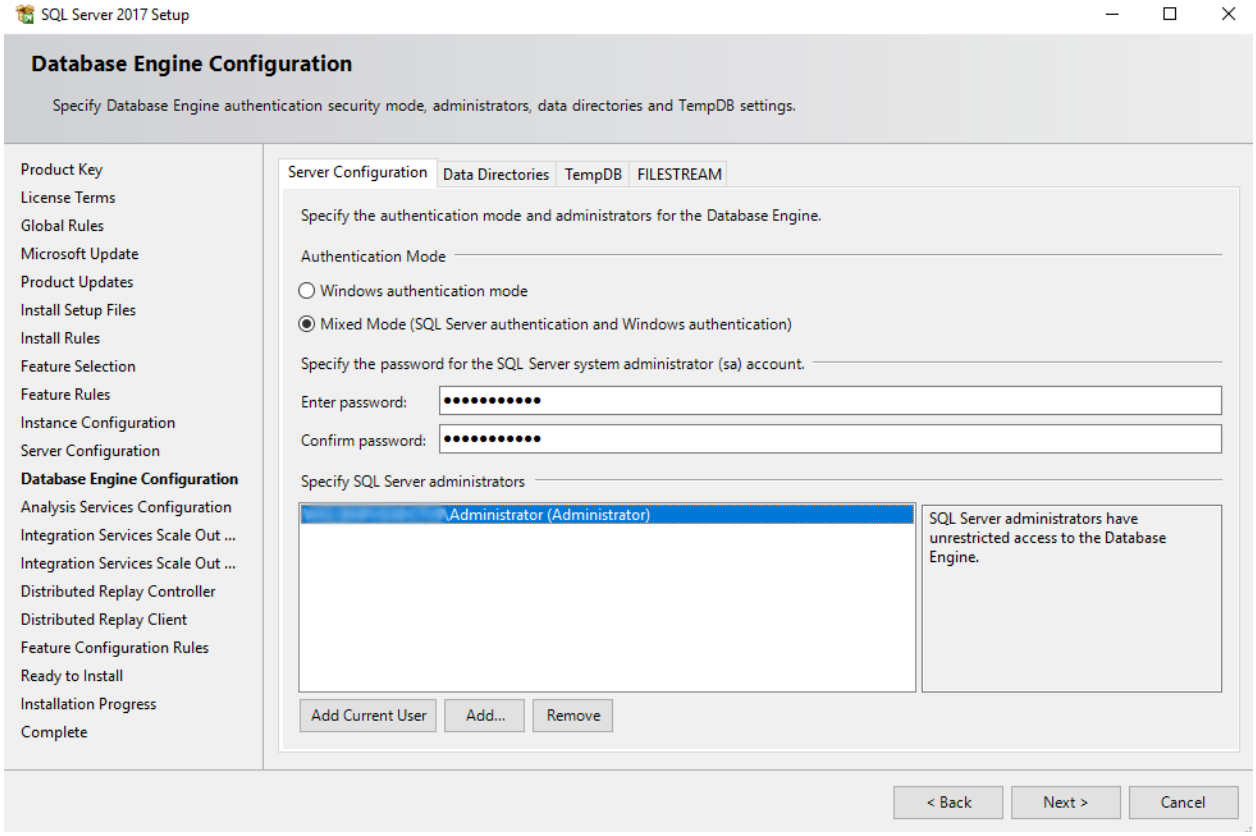


Рисунок 13

k. В окне Analysis Services Configuration также необходимо добавить текущего пользователя в список администраторов, нажав кнопку Add Current User, после чего дождаться появления пользователя в соответствующем списке и нажать Далее (Next);

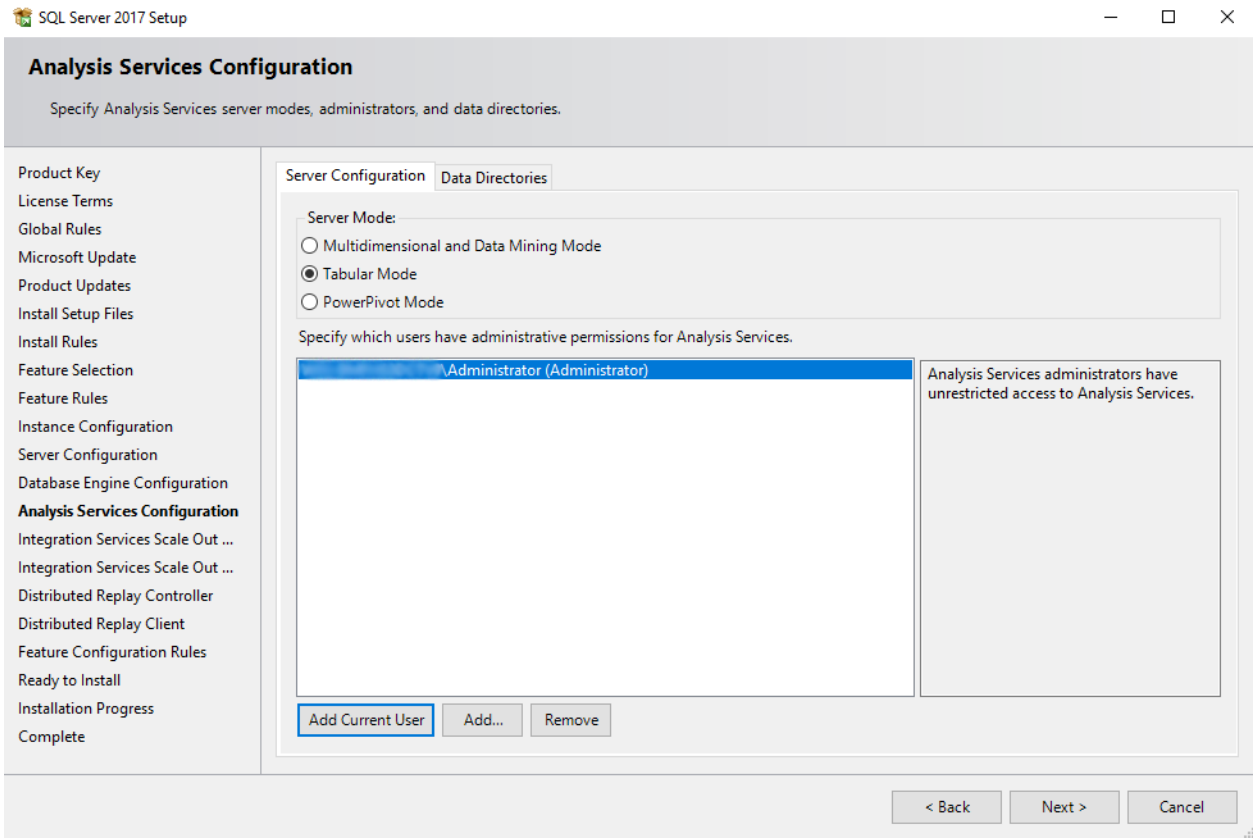


Рисунок 14

l. Следующие два окна (Integration Services Scale Out Configuration – Master Node и Integration Services Scale Out Configuration – Worker Node) оставить без изменений и нажать Далее (Next);
m. В окне Distributed Replay Controller необходимо добавить текущего пользователя в список администраторов, нажав кнопку Add Current User, после чего дождаться появления пользователя в соответствующем списке и нажать Далее (Next);
n. В окне Distributed Replay Client ввести в поле Controller Name значение OptiClient и нажать Далее (Next);

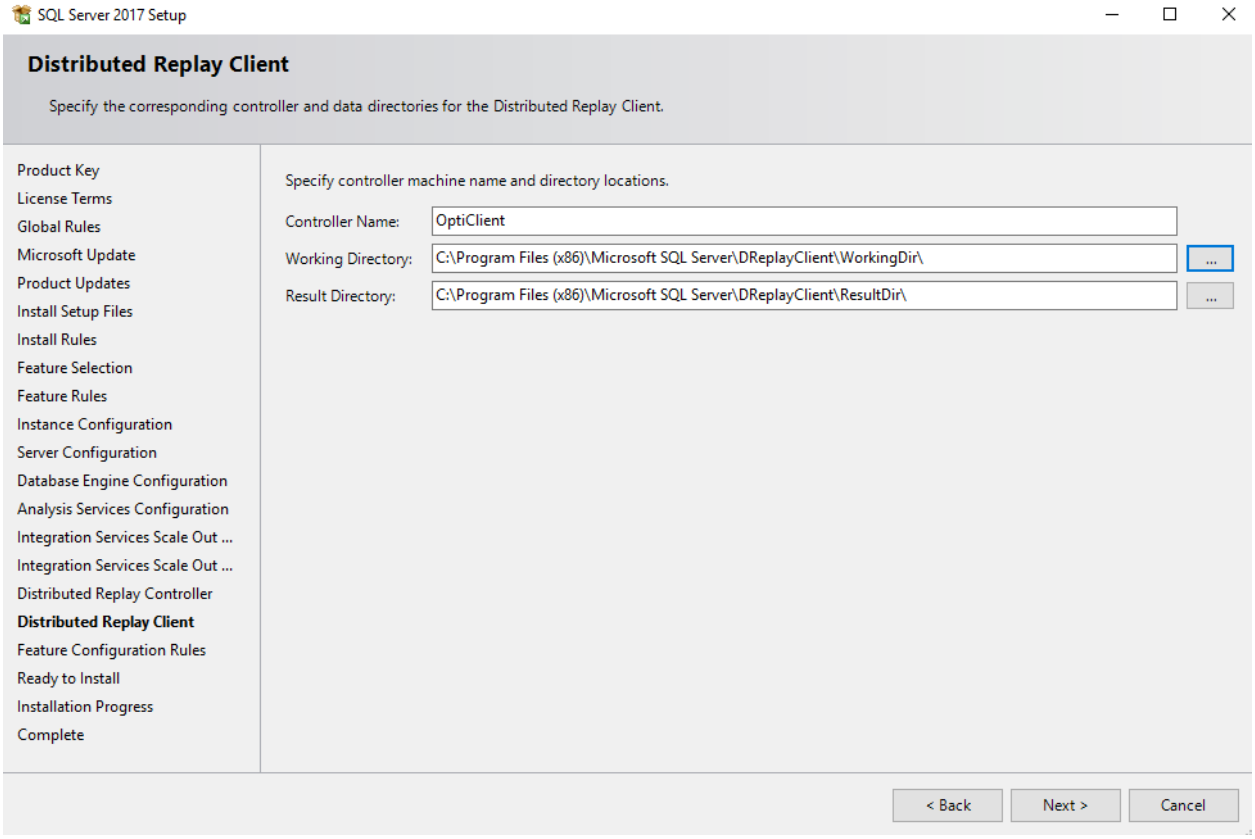


Рисунок 15

o. В появившемся окне подтверждения необходимо сверить приведённый список установленных компонентов с выбранным ранее и нажать Установить (Install);
p. Дождаться окончания работы мастера установки и закрыть его, а также открытое ранее окно SQL Server Installation Center;

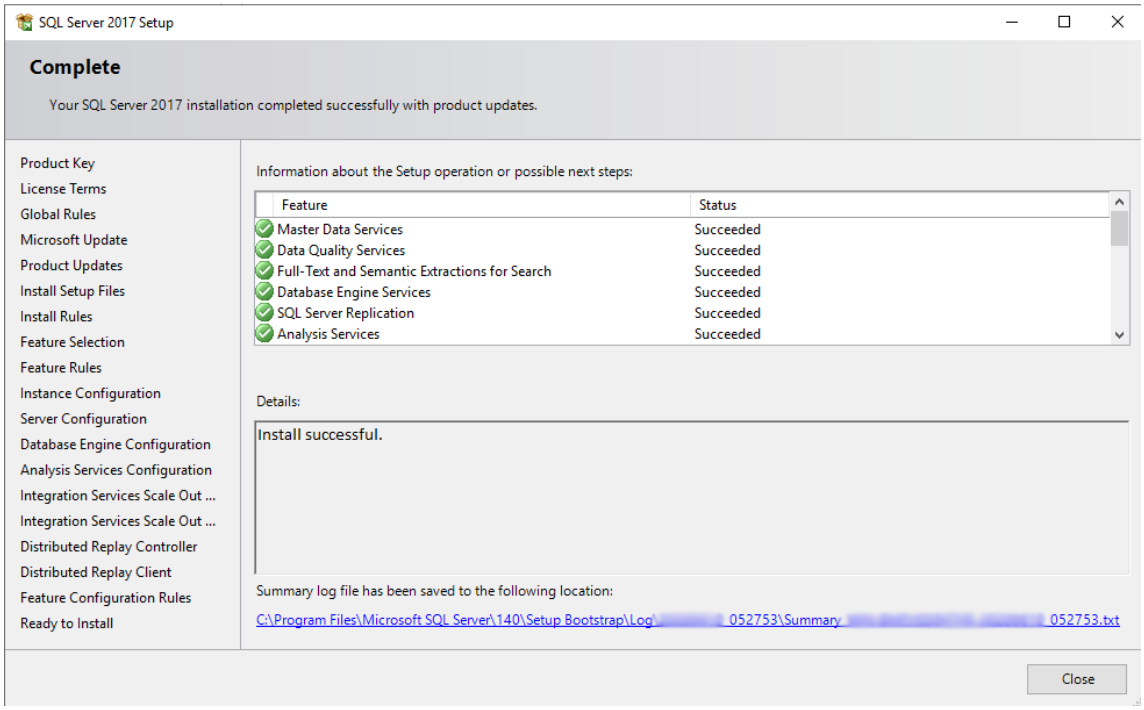


Рисунок 16

q. Запустить установочный файл SQL Server Management Studio;
r. Ознакомиться с лицензионным соглашением и нажать кнопку Install;

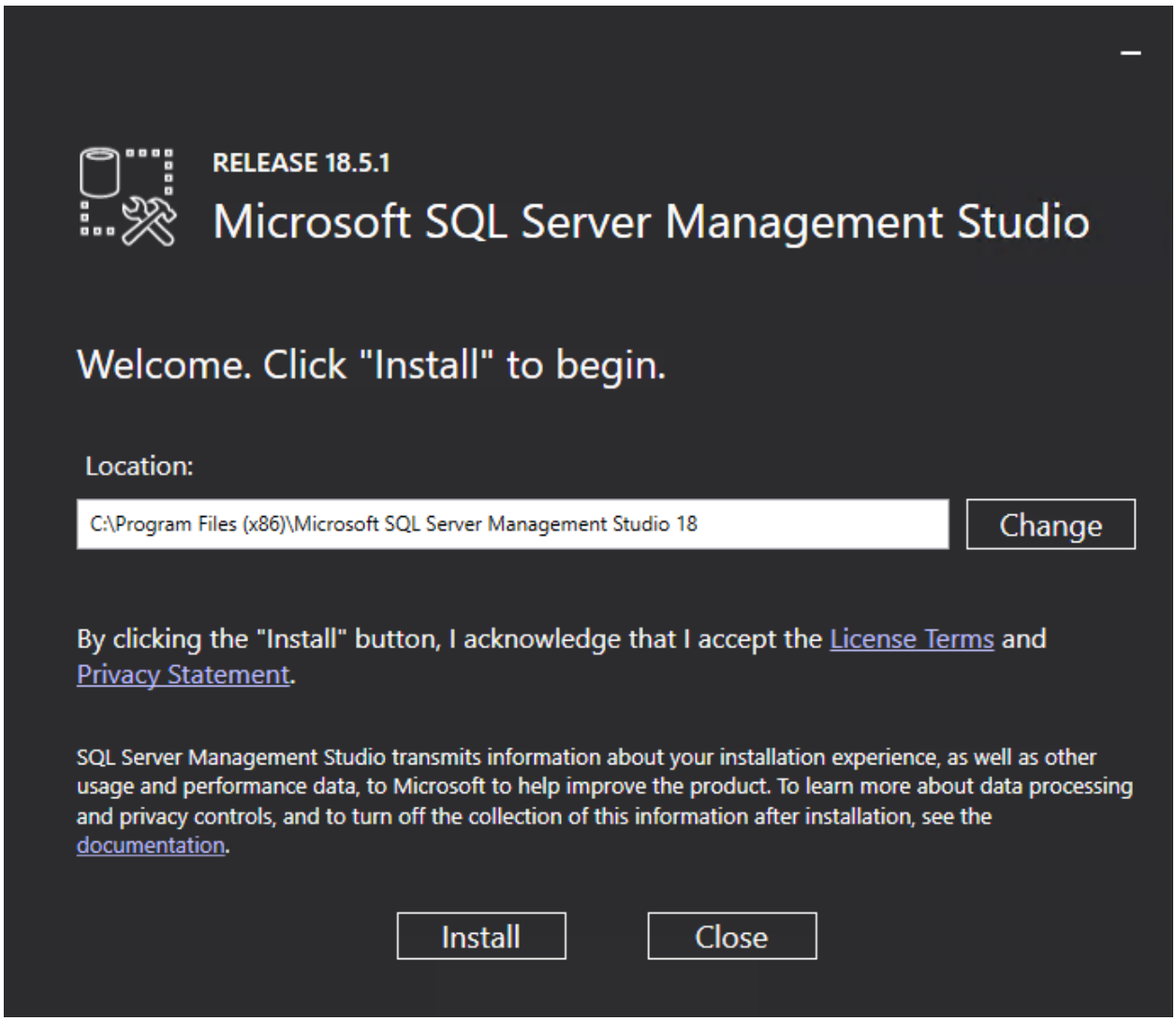


Рисунок 17

s. Дождаться окончания установки и согласиться на перезагрузку сервера, нажав кнопку Restart;

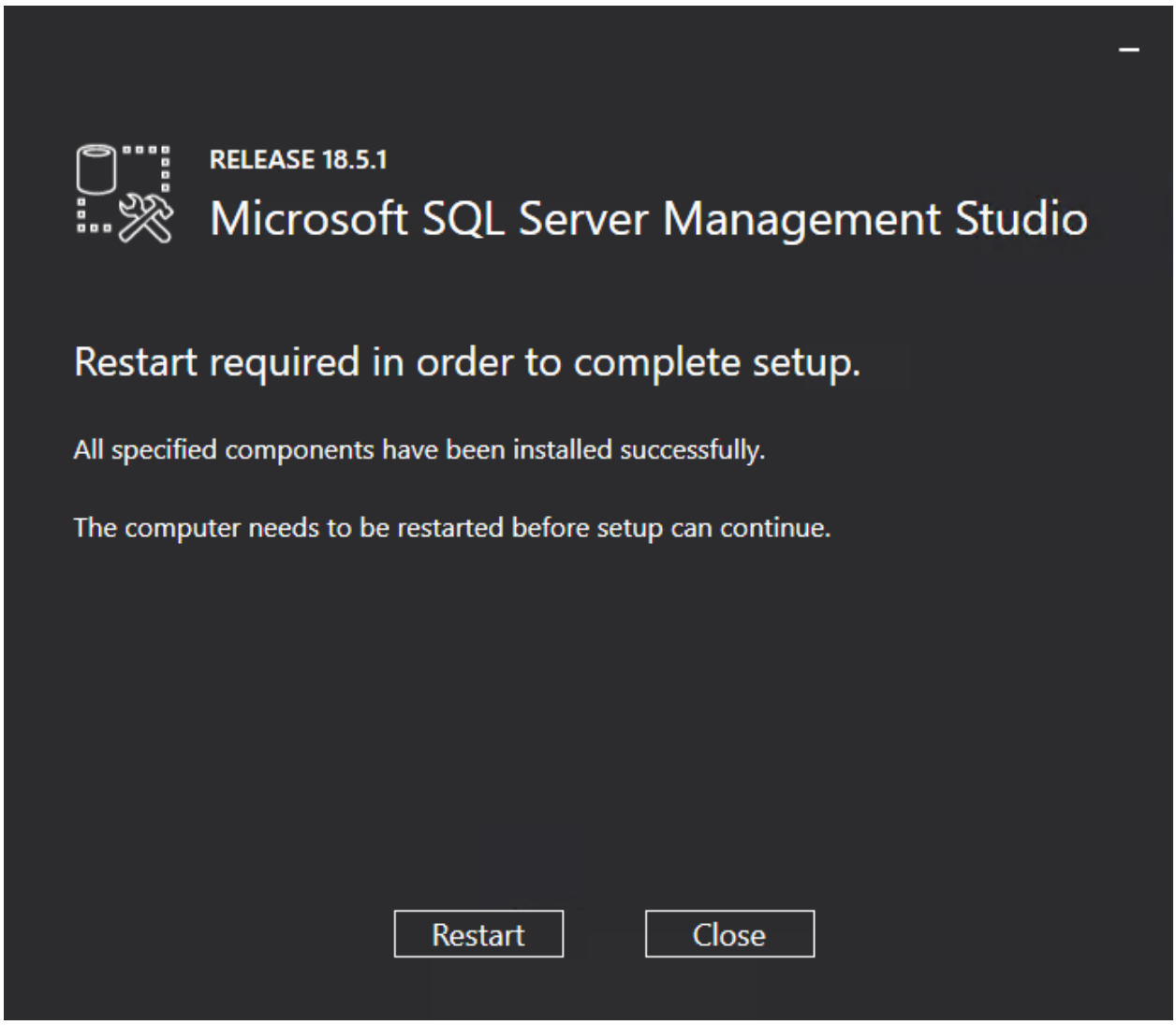


Рисунок 18

4) Установка Erlang/OTP 22.3

a. Запустить установочный файл;

b. В открывшемся окне выбрать все компоненты и нажать Далее (Next);

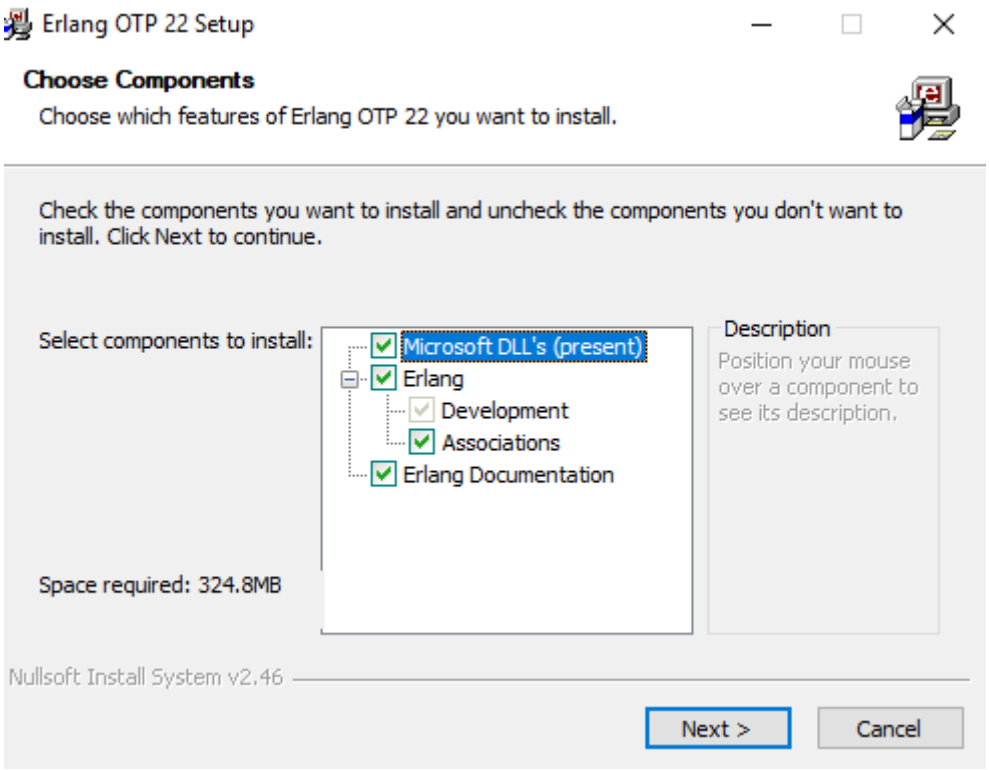


Рисунок 19

c. В следующем окне оставить значения по умолчанию и нажать Далее (Next), затем Установить (Install);
d. В появившемся окне установки Microsoft Visual C++ 2013 ознакомиться с лицензионным соглашением, подтвердить согласие с его условиями, установив галочку I agree to the terms and conditions и нажать Install, после чего дождаться окончания установки и закрыть это окно нажатием кнопки Закрыть (Close);
e. Дождаться окончания установки Erlang/OTP и закрыть мастер установки нажатием кнопки Close;

5) Установка RabbitMQ Server 3.8.4

a. Запустить установочный файл;
b. В открывшемся окне оставить значения по умолчанию и нажать Далее (Next), затем Установить (Install);
c. Дождаться окончания установки и закрыть мастер установки нажатием кнопки Next, затем Finish;
d. После установки необходимо до перезагрузки сервера заменить файл конфигурации advanced.config в папке %APPDATA%\RabbitMQ, содержимое которого описано в разделе «Замена конфигурационных файлов» данной Инструкции;

Настройка компонентов

1) Настройка Windows Defender Firewall

a. Открыть панель настройки встроенного брандмауэра, выбрав Пуск-Средства администрирования Windows-Монитор брандмауэра Защитника Windows в режиме повышенной безопасности (Start-Windows Administrative Tools-Windows Defender Firewall with Advanced Security);

b. Выбрать раздел Правила для входящих подключений (Inbound Rules);

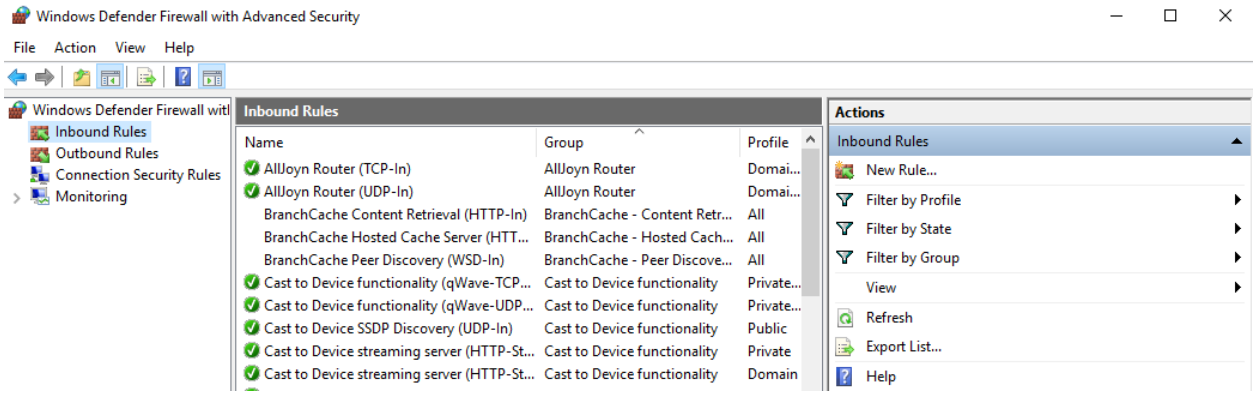


Рисунок 20

c. Выбрать пункт Создать правило… (New Rule…) в панели Действия (Actions);
d. В появившемся окне выбрать тип Для порта (Port) и нажать Далее (Next);

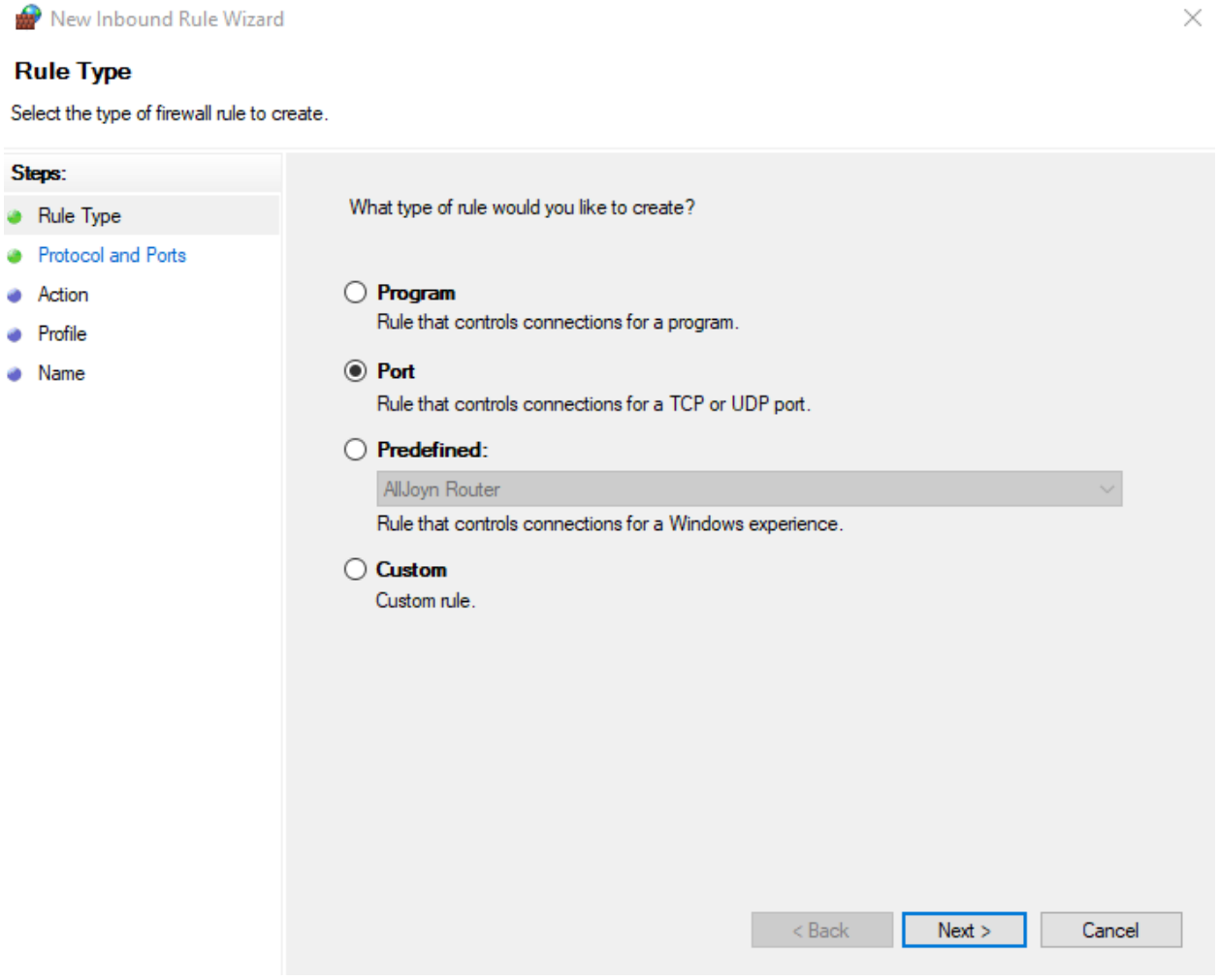


Рисунок 21

e. В окне настройки используемых протоколов и портов необходимо указать тип портов TCP и используемые порты (по умолчанию это 80, 443, 3000, 4000, 5000, 6001), после чего нажать Далее (Next);

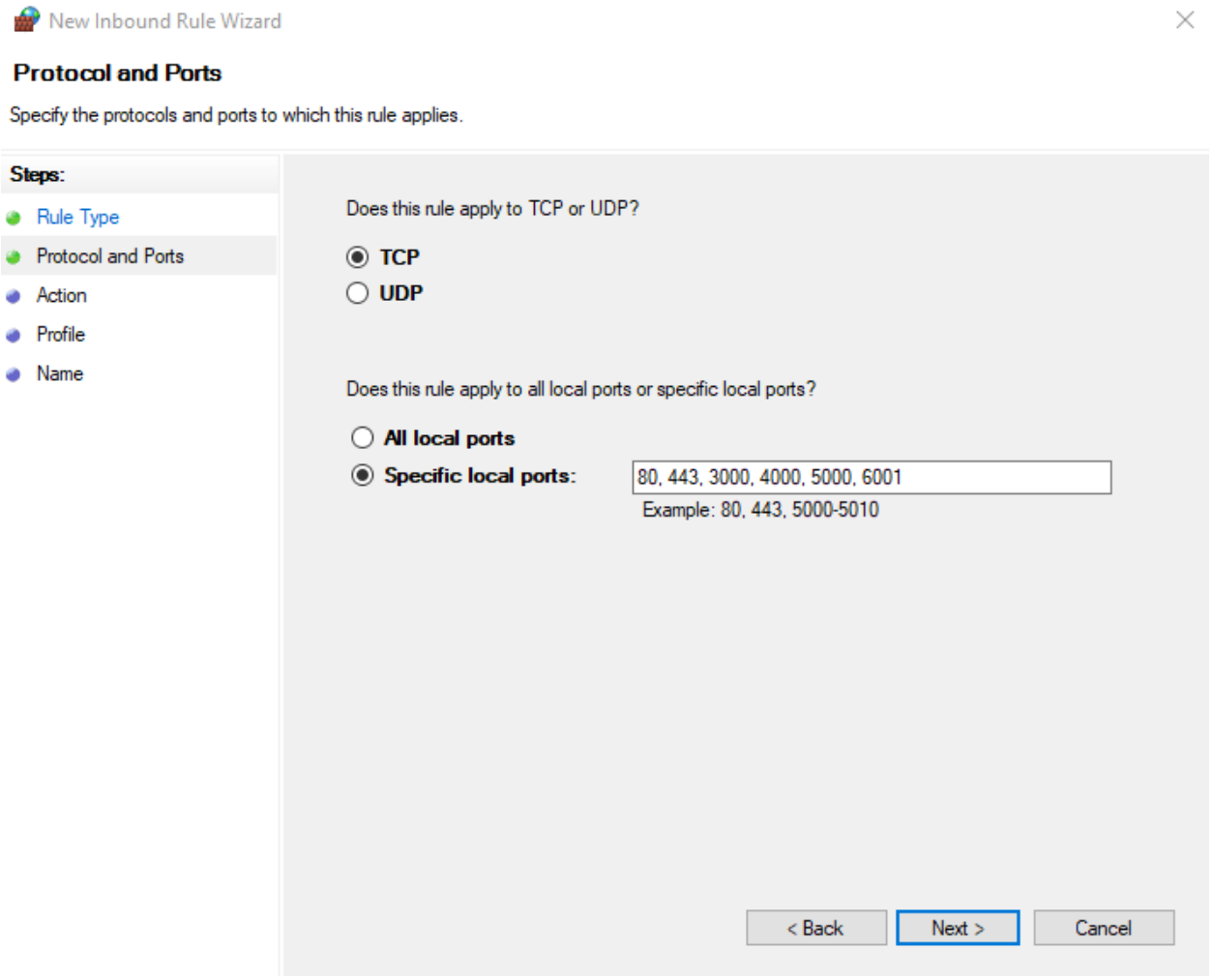


Рисунок 22

f. В следующем окне убедиться, что выбрано действие Разрешить подключение (Allow the connection) и нажать Далее (Next);

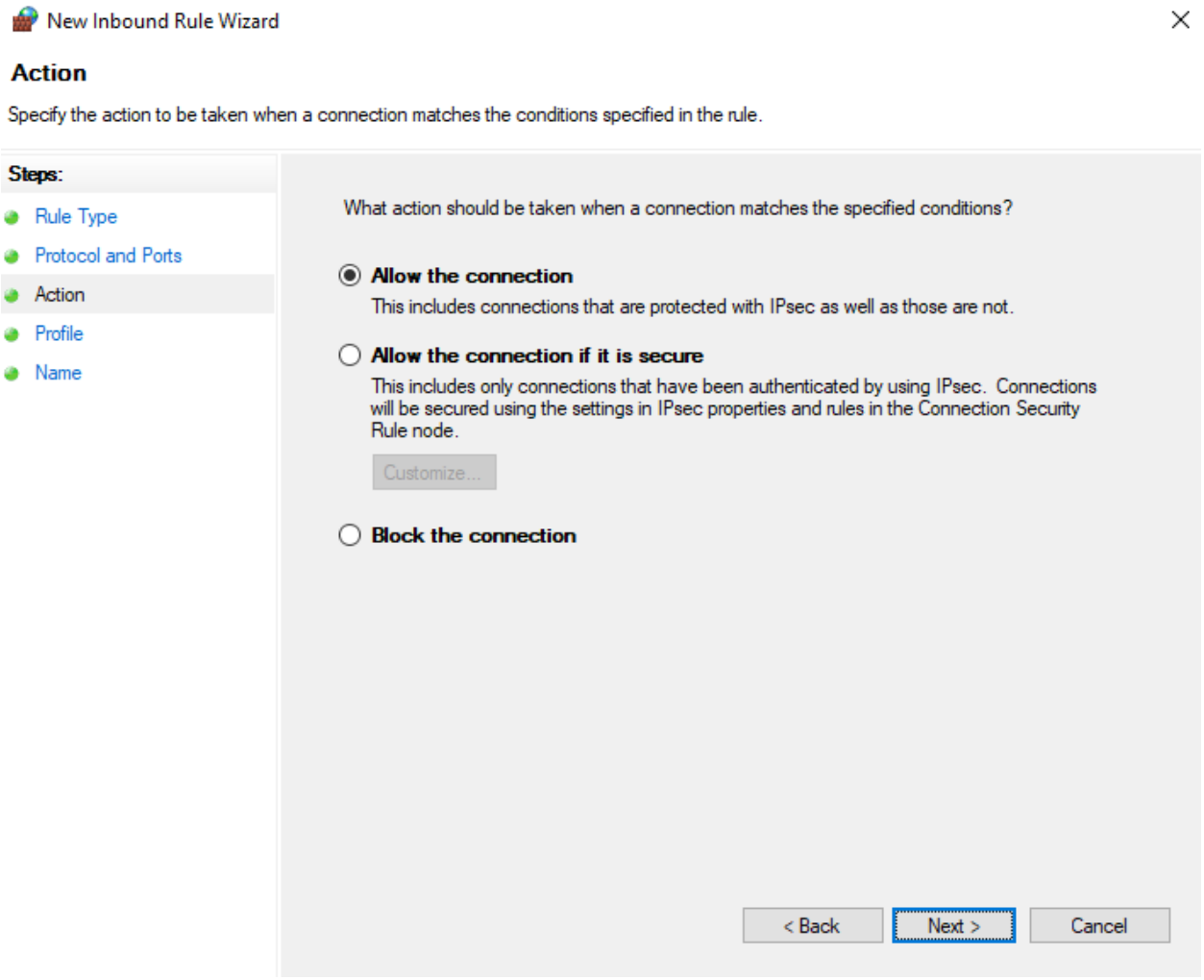


Рисунок 23

g. В окне Профиль (Profile) убедиться, что выбраны все три доступные варианта - Доменный (Domain), Частный (Private) и Публичный (Public), после чего нажать Далее (Next);

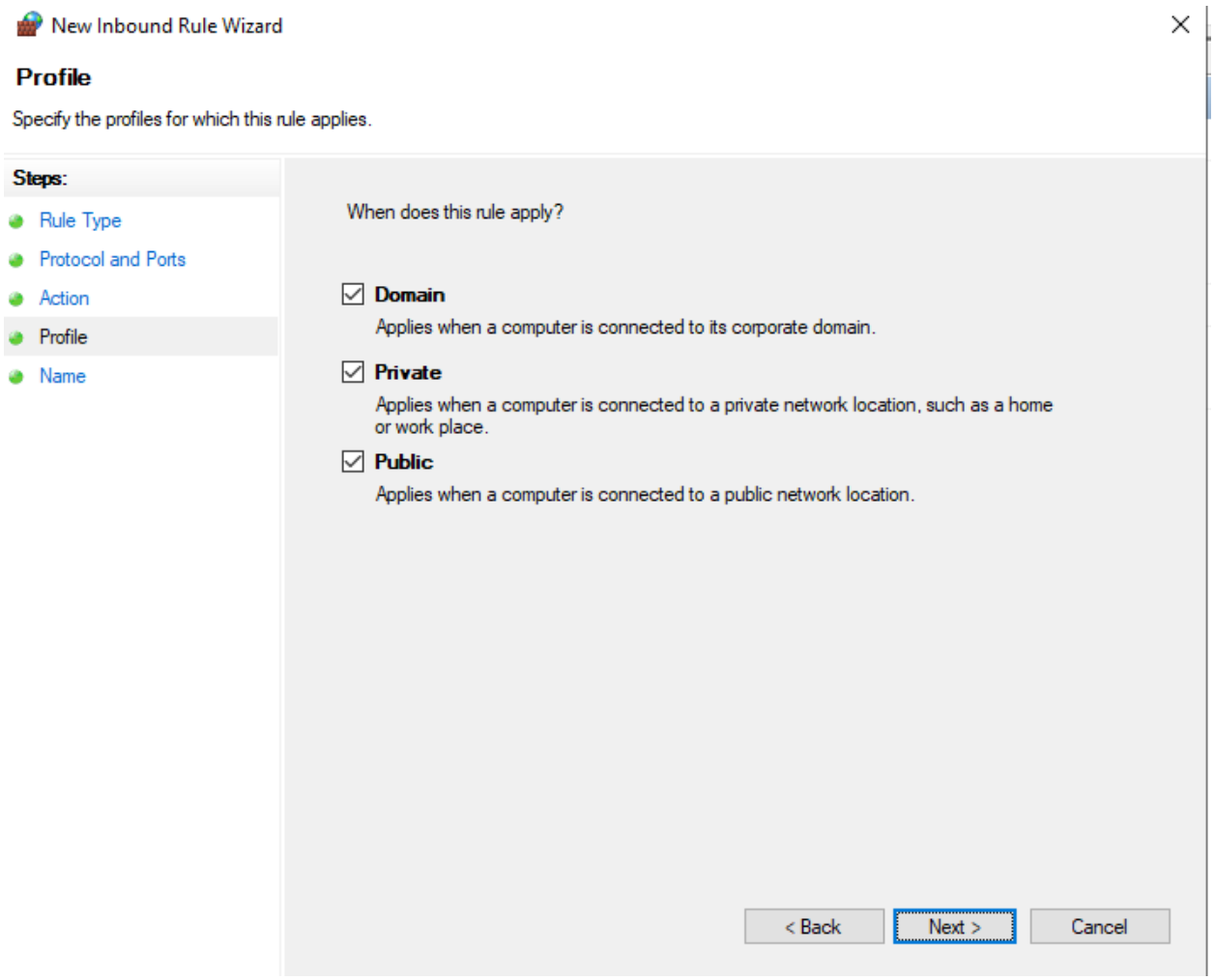


Рисунок 24

h. В завершающем окне Имя (Name) в соответствующем поле необходимо указать название правила – Элжур и нажать Готово (Finish);

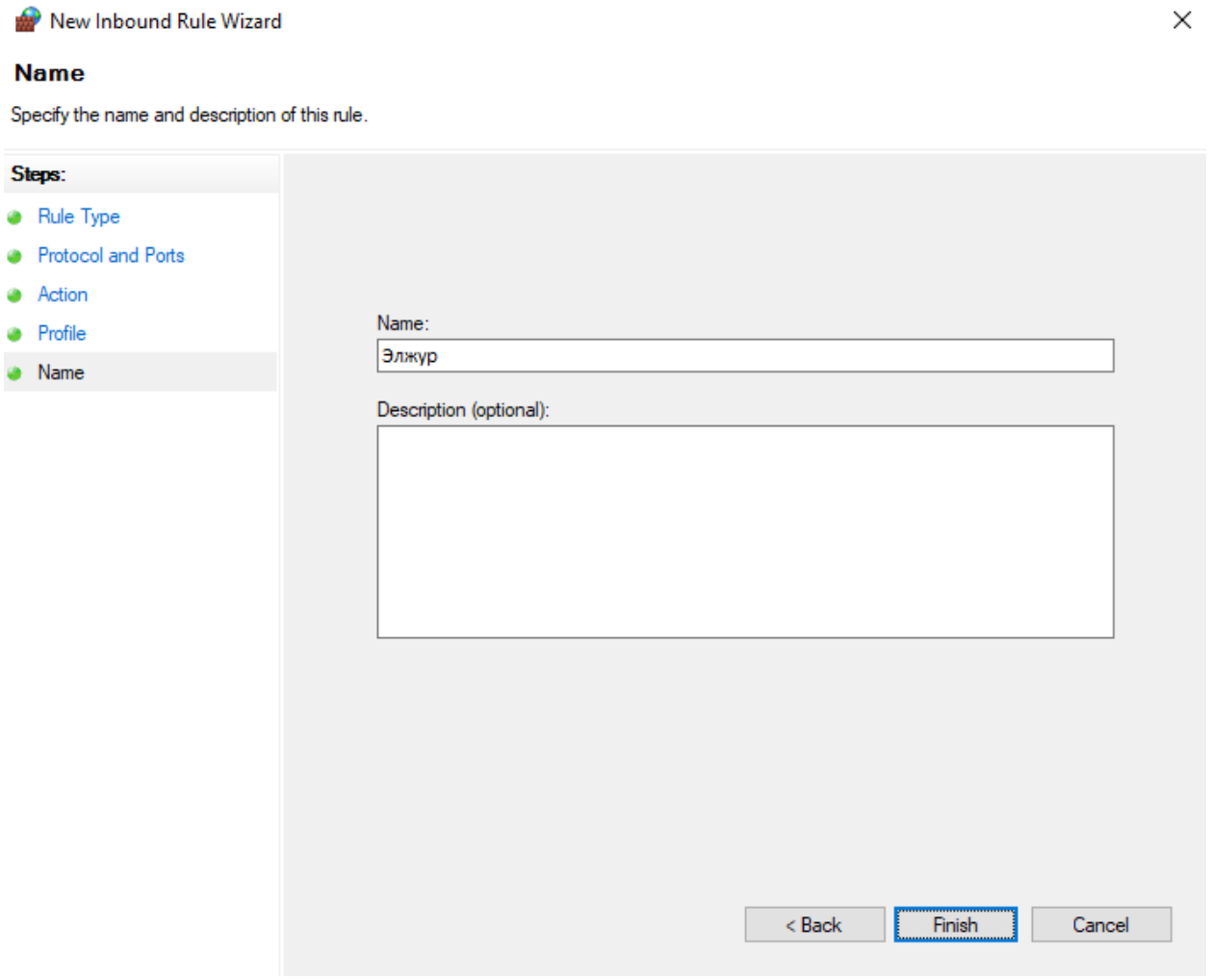


Рисунок 25

2) Создание служебной учётной записи

a. Открыть панель управления компьютером, выбрав Пуск-Средства администрирования Windows-Управление компьютером (Start-Windows Administrative Tools-Computer Management);
b. Выбрать раздел Локальные пользователи и группы (Local Users and Groups), после чего перейти в папку Пользователи (Users);
c. Нажать на пустую область в центральной панели правой кнопкой мыши и выбрать пункт Новый пользователь… (New User…);

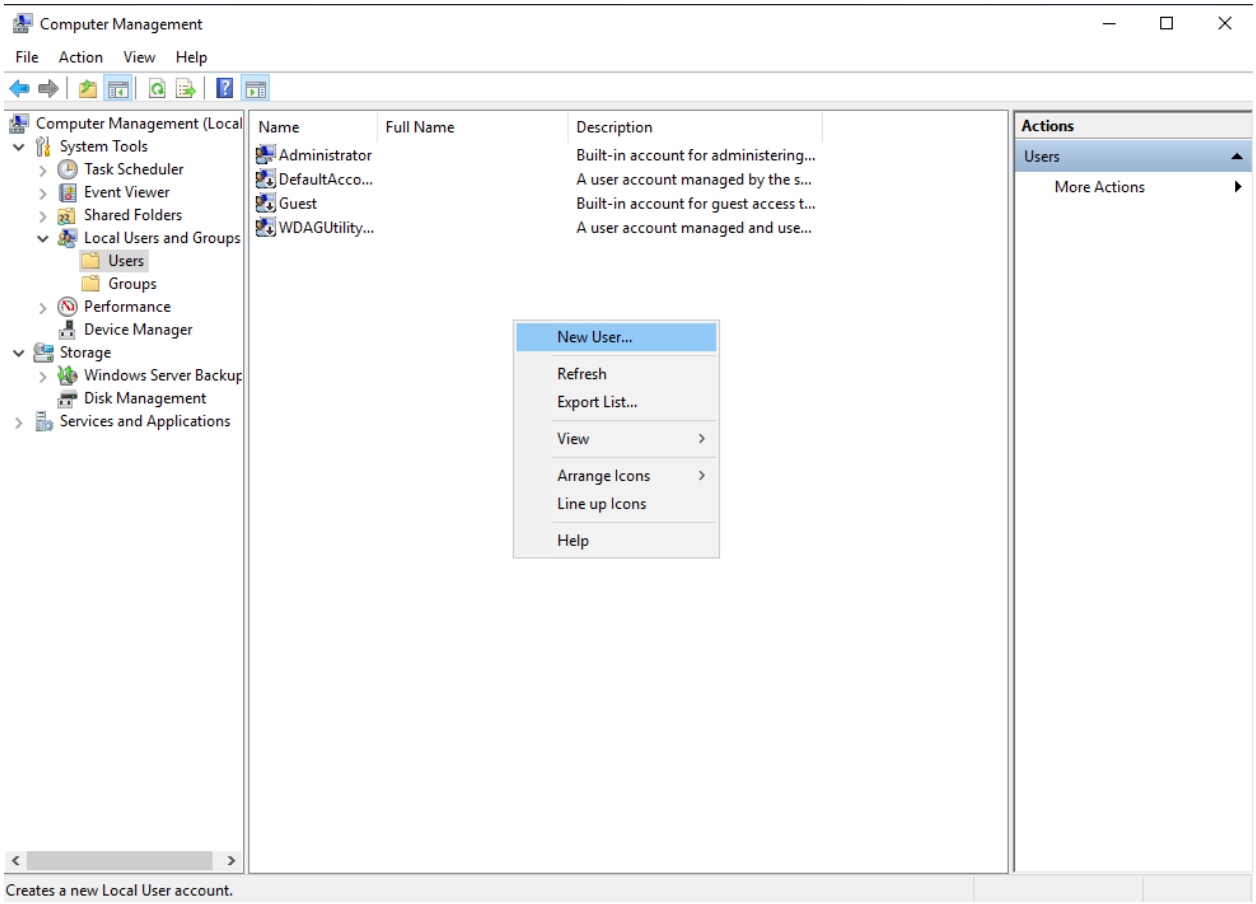


Рисунок 26

d. Ввести имя пользователя и пароль, соответствующий политике безопасности (по умолчанию: не менее 8 символов, должен содержать большие и маленькие буквы латинского алфавита и хотя бы одну цифру), после чего обязательно снять галочку Требовать смены пароля при следующем входе в систему (User must change password at next logon) и установить её в поле Срок действия пароля не ограничен (Password never expires), затем подтвердить создание пользователя, последовательно нажав Создать (Create) и Закрыть (Close);

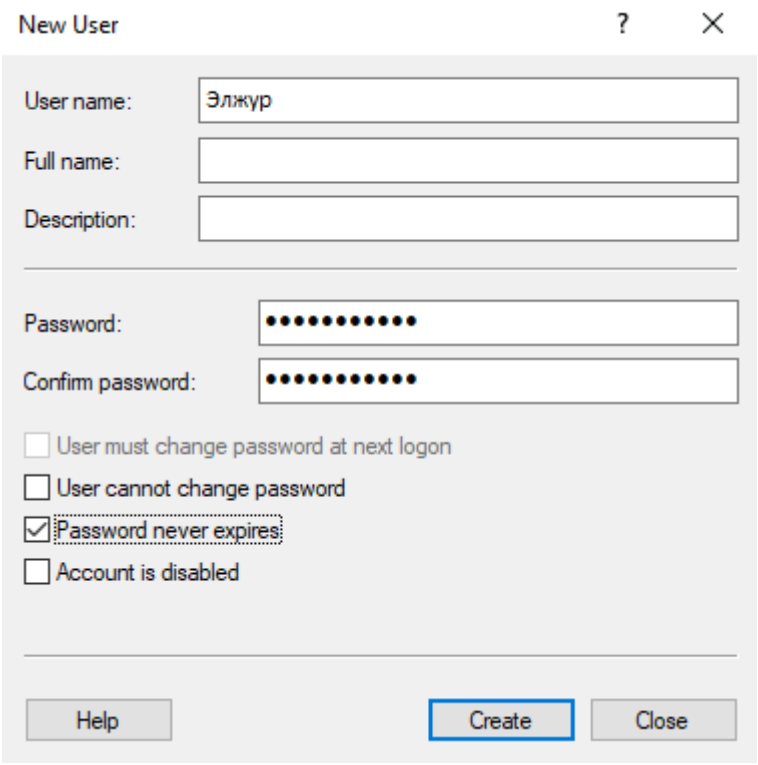


Рисунок 27

e. В открытом окне управления компьютером выбрать созданного пользователя и открыть его свойства, после чего перейти во вкладку Членство в группах (Member Of) и нажать кнопку Добавить… (Add…);

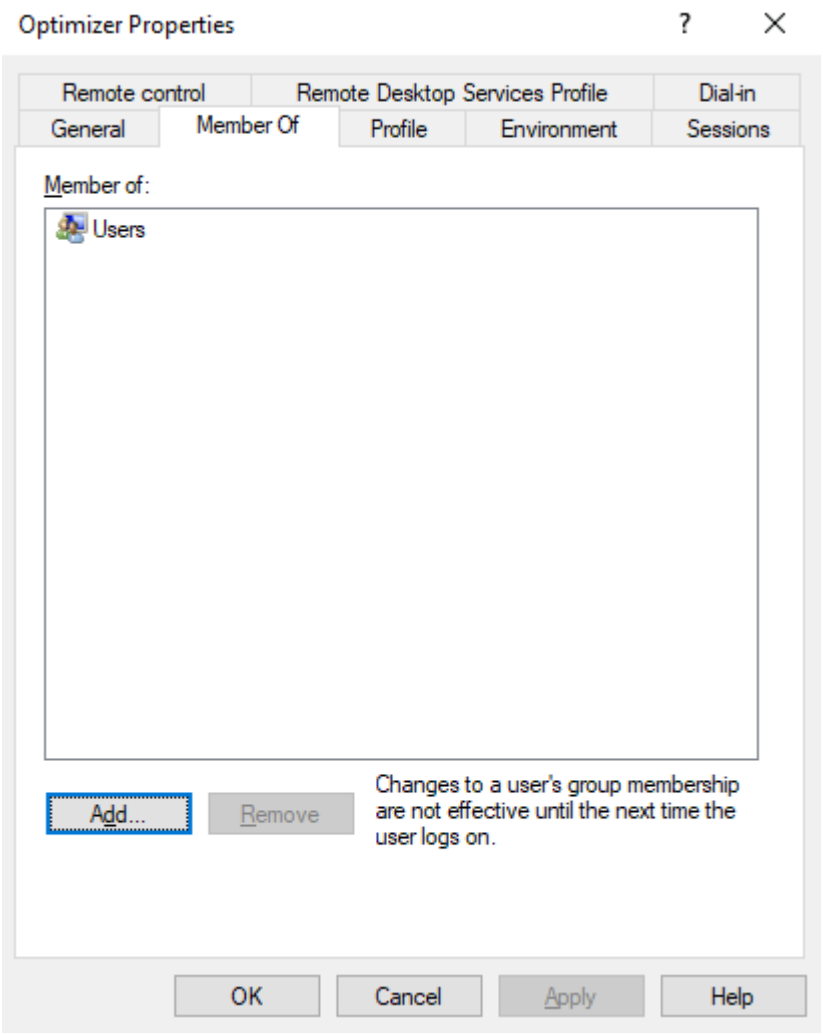


Рисунок 28

f. В открывшемся окне нажать кнопку Дополнительно… (Advanced…), после чего в появившемся окне нажать кнопку Поиск (Find Now);

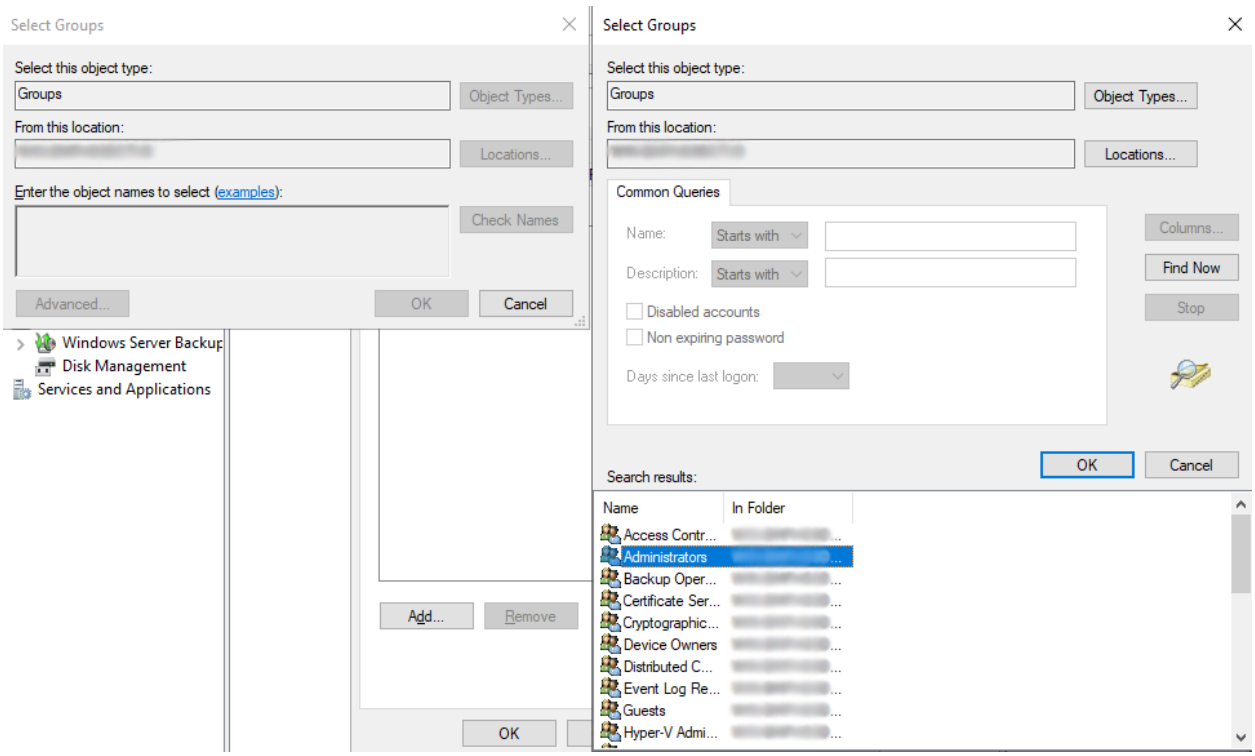


Рисунок 29

g. Двойным нажатием левой кнопки мыши выбрать группу Администраторы (Administrators), далее закрыть открытые ранее окна выбора группы и изменения свойств пользователя нажатием OK;

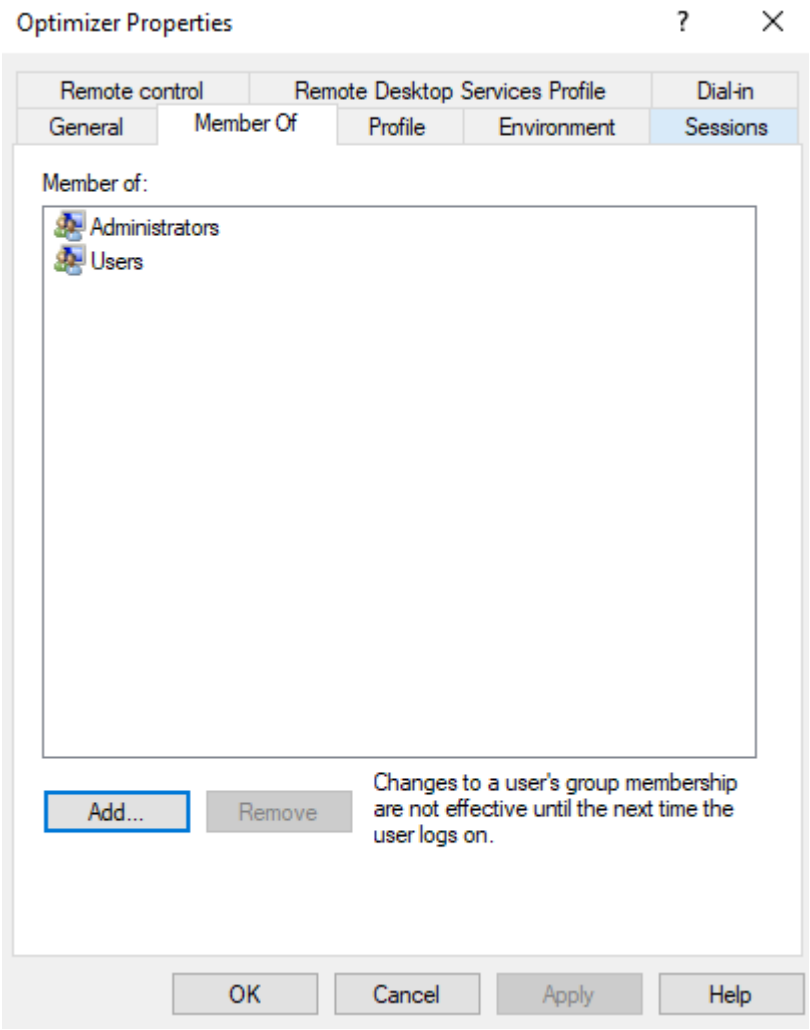


Рисунок 30

h. Закрыть окно управления компьютером.

3) Настройка RabbitMQ Server

a. Запустить командную строку с правами администратора и перейти в папку с исполняемыми файлами сервера RabbitMQ, используя команду cd “C:\Program Files\RabbitMQ Server\rabbitmq_server-3.8.4\sbin” ;
b. Выполнить команду rabbitmqctl add_user middle tier;
c. Выполнить команду rabbitmqctl set_permissions middle “.*” “.*” “.*”

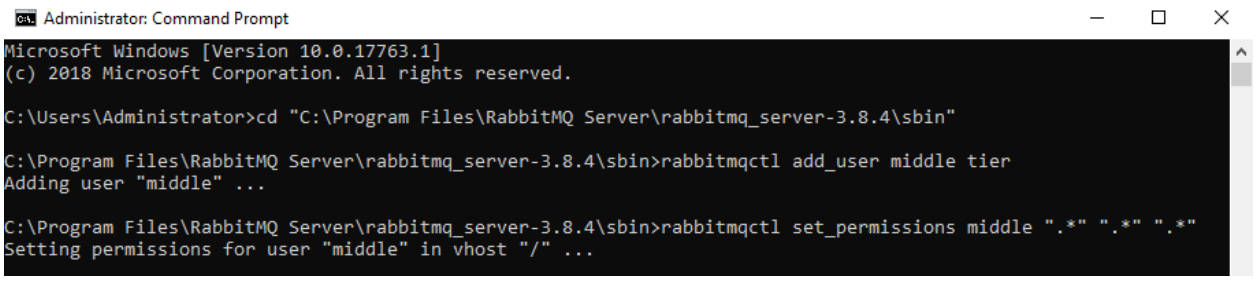


Рисунок 31

4) Настройка ПК Элжур

Для настройки компонентов ПК Элжур необходимо внести изменения в следующие конфигурационные файлы:

a. C:\SitesFolderRTK\UFM.FileService\appsettings.json
b. C:\SitesFolderRTK\PP.MiddleTier.Service\appsettings.json
c. C:\SitesFolderRTK\PP.MiddleTier.Service\Root.json
d. C:\SitesFolderRTK\UFM.Application\Root.json
e. C:\SitesFolderRTK\UFM.IdentityServer\Settings\appsettings.json
f. C:\SitesFolderRTK\UFM.Web\wwwroot\app\app.settings.js

Требуемые изменения для указанных файлов описаны в разделе «Замена конфигурационных файлов» данной Инструкции

5) Настройка SQL Server

a. Запустить SQL Server Management Studio от имени пользователя, который выполнял установку;
b. В окне Connect to Server выбрать текущий сервер и выбрать тип аутентификации Windows Authentication, после чего нажать Connect;

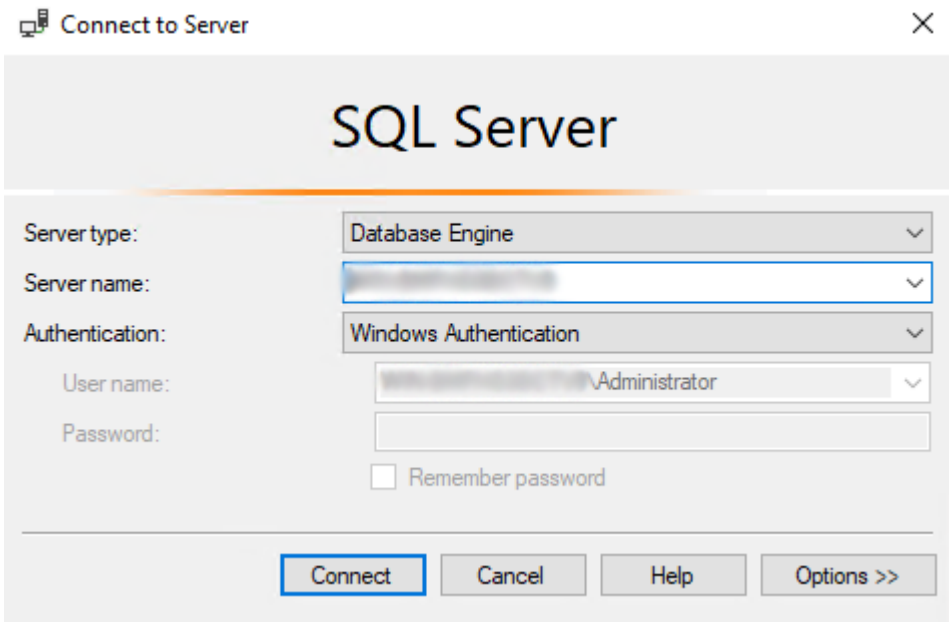


Рисунок 32

c. В панели Object Explorer выбрать раздел Security-Logins, нажать правой кнопкой мыши и выбрать пункт New Login…

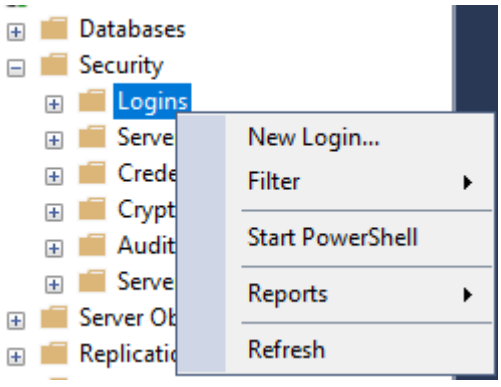


Рисунок 33

d. В открывшемся окне Login – New на вкладке General нажать кнопку Search… рядом с полем Login name, после чего в появившемся окне нажать кнопку Advanced…

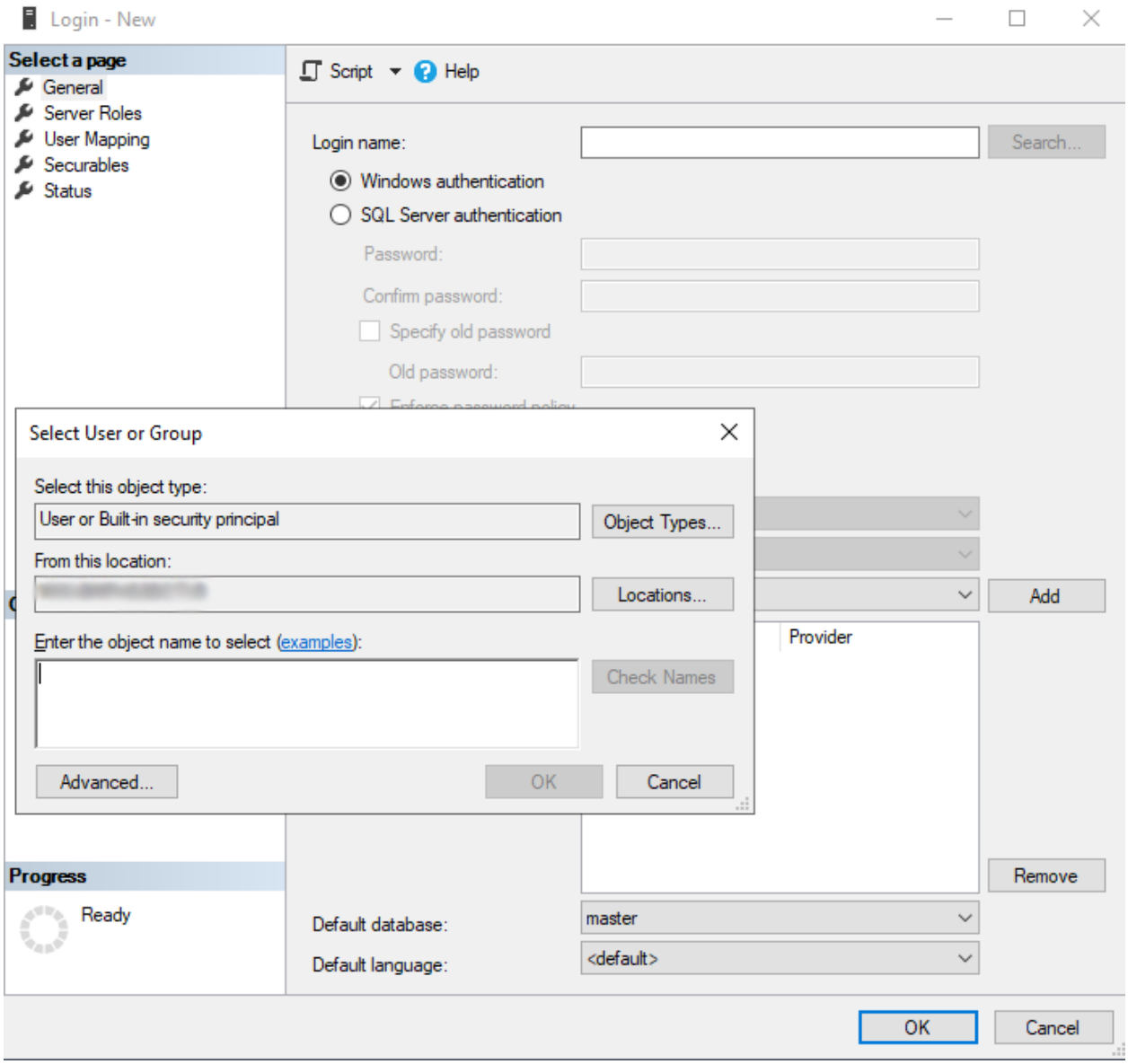


Рисунок 34

e. В окне Select User or Group нажать кнопку Find Now и в появившемся списке выбрать УЗ Элжур, созданную ранее, после чего закрыть окна с заголовком Select User or Group нажатием кнопки ОК;

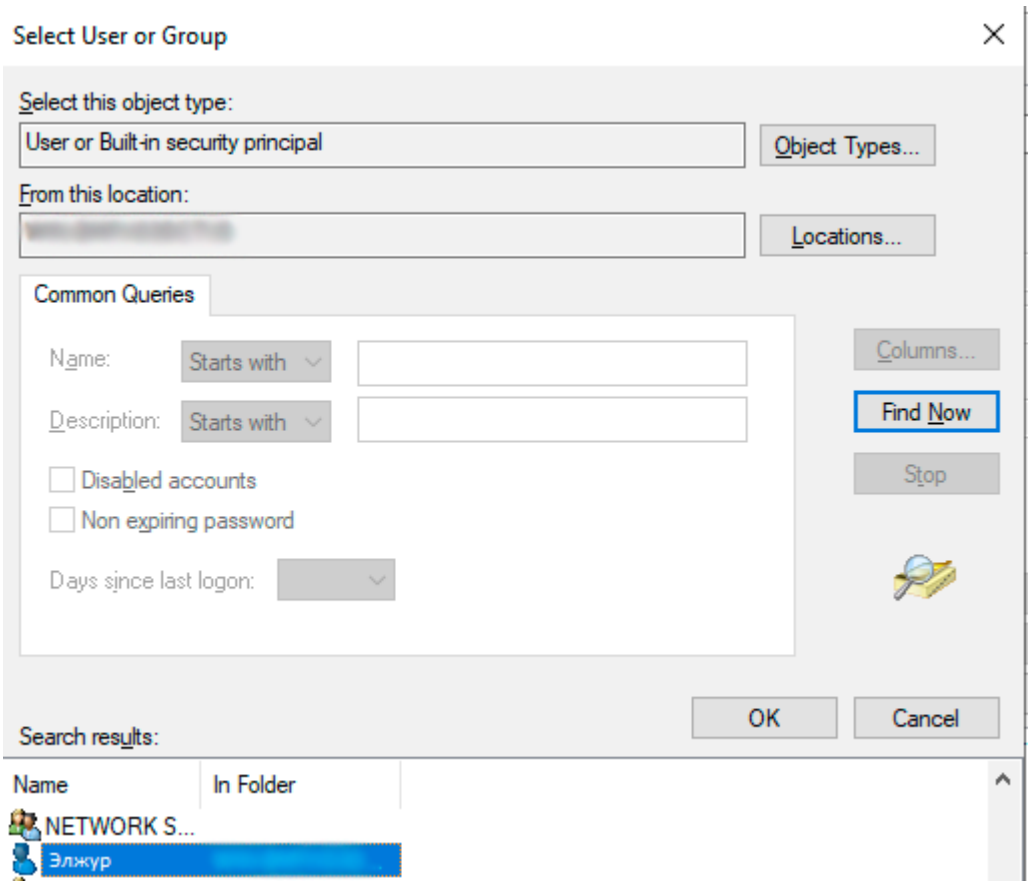


Рисунок 35

f. В окне Login – New убедиться, что в поле Login name появилось имя выбранной учётной записи, после чего на вкладке Server Roles выбрать Роль sysadmin, установив соответствующую галочку, затем нажать кнопку OK;

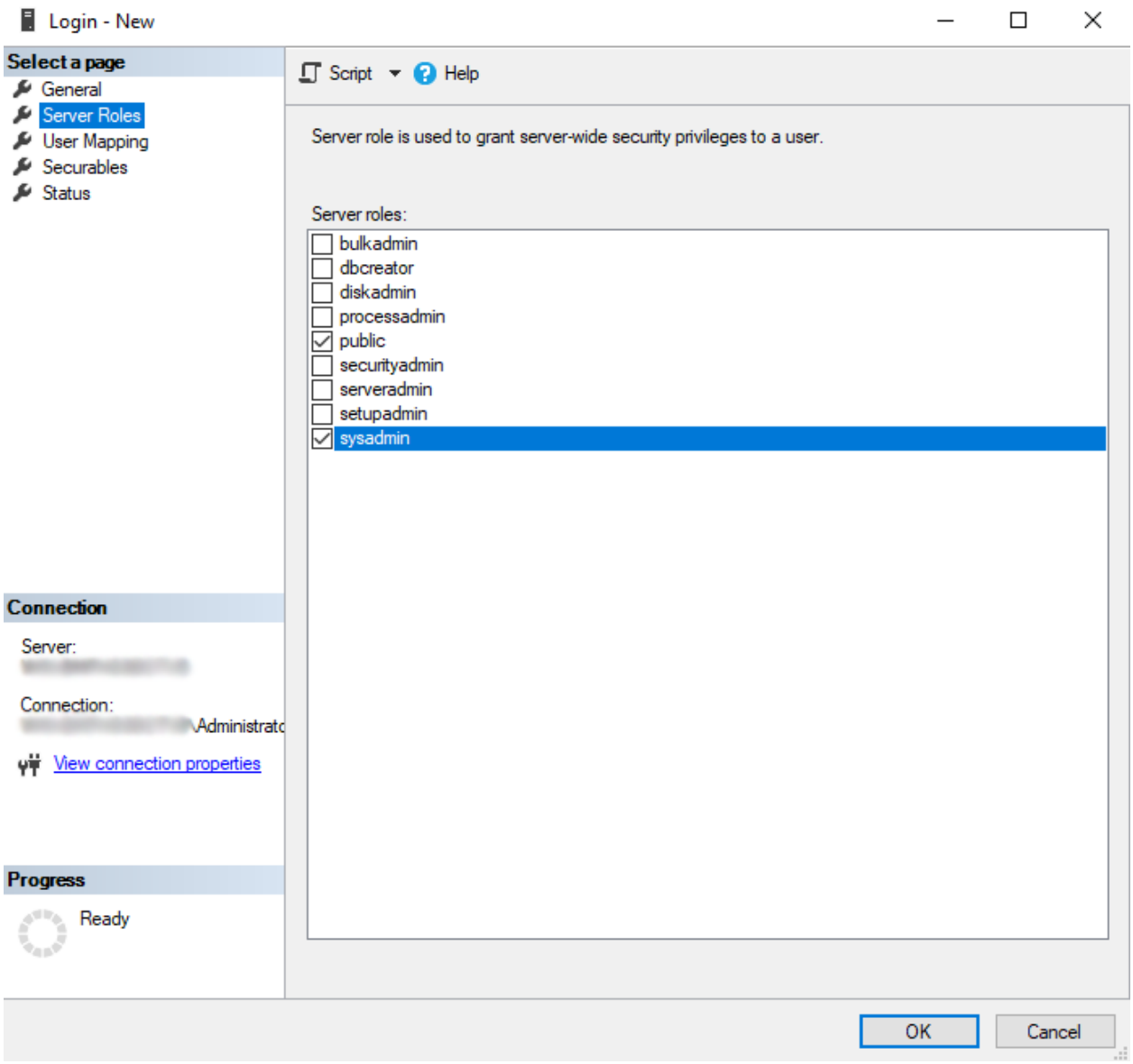


Рисунок 36

g. Закрыть SQL Server Management Studio.

6) Настройка IIS

a. Открыть окно настройки Internet Information Services (IIS), выбрав Пуск-Средства администрирования Windows- (Start-Windows Administrative Tools-Internet Information Services (IIS) Manager);
b. В панели (Connections) выбрать текущий сервер и перейти в раздел (Sites), после чего нажать правой кнопкой мыши на отображаемый сайт Default Web Site, выбрать пункт Удалить (Remove) и подтвердить удаление в диалоговом окне, нажав кнопку Да (Yes).

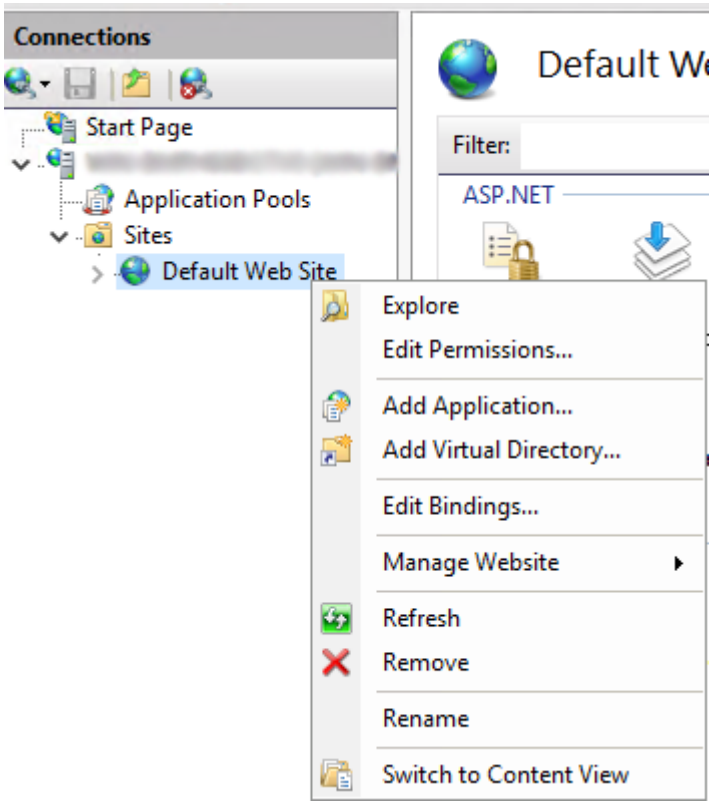


Рисунок 37

c. Перейти в раздел (Application Pools), нажать правой кнопкой мыши на свободное пространство в центральной панели и выбрать пункт (Add Application Pool…);

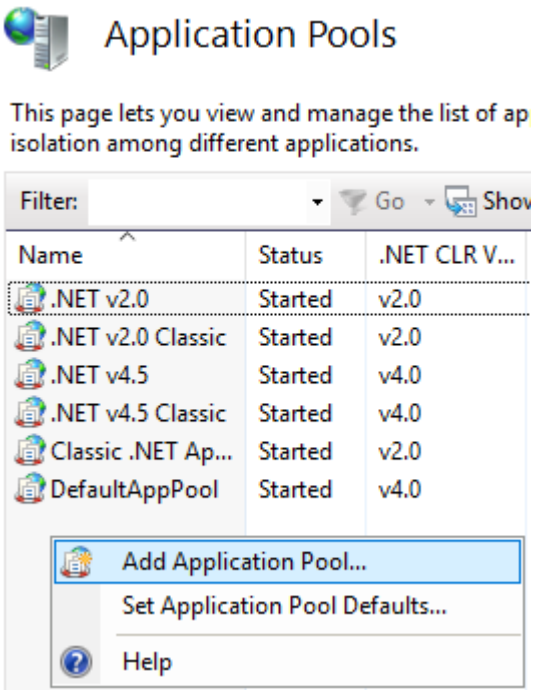


Рисунок 38

d. В открывшемся окне в поле Имя (Name) ввести название подключаемого компонента (UFM.Application) и подтвердить создание, нажав кнопку ОК.

Аналогичным образом создать пулы для UFM.FileService, UFM.IdentityServer, PP.MiddleTier.Service и UFM.Web;

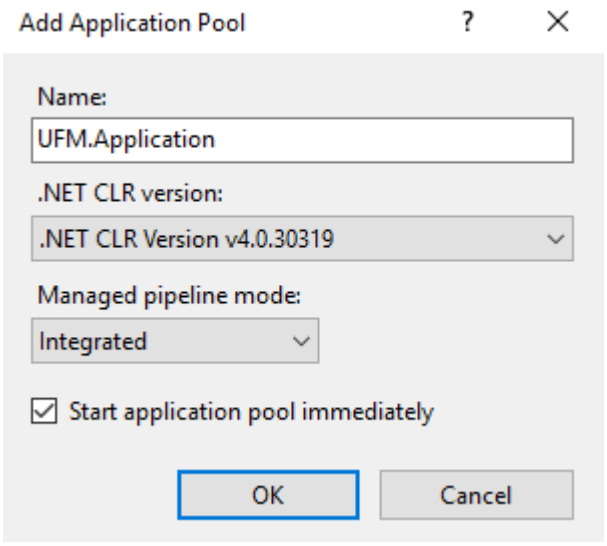


Рисунок 39

e. Нажать правой кнопкой мыши на созданный пул UFM.Application и выбрать пункт (Advanced Settings…);

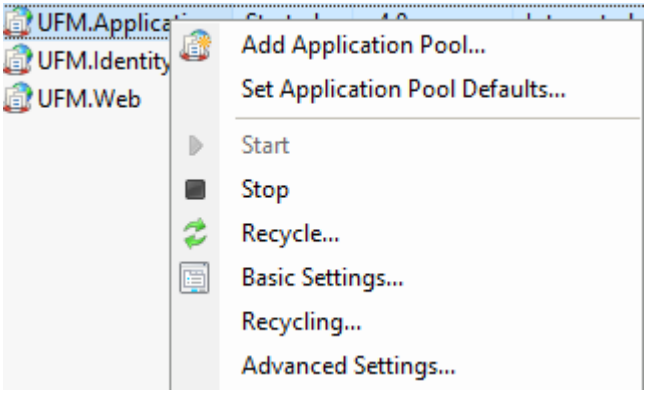


Рисунок 40

f. В разделе (Process Model) необходимо внести следующие изменения:
В поле (Identity) нажать на кнопку …

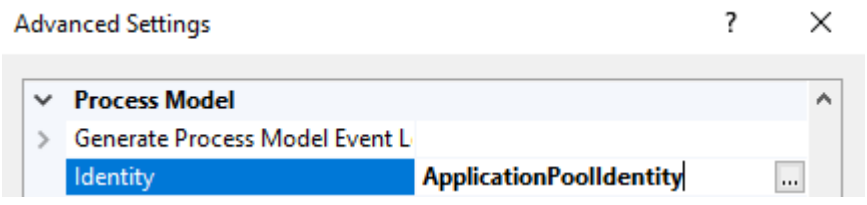


Рисунок 41

g. Выбрать значение (Custom account), нажать кнопку (Set…) и в открывшемся окне ввести данные от созданной ранее УЗ в формате .\Элжур, а также дважды указать пароль в соответствующих полях, после чего подтвердить изменения, дважды нажав ОК в окнах (Set Credentials) и (Application Pool Identity);

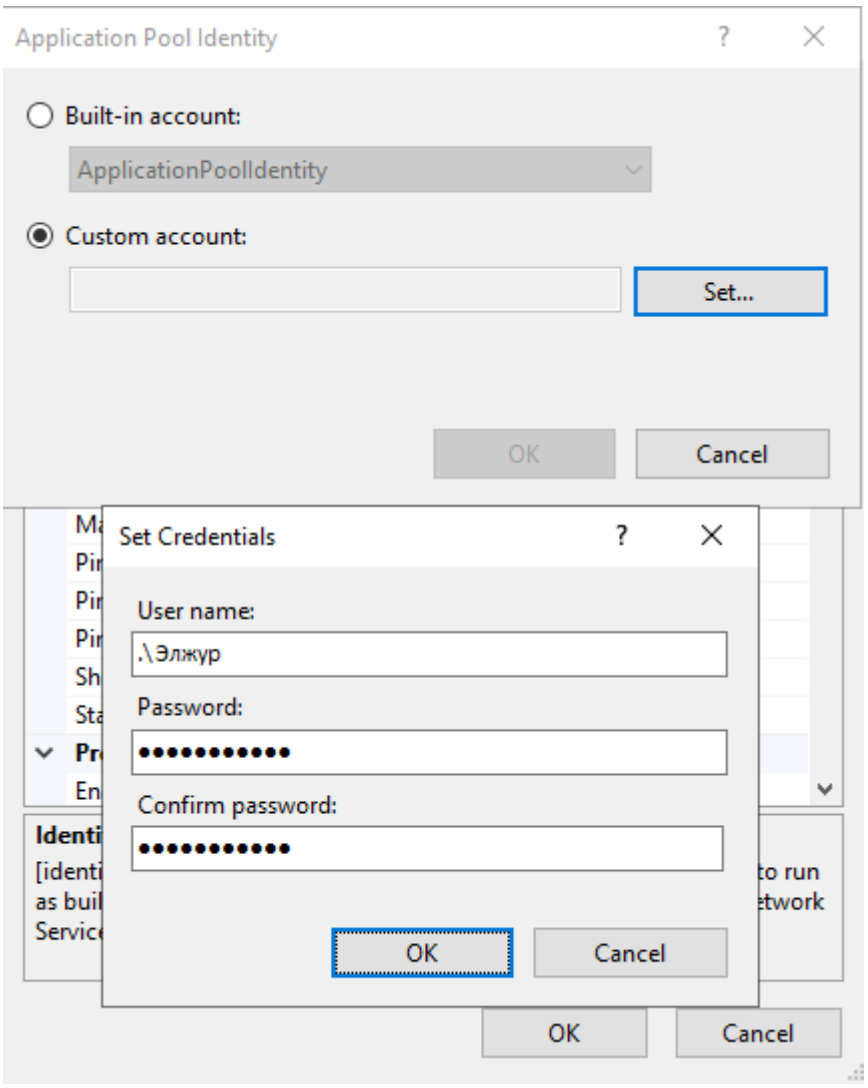


Рисунок 42

h. Изменить значение (Idle Time-out (minutes)) с 20 на 1740
Изменить значение (Load User Profile) с False на True
Сохранить изменения нажатием кнопки OK;

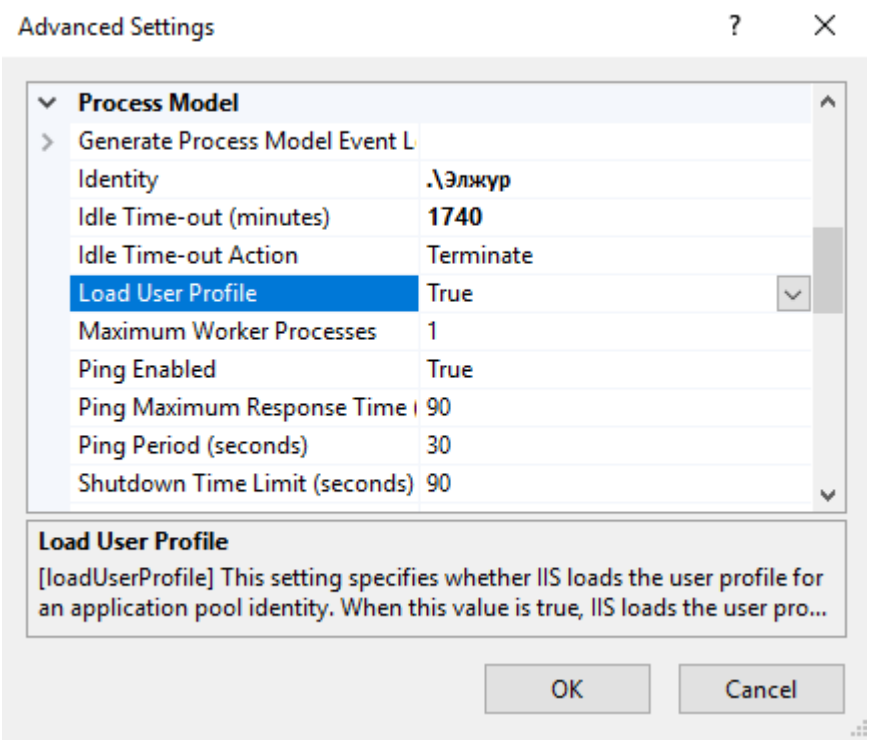


Рисунок 43

i. Аналогичные изменения произвести в пуле PP.MiddleTier.Service;
j. Для настройки пула UFM.IdentityServer также необходимо изменить значение поля (Identity) и (Load User Profile), остальные значения оставить по умолчанию;

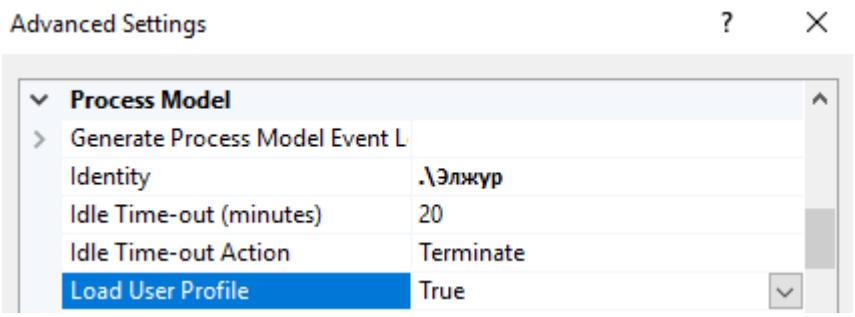


Рисунок 44

k. Перейти в раздел Sites, нажать правой кнопкой мыши на свободное пространство в центральной панели и выбрать пункт (Add Website…);

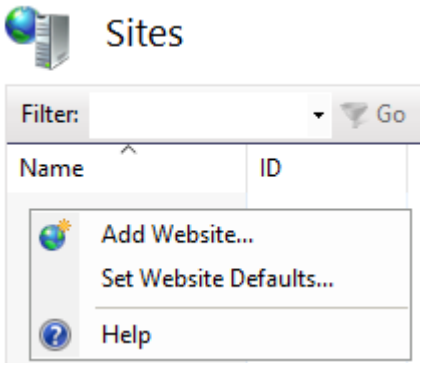


Рисунок 45

l. В открывшемся окне ввести имя сайта - UFM.Application, в поле (Physical Path:) указать путь к папке C:\SitesFolderRTK\UFM.Application и изменить используемый порт с 80 на 3000, после чего нажать ОК;

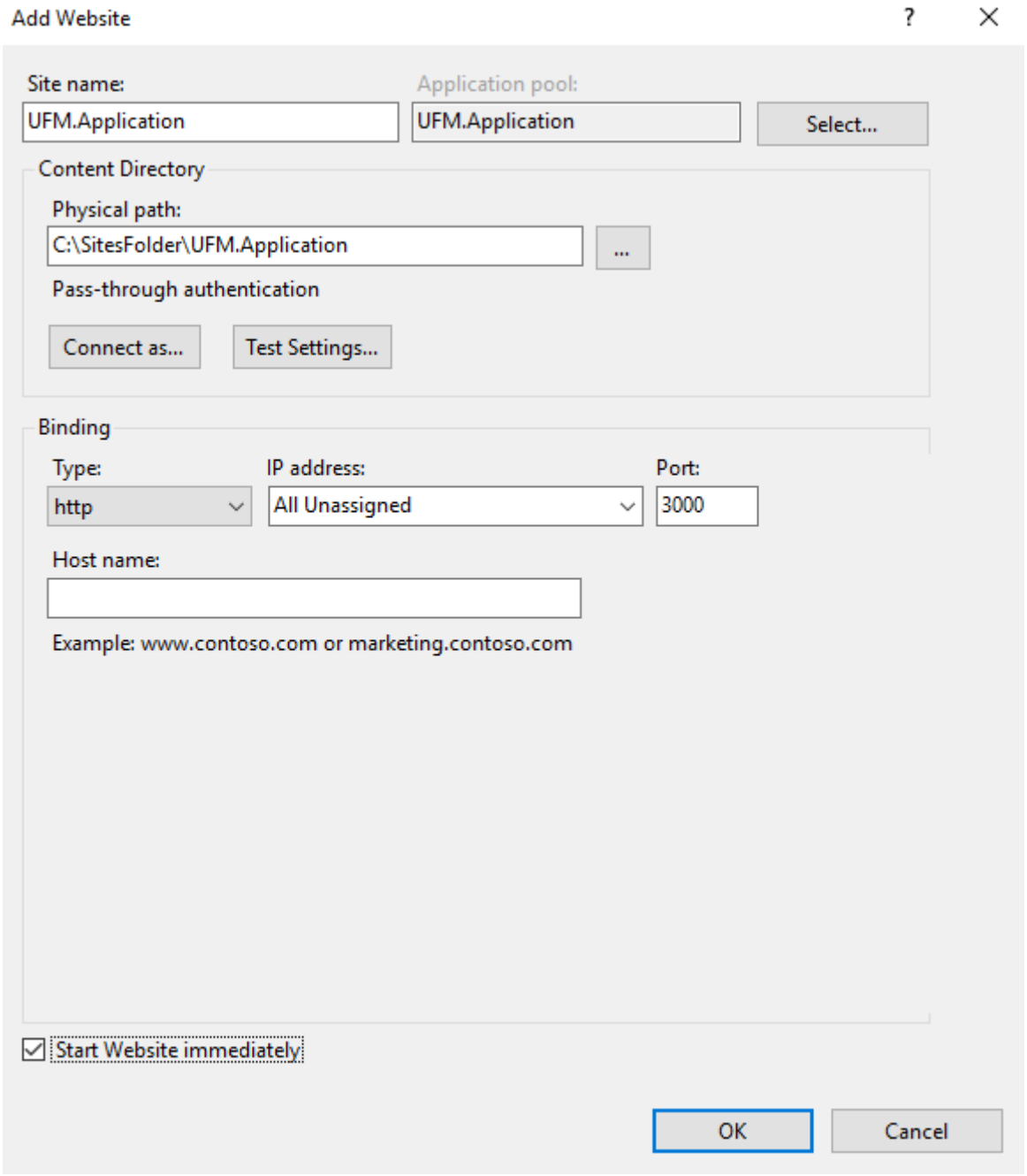


Рисунок 46

m. Аналогичным образом добавить сайты UFM.Web (путь C:\SitesFolderRTK\UFM.Web, порт 80), UFM.IdentityServer (путь C:\SitesFolderRTK\UFM.IdentityServer, порт 5000), PP.MiddleTier.Service (путь C:\SitesFolderRTK\PP.MiddleTier.Service, порт 4000), и UFM.FileService (путь C:\SitesFolderRTK\UFM.FileService, порт 6001);

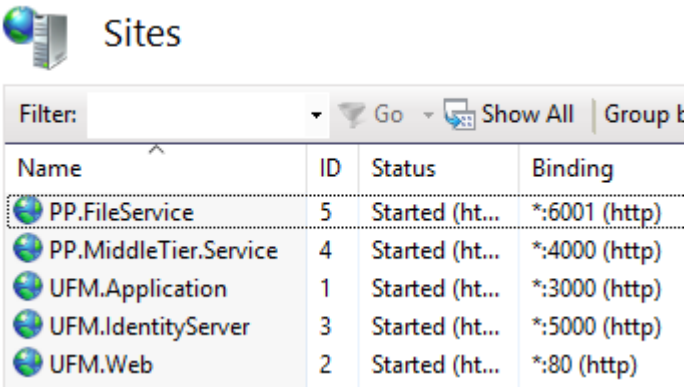


Рисунок 47

7) Инициализация компонентов

Для создания всех необходимых файлов приложения необходимо выполнить первый запуск каждого отдельного компонента.
Для этого необходимо через браузер обратиться к созданным сайтам в следующей последовательности:

a. UFM.Application (localhost:3000), обязательно дождаться отображения страницы с кодом ошибки 404 Not Found – загрузка может занять длительное время;

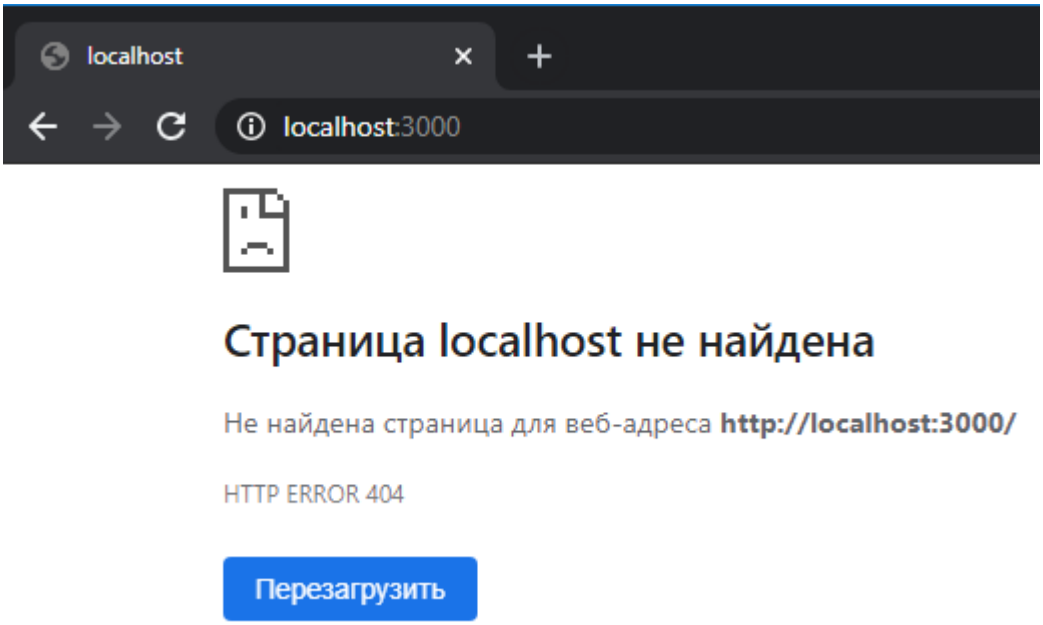


Рисунок 48

b. UFM.IdentityServer (localhost:5000), обязательно дождаться отображения страницы с кодом ошибки 404 Not Found – загрузка может занять длительное время;

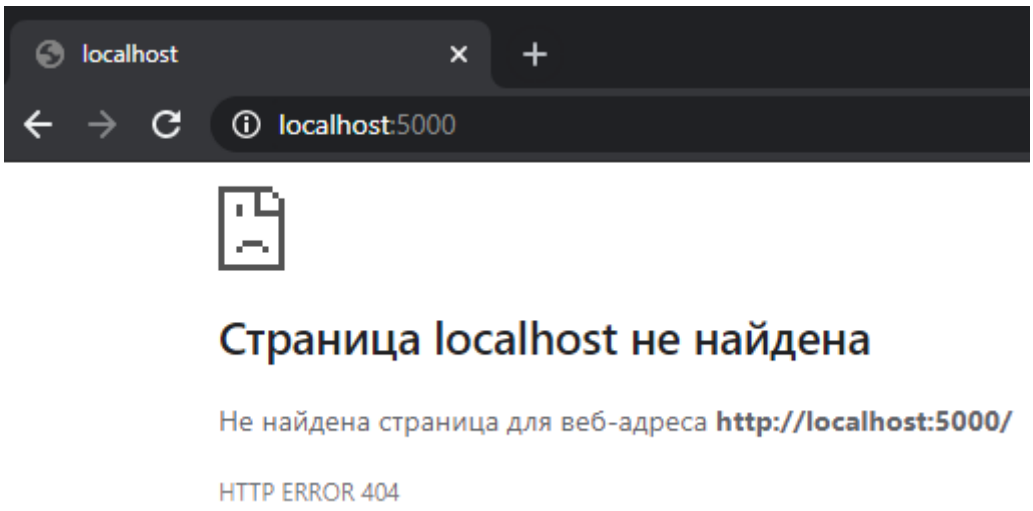


Рисунок 49

c. UFM.FileService (localhost:6001)
d. PP.MiddleTier.Service (localhost:4000)
e. UFM.Web (localhost:80), должна отобразиться форма входа в систему

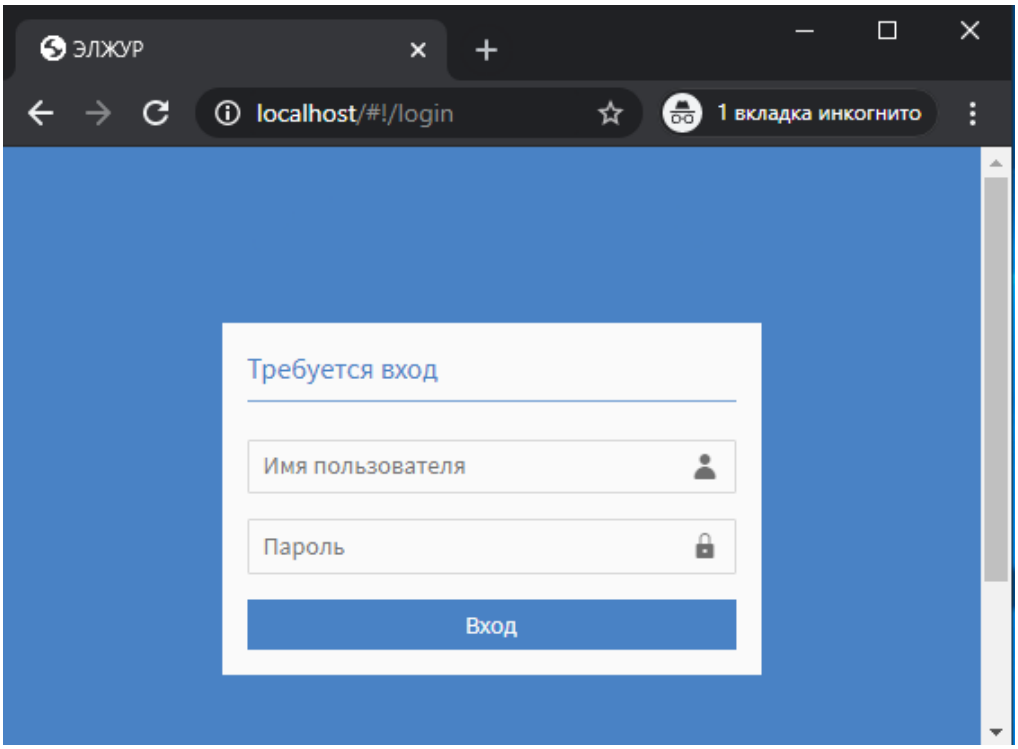


Рисунок 50

f. Закрыть окно браузера.

8) Установка и настройка службы чтения карт на рабочих станциях:

a. Запустить установочный файл
b. Убедиться, что установка будет производиться в папку по умолчанию (C:\CardReaderSRV) и нажать Далее
c. Дождаться завершения установки и проверить в диспетчере задач наличие и статус службы UFM.CardReaderService

9) Настройка MiddleTier

Настройка MiddleTier выполняется с помощью импорта настроек через утилиту PP.MiddleTier.Configuration:

a. Вкладка MobilePermissions

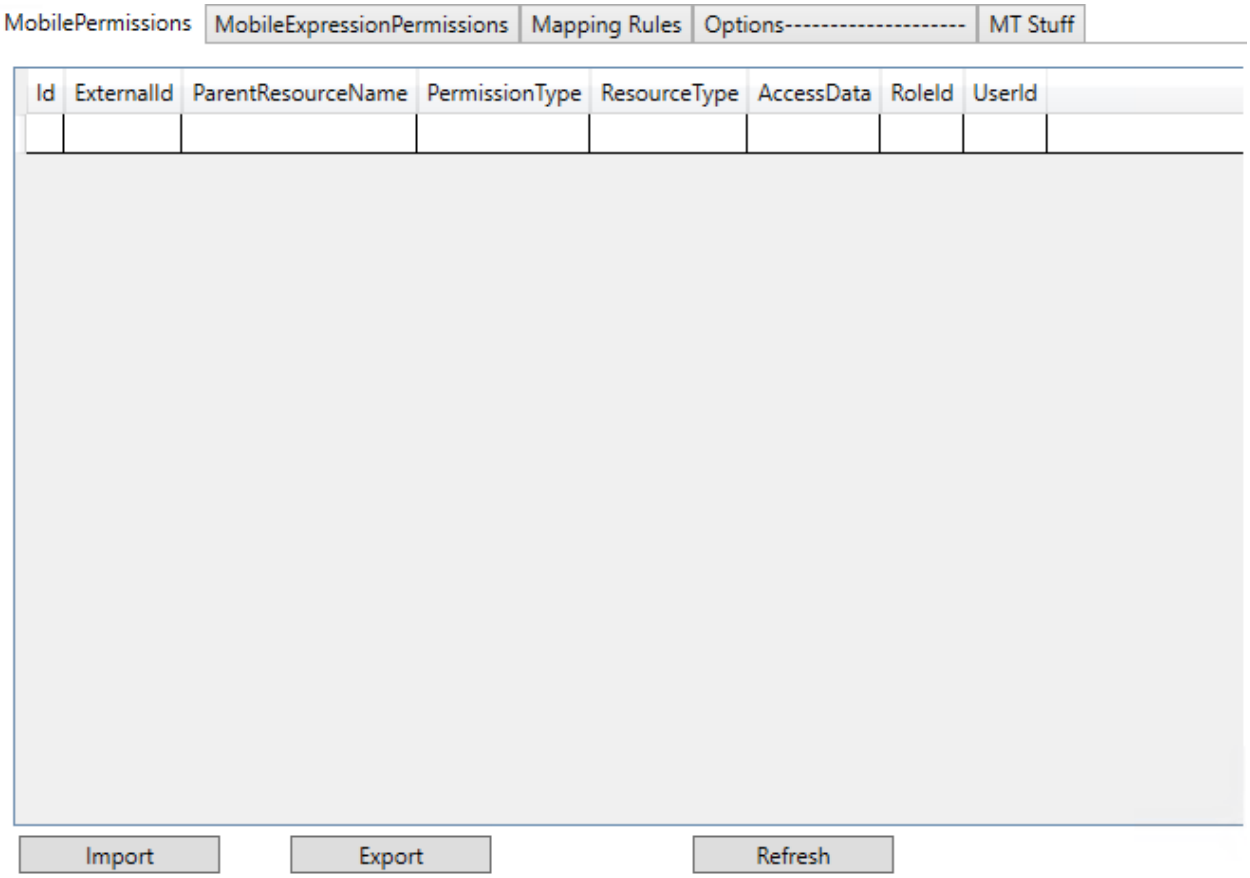


Рисунок 53

Нажать на кнопку Import и выбрать предоставленный с установщиком одноимённый файл

b. Вкладка MobileExpressionPermissions

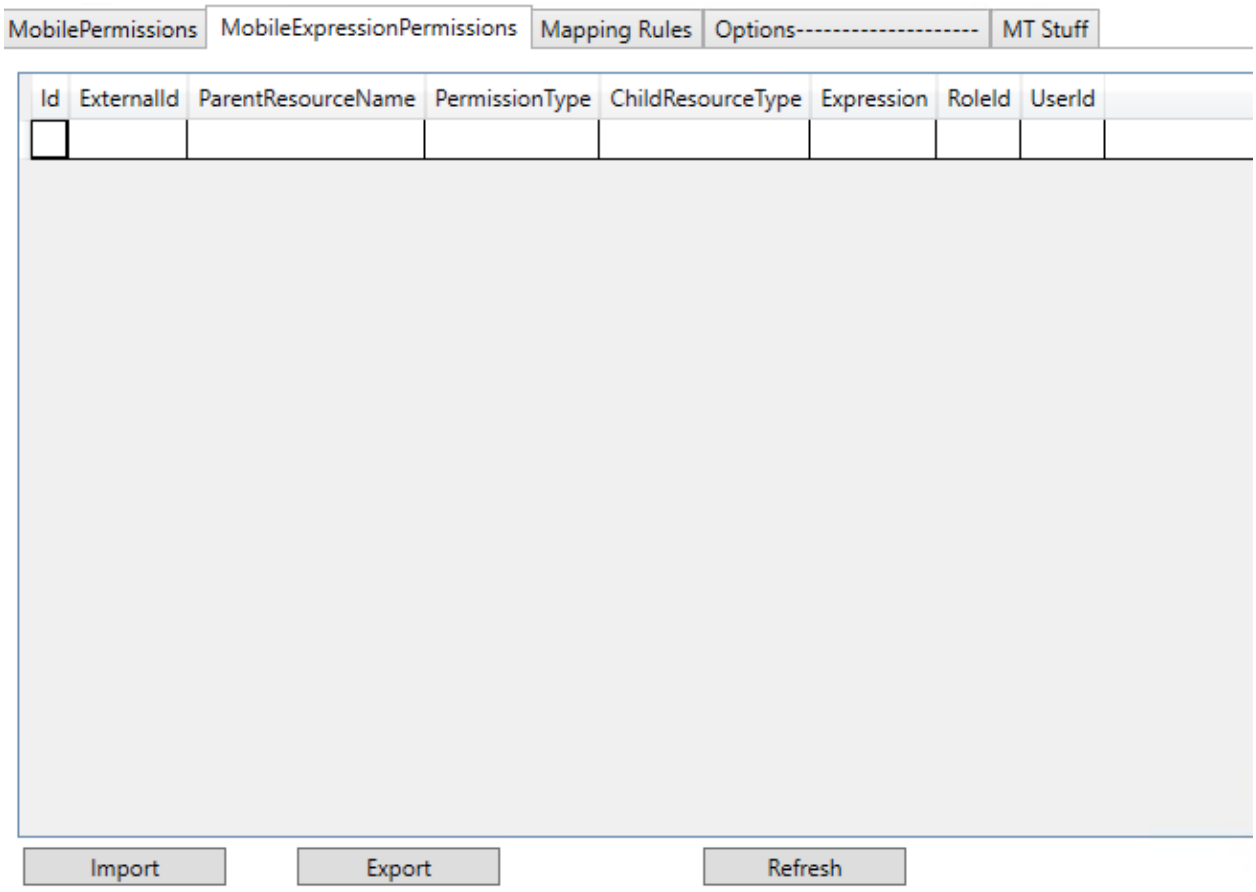


Рисунок 54

Нажать на кнопку Import и выбрать предоставленный с установщиком одноимённый файл

c. Вкладка Mapping Rules

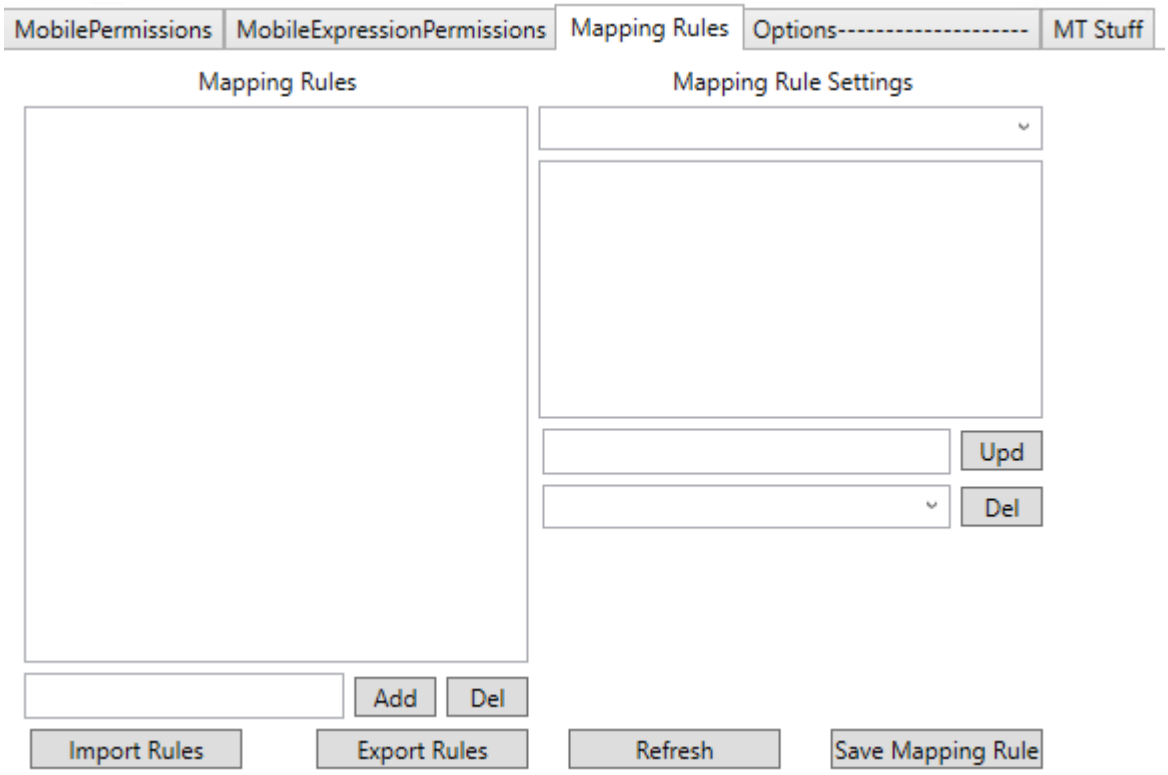


Рисунок 55

Нажать на кнопку Import Rules и выбрать предоставленный с установщиком одноимённый файл

10) Настройка подключения на мобильном устройстве (на ОС Android)

Для работы с web порталом на мобильном устройстве необходимо настроить подключение к корпоративной сети.

a. В шторке уведомлений необходимо перейти в настройки устройства

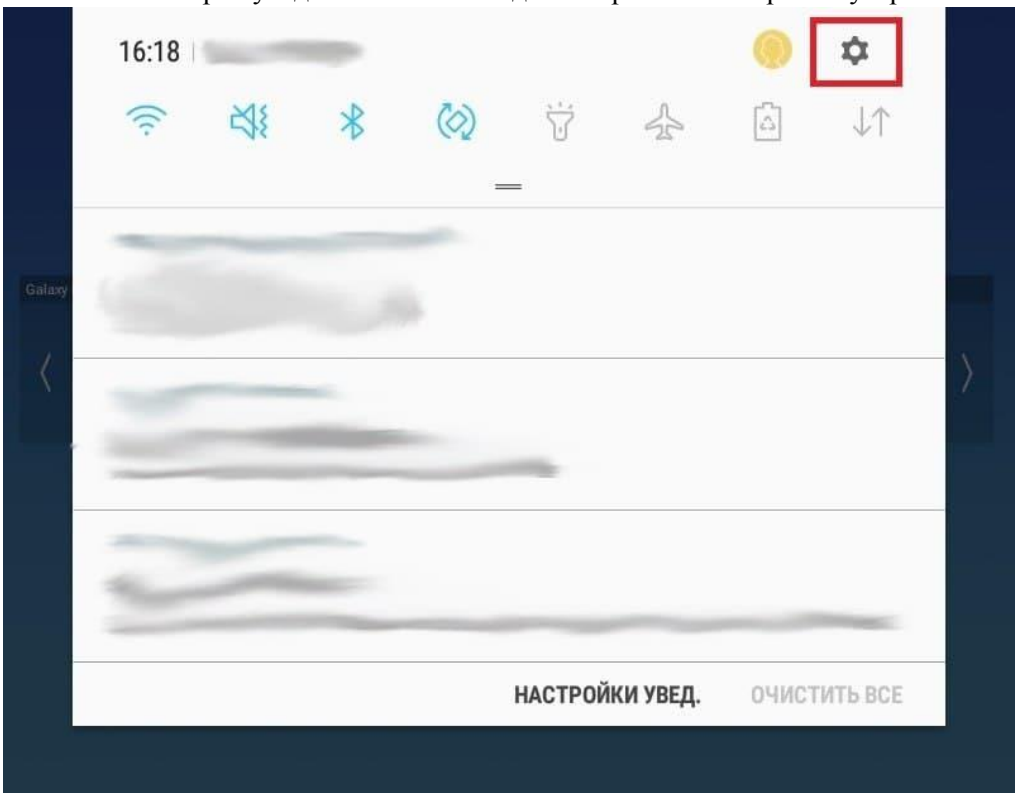


Рисунок 56

b. В открывшемся меню выбрать раздел «Подключения», затем последовательно нажать «Другие настройки» - «VPN»

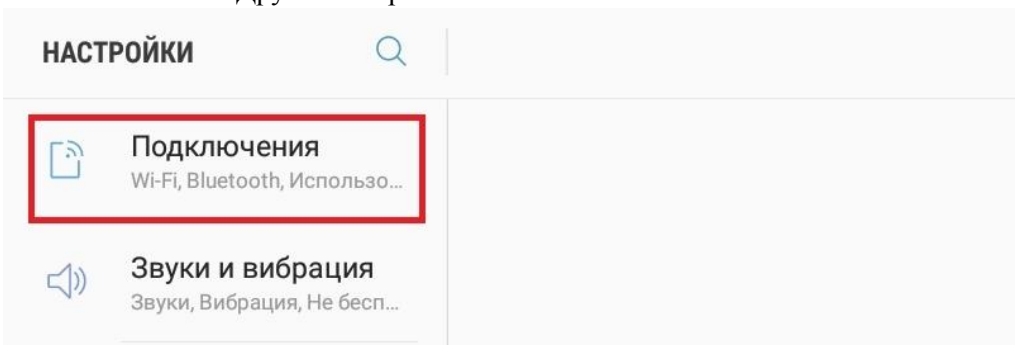


Рисунок 57

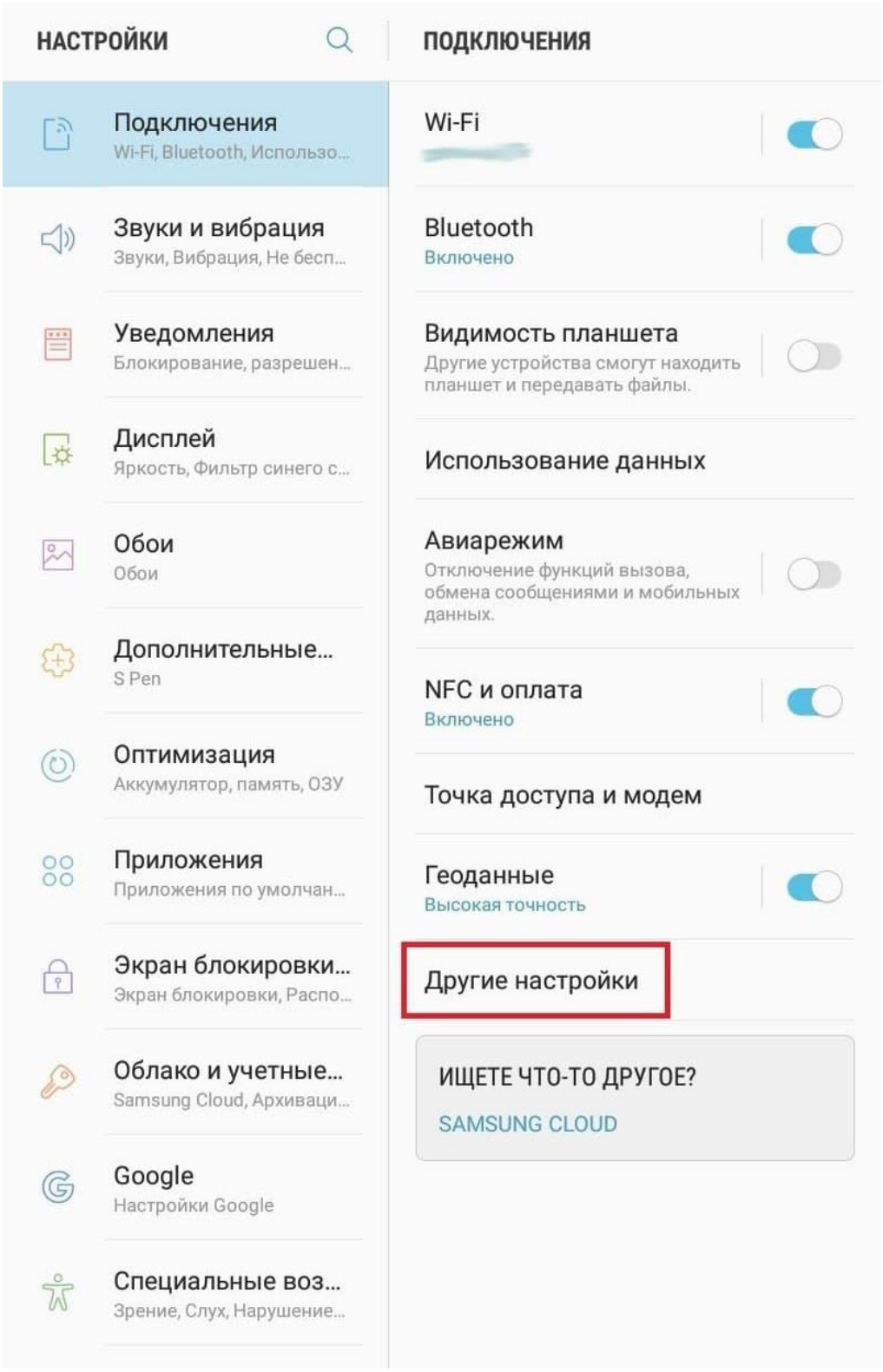

НАСТРОЙКИ
ПОДКЛЮЧЕНИЯ
Подключения
Wi-Fi, Bluetooth, Использо...
Звуки и вибрация
Звуки, Вибрация, Не бесп...
Уведомления
Блокирование, разрешен...
Дисплей
Яркость, Фильтр синего с...
Обои
Обои
Дополнительные...
S Pen
Оптимизация
Аккумулятор, память, ОЗУ
Приложения
Приложения по умолчан...
Экран блокировки...
Экран блокировки, Распо...
Облако и учетные...
Samsung Cloud, Архиваци...
Google
Настройки Google
Специальные воз...
Зрение, Слух, Нарушение...
Wi-Fi
Bluetooth
Включено
Видимость планшета
Другие устройства смогут находить планшет и передавать файлы.
Использование данных
Авиарежим
Отключение функций вызова, обмена сообщениями и мобильных данных.
NFC и оплата
Включено
Точка доступа и модем
Геоданные
Высокая точность
Другие настройки
ИЩЕТЕ ЧТО-ТО ДРУГОЕ?
SAMSUNG CLOUD

Рисунок 58

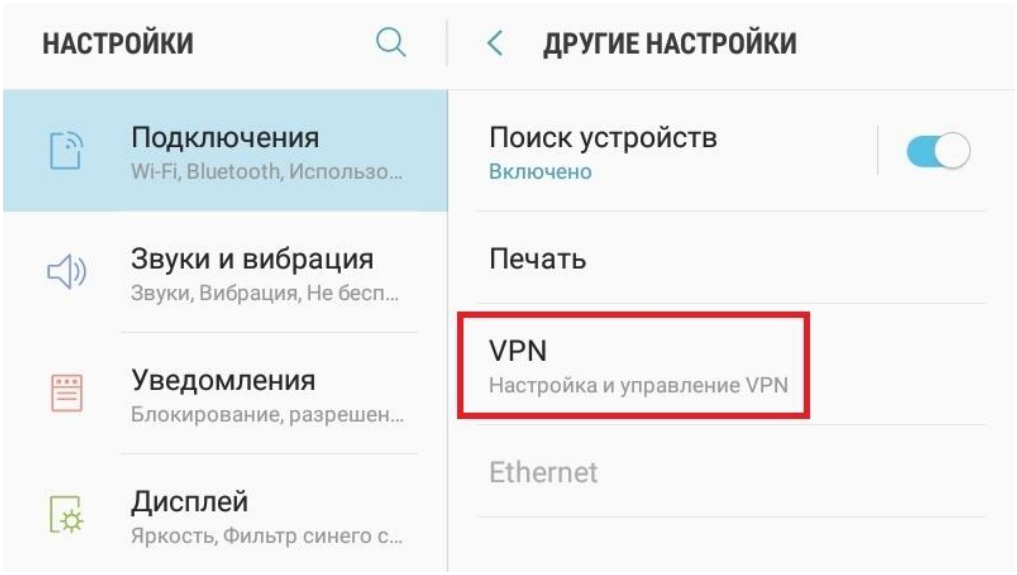


Рисунок 59

c. В правом верхнем углу нажать кнопку «Добавить VPN» и во всплывающем окне указать следующие данные:
Имя: MobileGTES
Тип: L2TP/IPSec PSK либо L2TP с общим ключом
Адрес сервера: IP-адрес, предоставленный вместе с учётными данными
Общий ключ IPSec: единый ключ, предоставленный с учётными данными
Имя пользователя и пароль: уникальные учётные данные
После заполнения нажать кнопку «Сохранить»

Рисунок 60

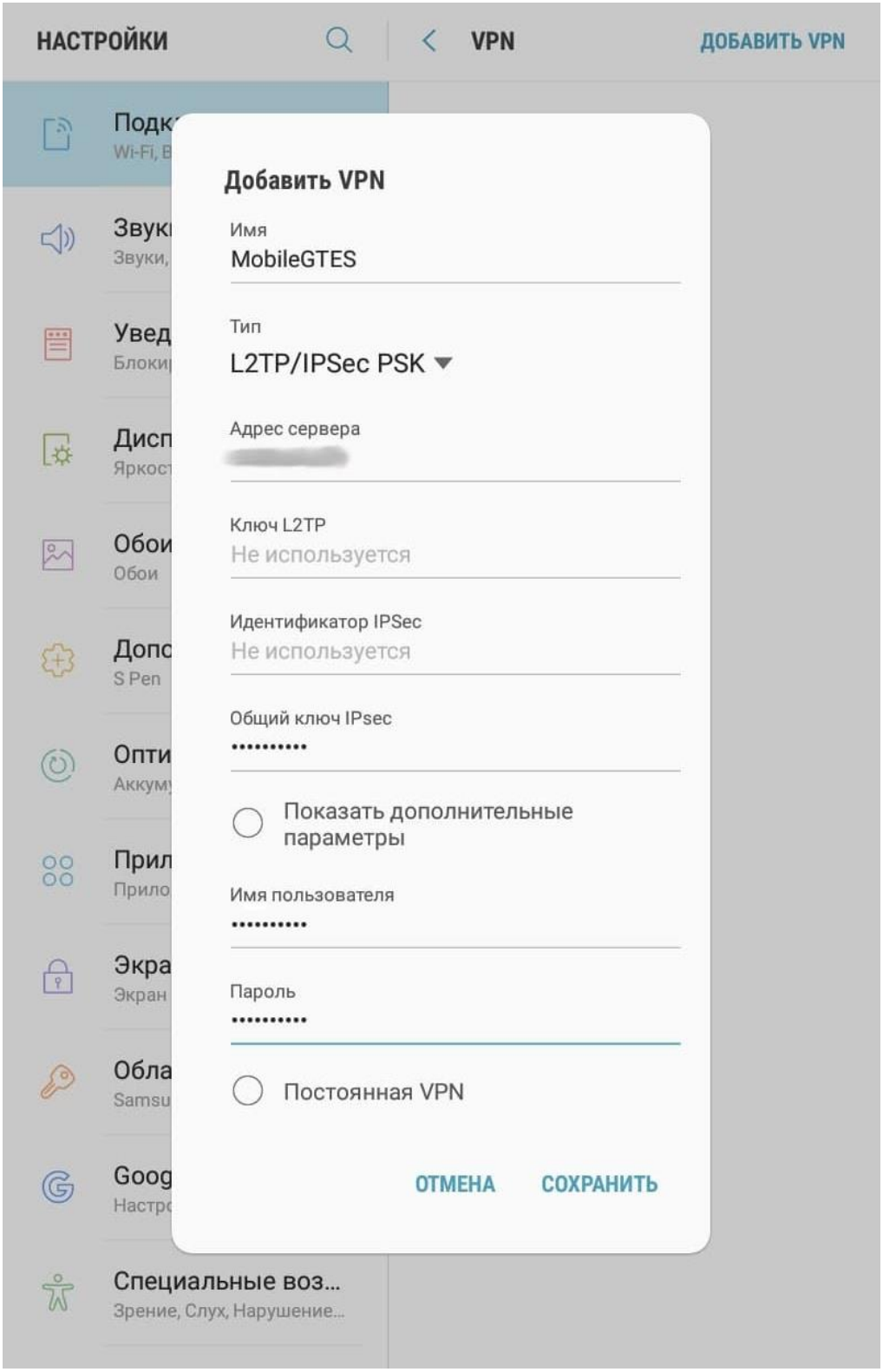


Рисунок 61

d. В списке доступных подключений появится новое подключение, которое и будет в дальнейшем использоваться для работы с порталом.

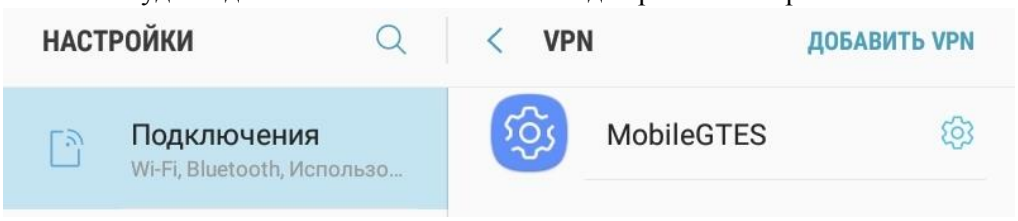


Рисунок 62

e. Для установления соединения необходимо выбрать соответствующее подключение VPN и нажать кнопку «Подключиться»

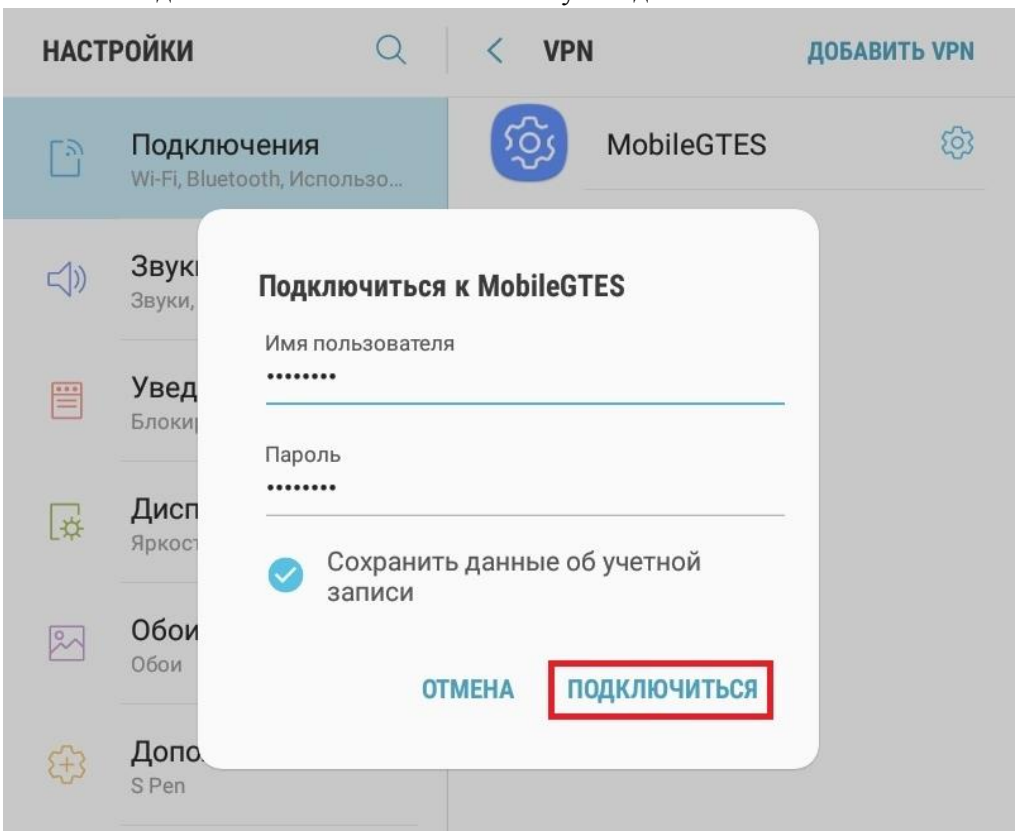


Рисунок 63

11) Настройка считывания NFC карт на мобильном устройстве (на ОС Android)

Для работы в web портале на мобильном устройстве с картами NFC необходимо выполнить следующие действия.

a. Открыть браузер Chrome
b. Перейти по ссылке chrome://flags

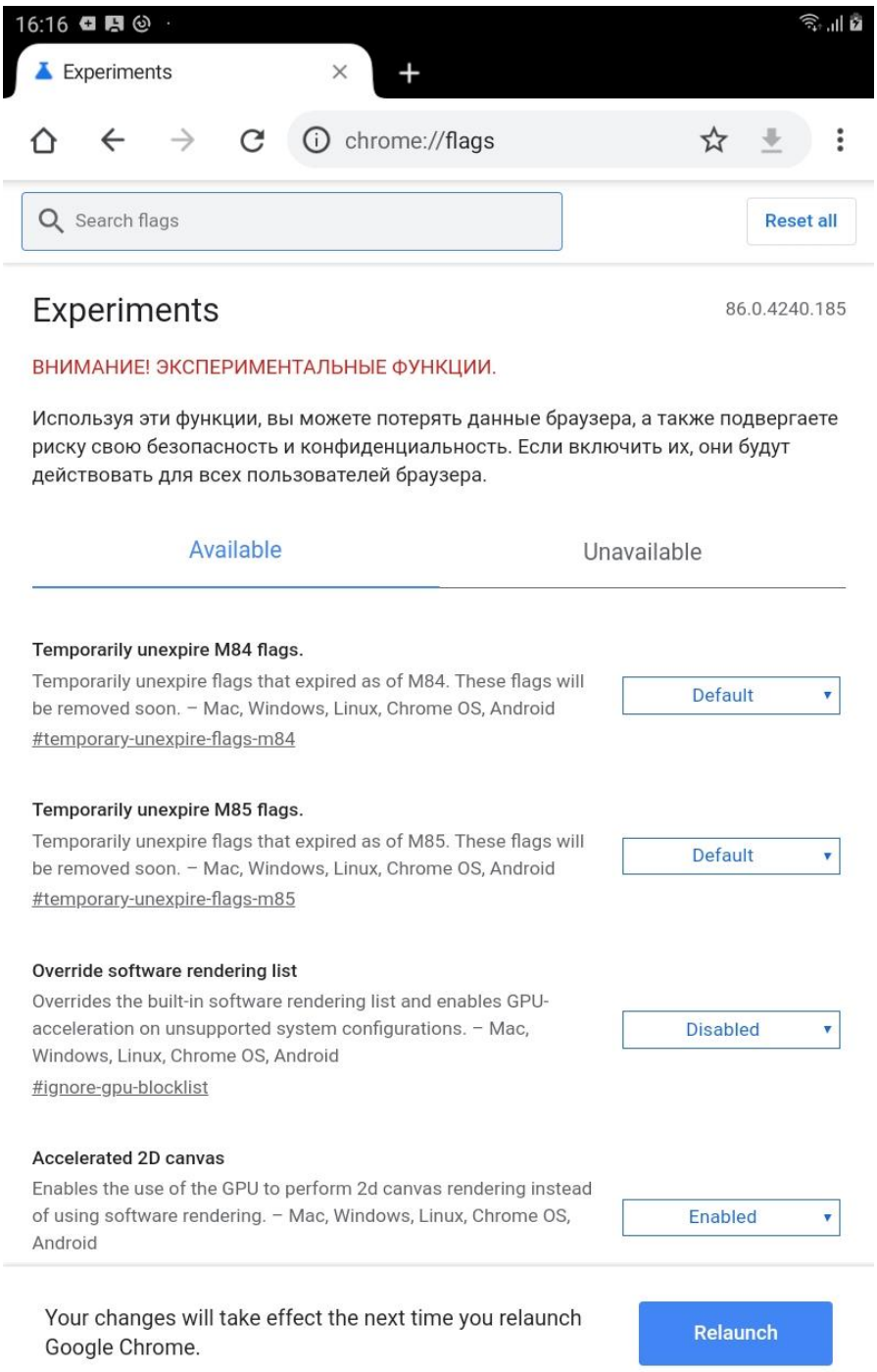


Рисунок 64

c. Найти флаг experimental-web-platform-features

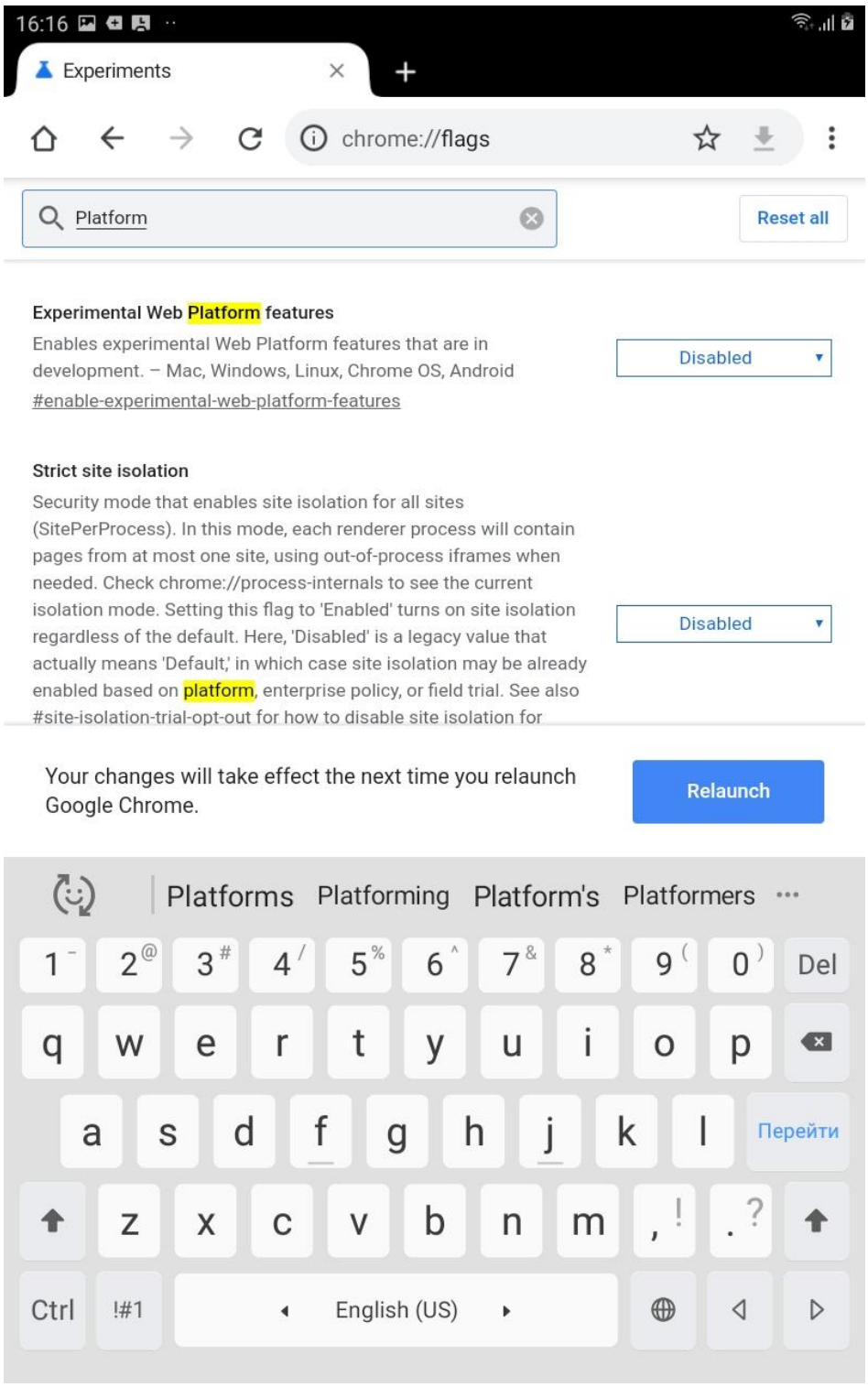


Рисунок 65

d. Переключить его во включенное положение

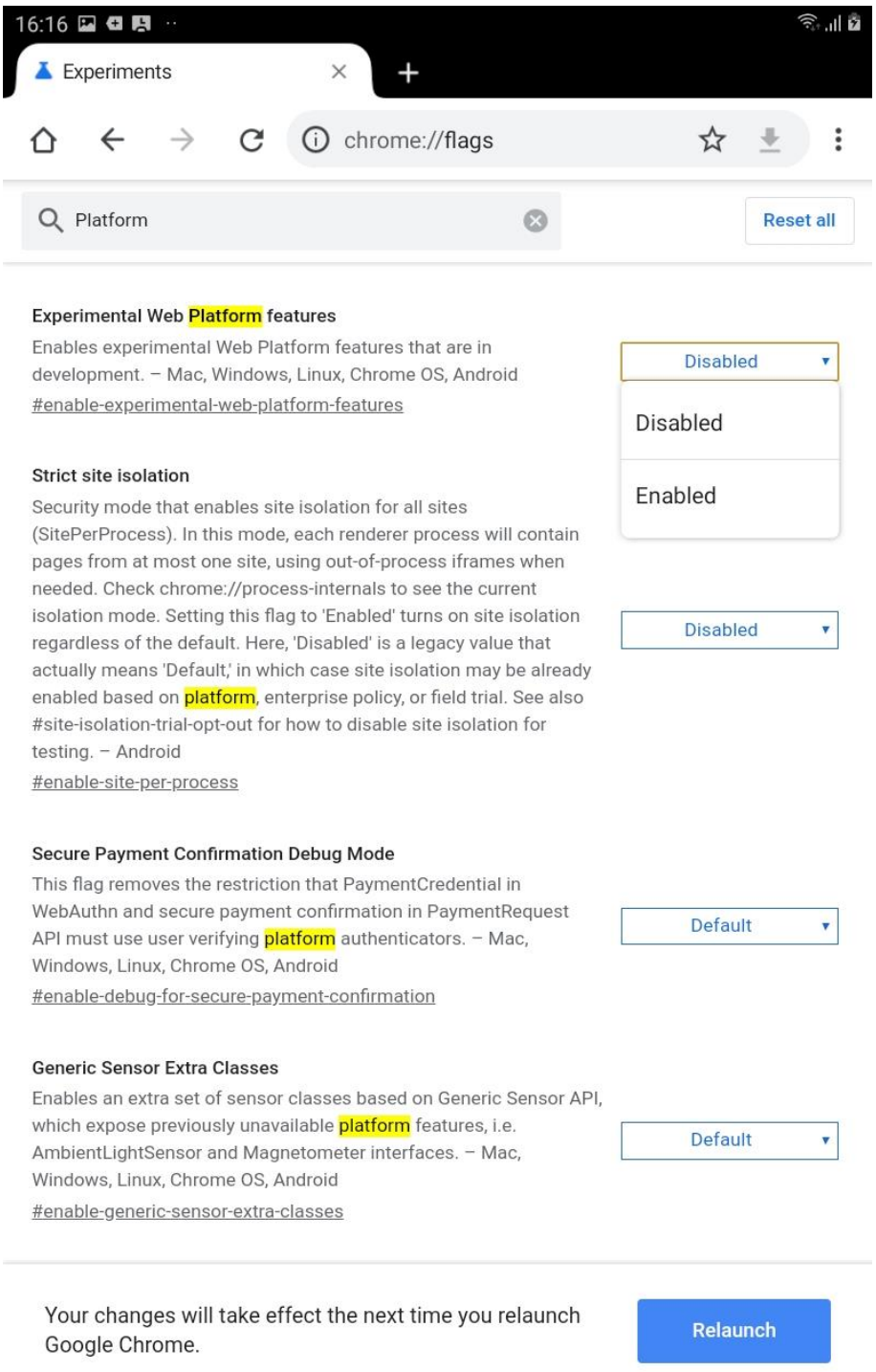

16:16
Experiments
chrome://flags
Platform
Reset all
Experimental Web Platform features
Enables experimental Web Platform features that are in development. – Mac, Windows, Linux, Chrome OS, Android
#enable-experimental-web-platform-features
Disabled
Disabled
Enabled
Strict site isolation
Security mode that enables site isolation for all sites (SitePerProcess). In this mode, each renderer process will contain pages from at most one site, using out-of-process iframes when needed. Check chrome://process-internals to see the current isolation mode. Setting this flag to 'Enabled' turns on site isolation regardless of the default. Here, 'Disabled' is a legacy value that actually means 'Default,' in which case site isolation may be already enabled based on platform, enterprise policy, or field trial. See also #site-isolation-trial-opt-out for how to disable site isolation for testing. – Android
#enable-site-per-process
Disabled
Secure Payment Confirmation Debug Mode
This flag removes the restriction that PaymentCredential in WebAuthn and secure payment confirmation in PaymentRequest API must use user verifying platform authenticators. – Mac, Windows, Linux, Chrome OS, Android
#enable-debug-for-secure-payment-confirmation
Default
Generic Sensor Extra Classes
Enables an extra set of sensor classes based on Generic Sensor API, which expose previously unavailable platform features, i.e. AmbientLightSensor and Magnetometer interfaces. – Mac, Windows, Linux, Chrome OS, Android
#enable-generic-sensor-extra-classes
Default
Your changes will take effect the next time you relaunch Google Chrome.
Relaunch

Рисунок 66

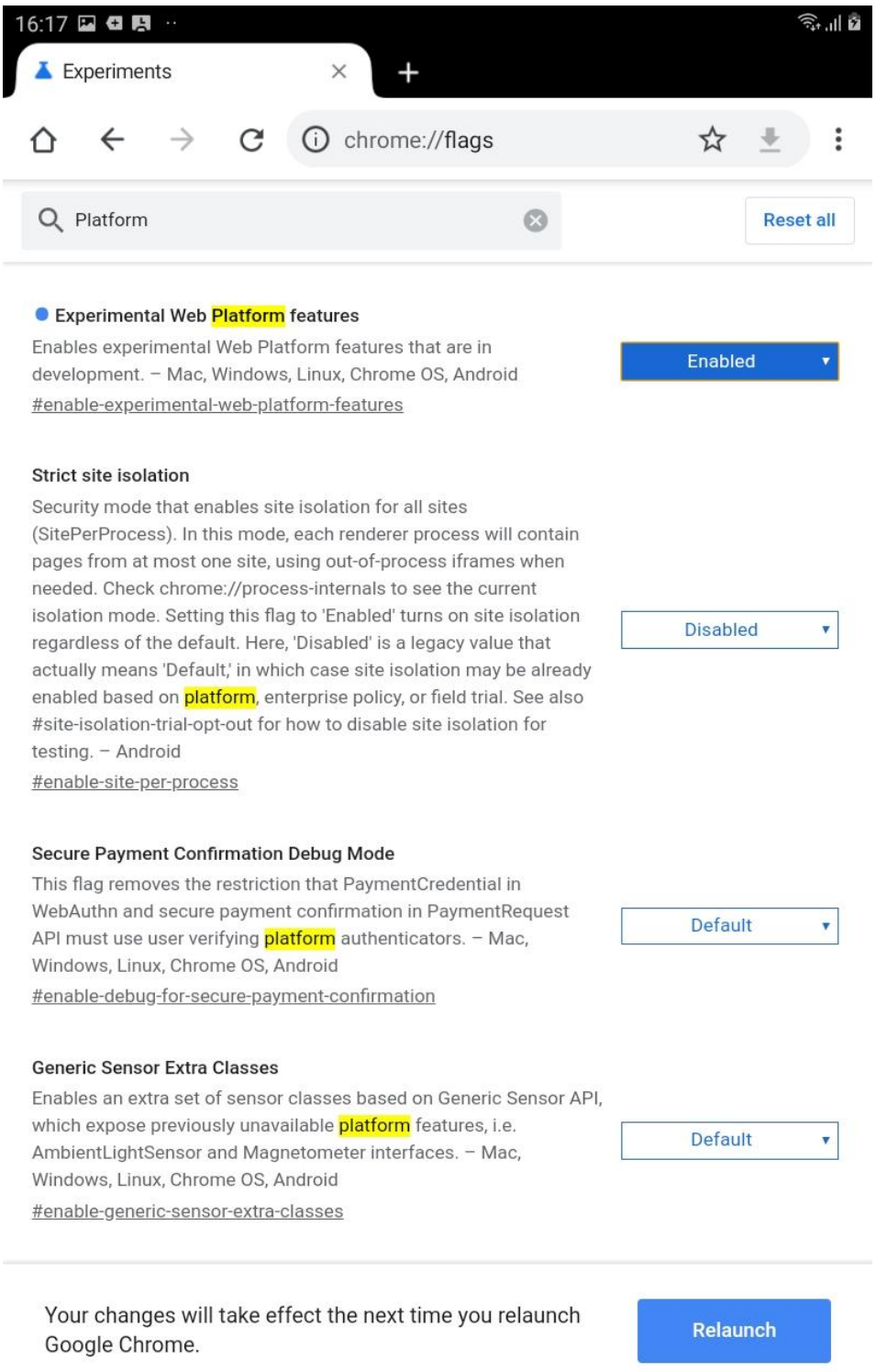
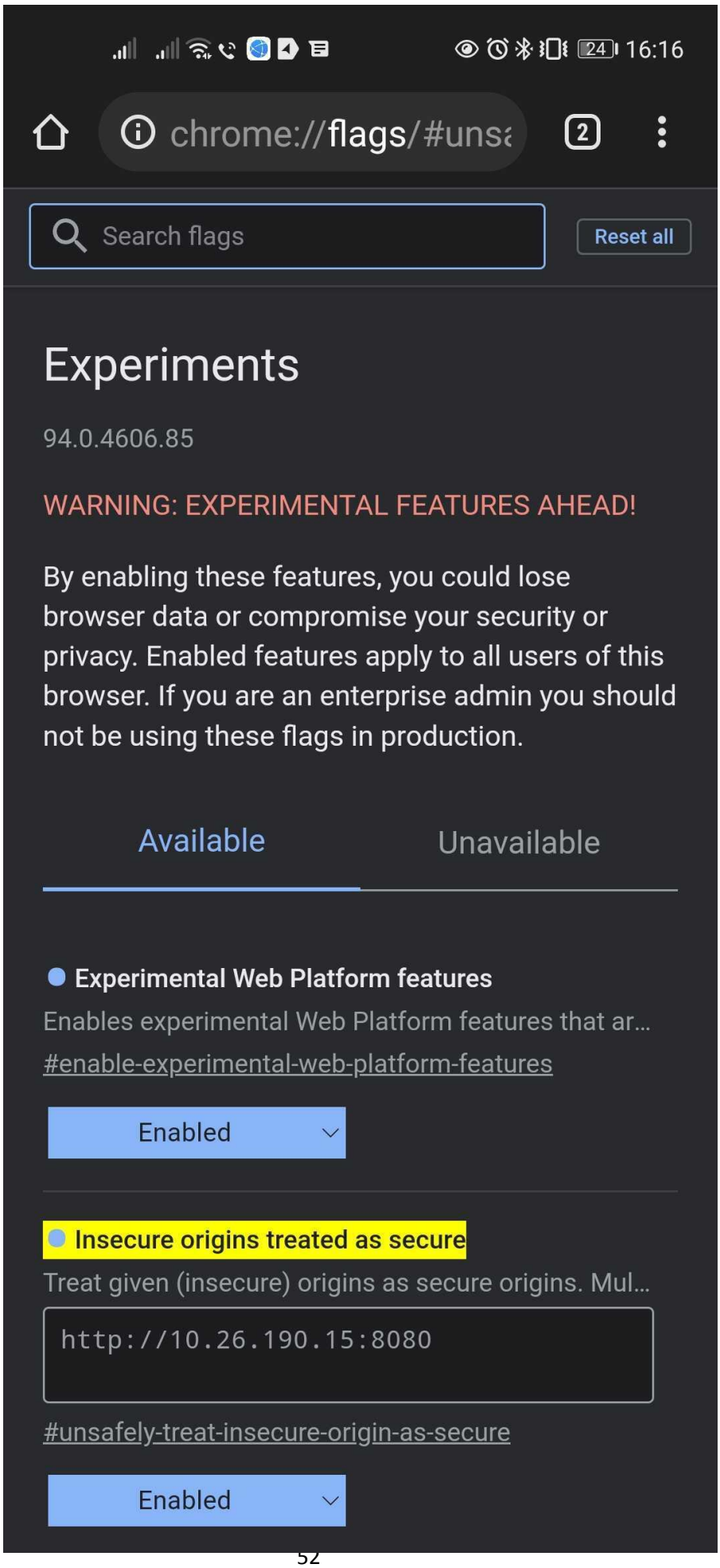


Рисунок 67

e. Добавить в настройку Insecure origins treated as secure адрес площадки с которой планируется работать с использованием карт.


16:16
chrome://flags/#unsa
2
Search flags
Reset all
Experiments
94.0.4606.85
WARNING: EXPERIMENTAL FEATURES AHEAD!
By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser. If you are an enterprise admin you should not be using these flags in production.
Available
Unavailable
Experimental Web Platform features
Enables experimental Web Platform features that ar...
#enable-experimental-web-platform-features
Enabled
Insecure origins treated as secure
Treat given (insecure) origins as secure origins. Mul...
http://10.26.190.15:8080
#unsafely-treat-insecure-origin-as-secure
Enabled

f. Перезагрузить браузер, нажав «Relaunch» внизу страницы
g. Убедиться, что экспериментальная функция включена

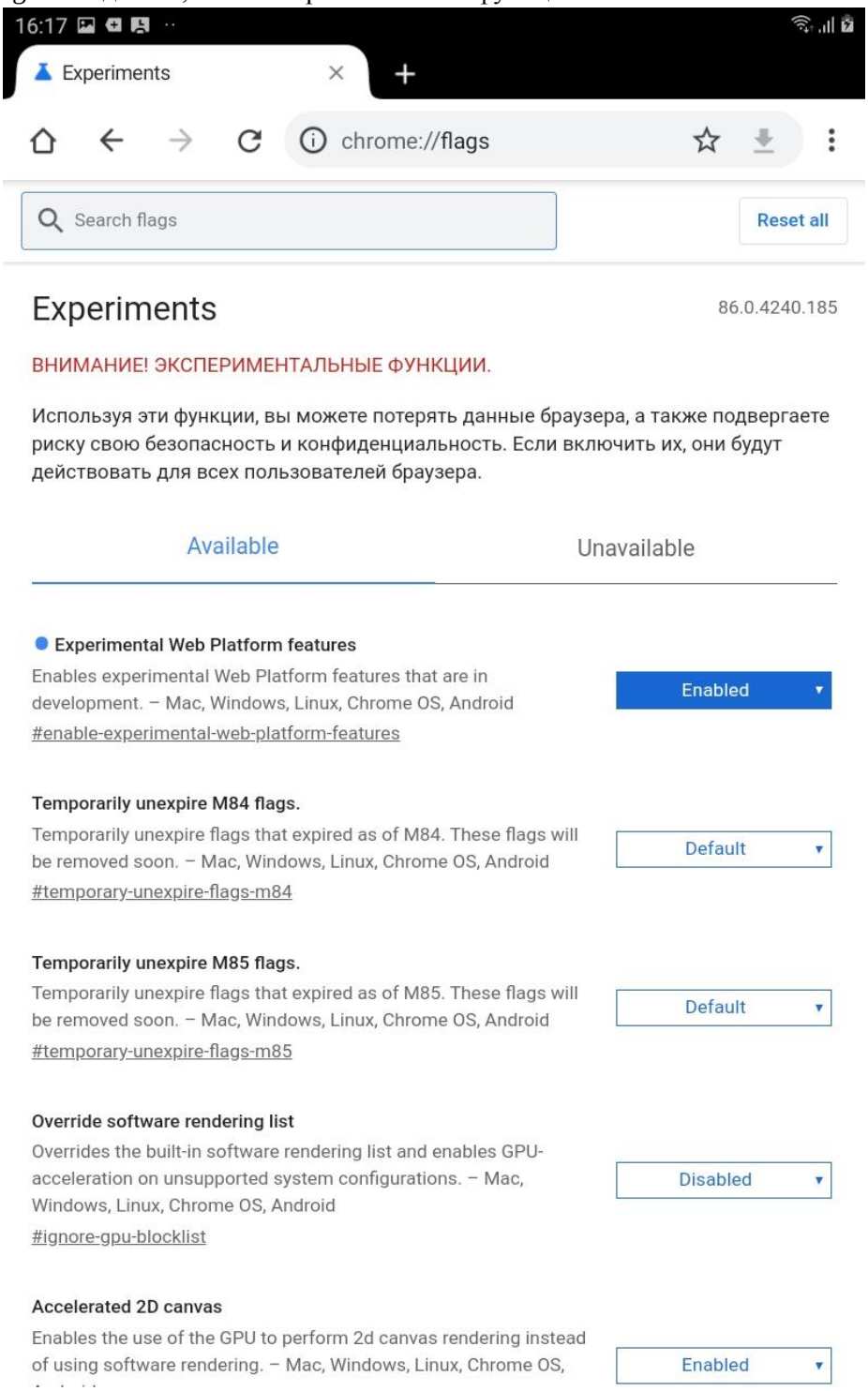


Рисунок 68

h. Перейти по адресу журналов, появится уведомление о незащищенном подключении, нужно нажать «Дополнительно»

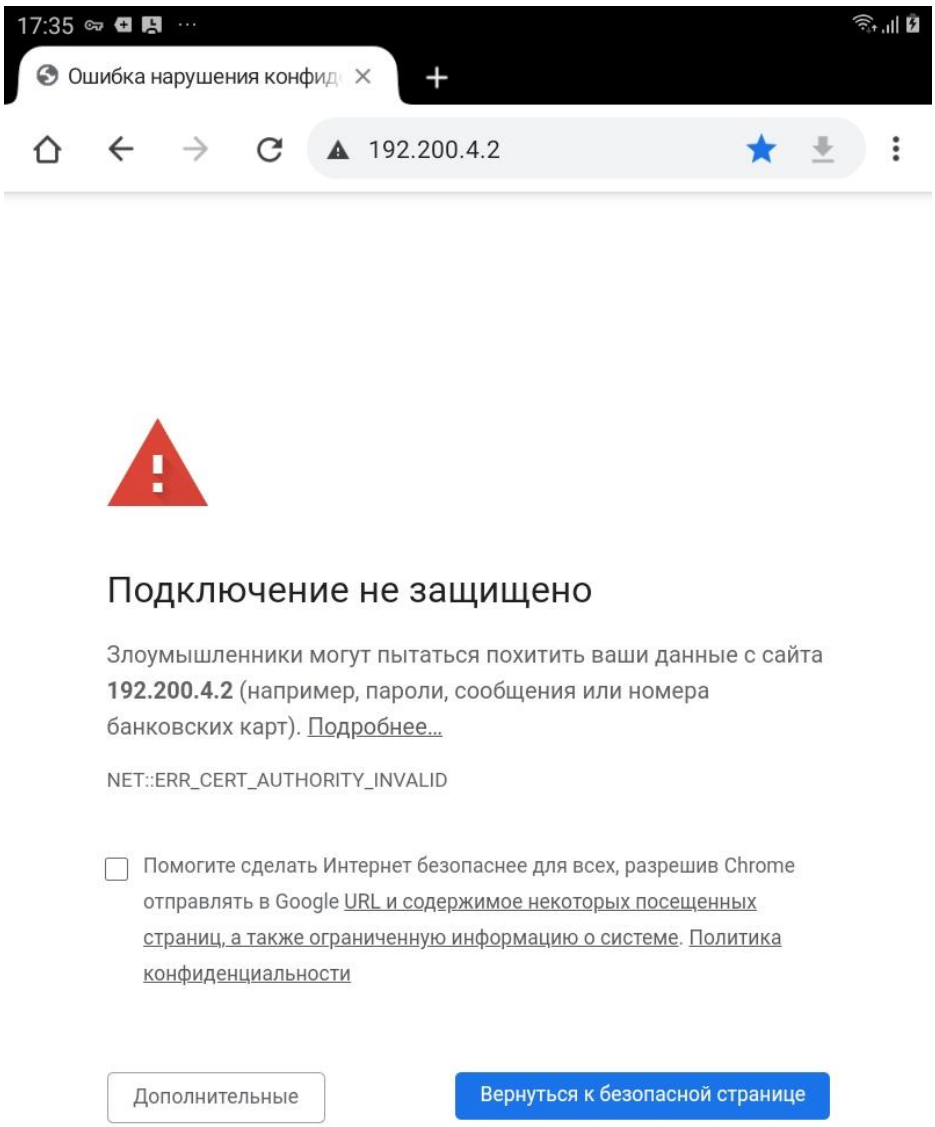


Рисунок 69

i. Далее нажать «Перейти на сайт…» внизу страницы

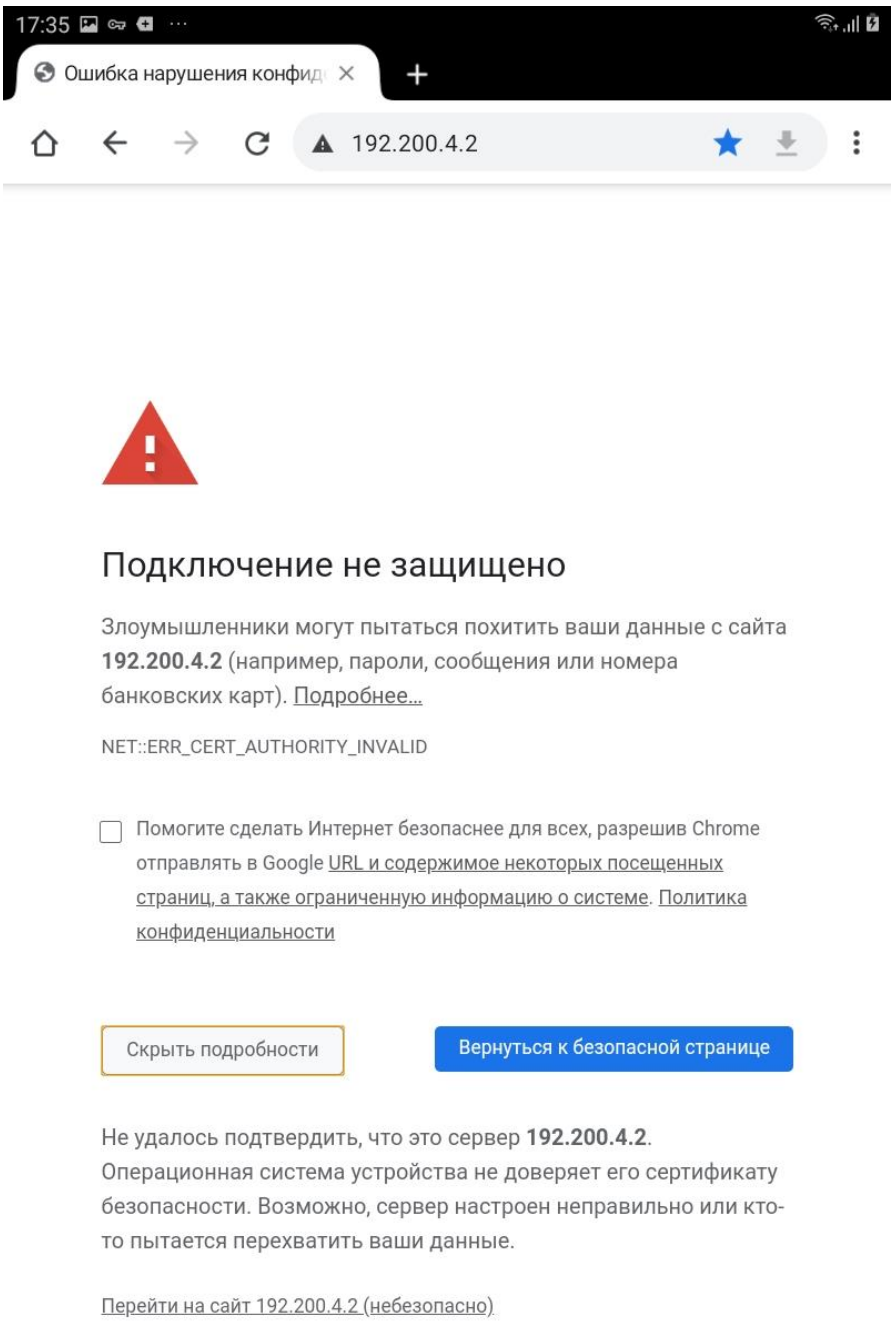


Рисунок 70

j. Откроется окно для авторизации. Ввести учетные данные и нажать «Вход».
k. Откроется Оперативный журнал. Нажать на кнопку «Считать NFC карту

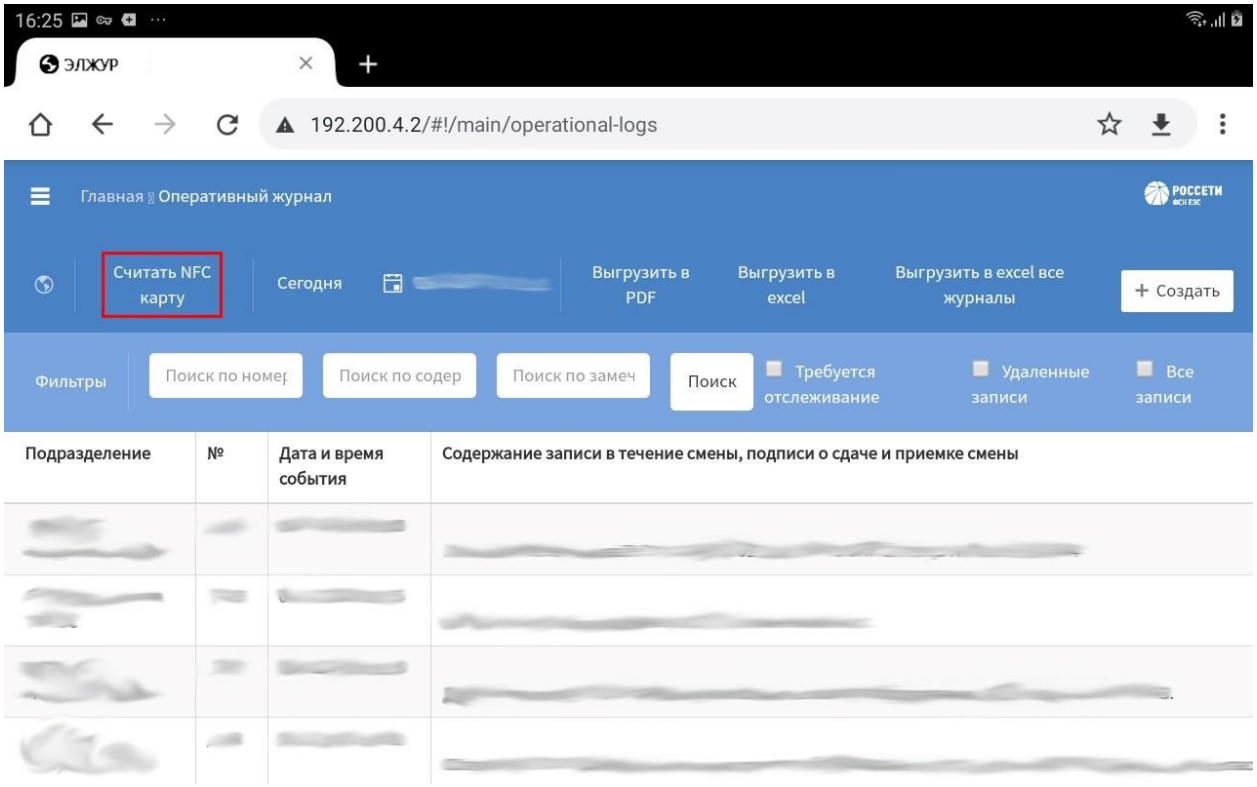


Рисунок 71

l. Появится окно для подтверждения Разрешения использовать NFC, нажать на кнопку «Разрешить»

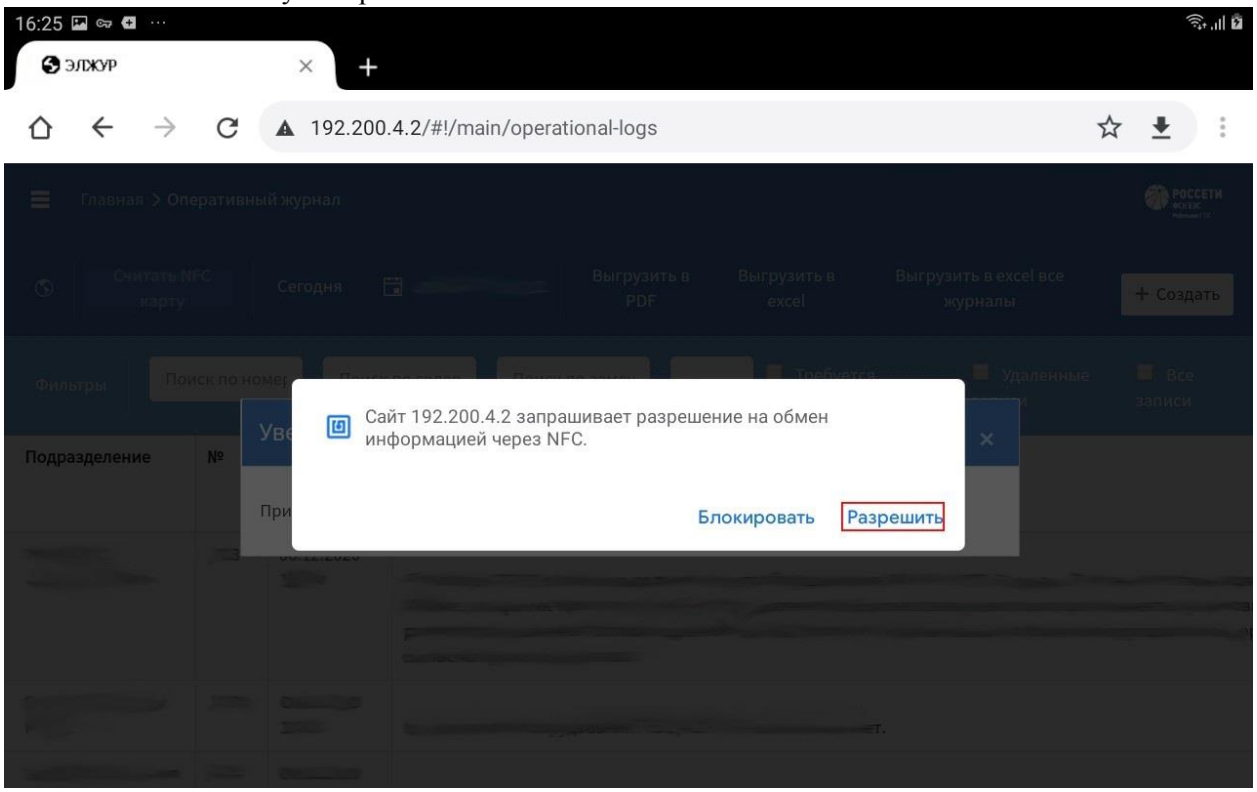


Рисунок 72

m. Приложить карту. Для этого нужно поднести карту к задней крышке ниже камеры планшета на расстояние не более 5 сантиметров

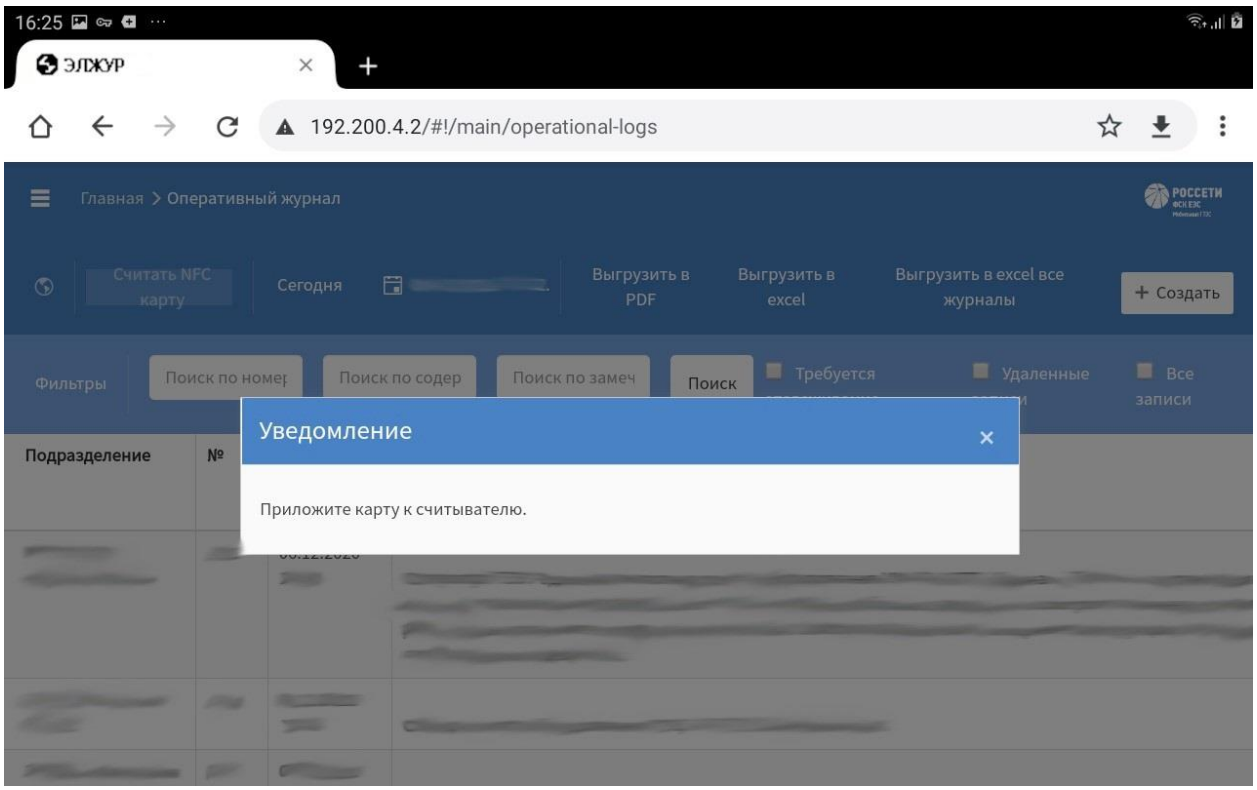


Рисунок 74

n. Проверить, что работа с NFC картами разрешена, можно нажав на треугольник с восклицательным знаком в строке адреса

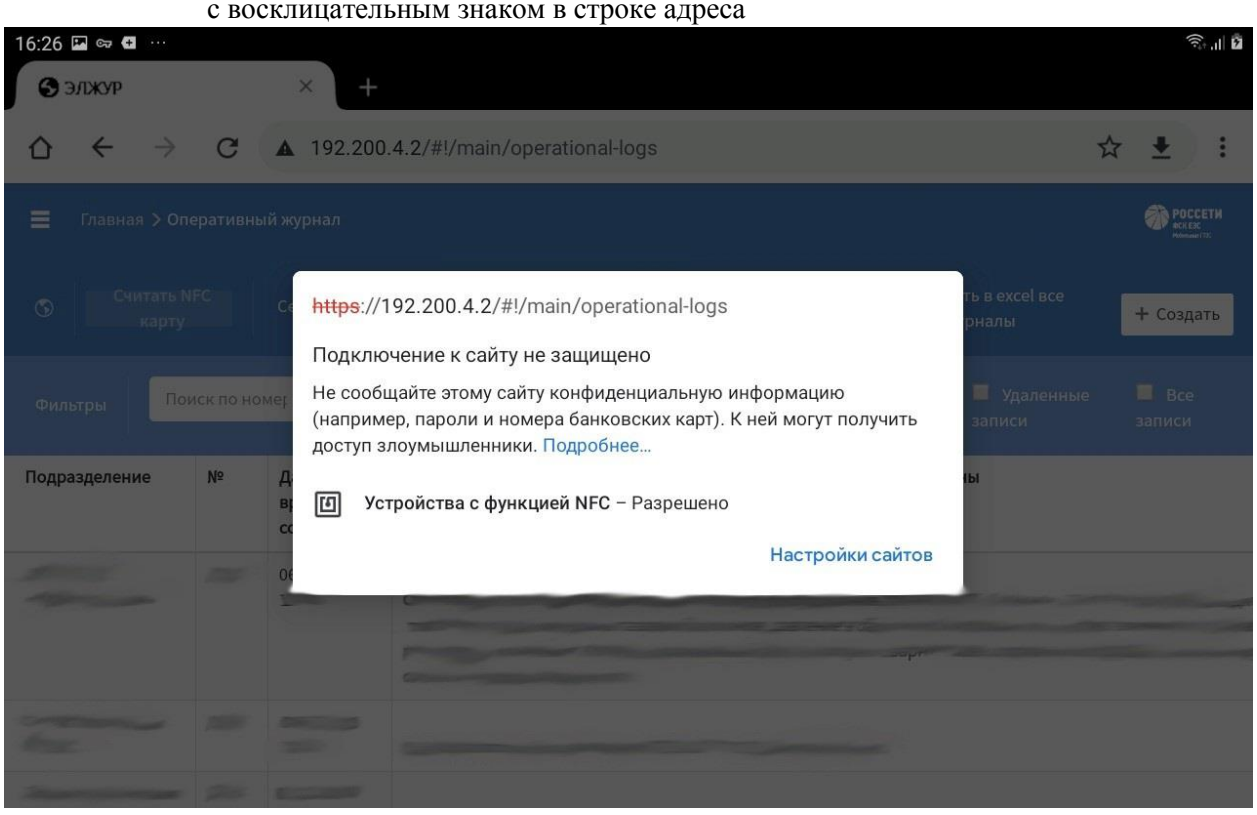


Рисунок 75

Замена конфигурационных файлов

1) RabbitMQ Server

a. Файл advanced.config должен содержать в себе следующие данные:

```
[
{rabbit, [
{tcp_listeners, [{"IP_адрес", 5672}]}
]}
].
```

, где вместо *IP_адрес* должен быть указан локальный IP сервера, на котором ведётся настройка приложения (например, 192.168.1.18)

2) Элжур

a. UFM.FileService

В файл appsettings.json необходимо внести следующие изменения:

i. В строке ConnectionStrings в разделе Default указать адрес базы данных текущей площадки формате (например, Data Source=.\\SQLEXPRESS;Initial Catalog=UFMDB_RTK;Persist Security Info=True;User ID={Имя пользователя};Password={Пароль})

b. PP.MiddleTier.Service

В файл appsettings.json необходимо внести следующие изменения:

i. В строке Authority указать внутреннюю ссылку на компонент UFM.IdentityServer в формате http://IP:port (например, http://192.168.1.18:5000)

В файл Root.json необходимо внести следующие изменения:

ii. В строке HostName указать внутренний адрес сервера, на котором установлен RabbitMQ Server в формате IP (например, 192.168.1.18)

c. UFM.Application

В файл Root.json необходимо внести следующие изменения:

i. В строке CrudServiceBaseUrl указать внутреннюю ссылку на компонент UFM.Application в формате http://IP:port (например, http://192.168.1.18:3000)

ii. В строке IdentityServiceBaseUrl указать внутреннюю ссылку на компонент UFM.IdentityServer в формате http://IP:port (например, http://192.168.1.18:5000)

iii. В строке HostName указать внутренний адрес сервера, на котором установлен RabbitMQ Server в формате IP (например, 192.168.1.18)

iv. В строке DBConnectionString указать имя сервера Microsoft SQL Server в формате Server=ServerName\\InstanceID (например, Элжур-DB\\MSSQLSERVER, либо .\\SQLEXPRESS – символ “.” вместо имени может использоваться только в случае, когда Элжур и Microsoft SQL Server установлены и запущены на одном сервере)

v. В строке IdentityServiceBaseUrl указать внутреннюю ссылку на компонент UFM.IdentityServer в формате http://IP:port (например, http://192.168.1.18:5000)

vi. В строке MiddleTierBaseUrl указать внутреннюю ссылку на компонент PP.MiddleTier.Service в формате http://IP:port (например, http://192.168.1.18:4000)

d. UFM.IdentityServer

В файл appsettings.json необходимо внести следующие изменения:

i. В строке DBConnectionString указать имя сервера Microsoft SQL Server в формате Server=ServerName\\InstanceID (например, Элжур-DB\\MSSQLSERVER, либо .\\SQLEXPRESS – символ “.” вместо имени может использоваться только в случае, когда Элжур и Microsoft SQL Server установлены и запущены на одном сервере)

ii. В строке IssuerUri указать внешний адрес сервера в формате http://URL или http://IP (например, http://test.com или http://8.8.8.8)

iii. В строке Authority указать внешнюю ссылку на компонент UFM.IdentityServer в формате http://URL:port или http://IP:port (например, http://test.com:5000 или http://8.8.8.8:5000)

e. UFM.Web

В файл app.settings.js необходимо внести следующие изменения:

i. В строке crudServiceDaseUrl указать внешнюю ссылку на компонент UFM.Application в формате http://URL:port или http://IP:port (например, http://test.com:3000 или http://8.8.8.8:3000)

ii. В строке identityServiceBaseUrl указать внешнюю ссылку на компонент UFM.IdentityServer в формате http://URL:port или http://IP:port (например, http://test.com:5000 или http://8.8.8.8:5000)

iii. В строке fileServiceBaseUrl указать внутреннюю ссылку на компонент UFM.FileService в формате http://IP:port (например, http://192.168.1.18:6001)

iv. В строке BarcodeServiceUrl указать внутреннюю ссылку на компонент UFM.IdentityServer в формате http://IP:port (например, http://192.168.1.18:5000)

v. Убедиться, что в строке CardReaderServiceUrl указан параметр http://localhost:9000/