Установка и настройка рабочего места для удалённого подключения к информационным ресурсам ГК «Росатом», при помощи средства криптографической защиты информации *«КриптоПро CSP» v. 4.0.9944*.

Руководство администратора безопасности органа криптографической защиты по установке и настройке АРМ для подключения к централизованным ИТ-ресурсам из сети Интернет.

Москва 2020

Оглавление

1. Общие положения.

1.1 Настоящий документ «*Установка и настройка рабочего места для удалённого подключения к информационным ресурсам ГК «Росатом», при помощи средства криптографической защиты информации «КриптоПро CSP» v. 4.0.9944*» (далее - Инструкция) устанавливает порядок действий, необходимых к выполнению администратором безопасности по настройке АРМ для удаленной работы с ИТ-ресурсами ГК «Росатом».

1.2 Соблюдение настоящей Инструкции является обязательным для администраторов безопасности органа криптографической защиты.

2. Аббревиатуры.

2.1 Аббревиатуры и расшифровки.

Аббревиатура	Расшифровка
ПК	Персональный компьютер
ПО	Программное обеспечение
СКЗИ	Средства криптографической защиты информации
ОКЗ	Орган криптографической защиты
ФСБ России	Федеральная служба безопасности Российской Федерации
АРМ	Автоматизированное рабочее место
СЗИ	Средство защиты информации
НСД	Несанкционированный доступ

3. Условия подключения АРМ к централизованным ИТ-ресурсам из сети Интернет.

3.1 Подключение АРМ к централизованным ИТ-ресурсам из сети Интерент возможно только после присоединения организации к Договору №22/2143-Д**Error! Bookmark not defined.**.

3.2 Для последующего доступа к централизованным ИТ-ресурсам, предоставления дистрибутива СКЗИ, централизованного учёта лицензиатом ФСБ России АО «Гринатом» подготовить заявление на организацию и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (с передачей СКЗИ). Вместе с заявлением руководитель организации предоставляет в ОКЗ АО «Гринатом» следующий комплект документов:

- Копию/скан-копию приказа о назначении Администраторов безопасности ОКЗ и лиц их замещающих (рекомендуется минимум два администратора безопасности с контактными данными) или оригинал заявления на услугу Администратора безопасности ОКЗ АО «Гринатом».
- Копию/скан-копию Перечня лиц, допускаемых к самостоятельной работе с СКЗИ.
- Копию/скан-копию Приказа о предоставлении прав подписей в системе(ах) (в случае использования платежных систем).

3.3 Установка на СКЗИ на АРМ может производиться, если:

- На АРМ установлено сертифицированное антивирусное средство с обновленной до актуальной базой данных;
- на АРМ отсутствуют права администратора;
- на АРМ имеется сертифицированное СЗИ от НСД.

4. Настройка рабочего места для удаленного подключения к ИТ-ресурсам Госкорпорации «Росатом».

4.1 Назначить встречу с пользователем для проведения работ (примерное время выполнения 25 минут).

4.2 Произвести установку СКЗИ КриптоПро CSP с дистрибутива, полученного в ОКЗ АО «Гринатом».

4.3 Для начала установки СКЗИ КриптоПро CSP необходимо дважды кликнуть на ярлык установщика. После появления приветственного окна необходимо нажать кнопку **Далее.**

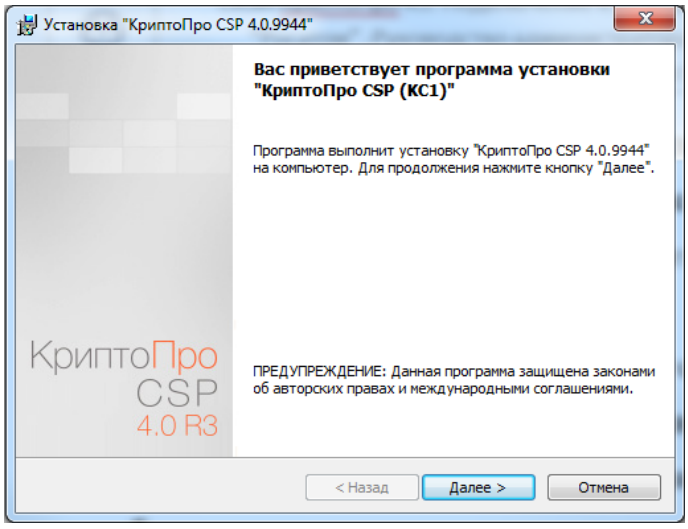


Рисунок 1. Приветственное окно установки.

4.4 Далее необходимо принять лицензионное соглашение и нажать кнопку **Далее.**

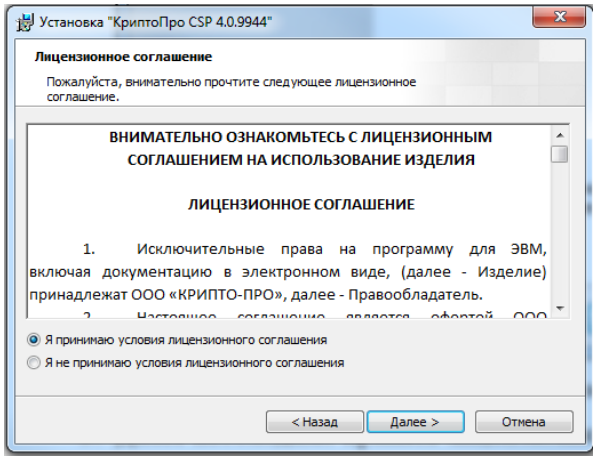


Рисунок 2. Лицензионное соглашение.

4.5 После принятия лицензионного соглашения, необходимо заполнить данные *пользователя, наименование организации* и *серийный номер* продукта (КриптоПро CSP 4.0.9944) и нажать кнопку **Далее**. (Для того, чтобы заполнить поле ***Серийный номер***, необходимо запросить лицензию в ОКЗ АО “Гринатом”. Телефон для связи с администратором безопасности ОКЗ: +7 (499) 949-49-19 доб: 5452. E-mail администратора ОКЗ: aibokz@greenatom.ru.)

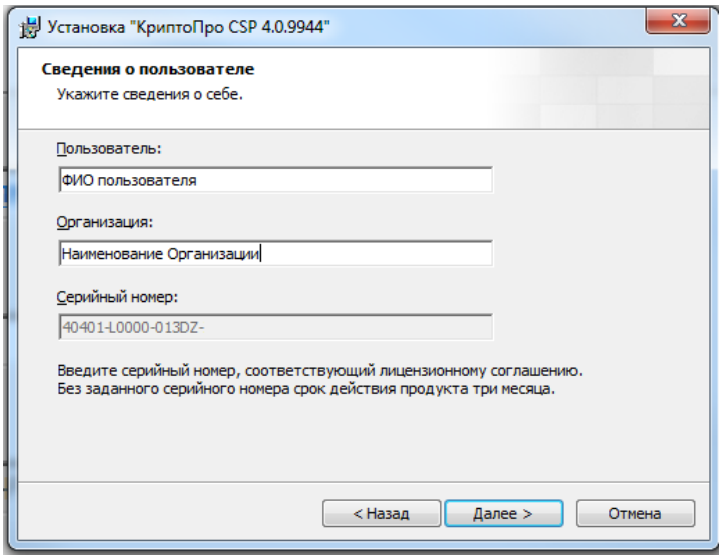


Рисунок 3. Сведения о пользователе.

4.6 Необходимо выбрать *выборочную установку*, нажав на кнопку **Выборочная** и кнопку **Далее.**

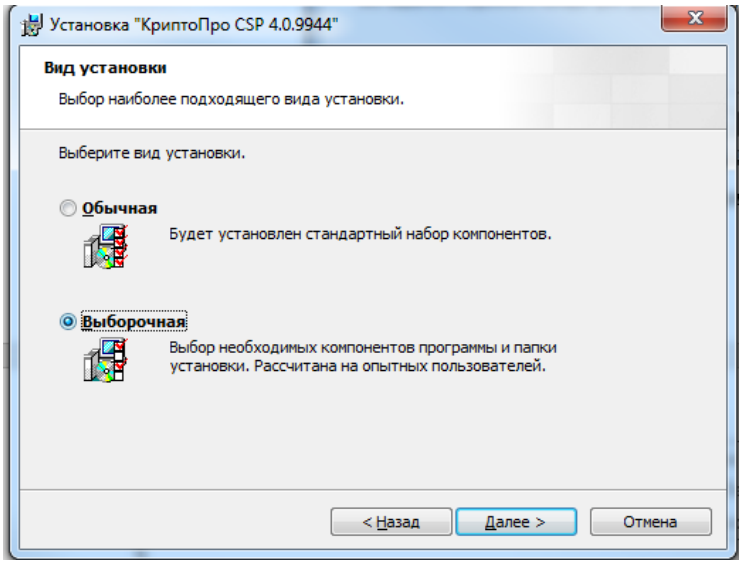


Рисунок 4. Вид установки.

4.7 Далее в появившемся окне необходимо нажать на каждый компонент из списка, рядом с которым стоит красный крест и выбрать **Данный компонент будет установлен на локальный жесткий диск**, после чего нажать кнопку **Далее.**

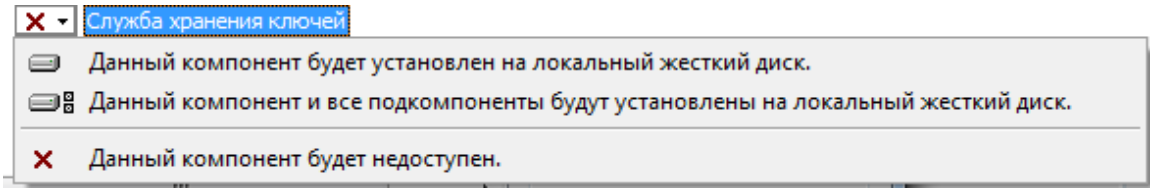


Рисунок 5. Установка всех компонентов.

4.8 Далее в появившемся окне необходимо оставить все по умолчанию и нажать кнопку **Установить**.

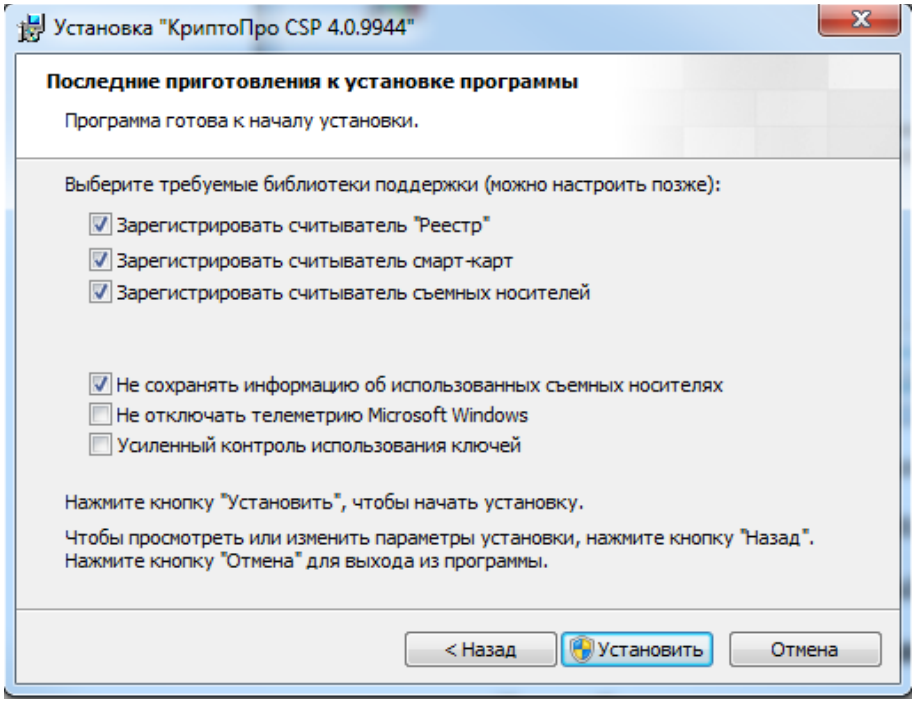


Рисунок 6. Окно выбора библиотек.

4.9 После успешной установки КриптоПро CSP v.4.0.9944 необходимо нажать кнопку **Готово** и перезагрузить ПК пользователя.

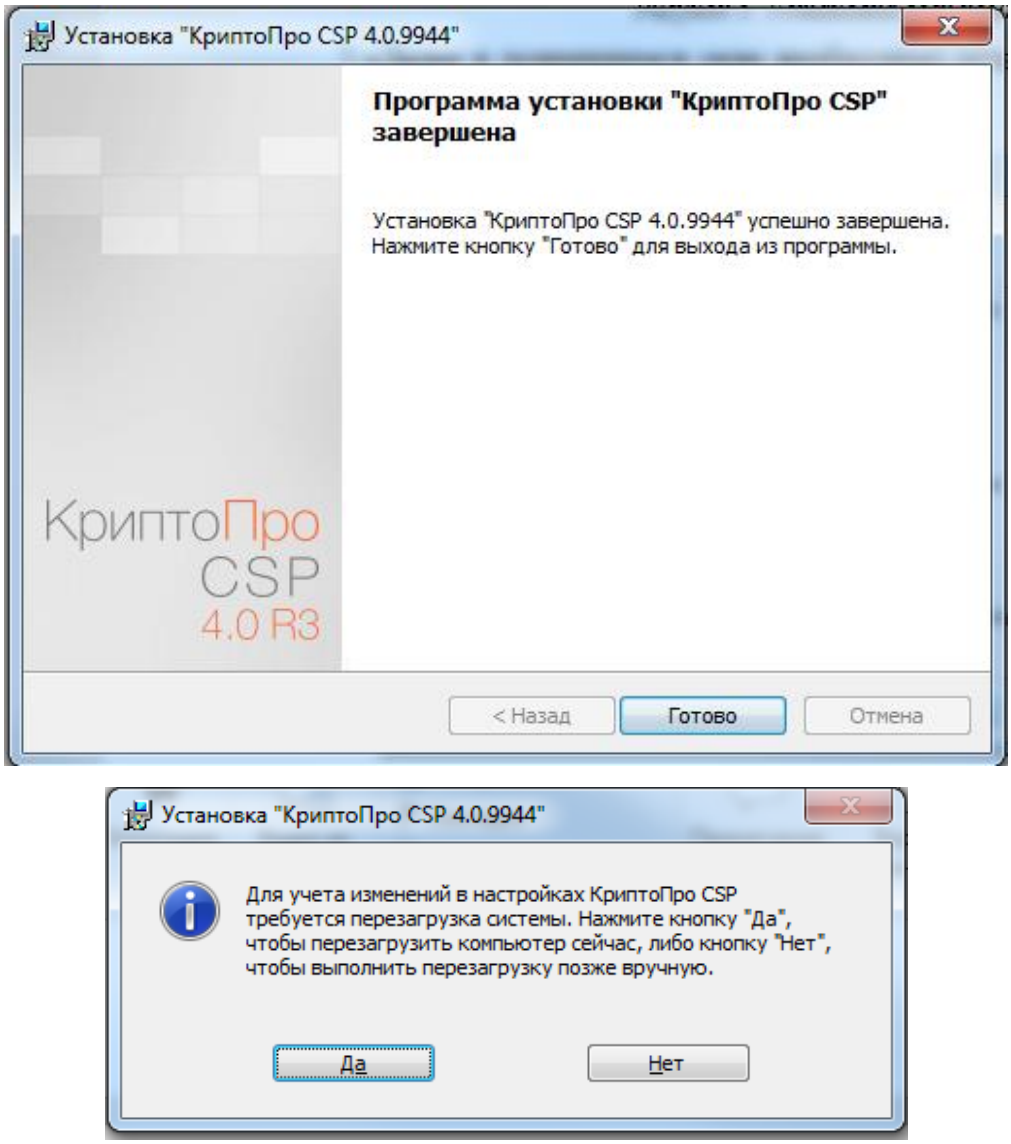


Рисунок 7. Завершение установки.

4.10 После перезагрузки ПК необходимо установить **Драйвер Рутокен**, находящийся на диске с дистрибутивом СКЗИ *«КриптоПро CSP»*. Для запуска установки драйвера необходимо двойным нажатием запустить его и в открывшемся окне нажать кнопку **Установить.**

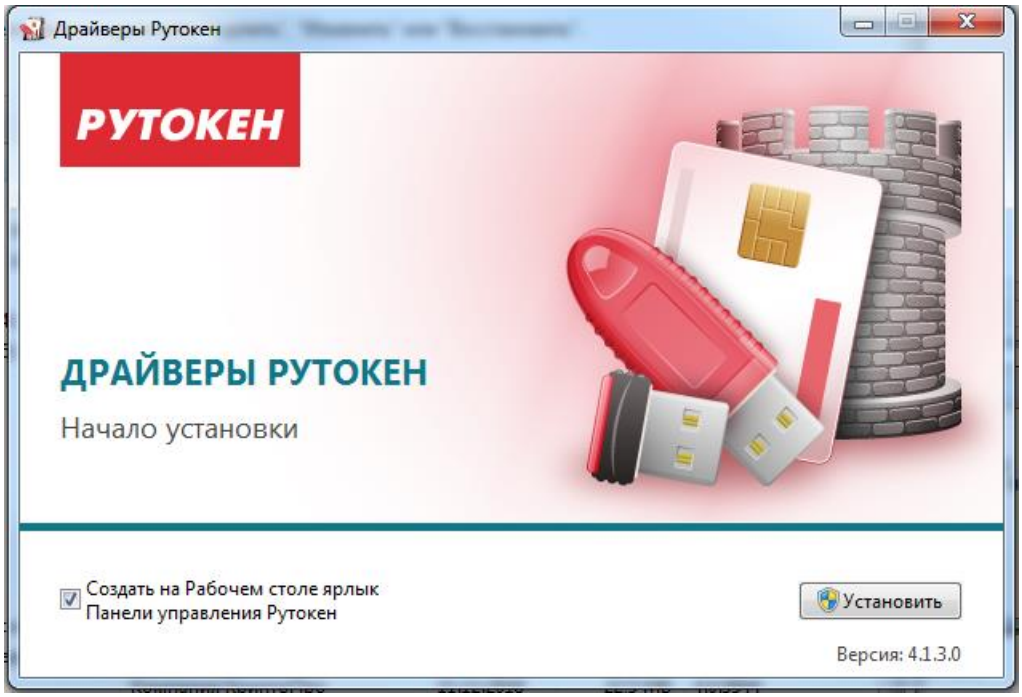


Рисунок 8. Установка драйвера Рутокен.

4.11 После процесса установки в появившемся окне необходимо нажать кнопку **Закрыть.**

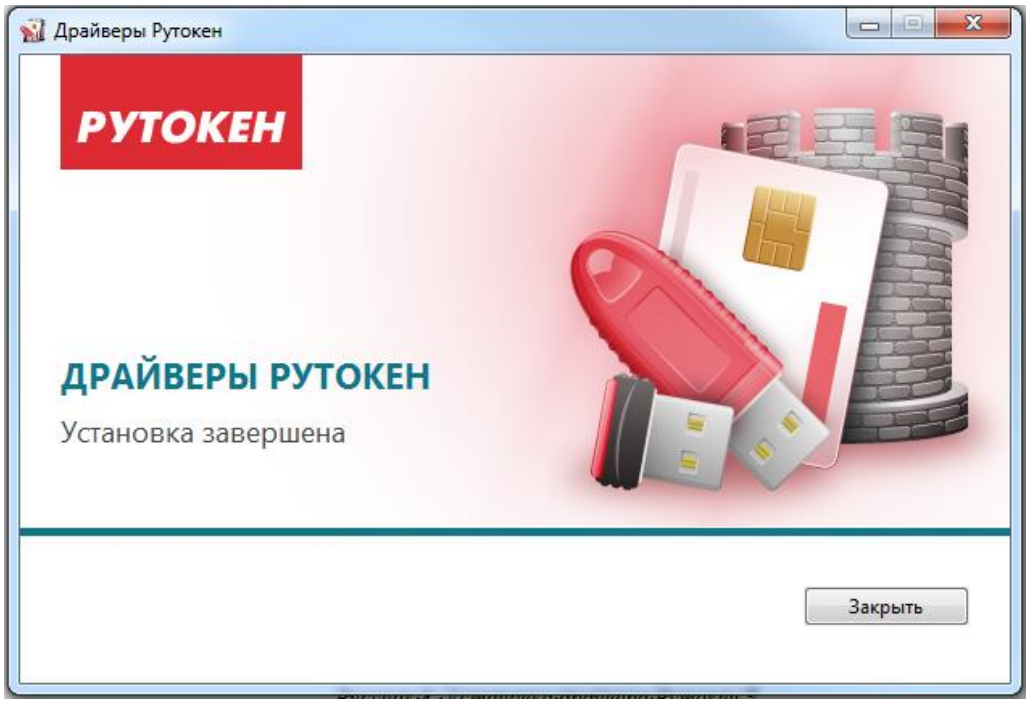


Рисунок 9. Завершение установки драйвера Рутокен.

4.12 Далее необходимо правильно настроить цепочки сертификатов в реестре сертификатов (актуальные сертификаты). Для этого необходимо дважды нажать на сертификат и в появившемся окне нажать кнопку далее.

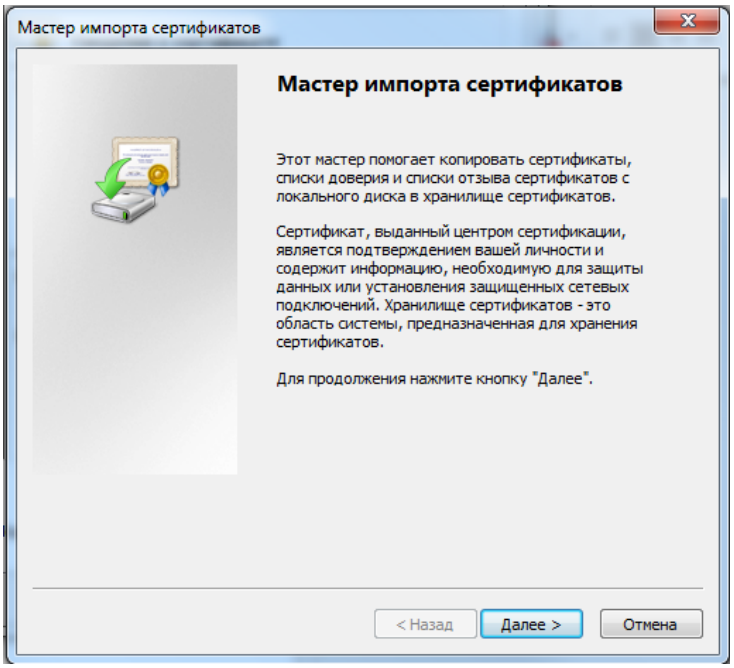


Рисунок 10. Мастер импорта сертификатоф.

4.13 В появившемся окне выбрать **Поместить сертификаты в выбранное хранилище** и нажать кнопку **Обзор**. Если в названии сертификата есть аббревиатура **GUC**, то его следует поместить в папку доверенные корневые центры сертификации. Если в названии есть **Greenatom**, то необходимо поместить в папку промежуточные центры сертификации, нажать кнопку **ОК** и кнопку **Далее.**

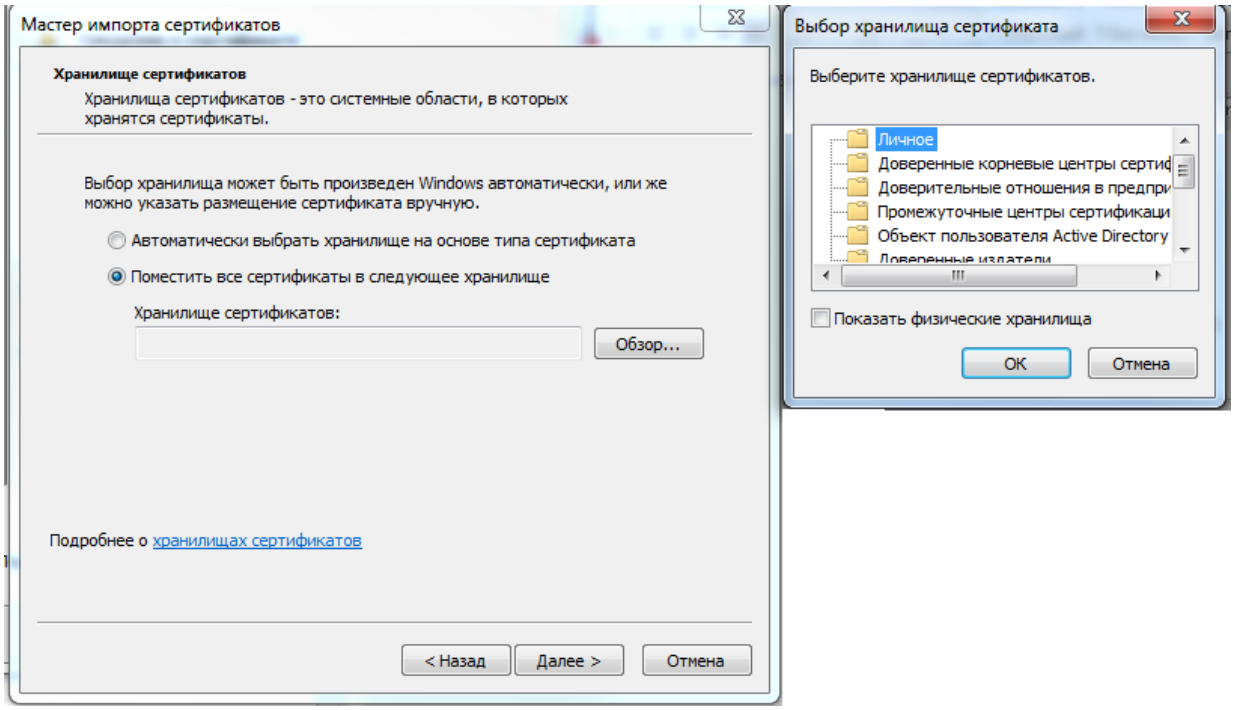


Рисунок 11. Выбор хранилища сертификатов.

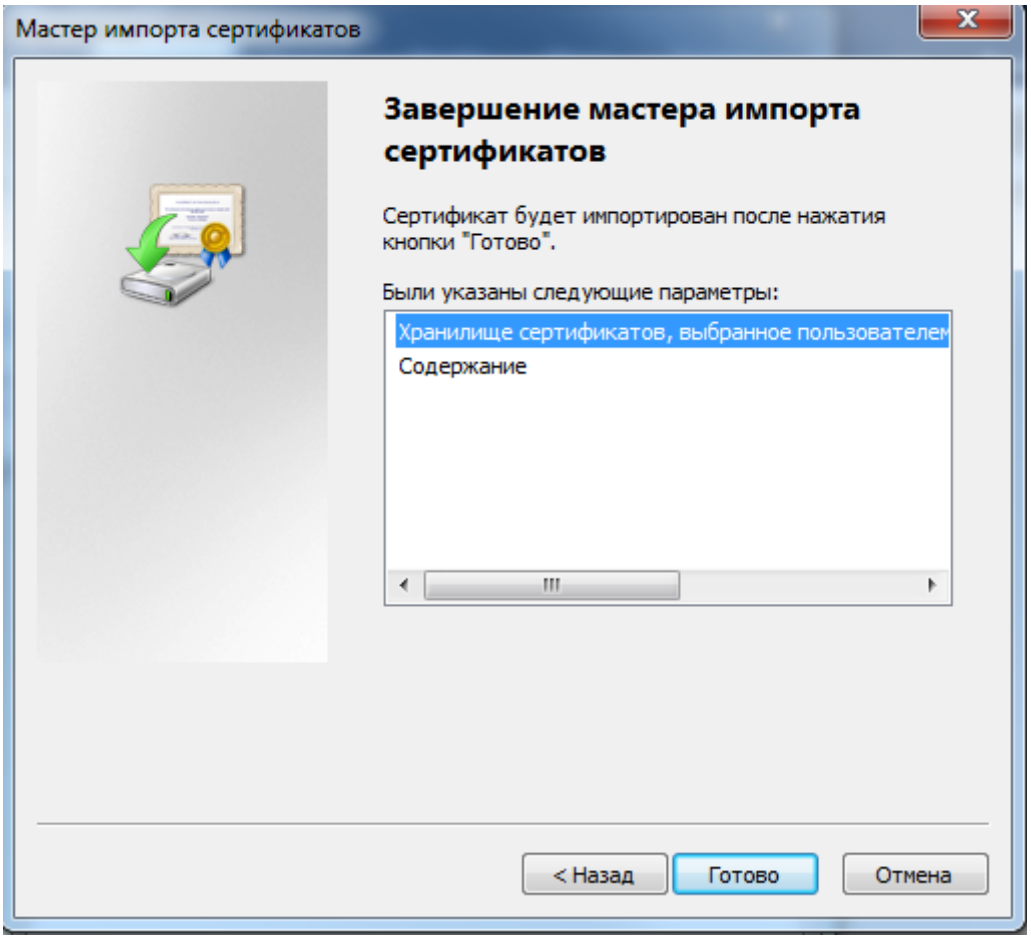


Рисунок 12. Завершение импорта сертификатов.

4.14 В появившемся окне необходимо нажать **Готово**. Данную процедуру(п. 4.12-4.14) необходимо проделать для двух сертификатов (**GUC** и **GreenAtom**).

4.15 Далее необходимо добавить сертификат пользователя в реестр сертификатов в папку личное, для этого необходимо вставит RUTOKEN в АРМ и запустить «*КриптоПро CSP*», нажать на вкладку сервис и кнопку **Посмотреть сертификаты в контейнере**.

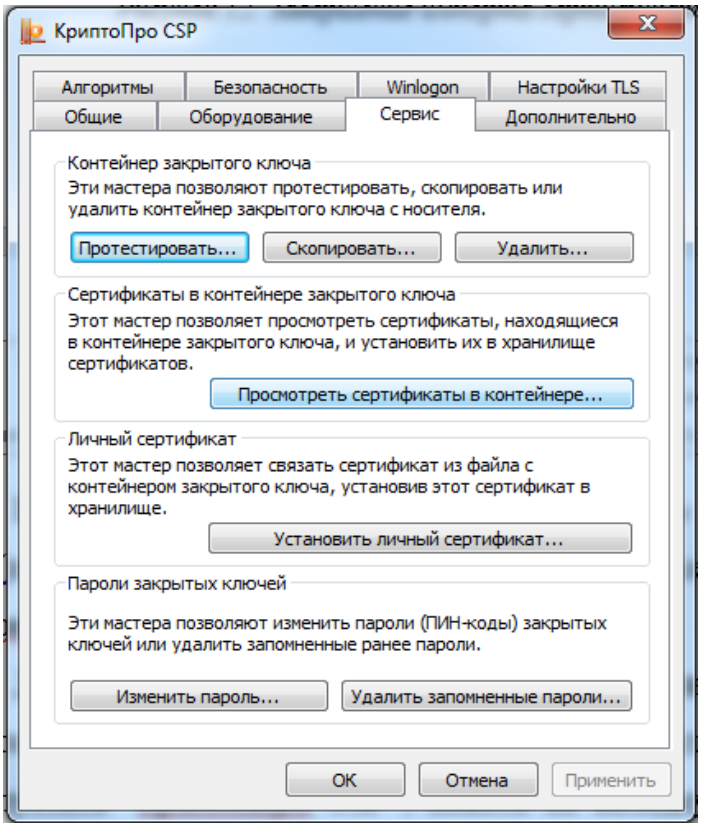


Рисунок 13. Добавление сертификата через КриптоПро.

4.16 В появившемся окне необходимо нажать кнопку **Обзор**, выбрать сертификат и нажать **OK.**

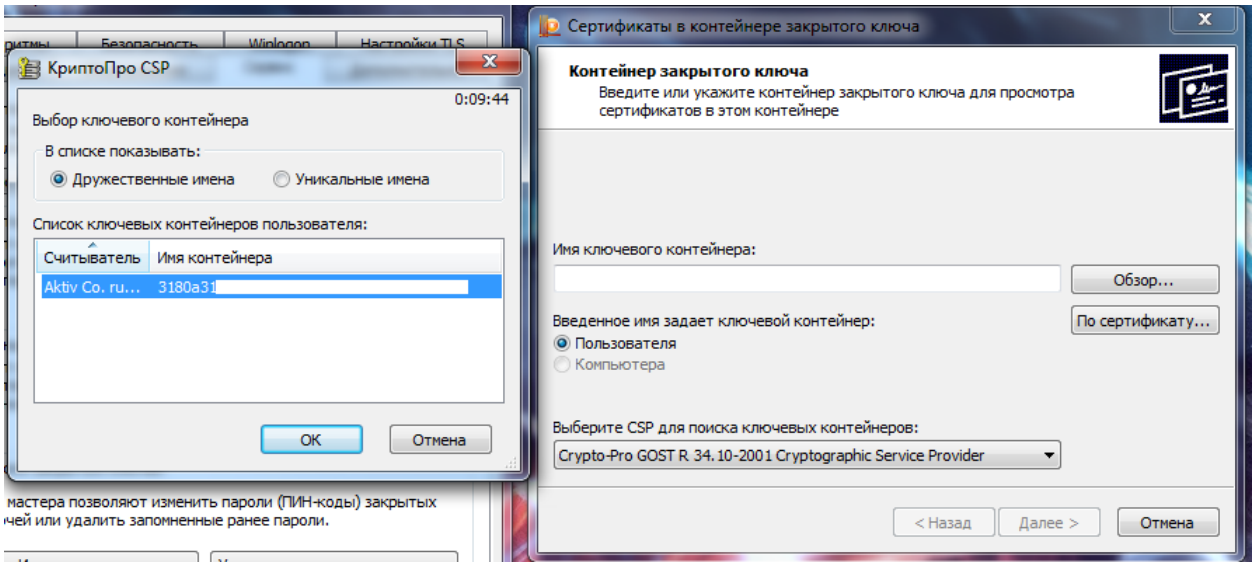


Рисунок 14. Добавление сертификата через КриптоПро.

4.17 После этого необходимо нажать **Далее**, **Установить** и **Готово.**

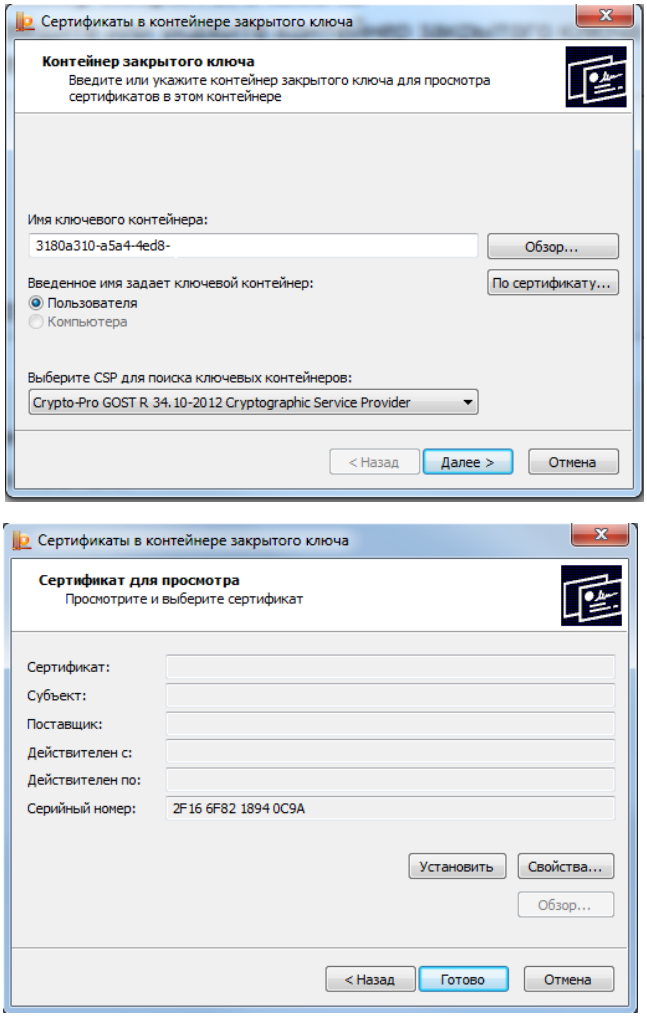


Рисунок 15. Добавление сертификата через КриптоПро.

4.18 После проделанных действий необходимо подготовить браузер **Internet Explorer** (в инструкции использовалась 10 версия Internet Explorer) для работы с удаленными рабочими столами. Для этого необходимо создать ярлык на рабочем столе, зайти в его свойства (правой кнопкой мыши на ярлык, свойства) и во вкладке **Ярлык,** в параметр **Объект** добавить следующее: *"C:\Program Files (x86)\Internet Explorer\iexplore.exe" https://srdw.rosatom.ru".*

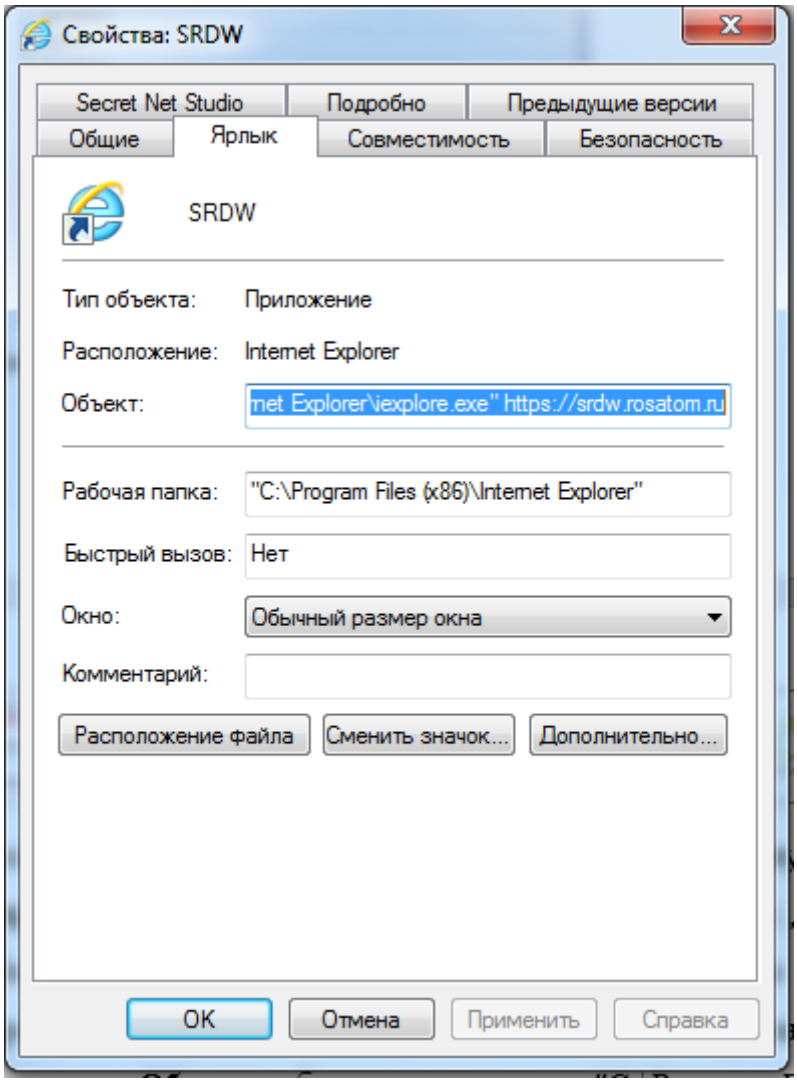


Рисунок 16. Настройка ярлыка для работы в SRDW.

4.19 Далее необходимо открыть ярлык и зайти в свойства браузера (сочетание клавиш Alt+X, выбрать **Свойства браузера**). Во вкладке безопасность необходимо выбрать **Интернет** и опустить ползунок до конца

вниз (уровень безопасности средний), далее выбрать **Надежные сайты** и выбрать уровень безопасности ниже среднего, также необходимо нажать на кнопку **Сайты** и добавить сайт https://srdw.rosatom.ru в надежные. Также во вкладке дополнительно, в параметрах безопасности необходимо выбрать **SSL 2.0, SSL 3.0, TLS 1.0**.

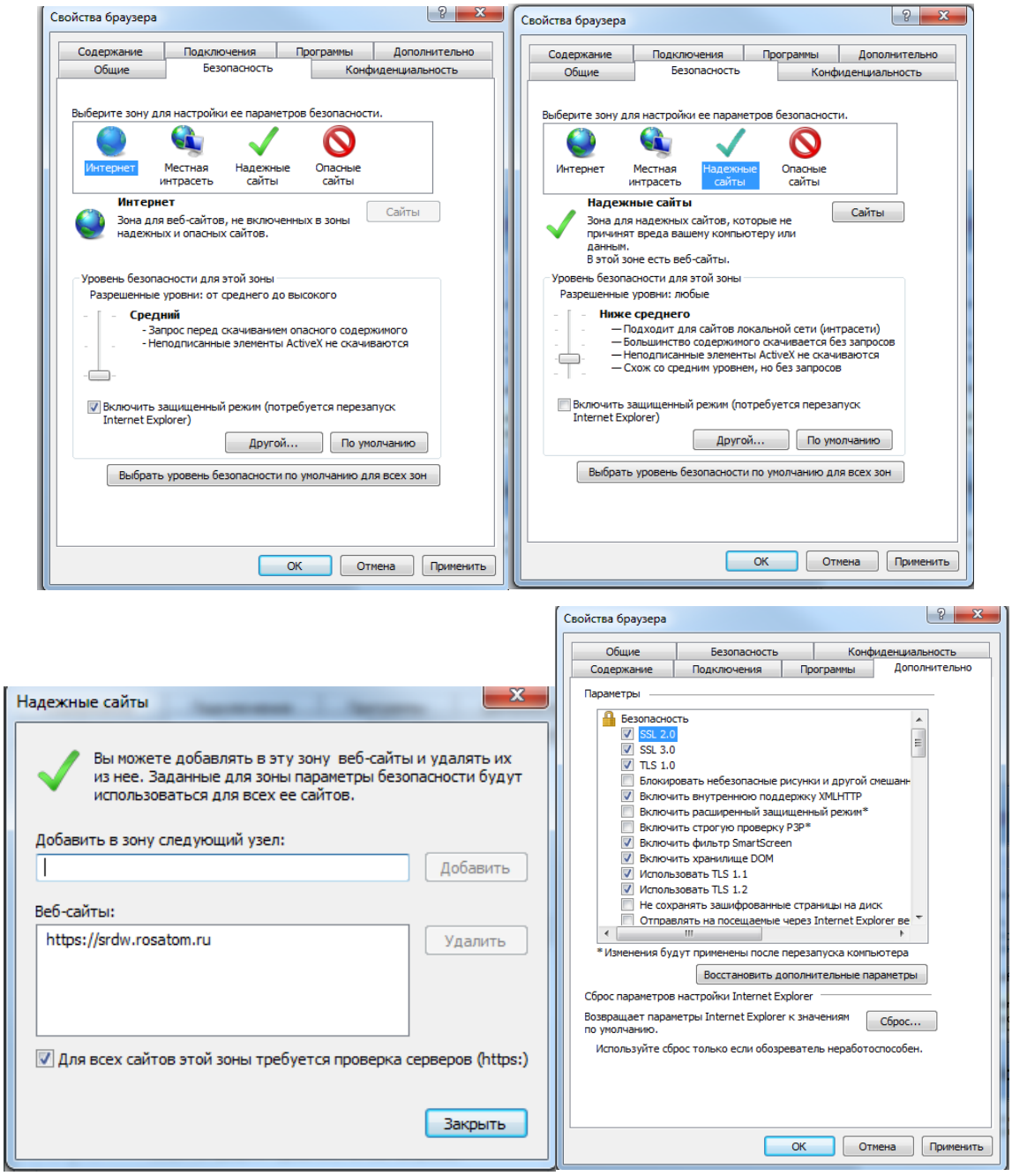


Рисунок 17. Настройка браузера для работы в SRDW.

4.20 После выполнения всех настроек браузера, его необходимо перезапустить.

Выполнив пункты 4.2 – 4.20 рабочее место пользователя будет настроено для удалённого подключения к информационным ресурсам ГК «Росатом», при помощи средства криптографической защиты информации «КриптоПро CSP» v. 4.0.9944**.**

5. Подключение к системе удаленных рабочих столов.

5.1 Для подключения к системе удаленных рабочих столов необходимо вставить сертификат проверки ключа электронной подписи в АРМ пользователя. Далее необходимо дважды кликнуть на настроенный Internet Explorer (пункт 4.18-4.19). Далее откроется страница входа в портал терминальных приложений ГК “Росатом”. В поле *Имя пользователя* необходимо ввести логин пользователя, такой же как от почты outlook. Далее необходимо заполнить поле пароль и нажать кнопку **Вход в систему.**

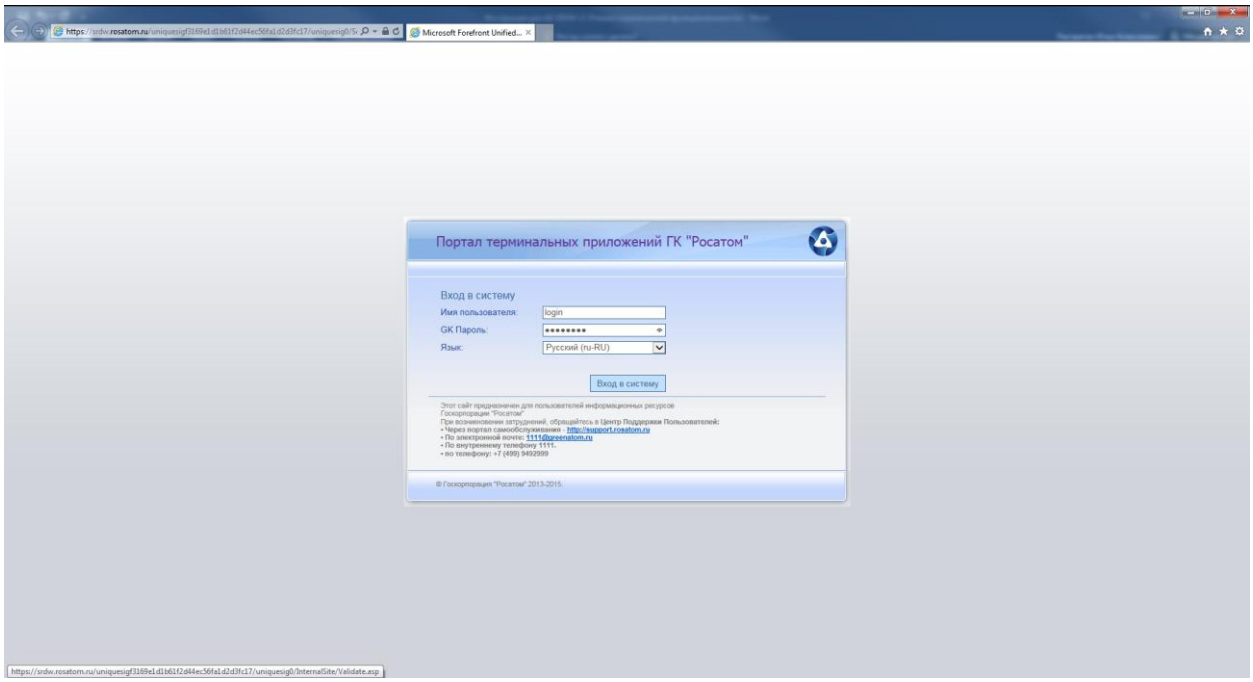


Рисунок 18. Вход в SRDW.

5.2 При правильном вводе логина и пароля появится всплывающее окно, в которое необходимо ввести Pin-код (находится в конверте с сертификатом проверки ключа электронной подписи).

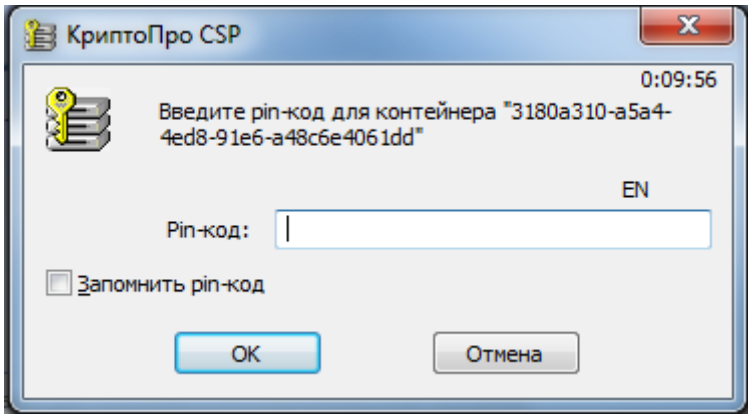
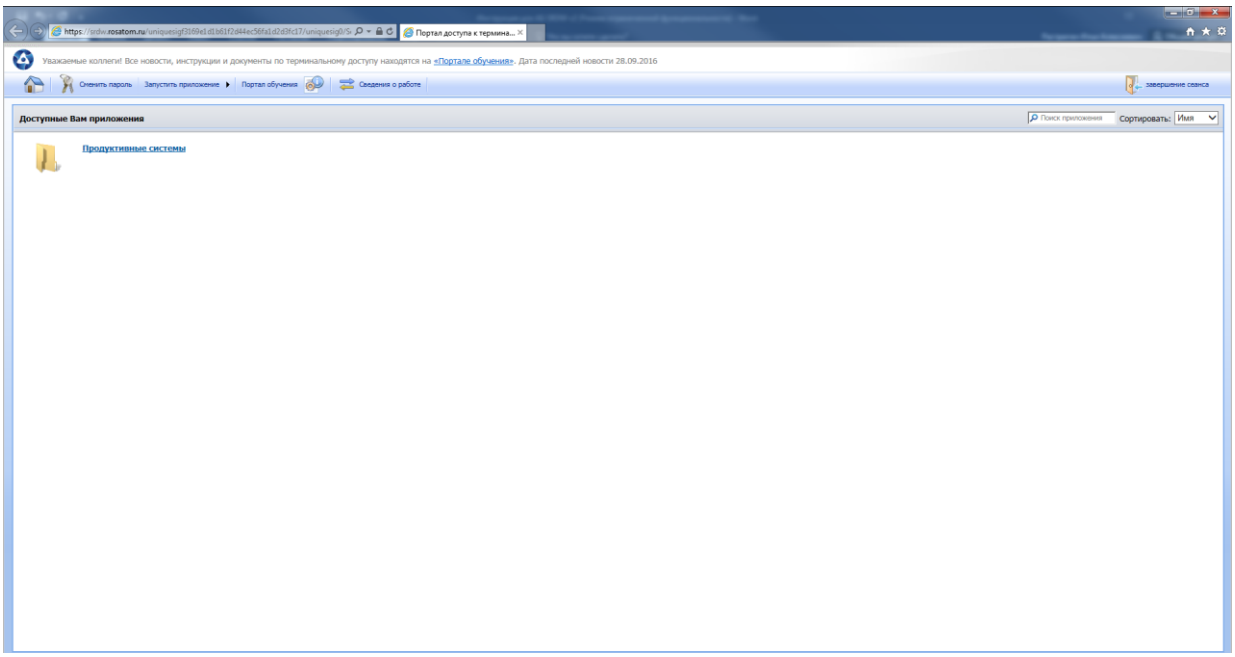


Рисунок 19.Окно ввода Pin-код.

5.3 Далее необходимо войти в папку *Продуктивные системы* и выбрать нужный портал.



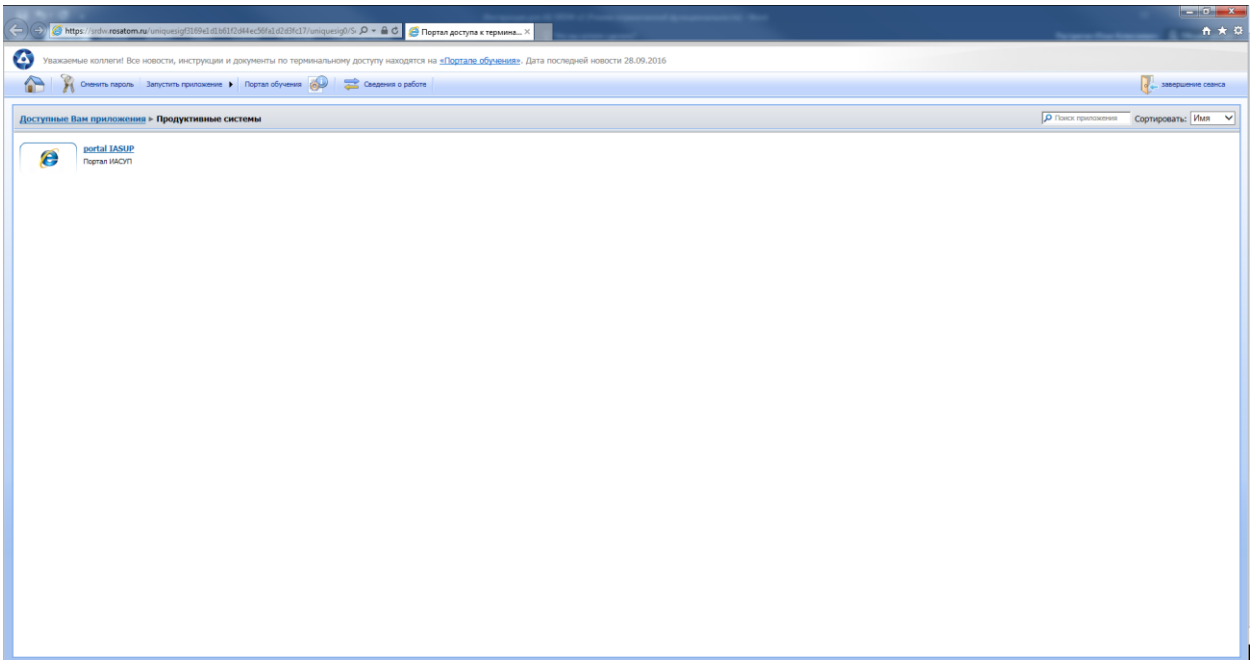


Рисунок 20. Продуктивные системы.

5.4 При нажатии на портал, появится всплывающее окно, которое запросит разрешение на запуск приложения RemoteApp. В этом окне необходимо нажать кнопку **Подключить**, после чего начнется подключение к порталу.

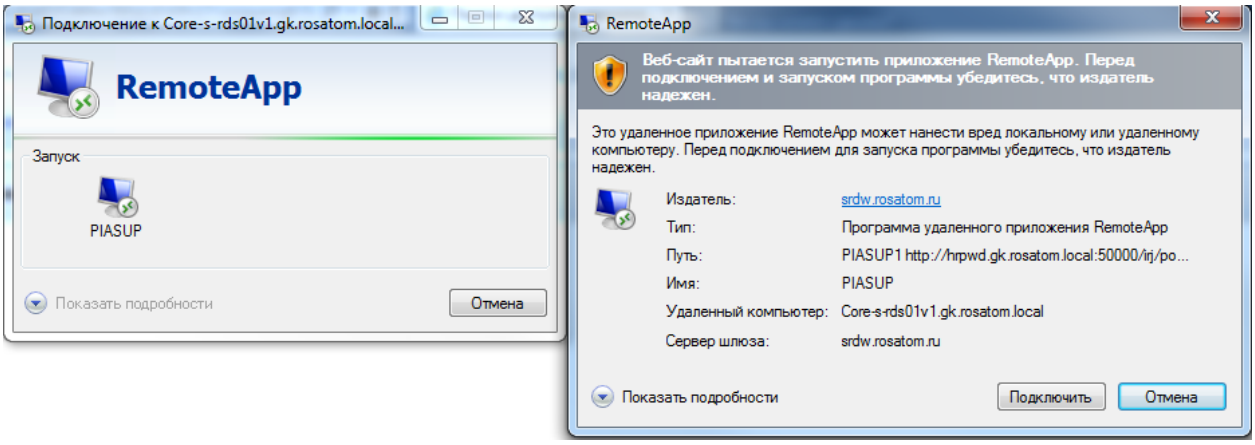


Рисунок 21. Подключение к порталу в продуктивных системах.

5.5 После запуска портала откроется новое окно с удаленным рабочим столом.

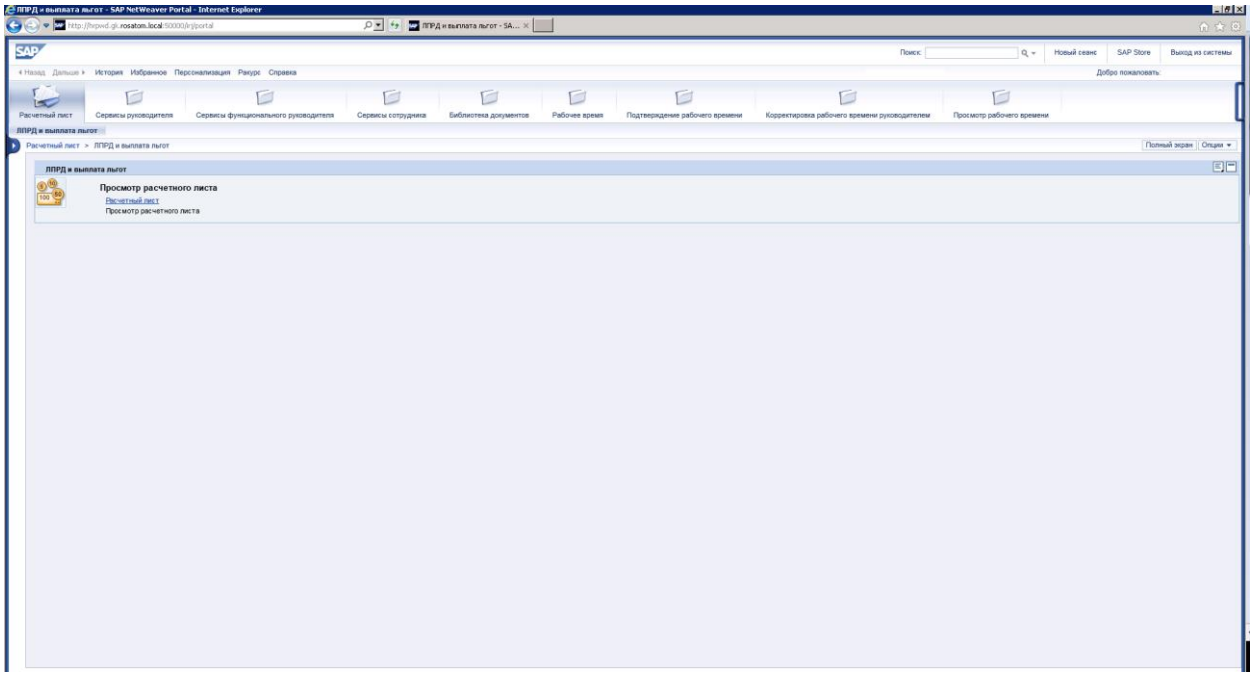


Рисунок 22. Окно портала IASUP.

Рабочее место настроено корректно, в случае если на АРМ пользователя выполнен успешный вход на портал через систему удаленных рабочих столов.